3 июня 2025 Москва, LOFT HALL#2

БЕКОН '25

Конференция по БЕзопасности
КОНтейнеров и контейнерных сред

Как соответствовать требованиям ФСТЭК, если у вас контейнеры и кластеры

Андрей Слепых

Эксперт департамента РБПО, НТЦ «Фобос-НТ»

О себе

БЕКОН

- Считаю, что современные испытательные лаборатории - это не только «бумажки», а в первую очередь инженеры
- Занимаюсь поиском поверхности атаки в ПО и анализом безопасности контейнеров
- Преподаю в вузах: МГТУ, ОГУ

Немного про нас

БЕКОН

- Испытательная лаборатория ФСТЭК России
- Занимаемся сертификацией ПО, аудитом и внедрением процессов РБПО
- Участвуем в разработке и актуализации Требований, Инф. писем, ГОСТов
- Проводим статический и динамический анализ open-source кода и предлагаем исправления в upstream

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

План

БЕКОН

1. Что есть сейчас?
2. Средство контейнеризации или
   Средство в контейнерном исполнении
3. Инвентаризация
4. Контроль целостности
5. Обеспечение совместимости
6. Минимизация привилегий
7. Управление доступом

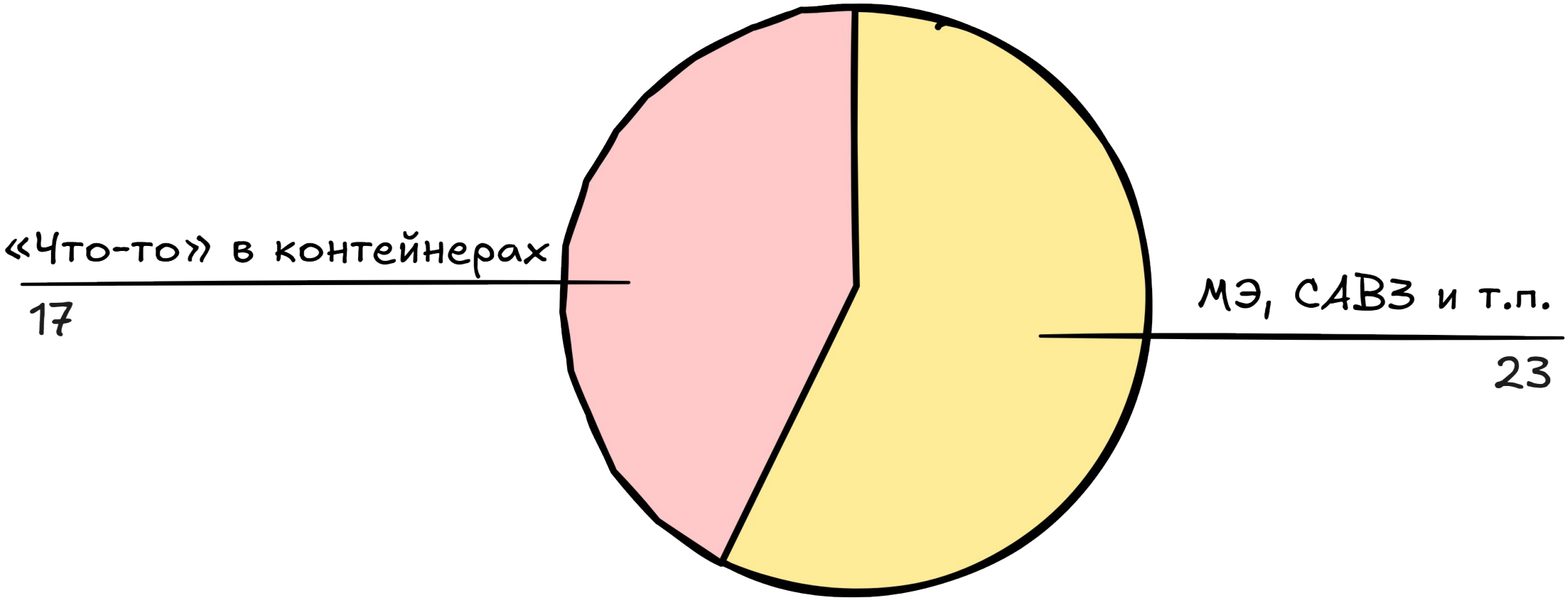
БЕКОН

Что есть сейчас?

Что есть сейчас?

БЕКОН

Что приходит к нам на сертификацию?

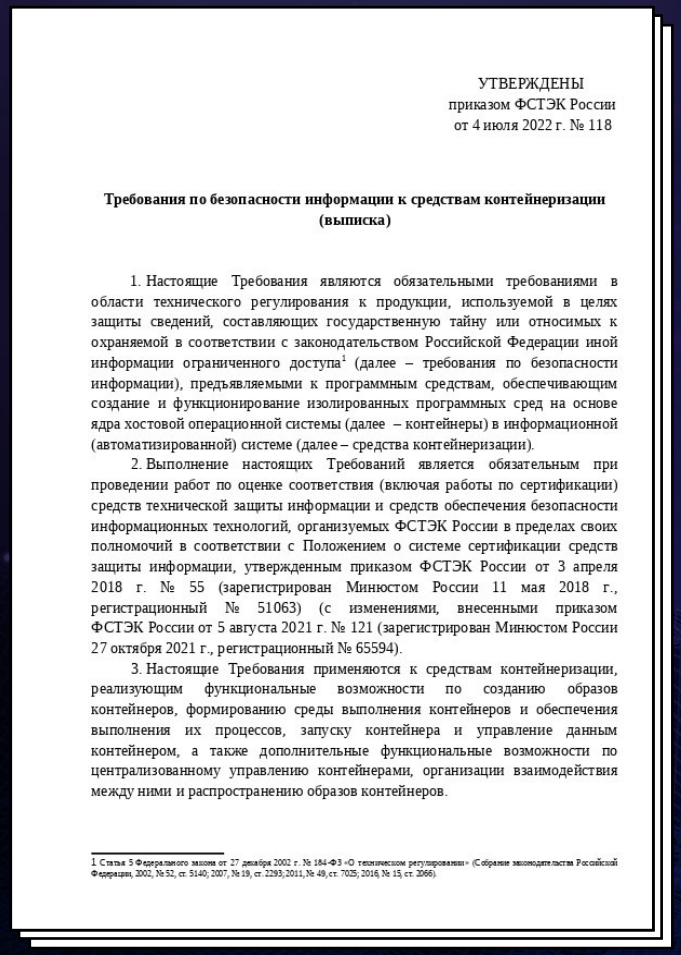


Всего проектов за первое полугодие 2025 г. - 40

Что есть сейчас?

БЕКОН

Требования по безопасности информации к средствам контейнеризации («Приказ № 118»)



УТВЕРЖДЕНЫ
приказом ФСТЭК России
от 4 июля 2022 г. № 118

Требования по безопасности информации к средствам контейнеризации (выписка)

1. Настоящие Требования являются обязательными требованиями в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа[1] (далее – требования по безопасности информации), предъявляемыми к программным средствам, обеспечивающим создание и функционирование изолированных программных сред на основе ядра хостовой операционной системы (далее – контейнеры) в информационной (автоматизированной) системе (далее – средства контейнеризации).

