hasher

Технология безопасной сборки пакетов дистрибутива

Дмитрий Левин Вартан Хачатуров

ALT Linux Team

12.05.2008

Инструментальные дистрибутивы

- Дистрибутивы 10 лет назад
  - Небольшой объём (менее 1 CD)
  - Узкие группы специалистов
  - Сборка пакетов непосредственно в хост-системе
- Современные дистрибутивы
  - Больший объём и разнообразие ПО (более 1 DVD)
  - Большое число разработчиков разной квалификации
  - Сборка дистрибутива в хост-системе стала `неудобной, ненадёжной и небезопасной`

Сборка в хост-системе: неудобство и ненадёжность

- Неоправданно большой размер сборочной среды
- Несовместимость инструментальных средств
- Необходимость прав администратора для установки произвольных пакетов в хост-систему
- Невозможность параллельной сборки пакетов с несовместимыми сборочными зависимостями
- Зависимость результата сборки от слабоуправляемого состава сборочной среды

Сборка в хост-системе: небезопасность

- Небезопасность самой хост-системы
  - запуск произвольного кода с правами администратора при установке пакетов, требуемых для сборки
- Небезопасность пользователя, занимающегося сборкой
  - запуск произвольного кода с правами сборщика непосредственно во время сборки
- Небезопасность сборок друг от друга
  - изменение сборочного окружения
  - непосредственное воздействие на последующие сборочные процессы

Сборка дистрибутива: источники угроз

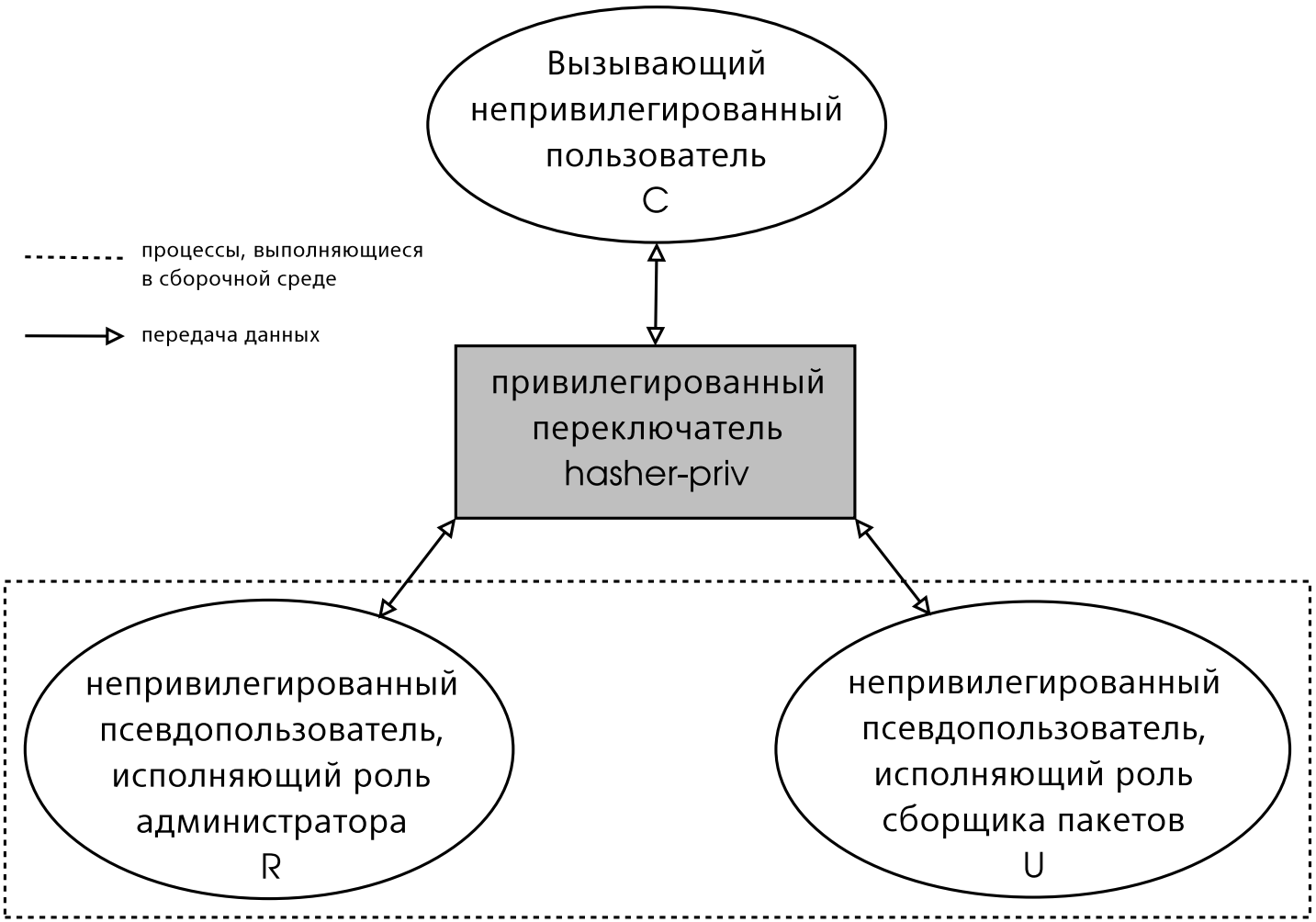
- Привлекательность компрометации дистрибутива
- Большое число разработчиков разной квалификации
- Компрометация клиентского ПО, используемого разработчиком
- Компрометация ПО, собираемого разработчиком
- Непосредственная атака на сборочную систему

