ООО «Базальт СПО»



Интеграция инструментов безопасной разработки в отечественную инфраструктуру разработки Сизиф

Построение кооперации

– Сотрудничество с международными проектами разработки свободных программ

– Построение кооперации с новыми партнерами (ОДКБ, ШОС, БРИКС) в области свободного ПО

– Сотрудничество с отечественными разработчиками по совместному обеспечению безопасности свободного ПО

– Обеспечение регулярной совместимости с отечественным прикладным ПО

Вклад в международные проекты разработки свободного ПО

Проект	Участие «Базальт СПО»
glibc	Основная системная библиотека. Выпускающий последней международной версии – сотрудник «Базальт СПО»
Kernel.org	• ядро Linux. Вклад «Базальт СПО» – модуль LSM, контролирующий запуск скриптовых приложений; • Включение в ядро поддержки крипто, соответствующего российским ГОСТам
SambaDC — служба каталогов, групповые политики	Наша реализация групповых политик взята за основу в международном проекте
Chroot (изолированное окружение для пакетов)	Использование изолированного окружения (chroot) для пакетов, которые могут быть атакованы извне
обеспечение совместимости с MS Active Directory	«Базальт СПО» создала патчи масштабирования систем для Samba DC
защищенный терминальный доступ	участие в проекте libssl («Базальт СПО» - один из ключевых разработчиков)
Strace – отслеживание системных вызовов между процессом и операционной системой (ядром)	Базальт СПО» - один из основных разработчиков проекта. При проверках ПО для сертификации во ФСТЭК многие отечественные компании используют трассировщик Strace

Вклад в международные проекты разработки свободного ПО

Проект	Участие «Базальт СПО»
Apt RPM – контроль цепочек зависимостей на основе RPM	«Базальт СПО» ведет проект
Xcat – управление узлами, используемыми в суперкомпьютерах	реализована возможность загрузки разнородных образов на разные узлы
Zabbix – система мониторинга	обеспечена возможность иерархического сбора информации
LSM (Linux Security Module)	создан дополнительный модуль
Мандатный доступ	«Базальт СПО» создал и развивает собственные политики
PVE - управление средой, в которой выполняются виртуальные окружения	собран специальный дистрибутив для разворачивания и управления виртуализацией
Технологии по сетевой ОС	создана специальная версия ОС для управления высокоскоростными пакетными процессорами коммутаторов маршрутизаторов (в частности, для сетевого устройства на базе Mellanox)
Alterator - модульная система управления	собственная разработка «Базальт СПО»

Совместный анализ кода

– Единая методология анализа и единый набор инструментов от ИСП РАН (SVACE, Crusher) и др. (Syzkaller и др.),

– Совместная работа над разметкой и исправлением кода, в т.ч. уязвимостей,

– Мы проводили фаззинг

1. qemu (qemu-5.2.0-alt6)
2. python3 (python3-3.7.4-alt3)
3. PAM (linux-pam-1.3.1.0.5.955b-alt2 - pam, libpam0, pam0)
4. openssh (openssh-7.9p1-alt1)
5. libvirt (libvirt-7.3.0-alt0.p9.1)
6. kernel (kernel-image-std-def-5.10.32-alt0.c9f, kernel-image-rt-4.19.184-alt1.rt75 и kernel-image-rt-4.19.189-alt1.rt78)
7. iptables (iptables-1.8.3-alt2)
8. docker-ce (docker-ce-19.03.13-alt2)
9. bash и sh (bash4-4.4.23-alt1)
10. ahttpd (alterator-fbi-5.49-alt1)

Расширение фаззинг-тестирования в отношении сетевых сервисов (dns, dhcp, почта)

Инфраструктура разработки. Используемый инструментарий

Проекты «Базальт СПО»