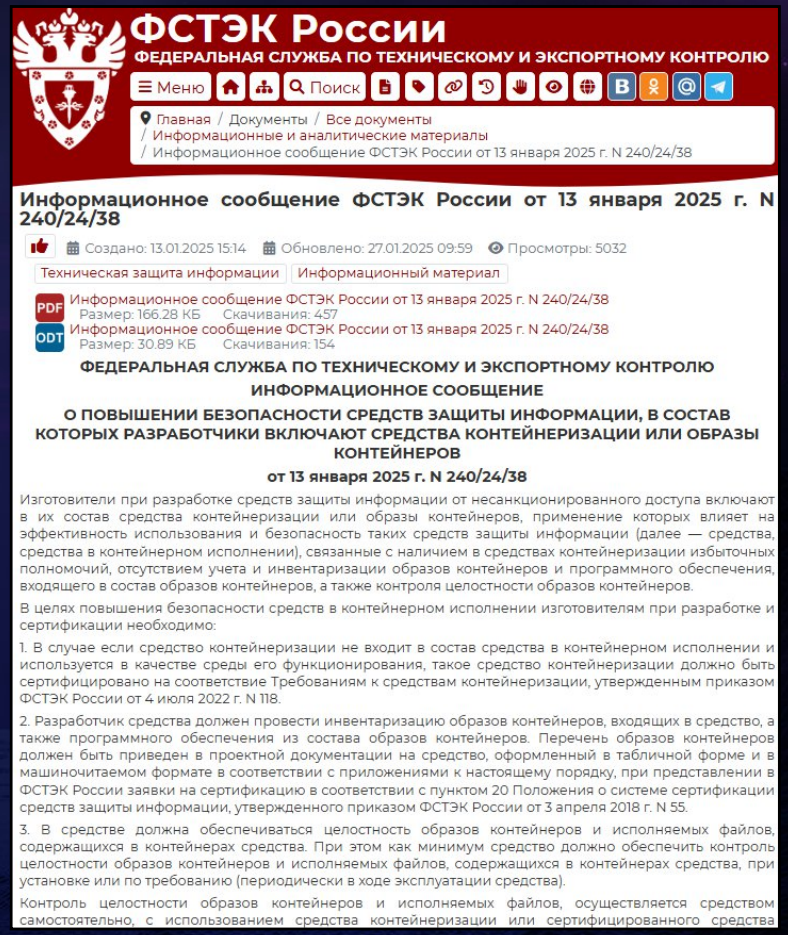
2. Выполнение настоящих Требований является обязательным при проведении работ по оценке соответствия (включая работы по сертификации) средств технической защиты информации и средств обеспечения безопасности информационных технологий, организуемых ФСТЭК России в пределах своих полномочий в соответствии с Положением о системе сертификации средств защиты информации, утвержденным приказом ФСТЭК России от 3 апреля 2018 г. № 55 (зарегистрирован Минюстом России 11 мая 2018 г., регистрационный № 51063) (с изменениями, внесенными приказом ФСТЭК России от 5 августа 2021 г. № 121 (зарегистрирован Минюстом России 27 октября 2021 г., регистрационный № 65594).

3. Настоящие Требования применяются к средствам контейнеризации, реализующим функциональные возможности по созданию образов контейнеров, формированию среды выполнения контейнеров и обеспечения выполнения их процессов, запуску контейнера и управление данным контейнером, а также дополнительные функциональные возможности по централизованному управлению контейнерами, организации взаимодействия между ними и распространению образов контейнеров.

1 Статья 5 Федерального закона от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» (Собрание законодательства Российской Федерации, 2002, № 52, ст. 5140; 2007, № 19, ст. 2293; 2011, № 49, ст. 7025; 2016, № 15, ст. 2066).

[Ссылка на Требования]

Информационное сообщение ФСТЭК России от 13 января 2025 г. N 240/24/38 О повышении безопасности средств защиты информации, в состав которых разработчики включают средства контейнеризации или образы контейнеров



ФСТЭК России
ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

Меню | Поиск

Главная / Документы / Все документы / Информационные и аналитические материалы / Информационное сообщение ФСТЭК России от 13 января 2025 г. N 240/24/38

Информационное сообщение ФСТЭК России от 13 января 2025 г. N 240/24/38

Создано: 13.01.2025 15:14 Обновлено: 27.01.2025 09:59 Просмотры: 5032

Техническая защита информации | Информационный материал

PDF Информационное сообщение ФСТЭК России от 13 января 2025 г. N 240/24/38
Размер: 166.28 КБ Скачивания: 457

ODT Информационное сообщение ФСТЭК России от 13 января 2025 г. N 240/24/38
Размер: 30.89 КБ Скачивания: 154

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ИНФОРМАЦИОННОЕ СООБЩЕНИЕ

О ПОВЫШЕНИИ БЕЗОПАСНОСТИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ, В СОСТАВ КОТОРЫХ РАЗРАБОТЧИКИ ВКЛЮЧАЮТ СРЕДСТВА КОНТЕЙНЕРИЗАЦИИ ИЛИ ОБРАЗЫ КОНТЕЙНЕРОВ

от 13 января 2025 г. N 240/24/38

Изготовители при разработке средств защиты информации от несанкционированного доступа включают в их состав средства контейнеризации или образы контейнеров, применение которых влияет на эффективность использования и безопасность таких средств защиты информации (далее — средства, средства в контейнерном исполнении), связанные с наличием в средствах контейнеризации избыточных полномочий, отсутствием учета и инвентаризации образов контейнеров и программного обеспечения, входящего в состав образов контейнеров, а также контроля целостности образов контейнеров.

В целях повышения безопасности средств в контейнерном исполнении изготовителям при разработке и сертификации необходимо:

1. В случае если средство контейнеризации не входит в состав средства в контейнерном исполнении и используется в качестве среды его функционирования, такое средство контейнеризации должно быть сертифицировано на соответствие Требованиям к средствам контейнеризации, утвержденным приказом ФСТЭК России от 4 июля 2022 г. N 118.

2. Разработчик средства должен провести инвентаризацию образов контейнеров, входящих в средство, а также программного обеспечения из состава образов контейнеров. Перечень образов контейнеров должен быть приведен в проектной документации на средство, оформленный в табличной форме и в машиночитаемом формате в соответствии с приложениями к настоящему порядку, при представлении в ФСТЭК России заявки на сертификацию в соответствии с пунктом 20 Положения о системе сертификации средств защиты информации, утвержденного приказом ФСТЭК России от 3 апреля 2018 г. N 55.

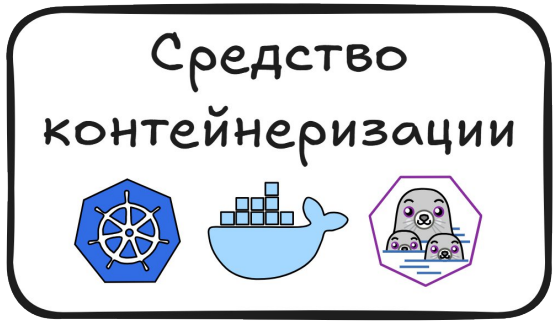
3. В средстве должна обеспечиваться целостность образов контейнеров и исполняемых файлов, содержащихся в контейнерах средства. При этом как минимум средство должно обеспечить контроль целостности образов контейнеров и исполняемых файлов, содержащихся в контейнерах средства, при установке или по требованию (периодически в ходе эксплуатации средства).