Требования к сборочной технологии

Технология сборки элементов дистрибутива должна

- не снижать уровень безопасности хост-системы
- обеспечивать собственную безопасность от атак со стороны пакетов
- обеспечивать безопасность сборки одних пакетов от атак со стороны других пакетов
- гарантировать надёжность (воспроизводимость) результатов сборки
- обеспечивать приемлемый уровень производительности

Архитектура hasher



Путь собираемого пакета

1. Порождение среды (aptbox) для работы с apt (C)
2. Удаление предыдущей сборочной среды (U, R, C)
3. Создание каркаса новой сборочной среды (C)
4. Порождение базовой установочной среды (C, R)
5. Порождение базовой сборочной среды (C, R)
6. Проверка исходного пакета (U)
7. Порождение сборочной среды для пакета (U, C, R)
8. Сборка пакета (U)

Каркас сборочной среды

Вспомогательные каталоги

```
drwxrwxr-t   C R   chroot
drwxr-xr-x   C R   chroot/dev
drwxr-xr-x   C R   chroot/dev/pts
drwx--x--x   C C   chroot/.host
drwxr-xr-x   C C   chroot/.in
drwxrwx--T   C U   chroot/.out
```

Статически слинкованные программы

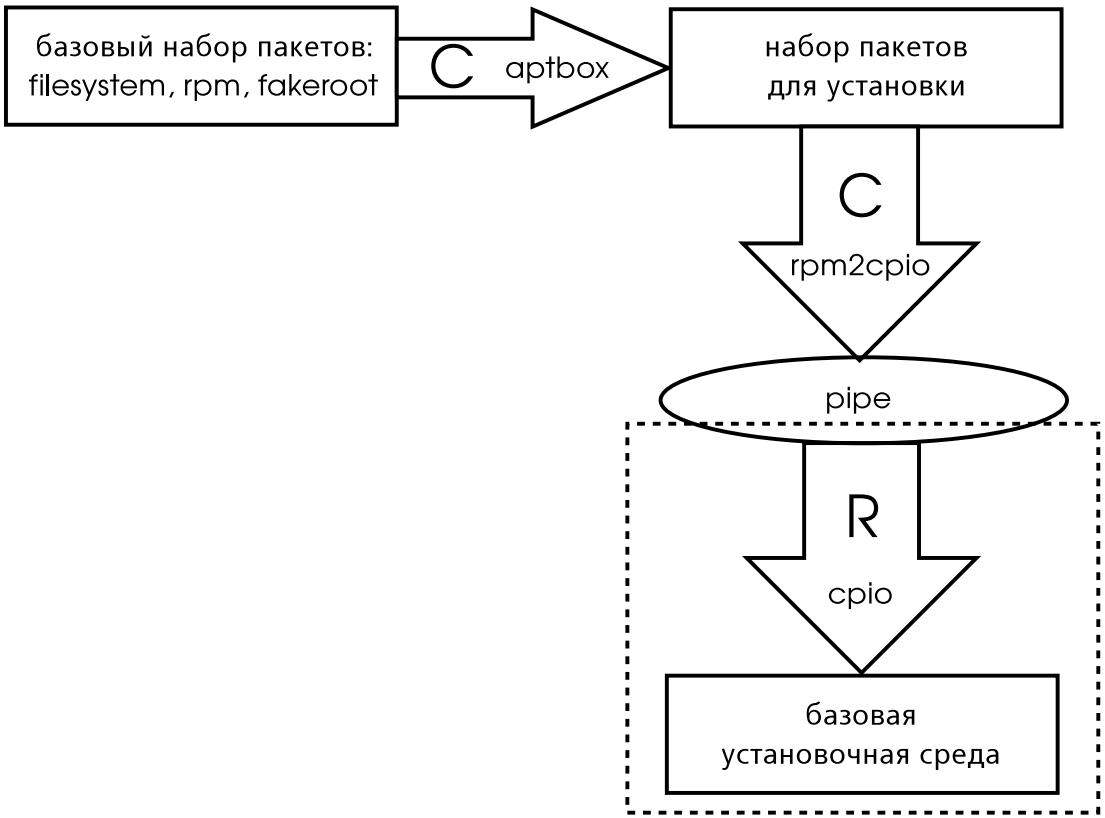
```
-rwxr-xr-x   C C   chroot/.host/cpio
-rwxr-xr-x   C C   chroot/.host/find
-rwxr-xr-x   C C   chroot/.host/sh
```