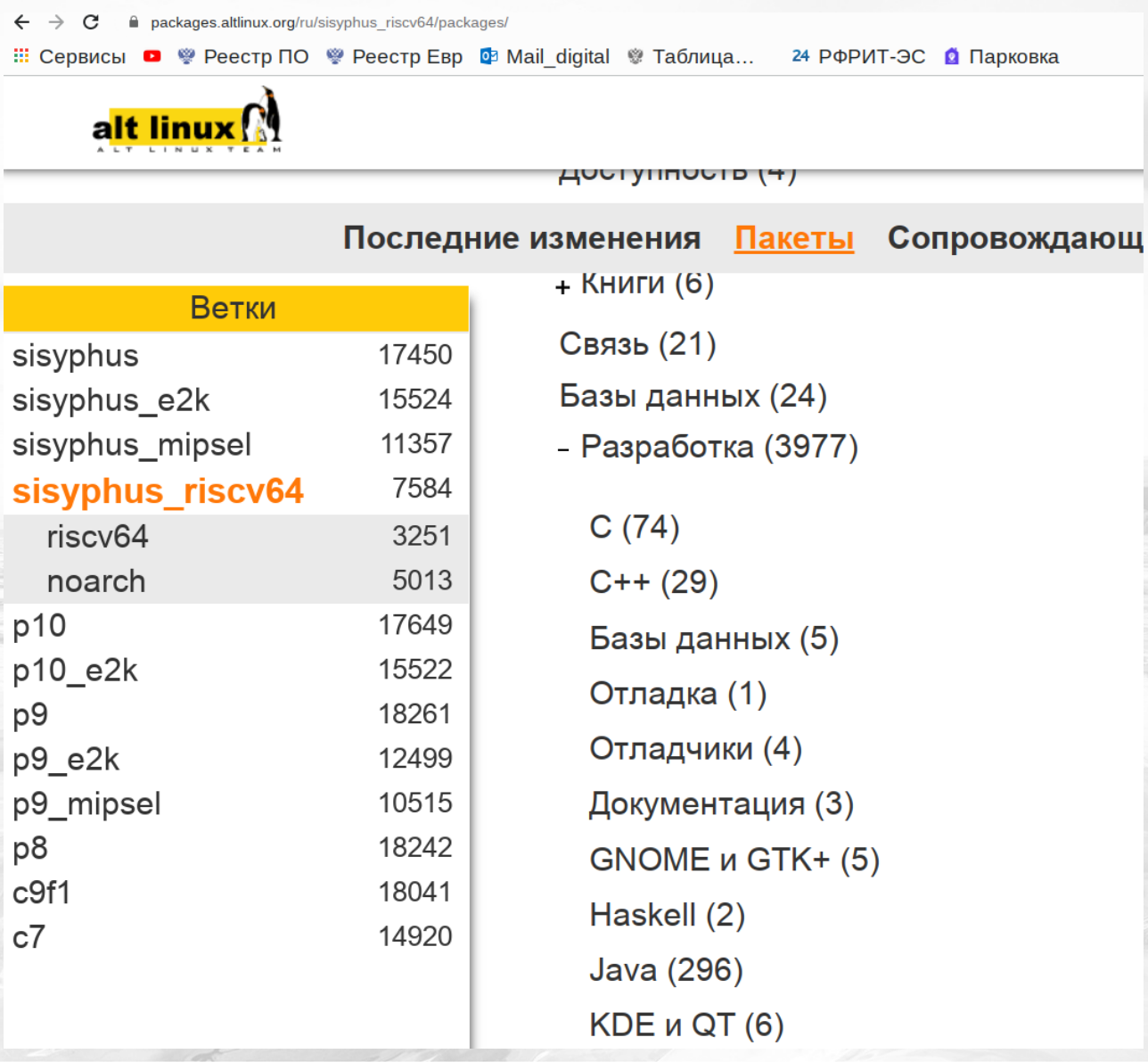
- Hasher - инструмент динамического создания «чистого», изолированного, безопасного окружения, в том числе для сборочной среды. Разработан российским вендором ОС на базе репозитория «Сизиф»
- Gear – инструмент сборки непосредственно из системы версионирования git
- Buildreq – инструмент, позволяющий искать зависимости сборки и оптимизировать их
- Repocop (включая Sisyphus check) – инструмент интеграционных тестов, с возможностью проверки по очень жестким условиям. Позволяет использовать различные модули проверки, проводить проверку по различным сценариям и анализировать полученный результат по многим параметрам.
- Alterator pkg – средство формирования групп пакетов (в частности, для дистрибутивов)
- Strace – инструмент отслеживание системных вызовов между процессом и операционной системой (ядром)
- Herodotus – система отслеживания критических изменений кода
- Mkimage – инструмент для формирования образа ОС для загрузочного носителя (в том числе загрузки по сети)
- Инструменты тестирования

