ООО «Базальт СПО»

Российский разработчик операционных систем «Альт»

basealt.ru

ОС «Альт» — платформа информационной безопасности

Чернобривченко Елена

Эксперт по информационной безопасности

chernobrivchenkoev@basealt.ru

Операционная система «Альт». Международный проект Сизиф. История и формирование

Сотрудничество IPLabs Linux Team, совместного проекта московской фирмы IPLabs и Института Логики, с Жилем Дювалем и MandrakeSoft началось вскоре после выхода Mandrake.

1999-2000 — на основе дистрибутива MandrakeLinux выпускаются пакеты русификации и создаётся его русская версия Linux-Mandrake Russian Edition. Разработчик — проект IPLabs Linux Team.

2000 — начинается постепенное замещение пакетов Mandrake собственными сборками. Существенно изменена система сборки и макросы пакетного менеджера RPM.

2001 — Linux-Mandrake Russian Edition Spring 2001 — это уже не просто русифицированный вариант Linux-Mandrake, а значительно модифицированный дистрибутив: переработана серверная часть, очень много новых пакетов и большое количество существенно измененных.

Операционная система «Альт».
Международный проект Сизиф. История и формирование

От IPLabs Linux Team к ALT Linux Team

После выхода Russian Edition число концептуальных отличий русской версии от международной стало очень велико. К этому времени в Mandrake сложилась своя команда разработчиков со своими взглядами и пристрастиями.

То же самое произошло и с IPlabs Linux Team. На базе значительно увеличившейся команды в 2001 году создана новая самостоятельная коммерческая организация «Альт Линукс», которая занимается свободными программами и выпускает все свои инициативные разработки под свободными лицензиями. Все члены нашей команды ALT Linux Team — программисты, лидеры и участники крупных международных проектов.

Впервые была осуществлена сборка и поддержка всех пакетов, впервые создан свой «дистрибутив в вечной разработке» — Sisyphus. Linux-Mandrake RE Spring 2001 не привязан ни к одной из версий Linux-Mandrake RE.

Операционная система «Альт».
Международный проект Сизиф. История и формирование

Выпуск дистрибутивов в защищённом исполнении на базе «Сизиф»

2003 — на базе «Сизифа» впервые начинают выпускаться дистрибутивы в защищённом исполнении (сертифицированные ФСТЭК) и продукты фирм-партнеров: например, межсетевой экран «ИВК Кольчуга», сертифицированный по требованиям Министерства обороны России и ФСТЭК России.

2005 — к версии 3.0 все пакеты Mandrake, инсталлятор и система конфигурирования полностью вытеснены собственными разработками ALT Linux Team.

Операционная система «Альт».
Международный проект Сизиф. История и формирование

APT — Advanced Packaging Tool

Усовершенствованное средство управления программными пакетами APT первоначально было разработано для управления пакетами в дистрибутиве Debian GNU/Linux.

Долгое время система APT была доступна только пользователям Debian GNU/Linux, поскольку поддерживала только один тип системы управления пакетами — применяемый в Debian GNU/Linux менеджер dpkg.

Dpkg несовместим с используемой в Linux Mandrake Russian Edition системой управления пакетами RPM, и эта несовместимость заключается не просто в выборе разных форматов, используемых для хранения данных о пакетах программ, она значительно глубже.

Однако APT изначально проектировалась как система, не зависящая от метода управления установленными в системе пакетами, и эта особенность позволила разработчикам ALT Linux Team реализовать в ней поддержку менеджера пакетов RPM.

Получили возможность использовать эту мощную систему APT , поддерживающая RPM.

Операционная система «Альт».
Международный проект Сизиф. История и формирование

Продолжение разработки защищённых решений на базе «Сизиф»

В период с 2006 по 2014 ООО «Альт Линукс» занимался разработкой, продажей и поддержкой решений и дистрибутивов ALT Linux на базе Sisyphus и стабильных веток репозитория, а также разработкой Sisyphus, поддержкой инфраструктуры Sisyphus. Выпускают три сертифицированных ФСТЭК дистрибутива: в 2008 Alt Linux Desktop 4, в 2011 ALT Linux SPT 6.0, в 2017 ALT Linux SPT 7.0.

Операционная система «Альт».
Международный проект Сизиф. История и формирование

Поддержка и развитие «Сизиф» передана «Базальт СПО»

2015 — учредители компании «Альт Линукс» приняли решение о прекращении деятельности и создании компании «Базальт СПО» с практически теми же разработчиками, которая взяла на себя ответственность за поддержку и развитие проекта «Сизифа». Вся инфраструктура обеспечивается компанией. Репозиторий находится в российской юрисдикции.

