Вопросы безопасности при разработке дистрибутивов Linux

Вартан Хачатуров Дмитрий Левин

ALTLinux Technology LLC

02.10.2008

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 (6 CD и более)
  - большое число (тысячи) разработчиков разной квалификации, часто лично не знакомых
  - миллионы пользователей, корпоративных и частных
  - сборка дистрибутива в хост-системе стала неудобной, ненадёжной и небезопасной, а атака на сборочную систему дистрибутива – чрезвычайно привлекательной

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 (6 CD и более)
  - большое число (тысячи) разработчиков разной квалификации, часто лично не знакомых
  - миллионы пользователей, корпоративных и частных
  - сборка дистрибутива в хост-системе стала `неудобной`, `ненадёжной` и `небезопасной`, а атака на сборочную систему дистрибутива – чрезвычайно привлекательной

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

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

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

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

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

Human factor: угрозы от разработчиков

- Обладая shell-аккаунтом на машины проекта, разработчик является потенциальной угрозой для работы проекта в целом
- Обладая правом загрузки на сервера проекта ПО, которое затем в автоматическом режиме становится доступным миллионам пользователей, разработчик является потенциальной угрозой для пользователей
- Личная встреча лидеров проекта с каждым из тысяч разработчиков невозможна

Human factor: угрозы от разработчиков

- Обладая shell-аккаунтом на машины проекта, разработчик является потенциальной угрозой для работы проекта в целом
- Обладая правом загрузки на сервера проекта ПО, которое затем в автоматическом режиме становится доступным миллионам пользователей, разработчик является потенциальной угрозой для пользователей
- Личная встреча лидеров проекта с каждым из тысяч разработчиков невозможна

Human factor: угрозы от разработчиков

- Обладая shell-аккаунтом на машины проекта, разработчик является потенциальной угрозой для работы проекта в целом
- Обладая правом загрузки на сервера проекта ПО, которое затем в автоматическом режиме становится доступным миллионам пользователей, разработчик является потенциальной угрозой для пользователей
- Личная встреча лидеров проекта с каждым из тысяч разработчиков невозможна

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: 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: 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: 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: 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 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 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

Debian New Maintainer Queue

Введение многоэтапной формальной процедуры приёма в стройные ряды разработчиков:

- Подтверждение заявки существующим участником проекта
- Назначение “ведущего” заявки
- Проверка технических и идеологических знаний
- Составление отчёта и создание аккаунта

Debian New Maintainer Queue

Введение многоэтапной формальной процедуры приёма в стройные ряды разработчиков:

- Подтверждение заявки существующим участником проекта
- Назначение “ведущего” заявки
- Проверка технических и идеологических знаний
- Составление отчёта и создание аккаунта

Debian New Maintainer Queue

Введение многоэтапной формальной процедуры приёма в стройные ряды разработчиков:

- Подтверждение заявки существующим участником проекта
- Назначение “ведущего” заявки
- Проверка технических и идеологических знаний
- Составление отчёта и создание аккаунта

Debian New Maintainer Queue

Введение многоэтапной формальной процедуры приёма в стройные ряды разработчиков:

- Подтверждение заявки существующим участником проекта
- Назначение “ведущего” заявки
- Проверка технических и идеологических знаний
- Составление отчёта и создание аккаунта

Debian New Maintainer Queue: WOT

Решение проблемы подтверждения личности – GnuPG (PGP) Web Of Trust.

- Для прохождения процедуры NM **необходима** подпись существующего участника проекта на ключе претендента
- Для получения подписи на ключе необходима проверка fingerprint'а – следовательно, необходима как минимум одна личная встреча претендента с **каким-либо** участником проекта
- Ключи разработчиков доступны в общем keyring
- Разработчики подписывают пакеты, проверка сборочной системой осуществляется при помощи keyring
- Любые операции с аккаунтом (смена пароля, адреса форвардинга) осуществляются при помощи писем, подписанных владельцем ключа
- Возможен перехват пассфразы

Debian New Maintainer Queue: WOT

Решение проблемы подтверждения личности – GnuPG (PGP) Web Of Trust.

- Для прохождения процедуры NM **необходима** подпись существующего участника проекта на ключе претендента
- Для получения подписи на ключе необходима проверка fingerprint'а – следовательно, необходима как минимум одна личная встреча претендента с **каким-либо** участником проекта
- Ключи разработчиков доступны в общем keyring
- Разработчики подписывают пакеты, проверка сборочной системой осуществляется при помощи keyring
- Любые операции с аккаунтом (смена пароля, адреса форвардинга) осуществляются при помощи писем, подписанных владельцем ключа
- Возможен перехват пассфразы

Debian New Maintainer Queue: WOT

Решение проблемы подтверждения личности – GnuPG (PGP) Web Of Trust.

