

ВЕБИНАР

Защищенная рабочая станция на базе ОС Astra Linux и Secret Disk

Мероприятие проведут эксперты ГК Astra Linux и «Аладдин Р.Д.», ведущих поставщиков отечественных ИТ-решений



Актуальность темы

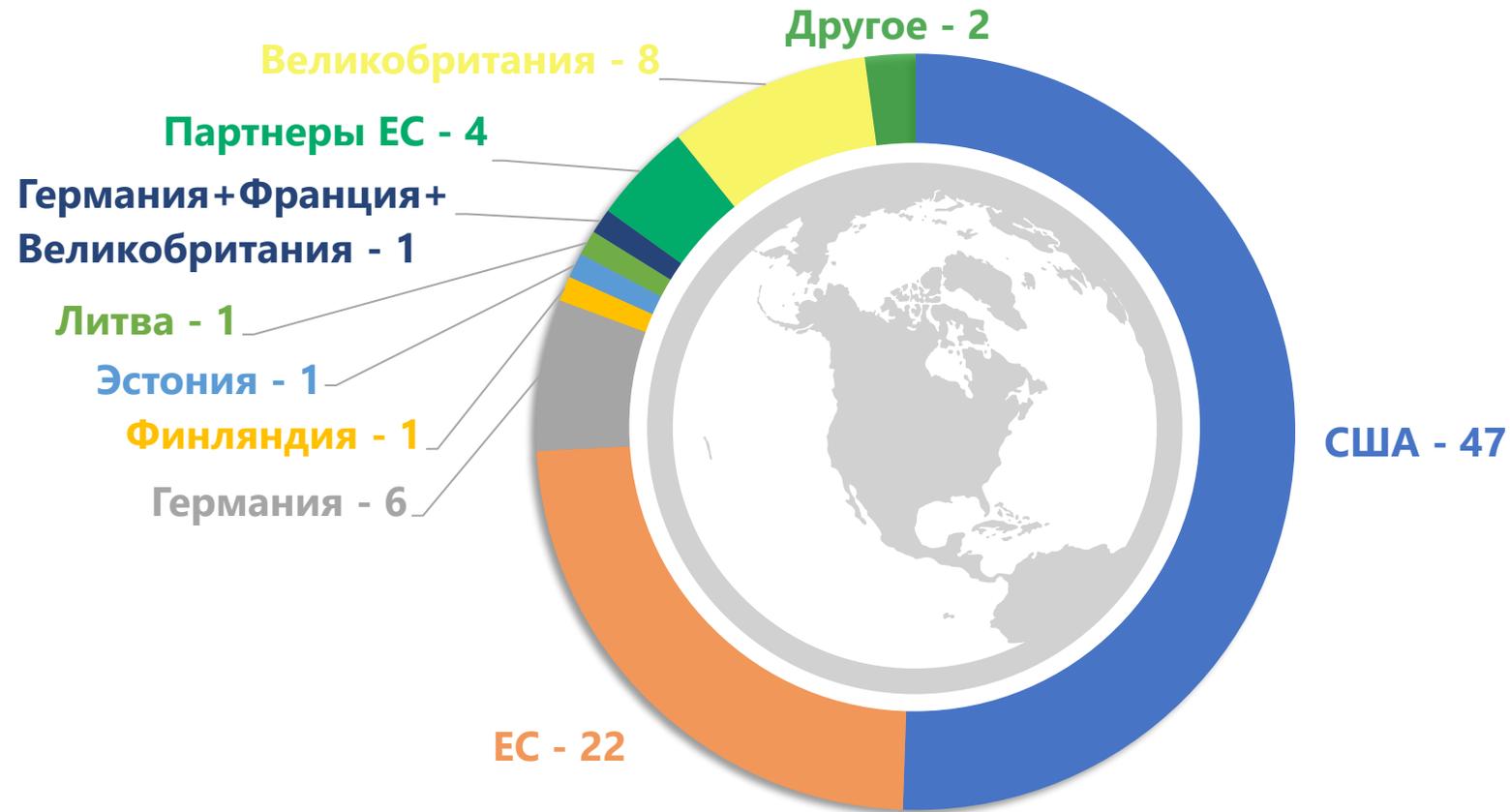
Новостной фон и текущий статус:

- Санкционное давление возрастает
- Геополитическая обстановка накалена
- Санкции за реагирование на санкции
- Двусторонний эффект ощущают все стороны



Статистика и тенденции

КОЛИЧЕСТВО САНКЦИОННЫХ ЭПИЗОДОВ В ОТНОШЕНИИ РОССИИ



Базовый план



Адаптация

Первичный переход на отечественное прикладное ПО с сохранением на компьютерах ОС Windows



Интеграция

Формирование инфраструктуры переходного периода. Создание гибридных систем управления Win/Linux



Полный переход

Полноценный ввод в эксплуатацию бизнес-приложений и электронных сервисов на отечественном ПО, ОС и СУБД

СДЕЛАНО У НАС

Ведущая ИТ платформа



ASTRA LINUX SPECIAL EDITION 1.7

WWW.ASTRALINUX.RU

Так было раньше...



Смоленск



Ленинград



Новоросийск

Так сейчас...



А что же с городами?

Режимы защищенности ОС

Орел

Базовый

ГИС 3 класса,
ИСПДн 3 уровня
защищенности и ниже

Воронеж

Расширенный

ГИС 1 класса,
ИСПДн 1 уровня
защищенности и ниже

Смоленск

Максимальный

Сведения, составляющие
государственную тайну
до степени секретности
«особой важности»
включительно и ниже

Что нового?

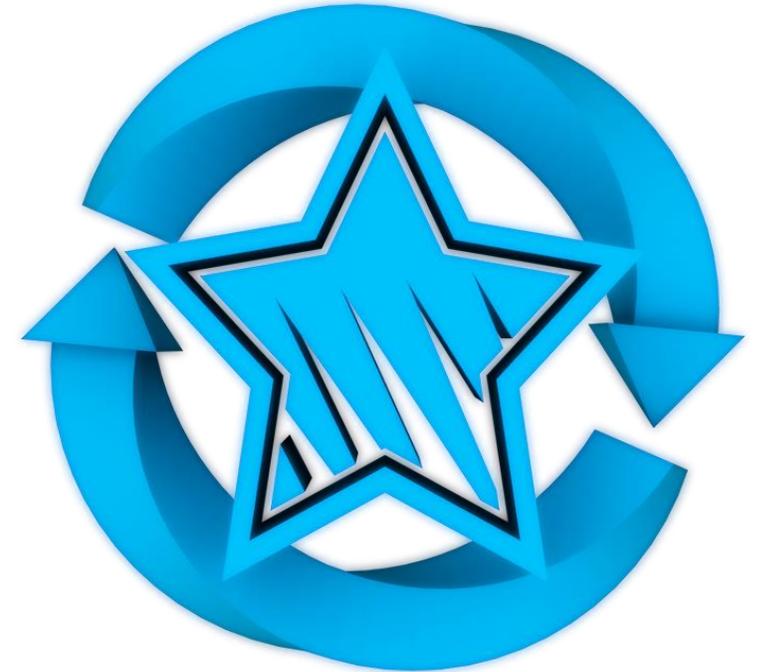
Очередное обновление

- Выбор режима защищенности ОС
- Переход на ядро 5.4 LTS
- Изменения в СЗИ (Parsec 3.0)
- Обновление интерфейса пользователя



Развитие СЗИ

- Отключаемые модули безопасности
- Файловой системы XFS с поддержкой снапшотов
- Безопасная изоляция docker-контейнеров
- Поддержка меток безопасности в протоколе IPv6 (Parsec)
- Система аудита (auditd, ksystemlog, system-config-audit)