Контроль целостности образов контейнеров и исполняемых файлов, осуществляется средством самостоятельно, с использованием средства контейнеризации или сертифицированного средства

[Ссылка на ИС ФСТЭК России № 240/24/38]

Глоссарий (в контексте ИС ФСТЭК России 240/24/38)

БЕКОН

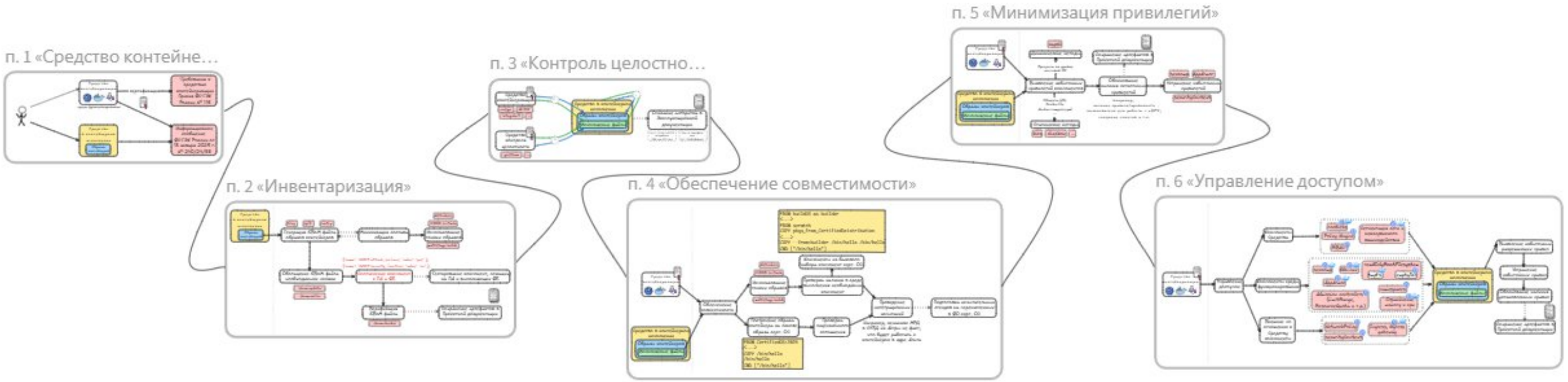


RUNTIME

ВАШИ ОБРАЗЫ И ПО

Карта по ИС ФСТЭК России 240/24/38

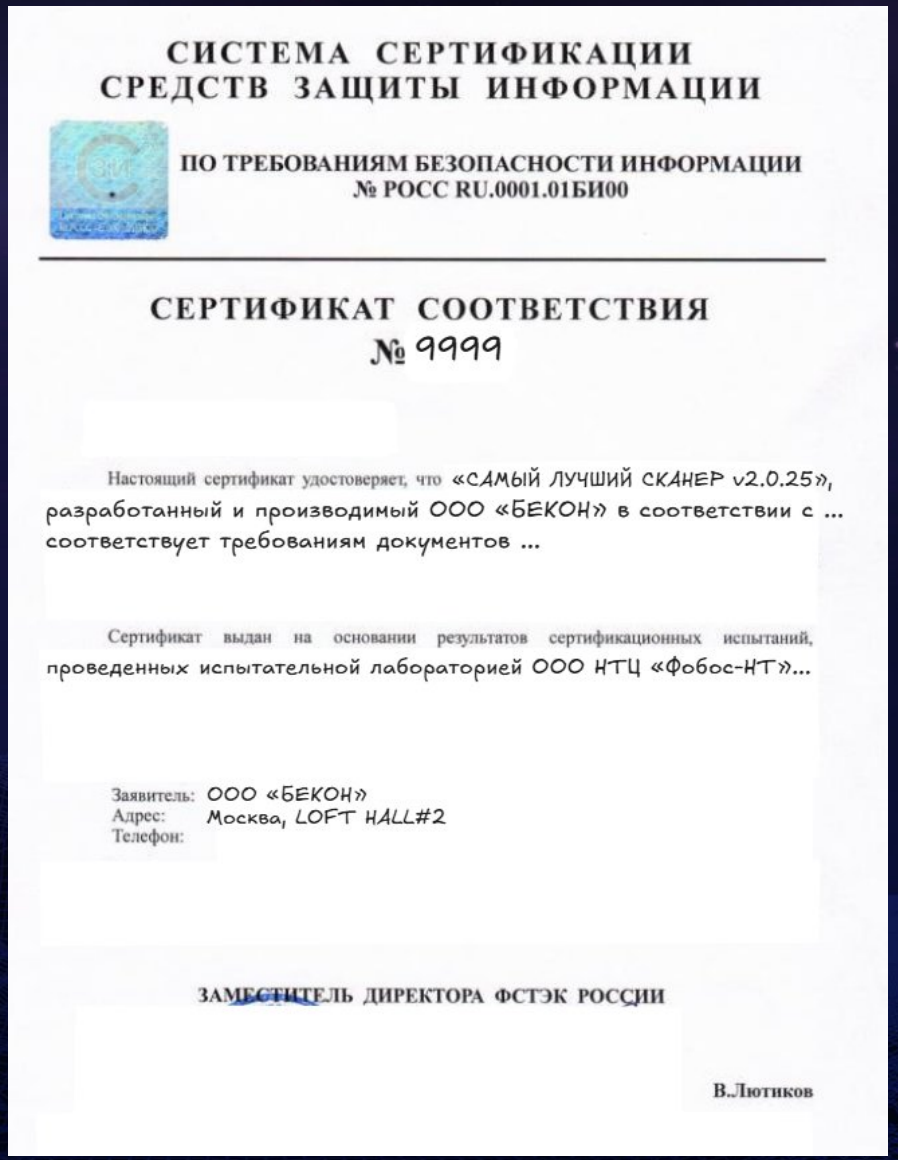
БЕКОН



Ссылка на Карту

Что вы хотите? Сертификат!

БЕКОН



СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 9999

Настоящий сертификат удостоверяет, что «САМЫЙ ЛУЧШИЙ СКАНЕР v2.0.25», разработанный и производимый ООО «БЕКОН» в соответствии с ... соответствует требованиям документов ...

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ООО НТЦ «Фобос-НТ»...

Заявитель: ООО «БЕКОН»
Адрес: Москва, LOFT HALL#2
Телефон:

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

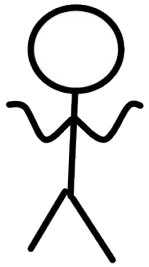
БЕКОН

Средство контейнеризации
или
Средство в контейнерном исполнении

«1. В случае если средство контейнеризации не входит в состав средства в контейнерном исполнении и используется в качестве среды его функционирования, такое средство контейнеризации должно быть сертифицировано на соответствие Требованиям к средствам контейнеризации, утвержденным приказом ФСТЭК России от 4 июля 2022 г. N 118.»