Существенная доработка

- RPM – базовый пакетный менеджер, обеспечивающий, в частности, межпакетный поиск зависимостей. Российским вендором ОС создан дополнительный функционал контроля зависимостей

Готовые инструменты разработки

- Git – стандартное хранилище с поддержкой версионирования
- Bugzilla – стандартный инструмент для сбора информации о проблемах и работы с ними


packages.altlinux.org/ru/sisyphus_riscv64/packages/
Сервисы
Реестр ПО
Реестр Евр
Mail_digital
Таблица...
РФРИТ-ЭС
Парковка
alt linux
ALT LINUX TEAM
Доступность (4)
Последние изменения
Пакеты
Сопровождающ
Ветки
sisyphus 17450
sisyphus_e2k 15524
sisyphus_mipsel 11357
sisyphus_riscv64 7584
riscv64 3251
noarch 5013
p10 17649
p10_e2k 15522
p9 18261
p9_e2k 12499
p9_mipsel 10515
p8 18242
c9f1 18041
c7 14920
+ Книги (6)
Связь (21)
Базы данных (24)
- Разработка (3977)
C (74)
C++ (29)
Базы данных (5)
Отладка (1)
Отладчики (4)
Документация (3)
GNOME и GTK+ (5)
Haskell (2)
Java (296)
KDE и QT (6)

base alt

Интеграция средств анализа в инфраструктуру разработки

В репозитории, из которого формируются сертифицированные дистрибутивы, выделяются классы пакетов:

– формирующие поверхность атаки (20)

- реализующие КСЗ (300)

– входящие в состав сертифицированного дистрибутива (2 000)

– прочие

При формировании репозитория (добавление пакетов), а также при обновлении пакетов, в зависимости от класса, до включения в репозиторий проводятся фаззинг, статический анализ, сборка под аудитом (логи сборки хранятся в ClickHouse).

В дистрибутив попадают только пакеты, собранные под аудитом.

Интеграция с этапом функционального тестирования и с системой управления задачами.

Импортозамещение

В этом разделе можно ознакомиться с тем, какие продукты предлагаются отечественными разработчиками для замещения определённых иностранных продуктов.

По разделам классификатора

Полный список замещаемого ПО →

- Аппаратное обеспечение
  - ПАК
  - Аппаратные СКЗИ
    - Ключевые носители
  - Аппаратные модули доверенной загрузки
  - СХД
  - Сетевое оборудование
- Встроенное ПО
  - ПО аппаратных ключей
  - ПО промышленных микроконтроллеров
- Операционные системы
  - Серверные ОС
  - ОС рабочих мест
  - Мобильные ОС
  - Встроенные ОС
- Системы виртуализации
  - Гипервизоры
  - Системы управления виртуализацией
  - Программно определяемые хранилища
  - VDI
- Системные утилиты
- СУБД и средства работы с данными
  - Реляционные СУБД
  - Нереляционные СУБД
  - СУБД для аналитики
  - ETL-системы
  - MDM-системы (Master Data Management)
  - Аналитические системы (BI)
  - Управление корпоративными данными (Data Governance)
  - Системы документооборота (СЭД), ECM-системы
  - PDF-вьюеры и редакторы
  - Базы знаний
- Лингвистическое ПО
- Офисные пакеты
- Коммуникационное ПО
  - Instant Messaging
  - E-mail серверы
  - E-mail клиентское ПО
  - Телефония
- Системы управления проектами
- Биллинговые системы
- CRM-системы
- ПО для промышленности
  - AMM-системы (управление промышленным производством)
  - CAD/ECAD/CAM/CAE-системы
  - SCADA
  - PDM - системы (Product Data Management)
  - PLM - системы (Product Lifecycle Management)
  - АСУТП
  - EAM-системы (управление активами предприятия)
  - Моделирование технических систем и объектов
  - IIoT (промышленный интернет вещей)
  - QA
  - QMS
  - LIMS
  - MES
- EMM/MDM/MAM-системы (управление мобильными устройствами/приложениями)