- Для прохождения процедуры NM **необходима** подпись существующего участника проекта на ключе претендента
- Для получения подписи на ключе необходима проверка fingerprint'а – следовательно, необходима как минимум одна личная встреча претендента с **каким-либо** участником проекта
- Ключи разработчиков доступны в общем keyring
- Разработчики подписывают пакеты, проверка сборочной системой осуществляется при помощи keyring
- Любые операции с аккаунтом (смена пароля, адреса форвардинга) осуществляются при помощи писем, подписанных владельцем ключа
- Возможен перехват пассфразы

Debian New Maintainer Queue: WOT

Решение проблемы подтверждения личности – GnuPG (PGP) Web Of Trust.

- Для прохождения процедуры NM **необходима** подпись существующего участника проекта на ключе претендента
- Для получения подписи на ключе необходима проверка fingerprint'а – следовательно, необходима как минимум одна личная встреча претендента с **каким-либо** участником проекта
- Ключи разработчиков доступны в общем keyring
- Разработчики подписывают пакеты, проверка сборочной системой осуществляется при помощи keyring
- Любые операции с аккаунтом (смена пароля, адреса форвардинга) осуществляются при помощи писем, подписанных владельцем ключа
- Возможен перехват пассфразы

Debian New Maintainer Queue: WOT

Решение проблемы подтверждения личности – GnuPG (PGP) Web Of Trust.

- Для прохождения процедуры NM **необходима** подпись существующего участника проекта на ключе претендента
- Для получения подписи на ключе необходима проверка fingerprint'а – следовательно, необходима как минимум одна личная встреча претендента с **каким-либо** участником проекта
- Ключи разработчиков доступны в общем keyring
- Разработчики подписывают пакеты, проверка сборочной системой осуществляется при помощи keyring
- Любые операции с аккаунтом (смена пароля, адреса форвардинга) осуществляются при помощи писем, подписанных владельцем ключа
- Возможен перехват пассфразы

Debian New Maintainer Queue: WOT

Решение проблемы подтверждения личности – GnuPG (PGP) Web Of Trust.

- Для прохождения процедуры NM **необходима** подпись существующего участника проекта на ключе претендента
- Для получения подписи на ключе необходима проверка fingerprint'а – следовательно, необходима как минимум одна личная встреча претендента с **каким-либо** участником проекта
- Ключи разработчиков доступны в общем keyring
- Разработчики подписывают пакеты, проверка сборочной системой осуществляется при помощи keyring
- Любые операции с аккаунтом (смена пароля, адреса форвардинга) осуществляются при помощи писем, подписанных владельцем ключа
- Возможен перехват пассфразы

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

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

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

Требования к сборочной технологии

Технология сборки элементов дистрибутива должна

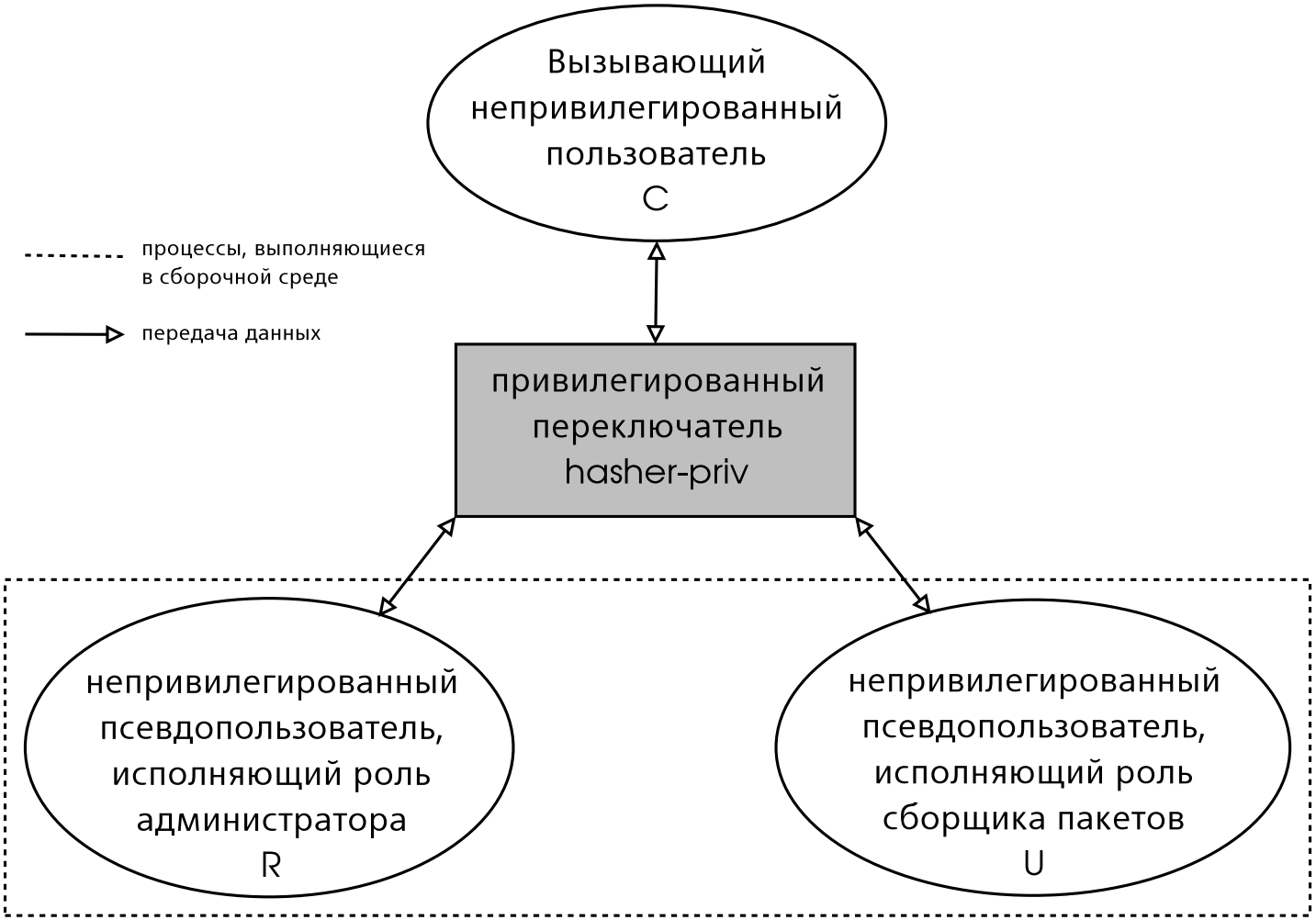
- не снижать уровень безопасности хост-системы
- обеспечивать собственную безопасность от атак со стороны пакетов
- обеспечивать безопасность сборки одних пакетов от атак со стороны других пакетов
- гарантировать надёжность (воспроизводимость) результатов сборки
- обеспечивать приемлемый уровень производительности