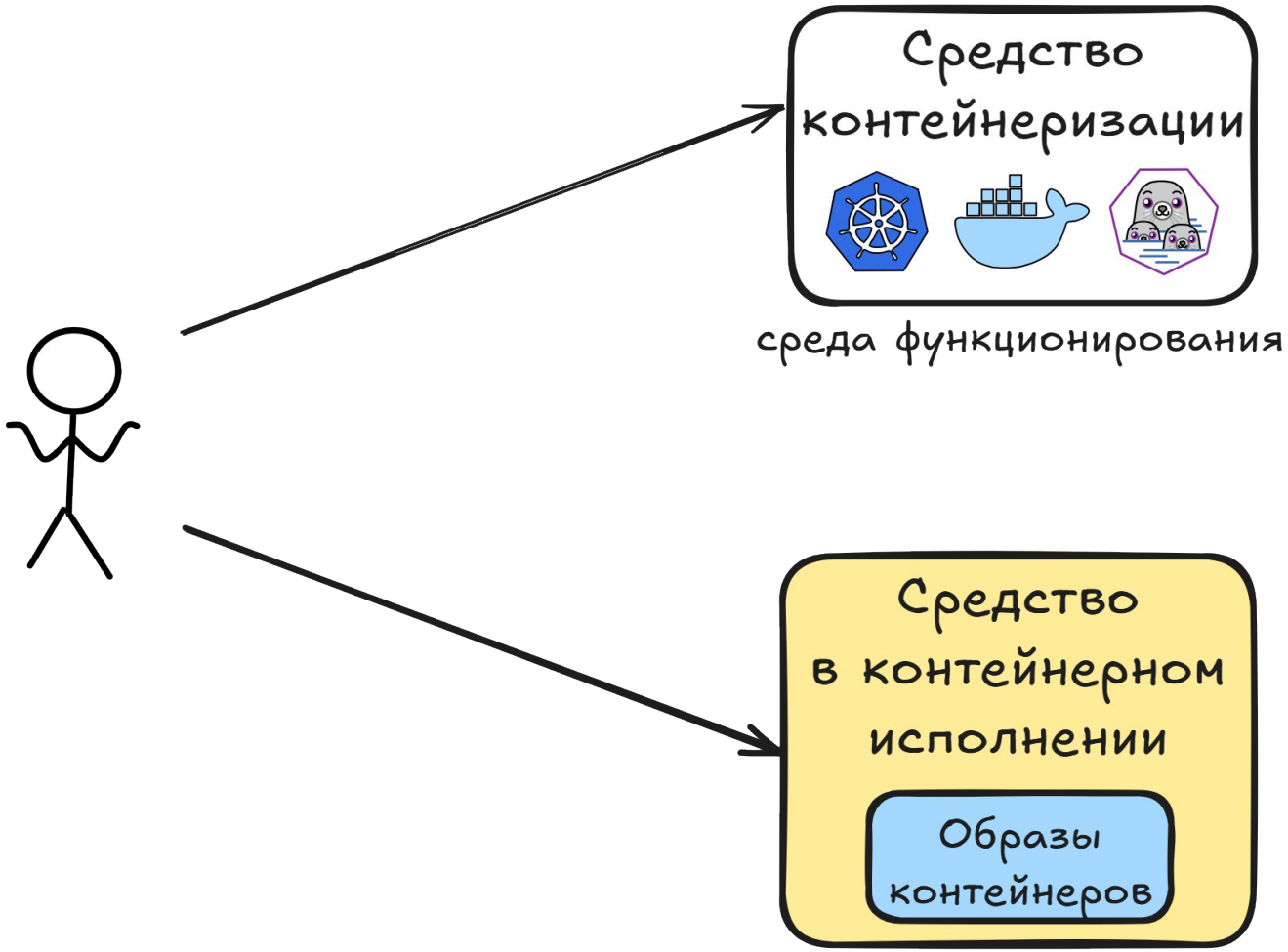
Средство контейнеризации или Средство в контейнерном исполнении?

БЕКОН



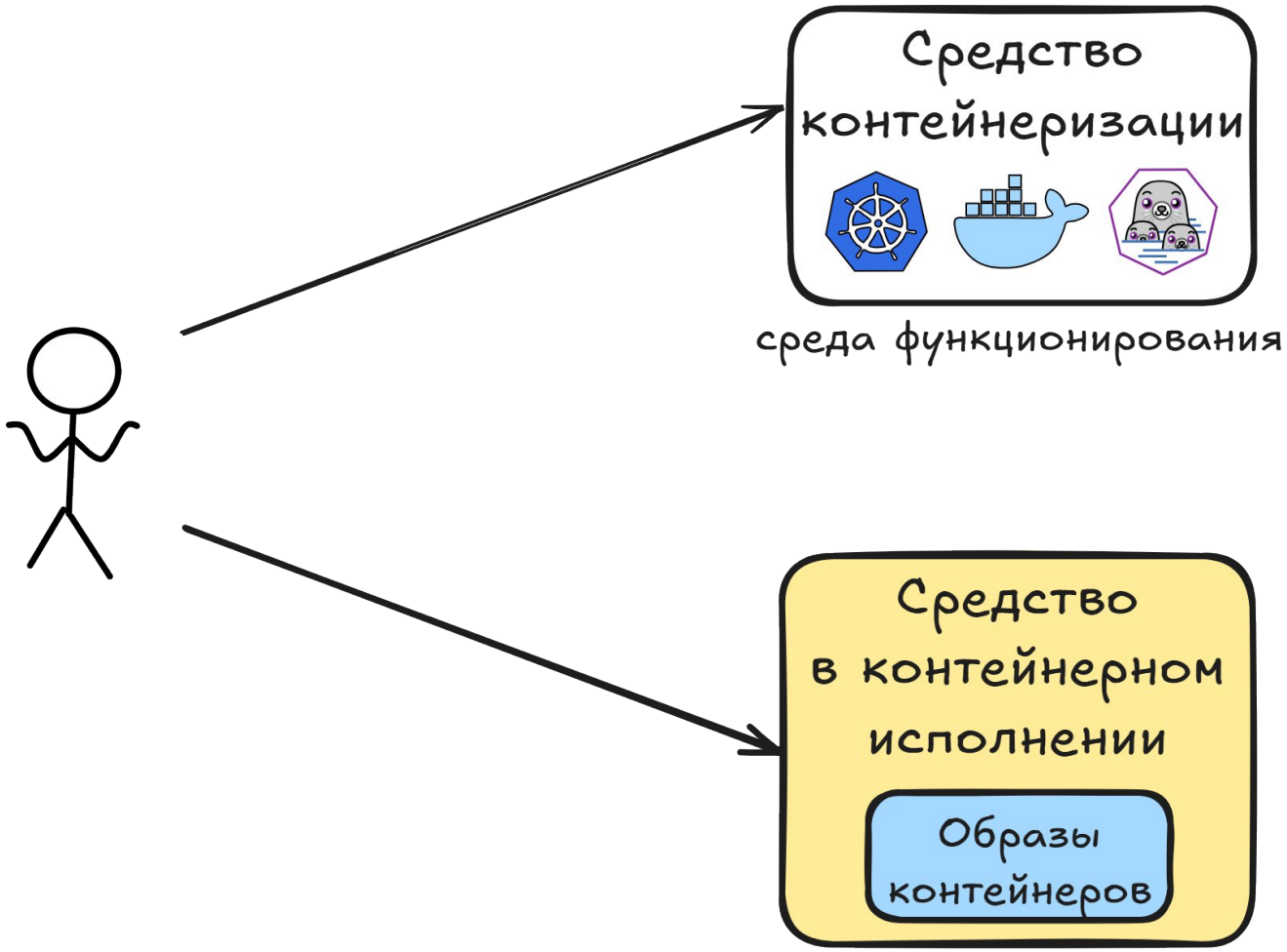
Средство контейнеризации или Средство в контейнерном исполнении?