Совместимо с ОС Альт

ПАК «МФЦ ПЛЮС»

«МФЦ ПЛЮС» — первый российский программно-аппаратный комплекс для автоматизации деятельности многофункциональных центров.

СОСТАВ ЕДИНОГО КОМПЛЕКСА ПРОГРАММНЫХ И АППАРАТНЫХ СРЕДСТВ «МФЦ ПЛЮС»:

Серверы Яхонт-УВМС

Серверы «Яхонт-УВМ Э12», «Яхонт-УВМ Э24», «Яхонт-УВМ Э124» — линейка российских серверов производства «НОРСИ-ТРАНС» на базе отечественных восьмиядерных процессоров «Эльбрус».

АИС «МФЦ ДЕЛО»

АИС МФЦ ДЕЛО — автоматизированная информационная система, предназначенная для информационного обеспечения МФЦ (разработана ЭОС). АИС позволяет автоматизировать процессы оказания государственных (муниципальных) услуг, а также минимизировать действия и ошибки сотрудников МФЦ в процессе приема, выдачи и обработки документов.

ОС «Альт Сервер»

ОС «Альт Сервер» — российская операционная система на основе ядра Linux разработки «Базальт СПО».

СУБД «PostgresPro»

СУБД Postgres Pro — российская система управления базами данных, разработанная компанией Postgres Professional с использованием свободно-распространяемой СУБД PostgreSQL.

АПК "ЗАСТАВА-ТК"

АПК "ЗАСТАВА-ТК" — это комплекс программных продуктов, обеспечивающих защиту корпоративных информационных систем на сетевом уровне с помощью технологий виртуальных частных сетей (VPN) и распределенного межсетевого экранирования (МЭ, FW).

СОСТАВ:

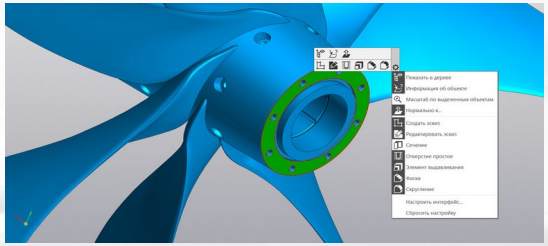
- Аппаратная платформа – компьютер в форм-факторе «тонкий клиент»
- Электронный идентификатор, аппаратно реализующий российские стандарты электронной подписи, шифрования, хэширования и являющийся ключевым носителем
- Операционная система «Альт»
- СКЗИ «КриптоПро CSP»
- Программное обеспечение на базе ЗАСТАВА-Клиент, версия 6
- ПО ESMART Token ГОСТ

Уникальность разработки:
АПК «ЗАСТАВА-ТК» – продукт с готовым набором средств защиты информации и сервисом электронной подписи, сертифицированный по классу КС3.

ОС «Альт» в составе программно-аппаратного стека «Инженерные решения»