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 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)

Путь 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)

Путь 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)

Путь 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)

Путь 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)

Путь 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)

Путь 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)

Путь 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

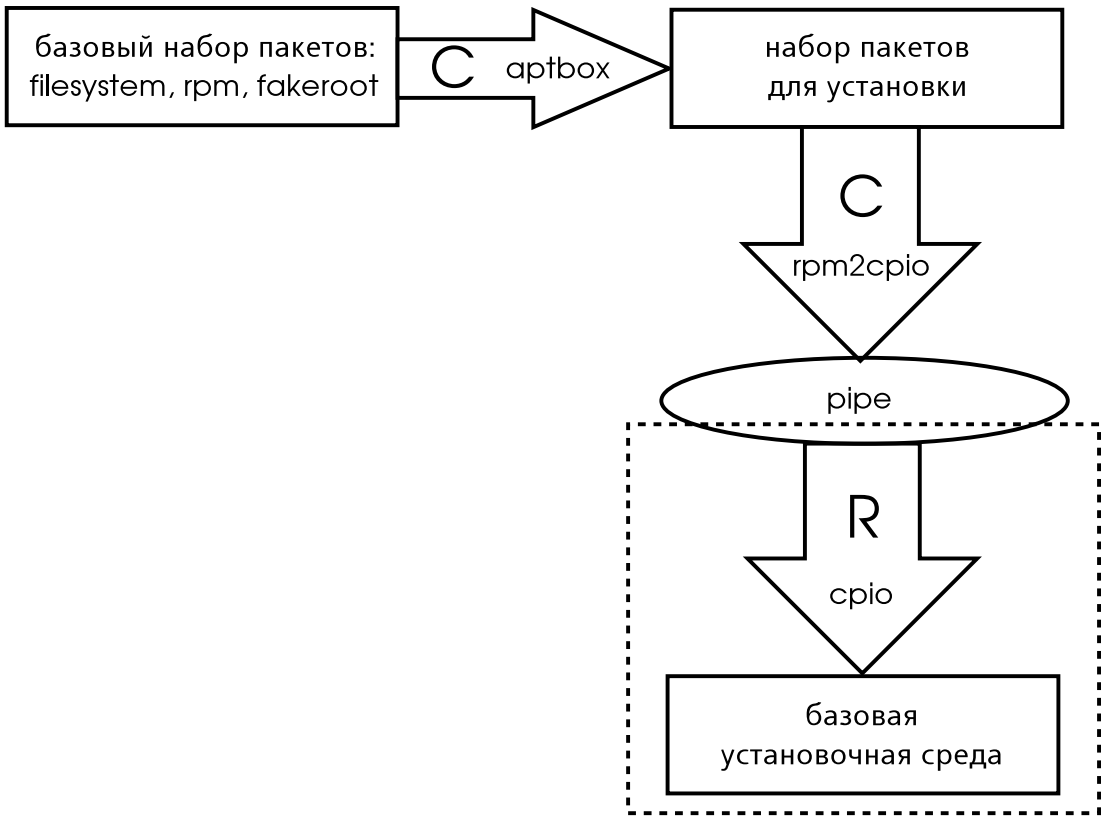
```
-rwxr-xr-x C C chroot/.host/cpio
-rwxr-xr-x C C chroot/.host/find
-rwxr-xr-x C C chroot/.host/sh
```