Параметры защиты информации

Уровень защищенности	Базовый	Усиленный	Максимальный
Гарантированное затирание удаляемых данных	 Недоступно	 Выкл	 Выкл
Замкнутая Программная Среда (ЗПС)	 Недоступно	 Выкл	 Выкл
Мандатное Управление Доступом (МРД)	 Недоступно	 Недоступно	 Вкл
Мандатный Контроль Целостности (МКЦ)	 Недоступно	 Вкл	 Вкл

Много безопасности даже в базовом режиме

Уровень защищенности	Базовый	Усиленный	Максимальный
Идентификация и аутентификация	✓ Вкл	✓ Вкл	✓ Вкл
Дискреционное управление доступом	✓ Вкл	✓ Вкл	✓ Вкл
Регистрация событий безопасности	✓ Вкл	✓ Вкл	✓ Вкл
Ограничение программной среды	✓ Вкл	✓ Вкл	✓ Вкл
Изоляция процессов	✓ Вкл	✓ Вкл	✓ Вкл
Защита памяти	✓ Вкл	✓ Вкл	✓ Вкл
Контроль целостности	✓ Вкл	✓ Вкл	✓ Вкл
Обеспечение надежного функционирования	✓ Вкл	✓ Вкл	✓ Вкл
Фильтрация сетевого потока	✓ Вкл	✓ Вкл	✓ Вкл
Маркировка документов	✓ Вкл	✓ Вкл	✓ Вкл
Защита среды виртуализации	✓ Вкл	✓ Вкл	✓ Вкл
Контроль подключения съемных машинных носителей	✓ Вкл	✓ Вкл	✓ Вкл
Использование ядра hardened	✓ Вкл	✓ Вкл	✓ Вкл

Secret Disk Personal

Персональная версия
Криптографическая
защита
конфиденциальной
информации на дисках
рабочих станций

01

Secret Disk Enterprise

Корпоративная версия
Криптографическая
защита информации на
множестве рабочих
станций пользователей с
централизованным
управлением

02

Secret Disk Server

Серверная версия
Криптографическая
защита информации на
дисках файловых
серверов и серверов
приложений

03

Secret Disk Linux

Персональная версия
Криптографическая
информация
конфиденциальной
информации на дисках
рабочих станций Linux

04

Информация о продукте

Характеристики:

- Прозрачное шифрование виртуальных дисков
- Встроенный модуль шифрования Secret Disk Crypto Engine
- Магма, Кузнечик, Эхинацея ГОСТ Р 34.12-2018 , ГОСТ 34.13-2018
- 2ФА пользователей на базе алгоритма ЭП ГОСТ Р 34.10-2018
- Поддержка ОС Astra Linux 1.7
- Поддержка ядра ОС: generic
- Поддержка файловой системы EXT4

Экспериментальные:

- Поддержка ядра Astra Linux в режиме hardened
- Поддержка мандатного режима PARSEC
- Поддержка пользователей домена Astra Linux Domain



ГК АСТРА и АО Аладдин Р.Д.

Защищенная рабочая станция на основе ОС Astra Linux SE и СКЗИ Secret Disk

- Глубоко интегрированное решение
- Полностью отечественный продукт
- Избыточный инструментарий безопасности

Преимущества:

- Надежная защита пользовательских данных
- Предотвращение утечек информации
- Защищенная работа в недоверенной среде
- Защищенный перенос информации
- Фиксация фактов доступа к информации



Сценарии:

- Защита информации на АРМ внутри периметра
- Гибридный график работы и «удаленка»
- Безопасный перенос информации
- Многопользовательская работа на АРМ
- Безопасное хранение информации на АРМ



Технические характеристики

ОС "Astra Linux SE"

- Набор инструментов защиты информации «на борту»
- Защищенный режим ядра ОС "hardened"
- Регулярные обновления безопасности

СКЗИ "Secret Disk"

- Шифрование виртуальных дисков
- Прозрачное шифрование информации
- Модуль шифрования Secret Disk Crypto Engine
- Магма, Кузнечик, Эхинацея ГОСТ Р 34.12-2015
- 2ФА на базе алгоритма ЭП ГОСТ Р 34.11-2012
- Ключевые контейнеры пользователей PKCS#11