2016 — все продукты семейства «Альт» включены в Единый реестр российских программ. Объявлено об отделении бранча платформы p8 от «Сизифа»; на её основе осуществлён выпуск коммерческих дистрибутивов «Альт». Начинает предоставляться техподдержка ОС «Альт» на всей территории страны в режиме 24/7/365. Получены лицензии ФСТЭК на деятельность по разработке и производству средств защиты конфиденциальной информации, а также на деятельность по технической защите конфиденциальной информации. Начали работу офисы разработки «Базальт СПО» в Москве, Санкт-Петербурге, Обнинске, Саратове.

Операционная система «Альт».
Международный проект Сизиф. История и формирование

Поддержка и развитие «Сизиф» передана «Базальт СПО»

2017 — стартует выпуск нативных сборок дистрибутивов с поддержкой процессоров «Эльбрус».

2018 — в репозитории «Сизиф» поддерживаются более 19 тыс. пакетов программ и различные аппаратные архитектуры: зарубежные (x86, x86-64) и отечественные («Эльбрус», Байкал-T1). Выпущена защищённая версия ОС Альт 8 СП для семи аппаратных платформ, сертифицированная по требованиям Министерства обороны России и ФСТЭК России (разработка компании «ИВК»).

2019 — выпуск платформы p9. Наряду с архитектурами x86, ALT p9 поддерживает 6 новых аппаратных архитектур. Серьёзные изменения в apt и rpm. Центр приложений установка не пакетов, а приложений (с показом снимков экрана, рейтингами, локализованным описанием) — gnome-software и discover. Единый пакет samba, контроллер домена можно установить на любой дистрибутив с любой средой.

Базальт СПО сотрудничает с Технологическим центром исследования безопасности ядра Linux

Компания сотрудничает с Технологическим центром исследования безопасности ядра Linux, созданным в 2021 г. на базе Института системного программирования Российской академии наук (ИСП РАН).

Разработчики ОС «Альт» участвуют в тестировании безопасности ядра Linux и с учётом полученных результатов выпускают собственные сборки ядра.

Участвуем в рабочей группе по доверенной загрузке.

2022 — «Альт» одна из первых — операционная система, которая перешла на ядро Linux 5.10, поддерживаемое Технологическим центром исследования безопасности ядра Linux.

На протяжении всей истории своего развития операционные системы семейства «Альт» разрабатывались, как решения с повышенными требованиями по безопасности.

Совместный анализ кода с Технологическим центром исследования безопасности ядра Linux

Единая методология анализа и единый набор инструментов от ИСП РАН:
SVACE, Crusher, Natch.
Свободные инструменты:
Syzkaller, AFL++, libFuzzer, python-afl, Atheris, klee, go-fuzz

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

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

Мы проводим фаззинг

...и это не полный список.

Вклад «Базальт СПО» в международные проекты разработки свободного ПО

Сотрудничество с международными проектами разработки свободных программ

Сотрудничество с отечественными разработчиками по совместному обеспечению безопасности свободного ПО

Проект	Участие «Базальт СПО»
glibc — основная системная библиотека. Выпускающий последней международной версии — сотрудник «Базальт СПО». Опережающее устранение уязвимостей.	
Kernel.org	Ядро Linux. Вклад «Базальт СПО» — модуль LSM, контролирующий запуск скриптовых приложений; включение поддержки крипто, соответствующего российским ГОСТам.

Вклад «Базальт СПО» в международные проекты разработки свободного ПО

Проект	Участие «Базальт СПО»
Харденинг (усиление безопасности)	Участие в проектах Kernel, Glibc, libssl, GCC и др. В частности — в проекте Open Wall Linux (OWL) (среди ключевых участников проекта двое – сотрудники «Базальт СПО»).
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
SambaDC — служба каталогов, групповые политики	Наша реализация групповых политик взята за основу в международном проекте
Защищённый терминальный доступ	Участие в проекте libssl («Базальт СПО» — один из ключевых разработчиков)