БЕКОН



Средство контейнеризации или Средство в контейнерном исполнении?

БЕКОН

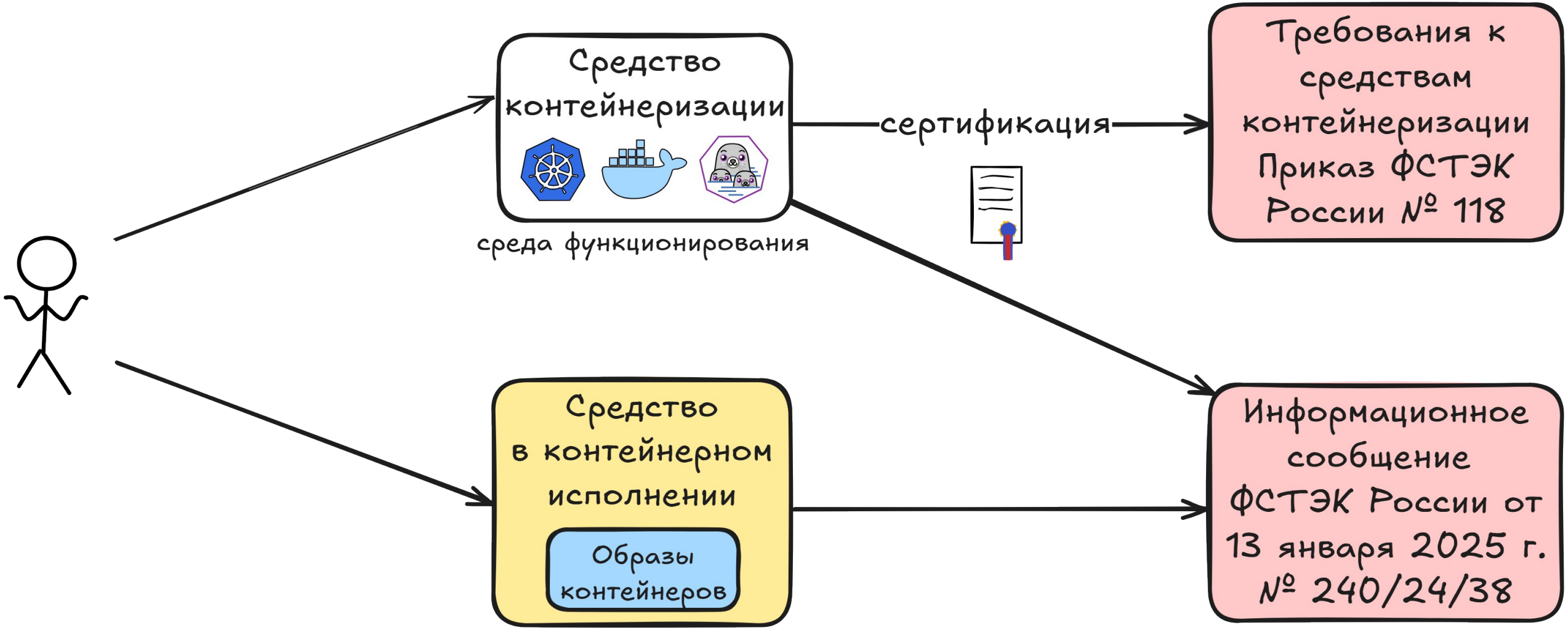


Требования к средствам контейнеризации Приказ ФСТЭК России № 118

Информационное сообщение ФСТЭК России от 13 января 2025 г. № 240/24/38

Средство контейнеризации или Средство в контейнерном исполнении?

БЕКОН



БЕКОН

Инвентаризация

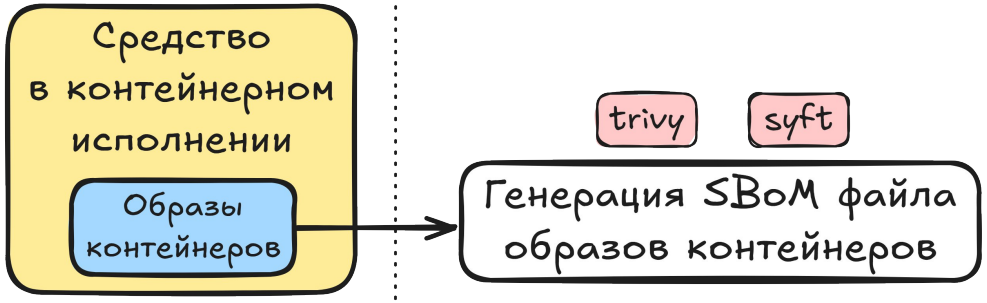
«2. Разработчик средства должен провести инвентаризацию образов контейнеров, входящих в средство, а также ПО из состава контейнеров. Перечень образов должен быть приведен в проектной документации на средство, оформленный в табличной форме и в машиночитаемом формате в соответствии с приложениями к настоящему порядку, при предоставлении в ФСТЭК России заявки на сертификацию <...>»