Фиксированный набор файлов устройств

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

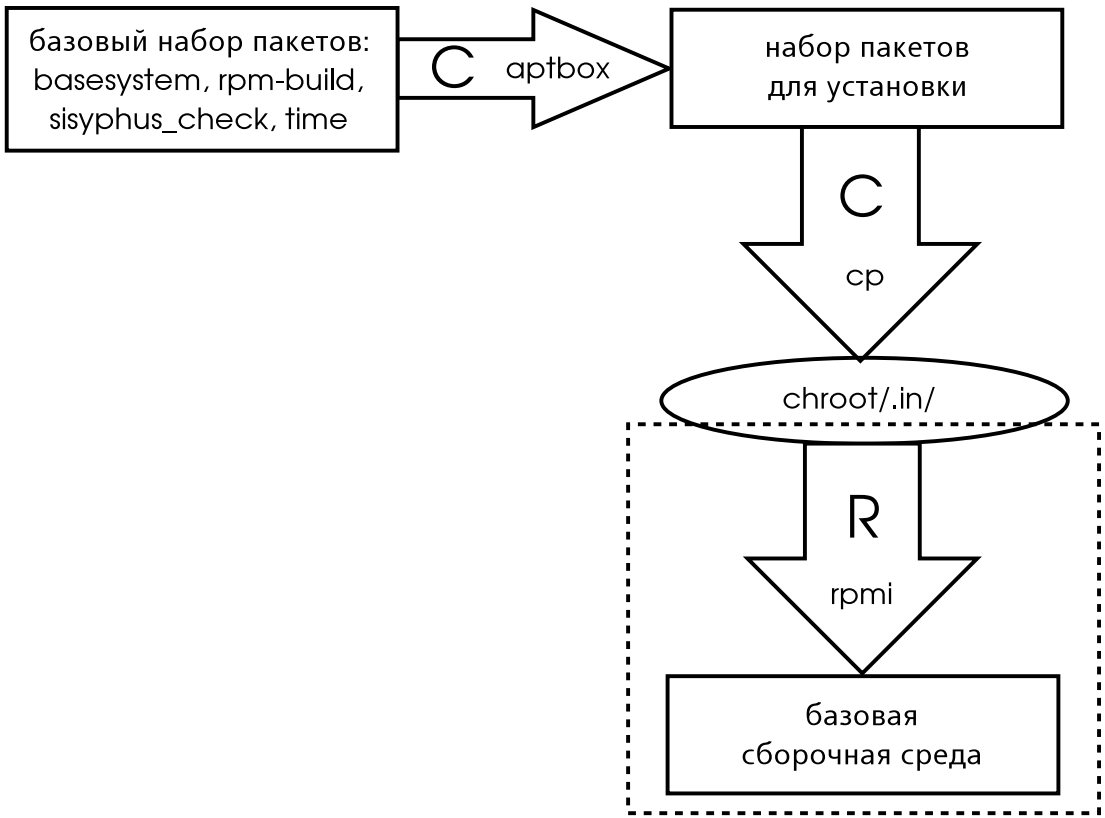
Базовая установочная среда

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