Фиксированный набор файлов устройств

```
crw-rw-rw-   root root   1, 3 chroot/dev/null
crw-rw-rw-   root root   1, 5 chroot/dev/zero
crw-rw-rw-   root root   1, 7 chroot/dev/full
crw-r--r--   root root   1, 9 chroot/dev/random
crw-r--r--   root root   1, 9 chroot/dev/urandom
```

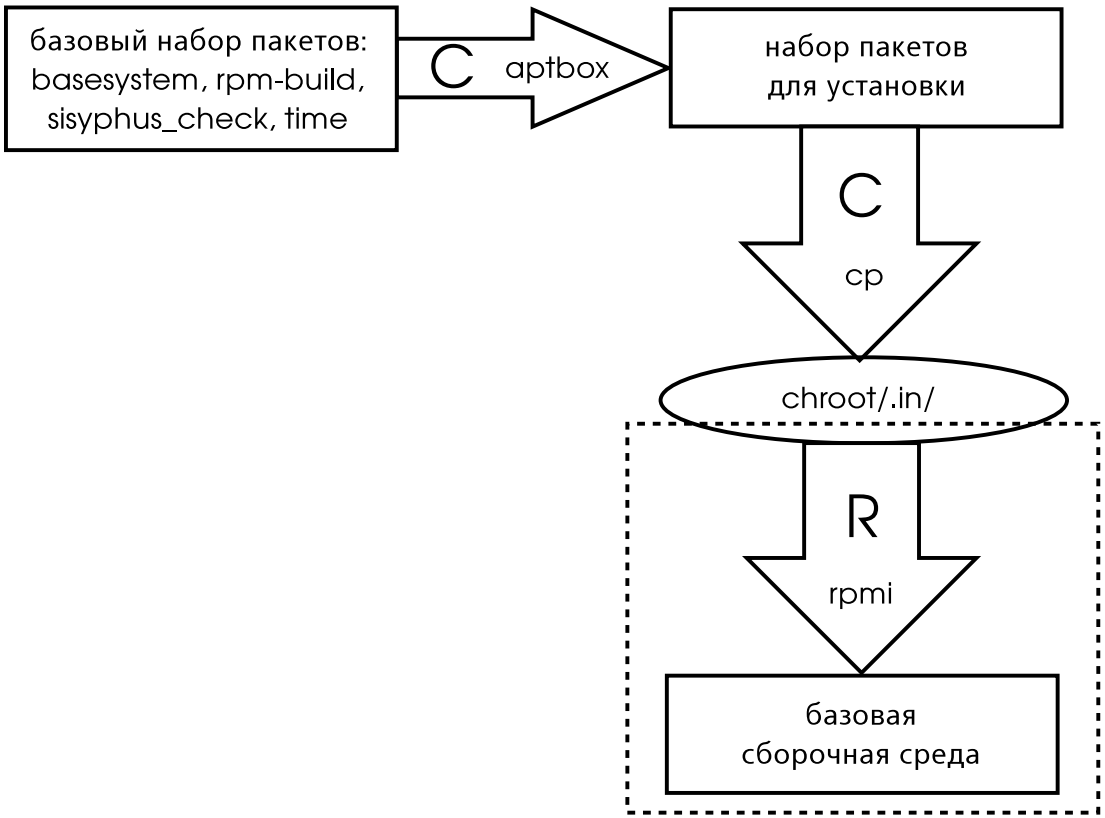
Базовая установочная среда

Каркас + набор средств, необходимых для штатной установки пакетов в эту среду.