Инвентаризация

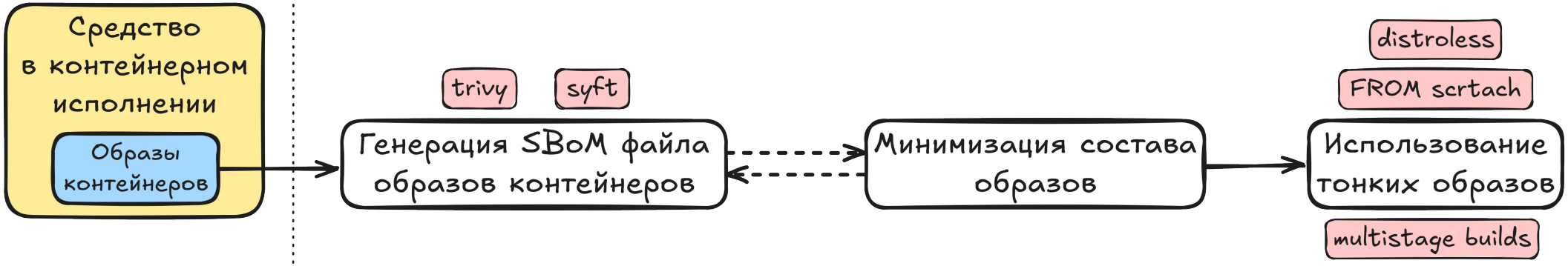
БЕКОН

Инвентаризация

БЕКОН



Инвентаризация



БЕКОН

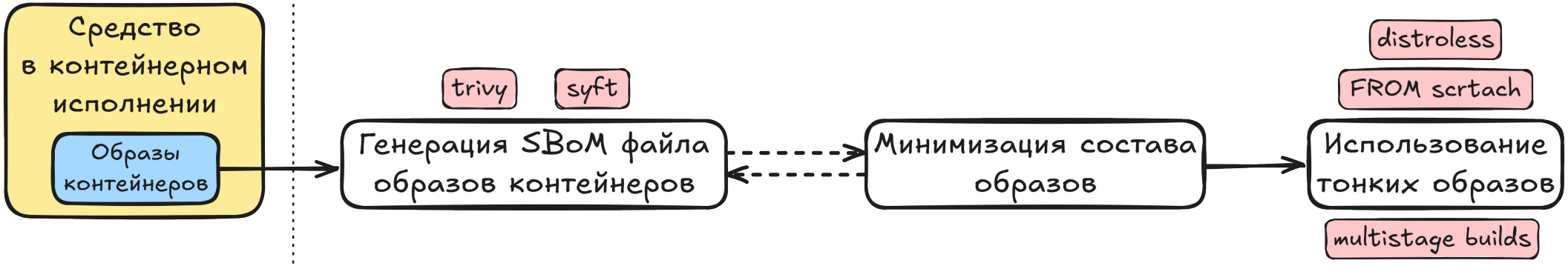
Латаем огрехи в образах приложений до рантайма, во время и после

Анатолий Карпенко
Luntry

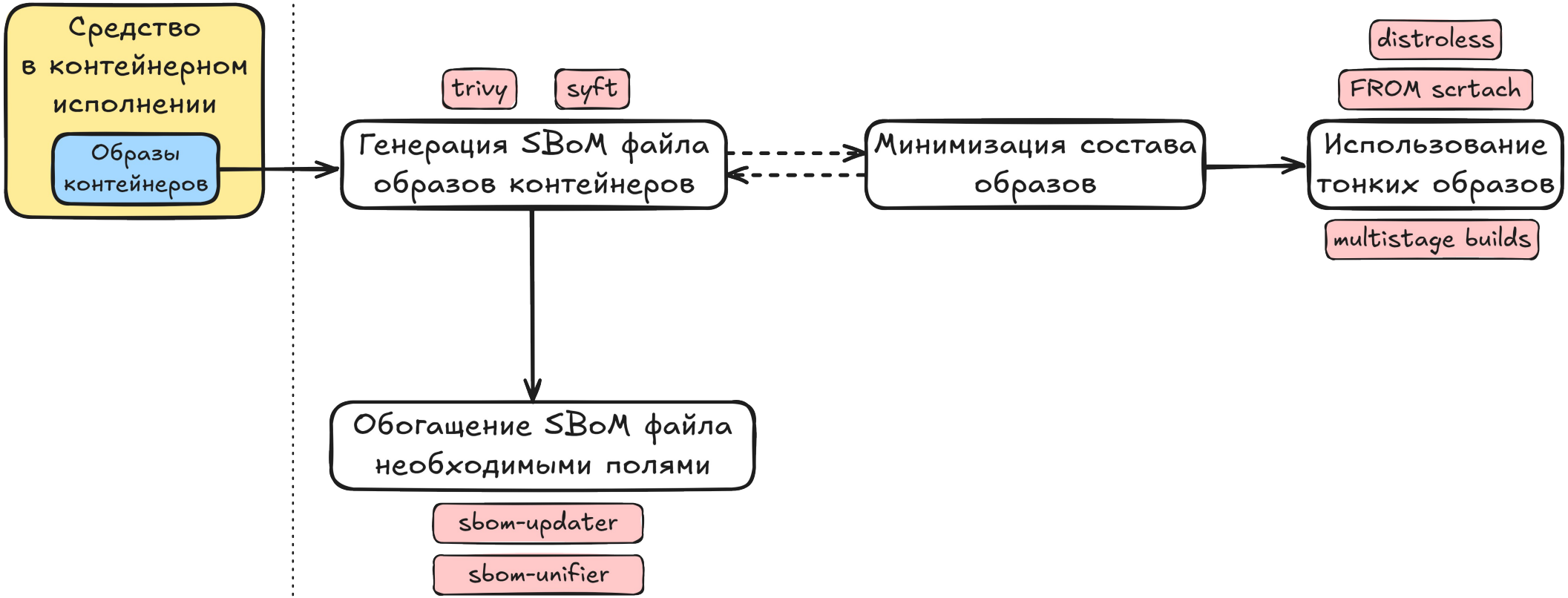
@rusdacent

Ссылка на доклад

Инвентаризация

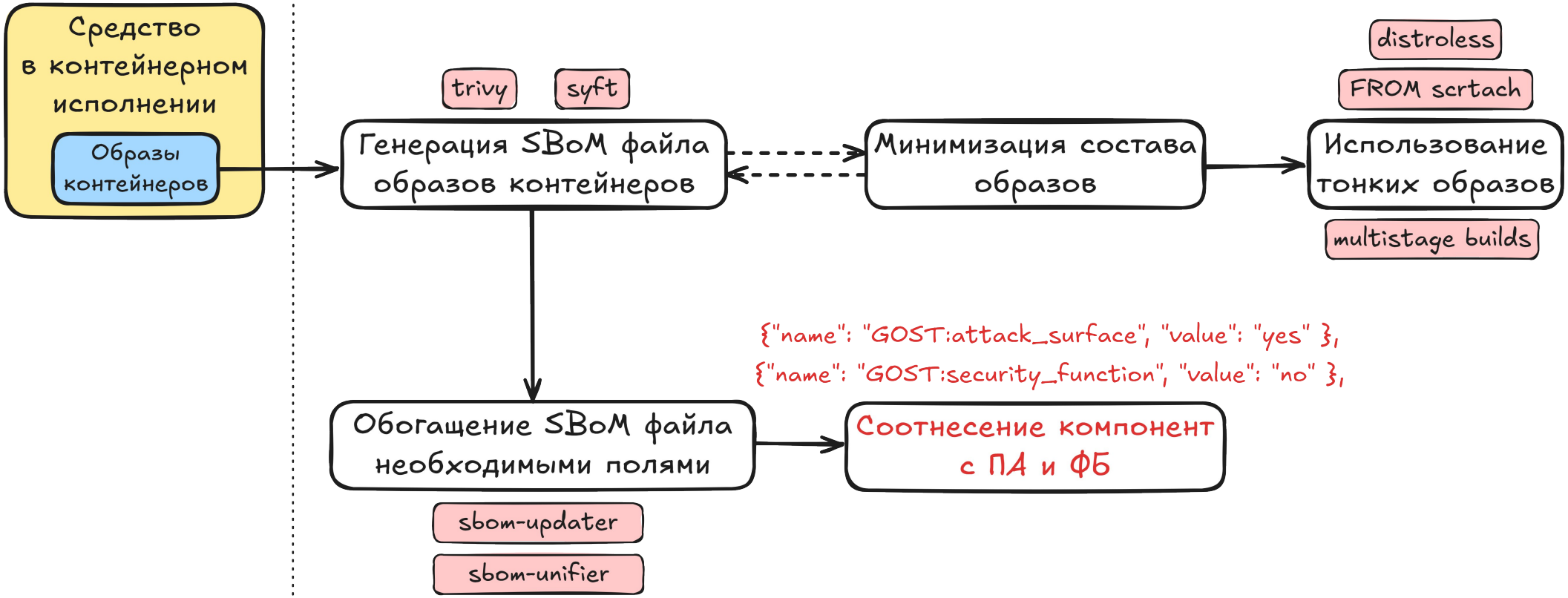


Инвентаризация



Инвентаризация

БЕКОН



Инвентаризация

БЕКОН


```
{
"bomFormat": "CycloneDX",
"specVersion": "1.6",
"version": 1,
"metadata": {
      "component": {
            "type": "application",
            "name": "САМЫЙ ЛУЧШИЙ СКАНЕР",
            "version": "v.2.0.25",
            "manufacturer": {"name": "БЕКОН"}
      }
},
"components": [
```