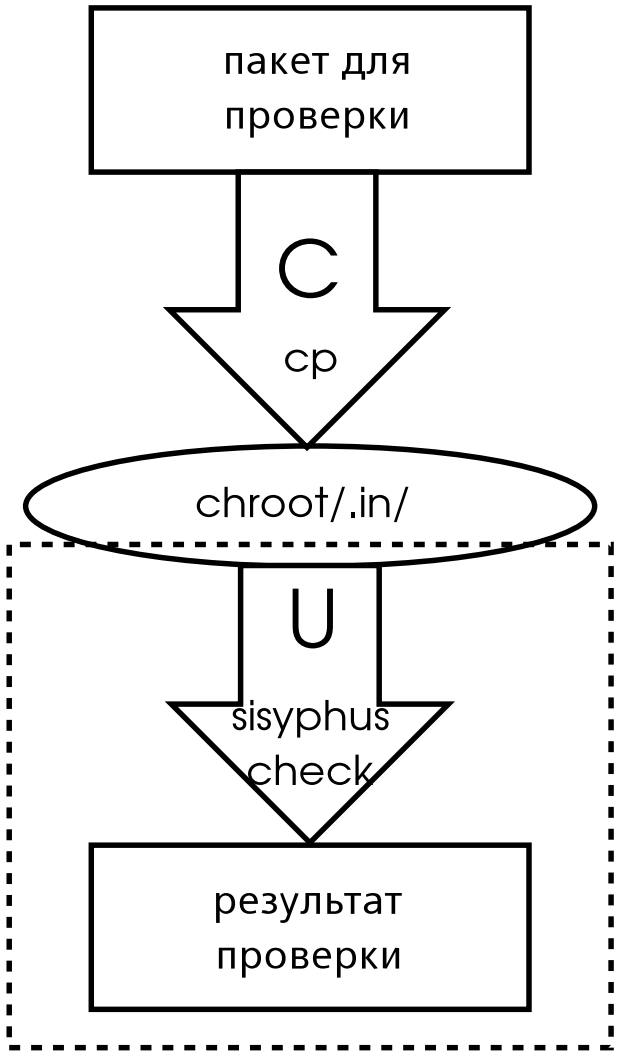


Базовая сборочная среда

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

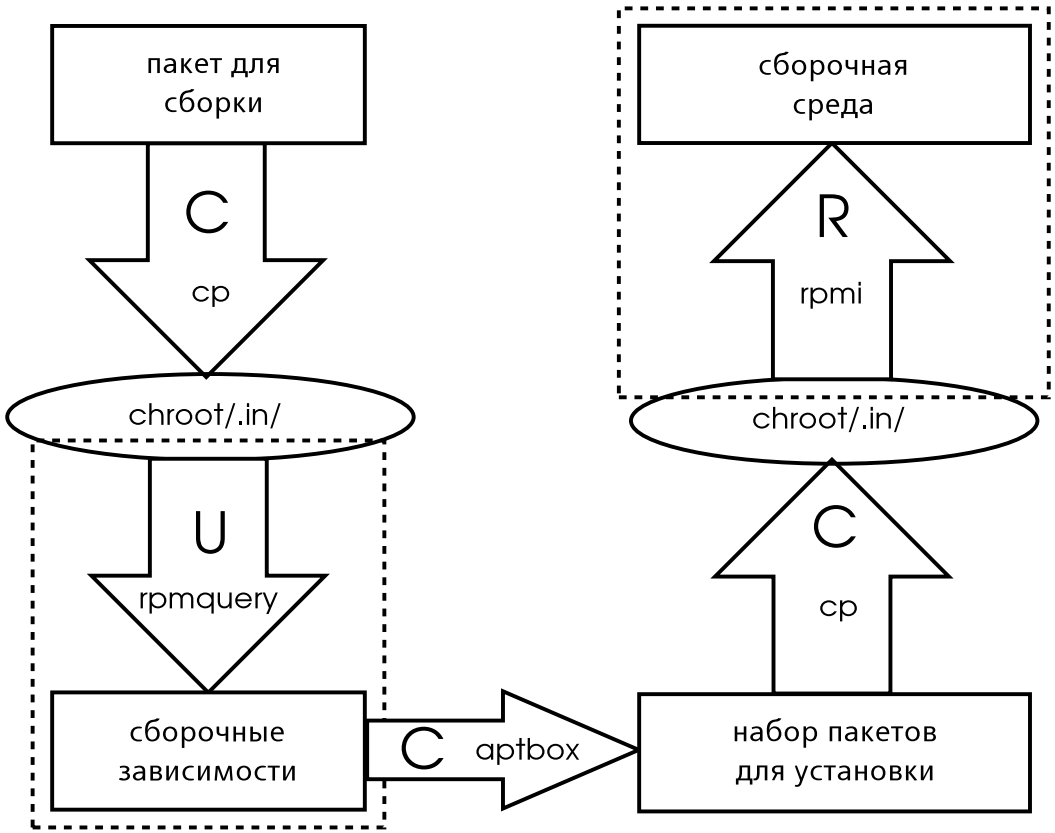