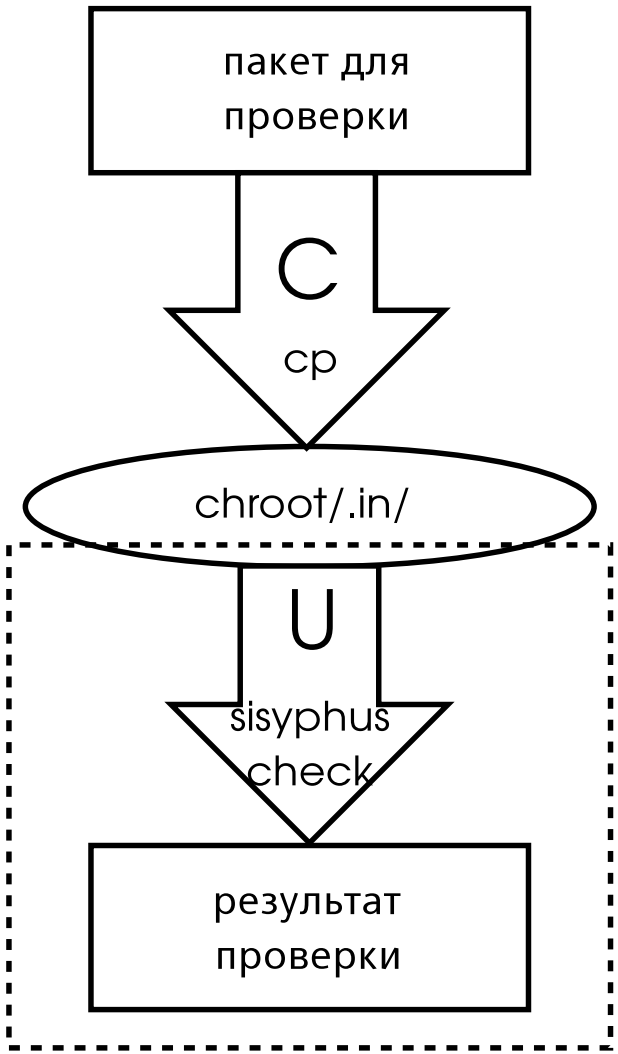


Базовая сборочная среда

Базовая установочная среда + набор пакетов, необходимых для сборки любого пакета