ТеСИС

Программный комплекс для конструкторов, инженеров и технологов FlowVision



Компас_3D АСКОН

base alt

ОС «Альт» для серверов и рабочих станций

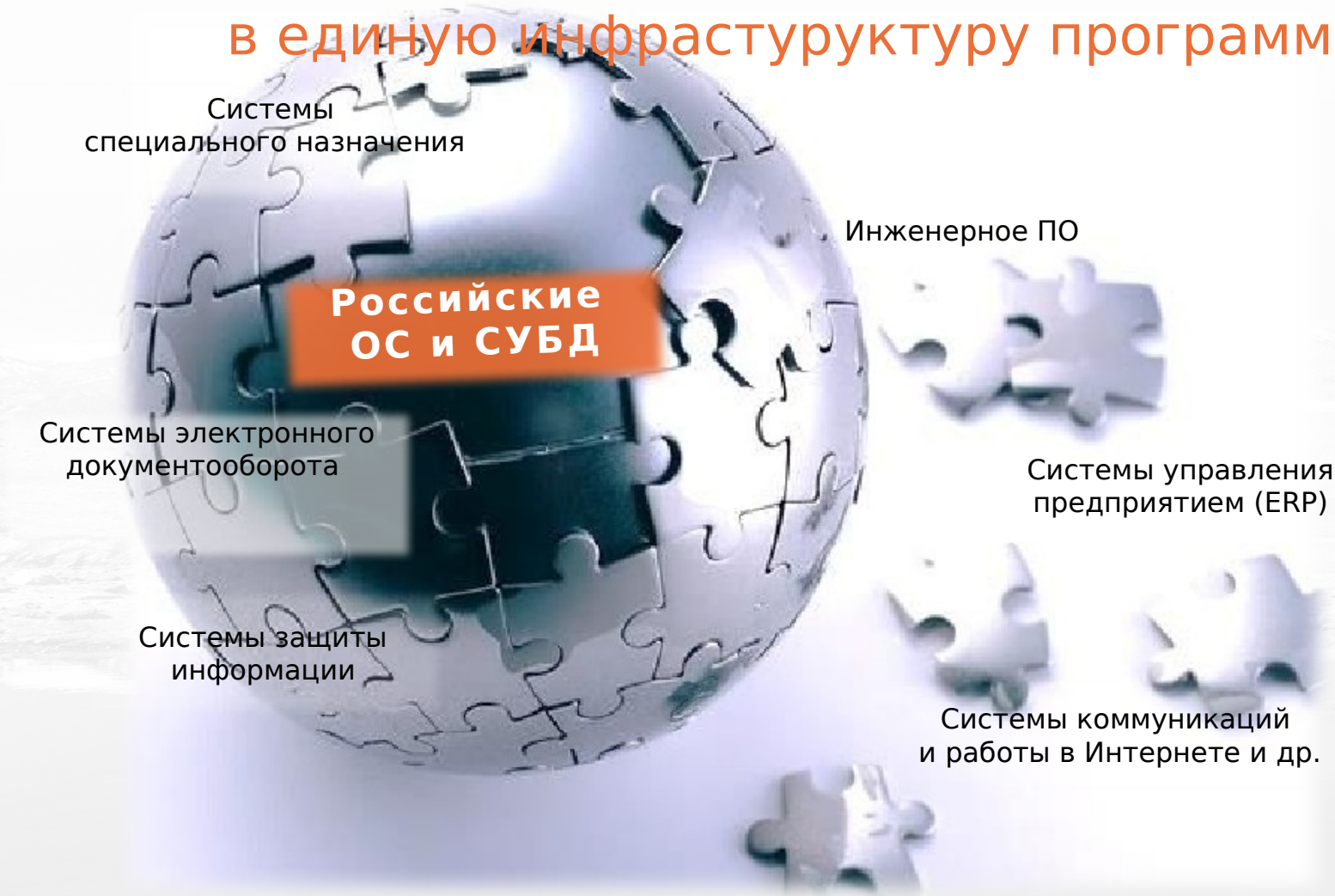
Серверы, рабочие станции и суперкомпьютеры на основе российского процессора «Эльбрус»

МЦСТ ЭЛЬБРУС





Обеспечить встраивание прикладных программ в единую инфрастуруктуру программной платформы



– использование системных библиотек,
– централизованное закрытие уязвимостей в используемых библиотеках,
– регулярный контроль зависимостей,
– использование пакетов и контейнеров.

Общее число пакетов ~2000
Число пакетов КС3 ~300
Число пакетов границы ~20

Статанализаторы:
C/C++
gcc -fanalyze
cppcheck
Intel control-flag
платные
svace
Еще бывает
PVS-Studio
Python : bandit
Shell: shellcheck