Проверка исходного пакета

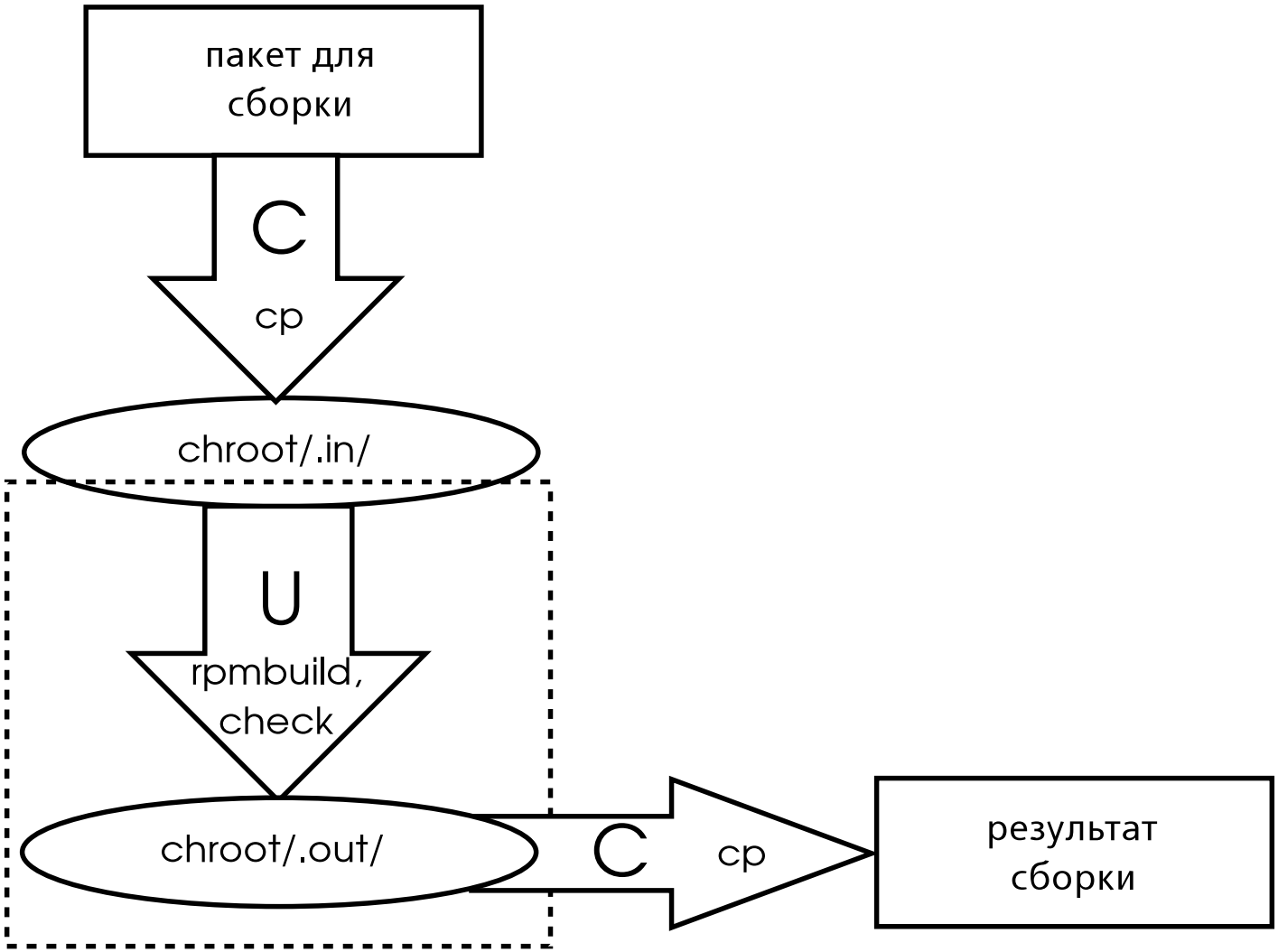


Сборочная среда

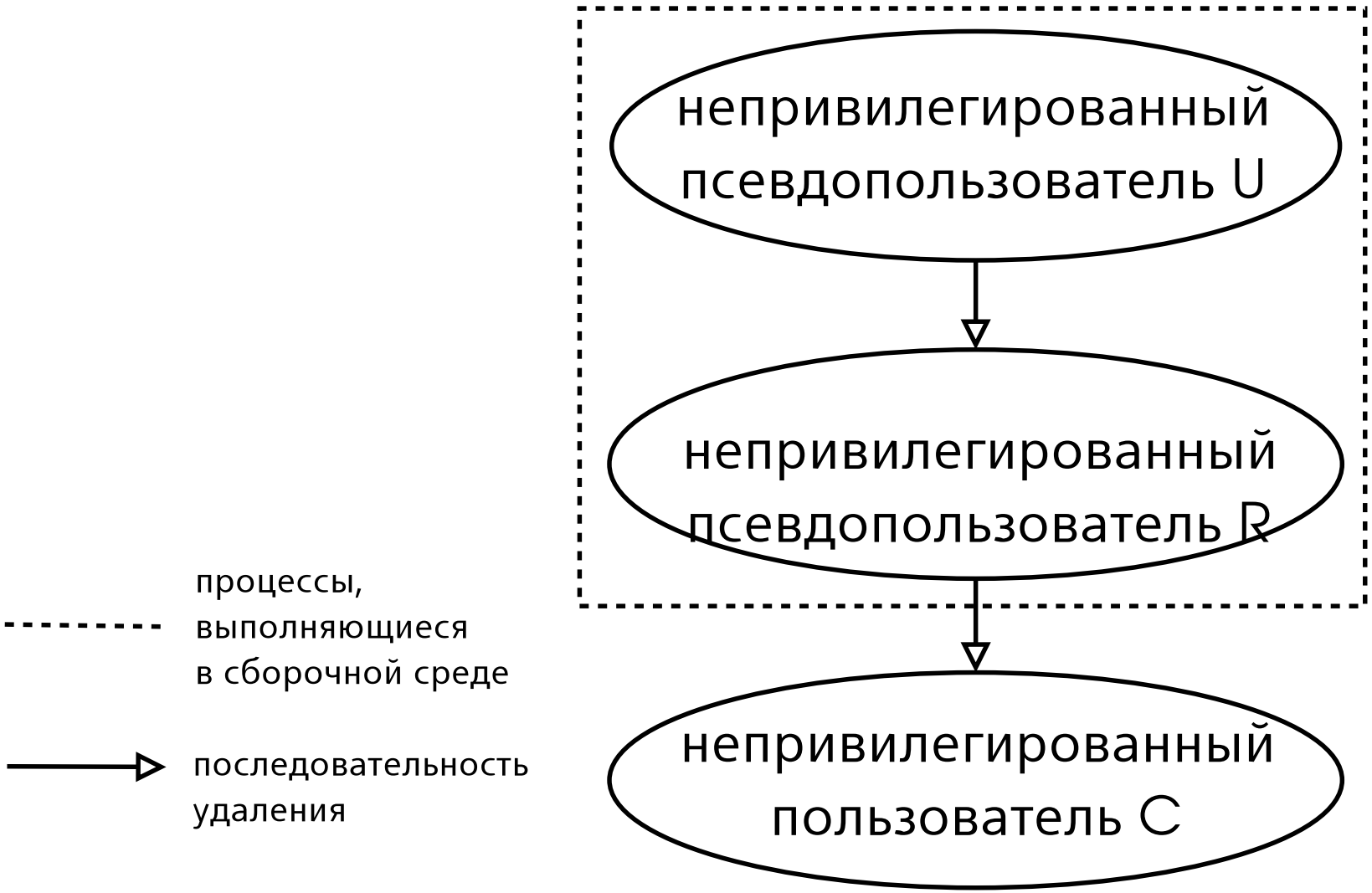
Базовая сборочная среда + набор пакетов, необходимых для сборки данного пакета