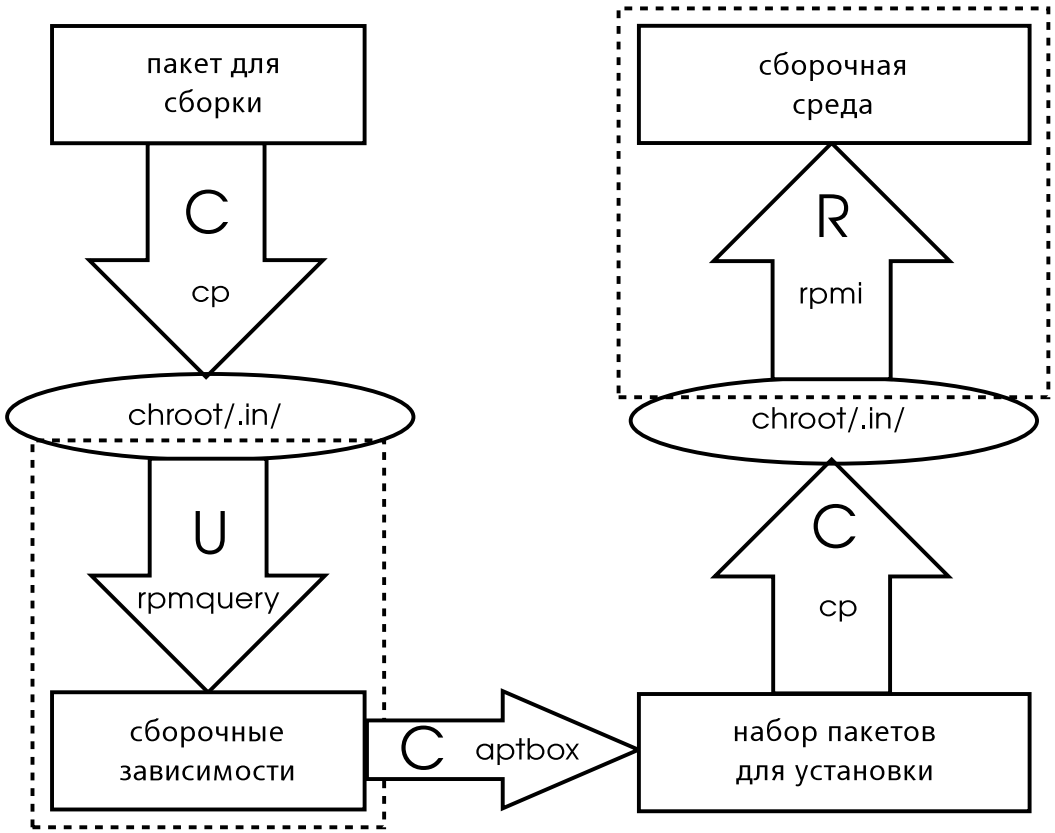


Проверка исходного пакета

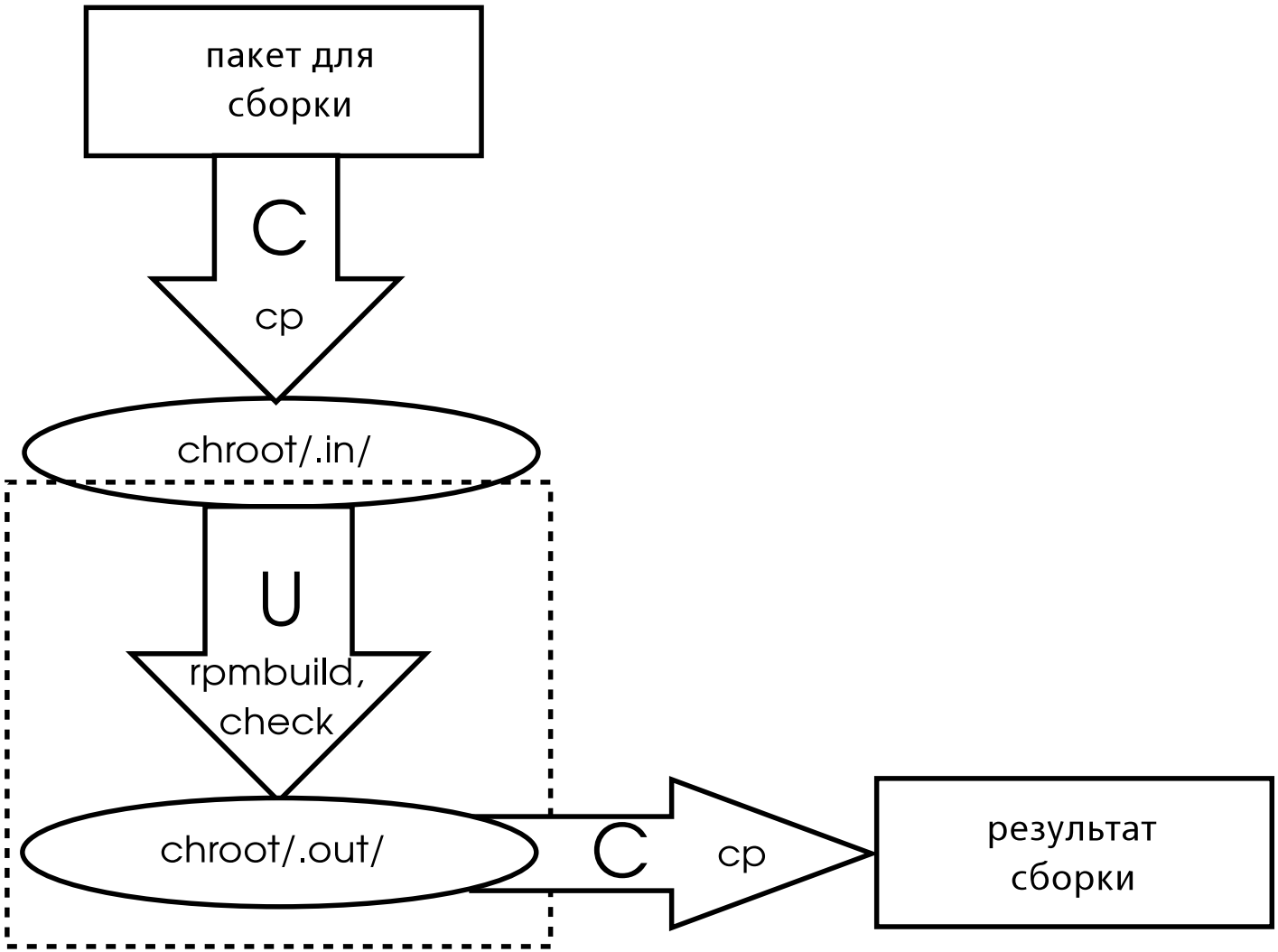