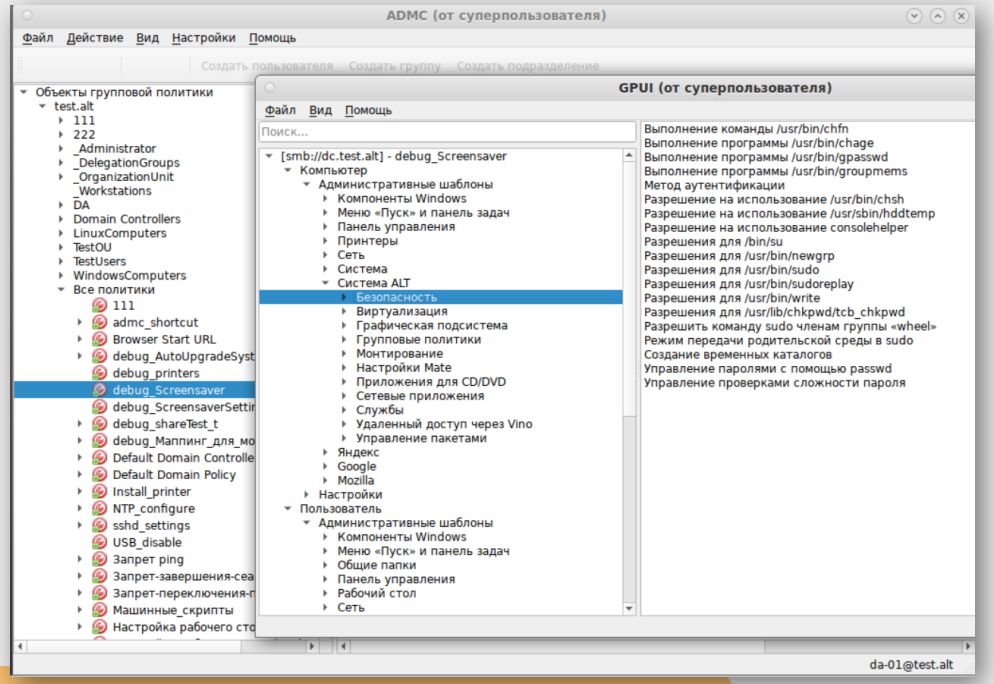
Вклад «Базальт СПО» в международные проекты разработки свободного ПО

Проект	Участие «Базальт СПО»
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.
Apt RPM — контроль цепочек зависимостей на основе RPM	«Базальт СПО» ведёт проект
Xcat — управление узлами, используемыми в суперком-пьютерах	Реализована возможность загрузки разнородных образов на разные узлы
Zabbix — система мониторинга	Обеспечена возможность иерархического сбора информации
LSM (Linux Security Module)	Создан дополнительный модуль

Вклад «Базальт СПО» в международные проекты разработки свободного ПО

Проект	Участие «Базальт СПО»
SE Linux	«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	Инсталлятор и система управления — собственная разработка «Базальт СПО»

«Базальт СПО» развивает групповые политики



Доработаны графические инструменты управления ADMC и GPUI

За прошедший период нами усовершенствовано и разработано более 10 политик:

1. Управление ini файлами.
2. Подключение сетевых дисков.
3. Политики управления браузерами firefox, chromium, yandex.
4. Копирование файлов.
5. Создание папок.
6. Сценарии (скрипты), пользовательские/-машинные.
7. Создание ярлыков.
8. Управление реестром Windows.
9. Политика замыкания.

и многие другие.

https://www.altlinux.org/Групповые_политики

Безопасная инфраструктура разработки, опережающее устранение уязвимостей

Соответствует ГОСТ Р 54593-2001 «Информационные технологи». «Свободное программное обеспечение».

Воспроизводимая сборка, с точностью до контрольной суммы (в виртуальной сборочной среде, динамически создаваемой на основе зависимостей с помощью технологии hasher). Обеспечивает безопасность и воспроизводимость сборки, упрощает проверки ОС.

Использование специальных опций компилятора (многие warning квалифицируются как ошибки, контроль выхода за границу массива, переполнения буфера, рандомизация адресов имен и др.), что позволяет обеспечить дополнительную защиту (уменьшает возможность атак).

Превентивные меры по обеспечению безопасности

Зачистка переменных окружения при получении новых пользовательских привилегий (реализовано только у «Базальт СПО» и Open Wall Linux). Дифференциация привилегий: запрет на наследование прав при переходе на другой уровень привилегий, что ограничивает диапазон действий пользователя до реально необходимого.

Применение модуля ядра LSM (собственная разработка «Базальт СПО»), который реализует запрет хранить вместе с данными программы на интерпретируемых языках. Это позволяет исключить запись данных в ту область, где лежит код, и сделать её доступной только для чтения, что повышает защищенность системы в целом. Данная разработка «Базальт СПО» — первая в мировой практике разработки СПО.

Практический опыт внедрения SDL в компании. Растим штатную большую SDL-команду

Проблемы с компетенциями. При наборе сотрудников в отдел безопасности разработки программного обеспечения многие кандидаты не имеют предыдущего опыта связанного с динамическим тестированием.

Но нас это не останавливает — мы увеличиваем штат, развиваем компетенции наших специалистов.

Практический опыт внедрения SDL в компании. Технические и инструментальные средства

Инструментальные средства динамического анализа, программы-фаззеры представлены: как свободным ПО с открытым исходным кодом, так и проприетарными продуктами. Недостатка в средствах нет.

Скорее присутствует обратная проблема: из всего многообразия выбрать подходящий для задачи инструмент.