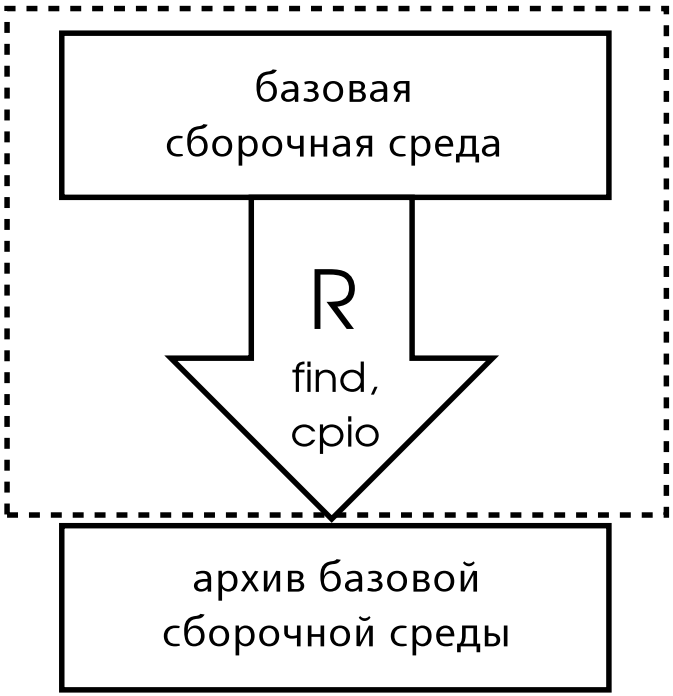
Сборка пакета

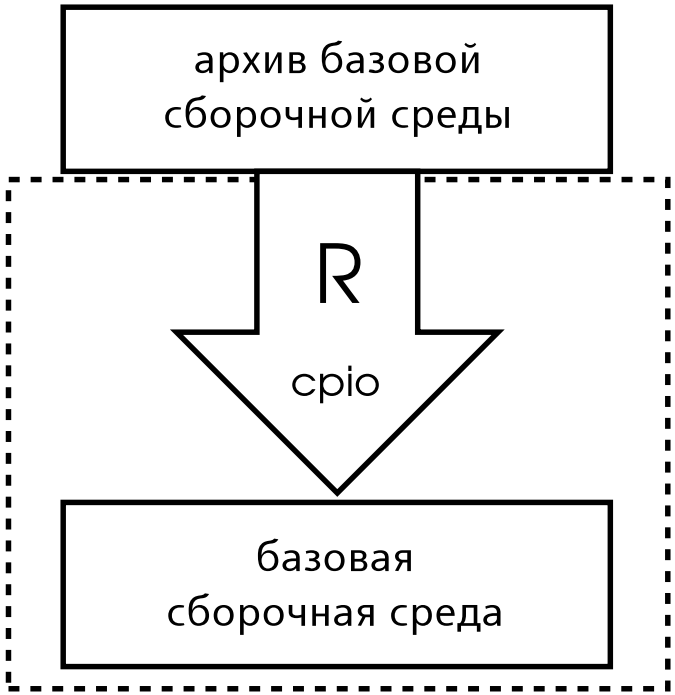


Удаление сборочной среды

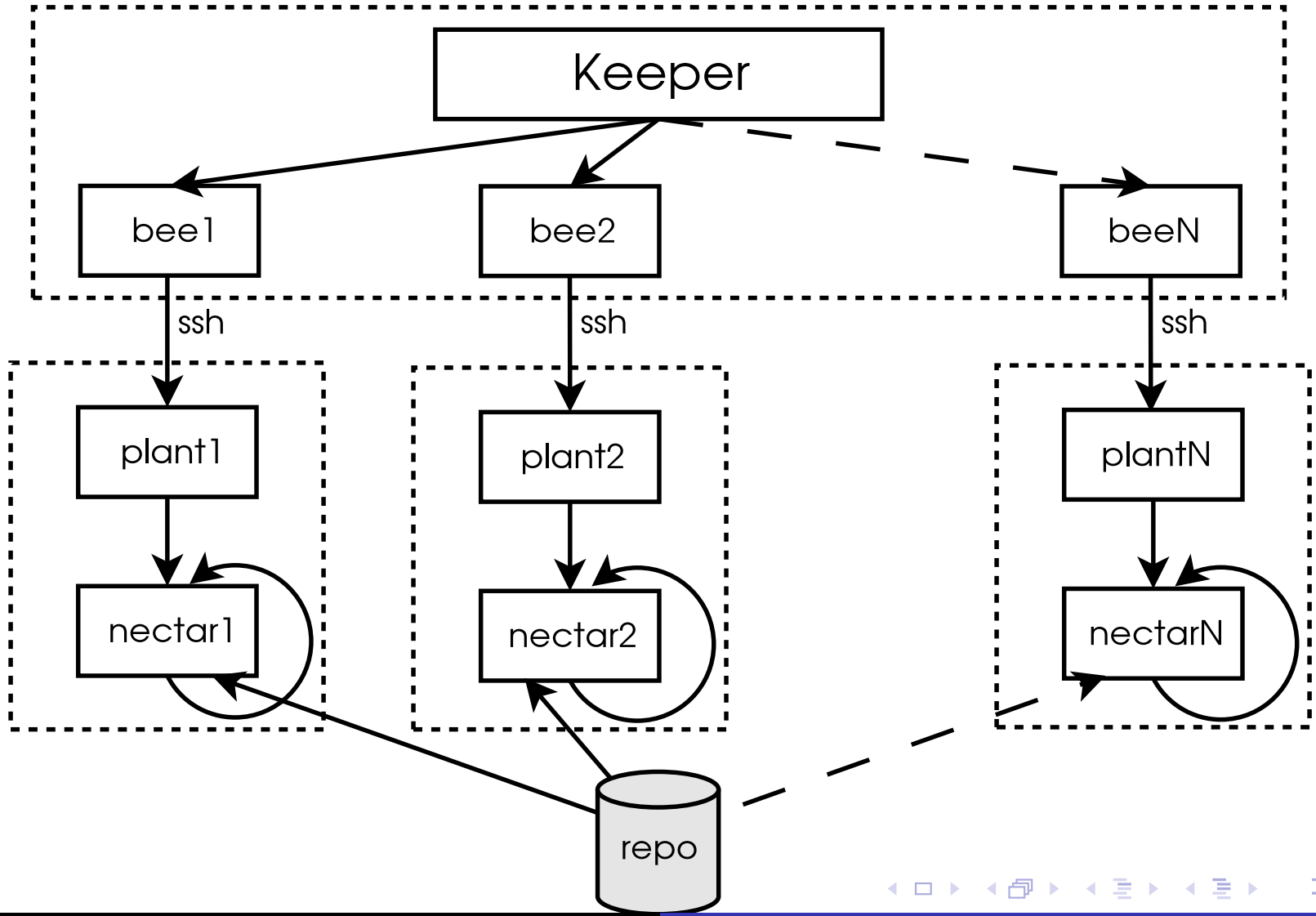


Кэширование базовой сборочной среды





beehive: распределённая сборка



Дополнительная информация

"Домашняя страничка" hasher
`http://git.altlinux.org/people/ldv/packages/hasher.git`

Вопросы?