Сборочная среда

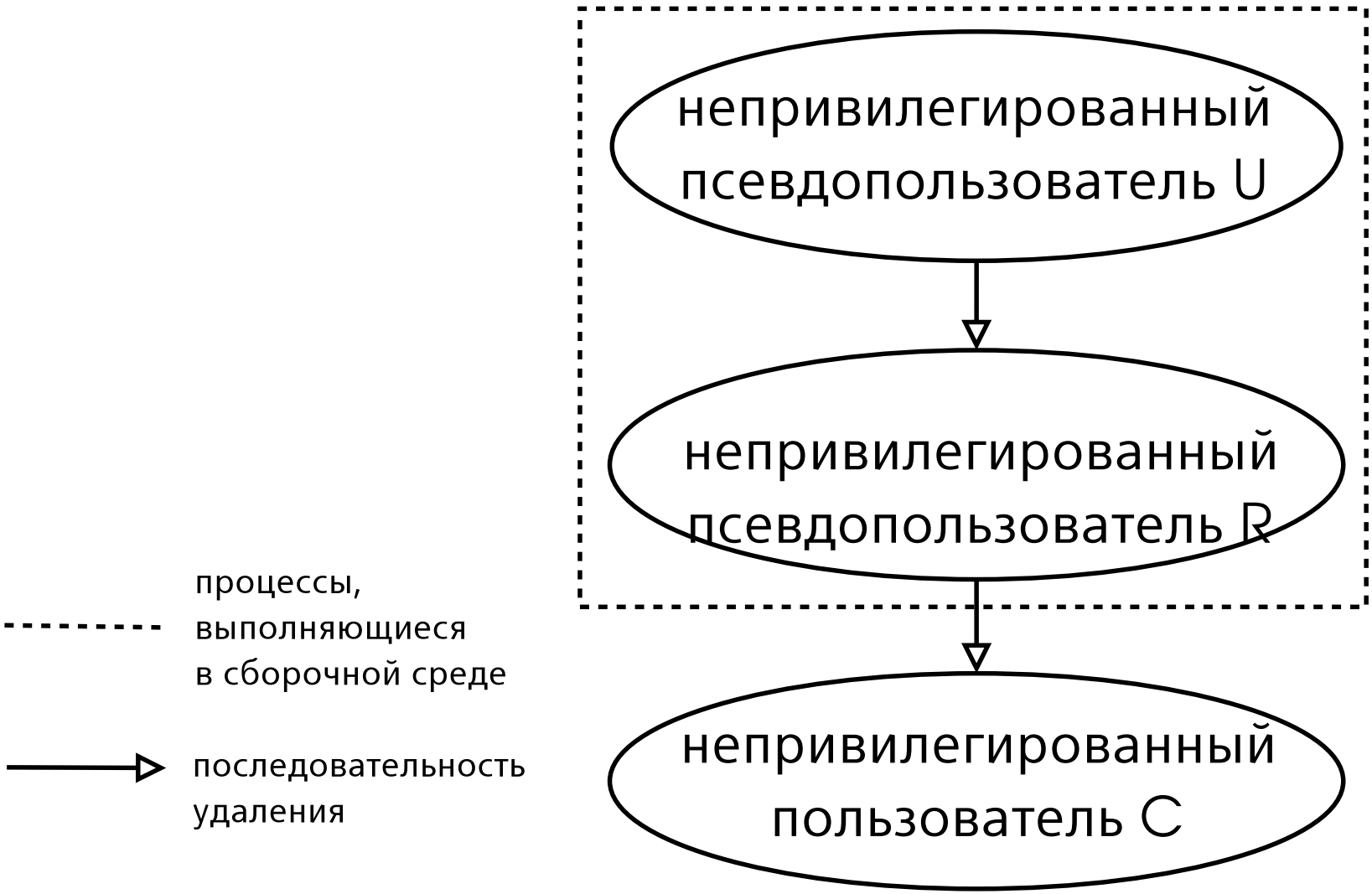
Базовая сборочная среда + набор пакетов, необходимых для сборки данного пакета