Практический опыт внедрения SDL в компании. Статический анализ

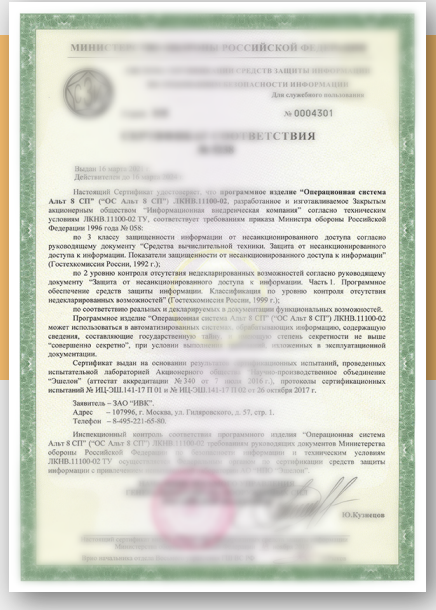
- По выявленной статанализатором ошибке сложно понять реальную угрозу эксплуатации этой ошибки как уязвимости. Хотя сейчас становится уже легче анализаторы совершенствуются.
- Закрытие уязвимости — сложный процесс для разработчика, требует квалификации и способен внести новые ошибки.
- Для многих пакетов приводит к исправлениям других пакетов (например библиотек) и бывают ситуации нарастания исправлений, как снежный ком.
- Чем более старое ПО, тем сложнее там исправлять ошибки, в частности из-за окончания срока поддержки программного обеспечения производителем.
- Чем более новое программное обеспечение, тем больше вероятности найти там свежие ошибки.

«Базальт СПО» — тестирование безопасного компилятора

Организовать тестирование на базе репозитория «Сизиф» конвейер расширенной апробации безопасного компилятора на основе GCC, создаваемого по заказу ФСТЭК России.

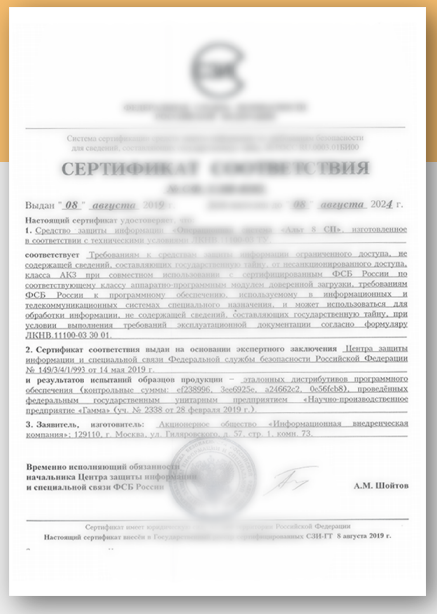
Переиспользование пакетов из репозитория, собираемых с помощью данного компилятора, позволит экономить ресурсы разработчиков и при этом повысить качество и защищенность программных продуктов.

ОС «Альт 8 СП»



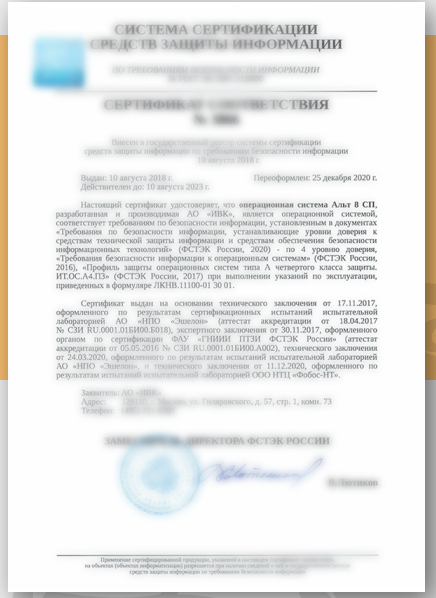
Сертификат МО России (№5238 от 16.03.2021):

- требования безопасности информации к операционным системам» типа А второго класса защиты;
- по 2 уровню контроля отсутствия недекларированных возможностей;
- соответствие реальных и декларируемых в документации возможностей;
- может использоваться в автоматизированных системах, обрабатывающих сведения государственной тайны со степенью секретности не выше «совершенно секретно».



Сертификат ФСБ России (№СФ/СЗИ-0283 от 08.08.2019):

- соответствие требованиям СЗИ ограниченного доступа, не содержащих сведений, составляющих государственную тайну, от НСД, класс АК3.



Сертификат ФСТЭК России (№3866 от 10.08.2018 переоформлен 25.12.2020): требования к ОС 4 класса защиты ИТ.ОС.А4.ПЗ

- 4-й уровень доверия
- работа с персональными данными
- работа с критической информационной инфраструктурой
- работа с конфиденциальной информацией
- работа со средствами виртуализации