Образ контейнера "loadbalancer"

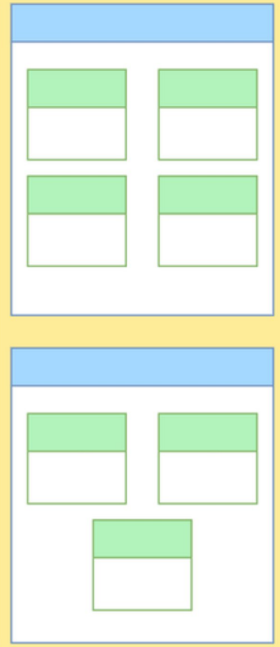

```
"type": "container",
"name": "loadbalancer",
"version": "v.10.2.0",
"properties": [
      {"name": "GOST:attack_surface", "value": "yes" },
      {"name": "GOST:security_function", "value": "yes" },
],
"components": [
```


Пакет "nginx"


```
"type": "application",
"name": "nginx",
"version": "1.24.4",
"properties": [
      {"name": "GOST:attack_surface", "value": "yes" },
      {"name": "GOST:security_function", "value": "no" },
      {"name": "GOST:provided_by", "value": "CertifiedDistr" }
],
```


Пакет "gateway_controller"

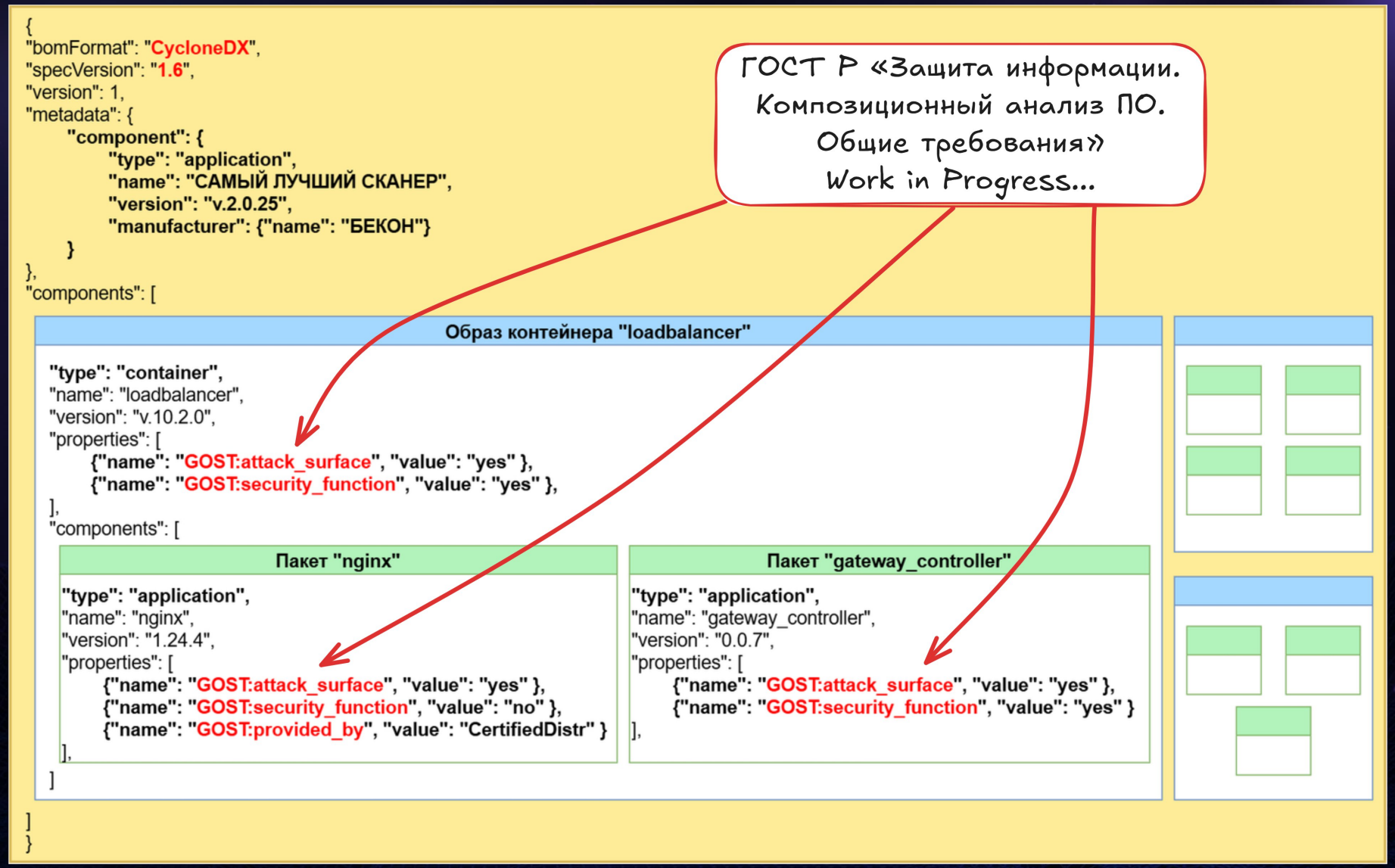

```
"type": "application",
"name": "gateway_controller",
"version": "0.0.7",
"properties": [
      {"name": "GOST:attack_surface", "value": "yes" },
      {"name": "GOST:security_function", "value": "yes" }
],
```