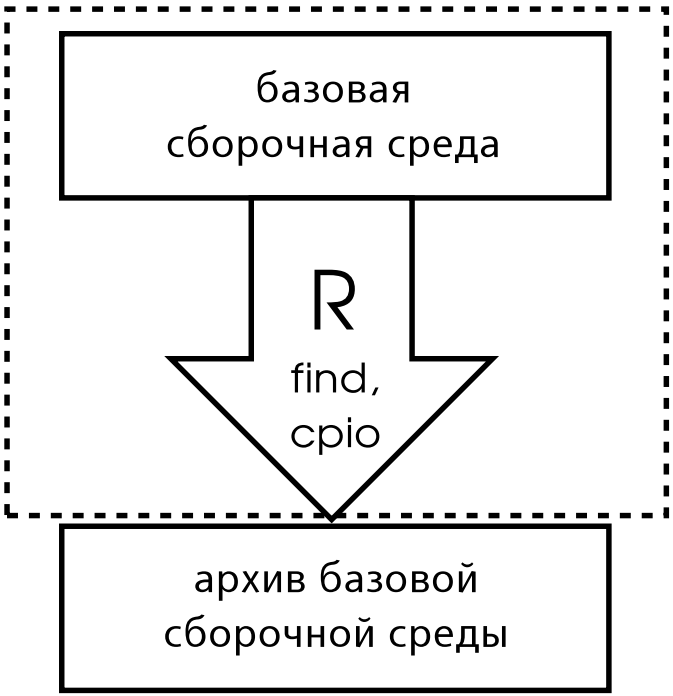
Сборка пакета

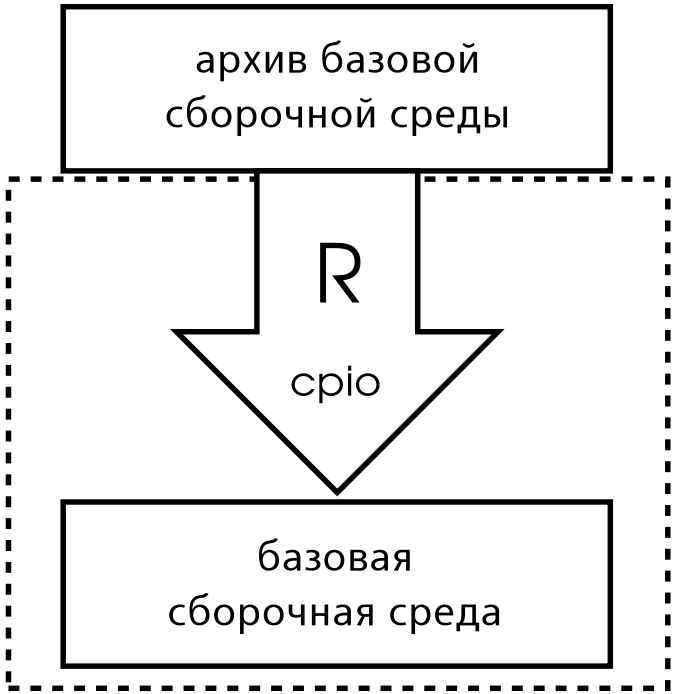


Удаление сборочной среды

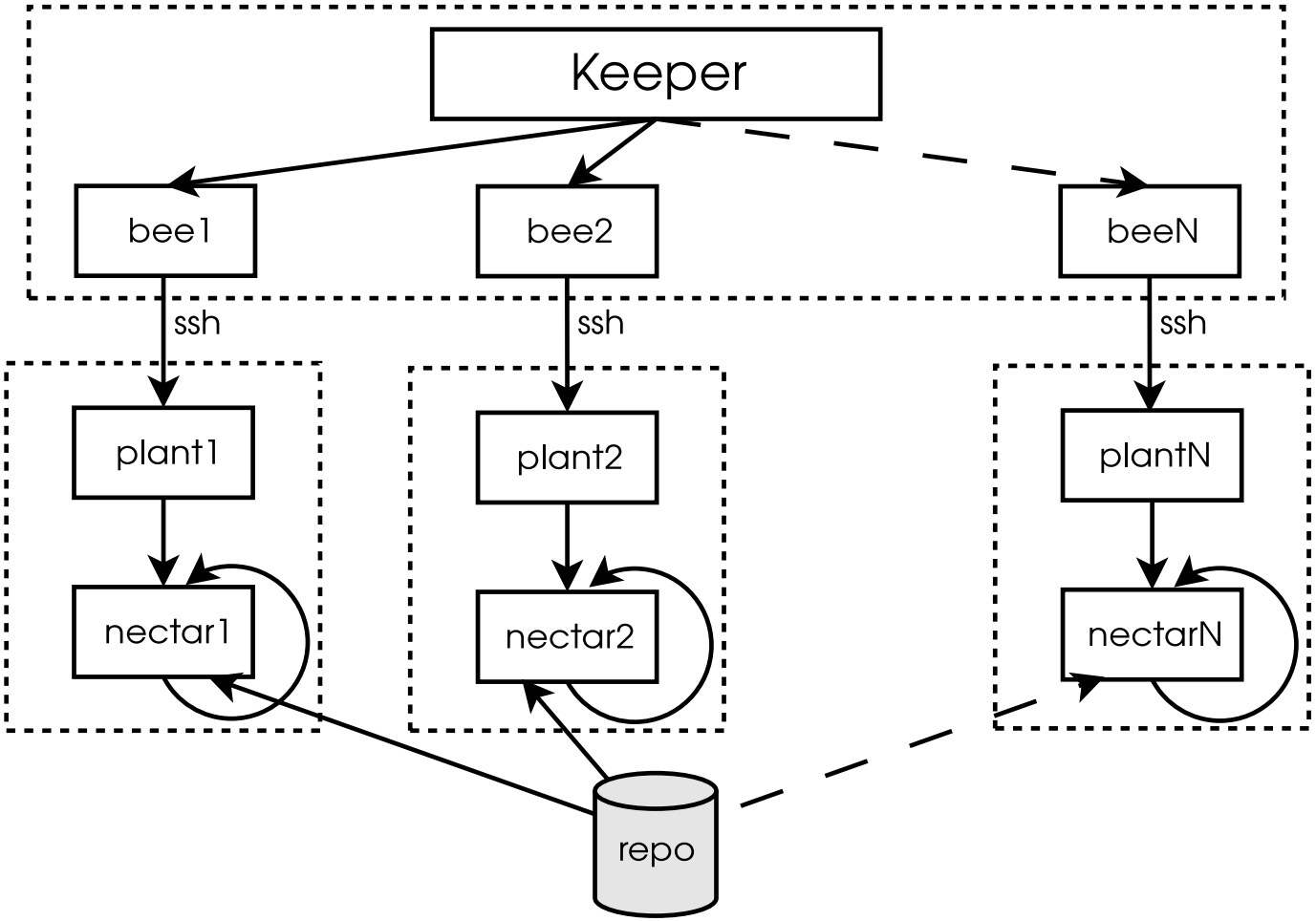


Кэширование базовой сборочной среды





beehive: распределённая сборка пакетов



Изолированное выполнение приложений

- Тестирование программ в эталонной среде
- Отладка программ
- Запуск недоверенных приложений, требующих изолированной среды выполнения по соображениям безопасности
- Обработка недоверенных данных, требующая изолированной среды выполнения по соображениям безопасности

Дополнительная информация

“Домашняя страничка” hasher
`http://ftp.altlinux.org/pub/people/ldv/hasher/`

Вопросы?