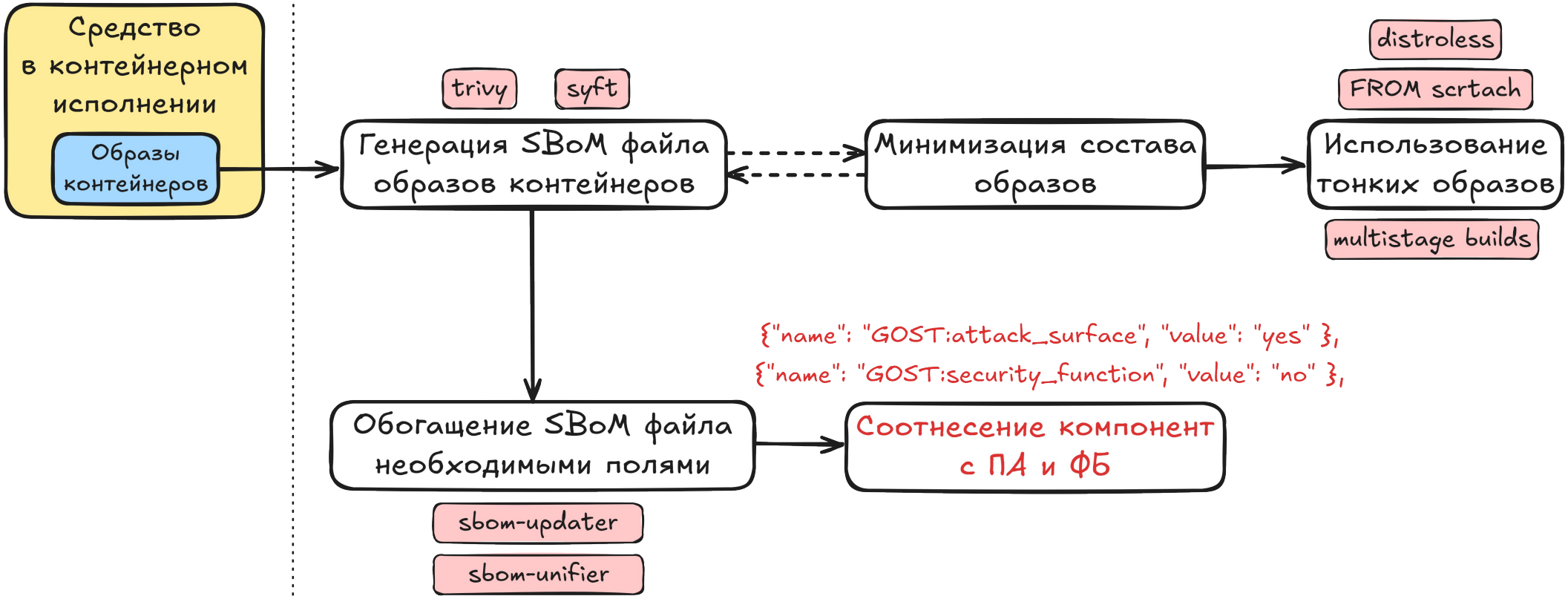

```
]
}
```

Инвентаризация

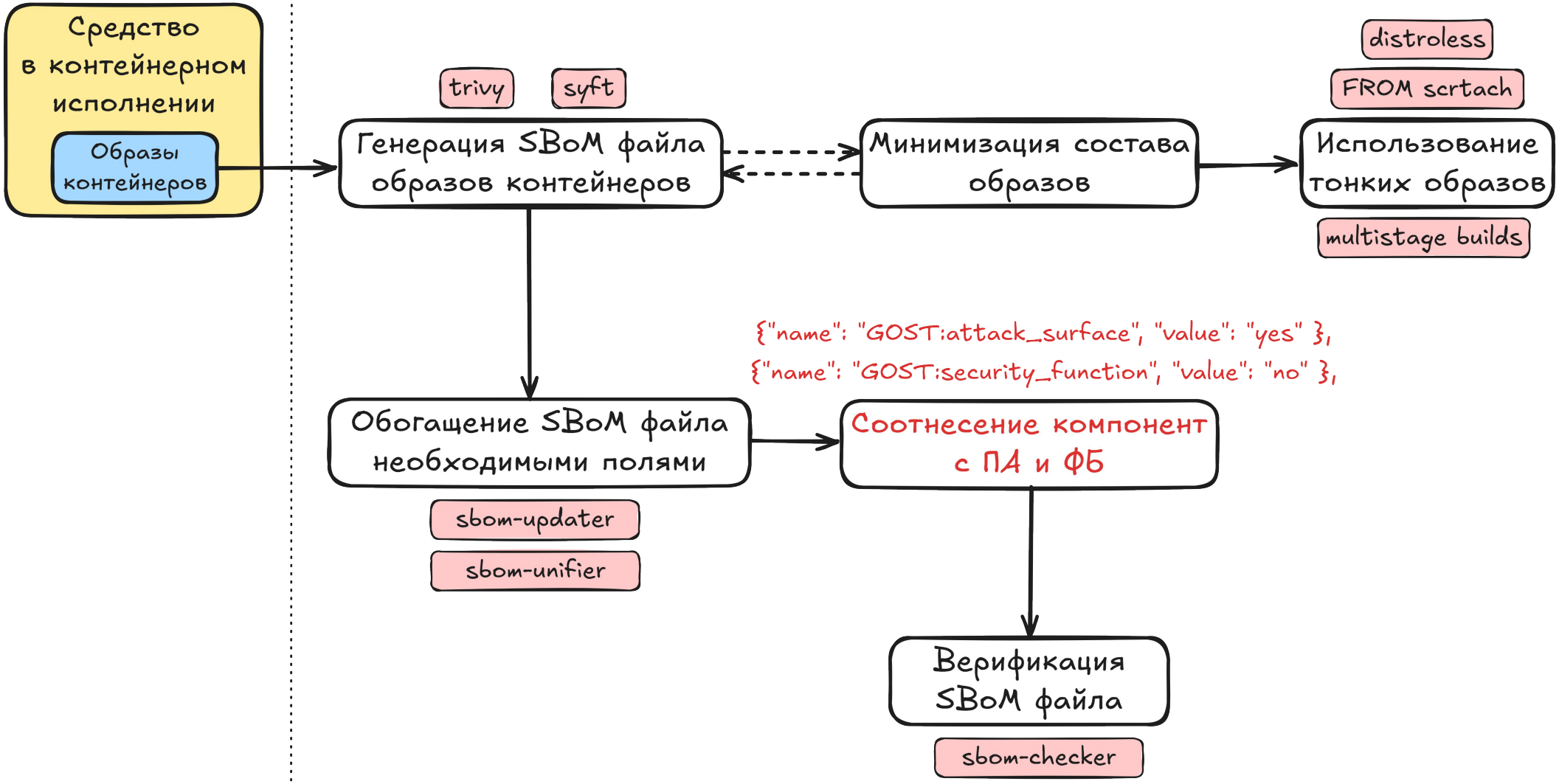
БЕКОН



Инвентаризация



Инвентаризация



Инвентаризация

БЕКОН

> git clone https://gitlab.community.ispras.ru/sdl-tools/sbom-checker.git

Центр исследования безопасности системного ПО ФСТЭК России на базе ИСП РАН

sbom-updater

```
prompt> python sbom-updater.py --help

usage: sbom-updater.py [-h] [--props] [--app-name APP_NAME]
                       [--app-version APP_VERSION]
                       [--manufacturer MANUFACTURER] [--ref] [--fix-all]
                       [--update OLD_SBOM] [-v]
                       input output

изменение sbom-файлов

positional arguments:
  input

  output
```

sbom-unifier

```
prompt> python sbom-unifier.py --help

usage: sbom-unifier.py [-h] --app-name APP_NAME --app-version APP_VERSION
                       --manufacturer MANUFACTURER
                       input [input ...] output

объединение sbom-файлов

positional arguments:
  input

  output
```

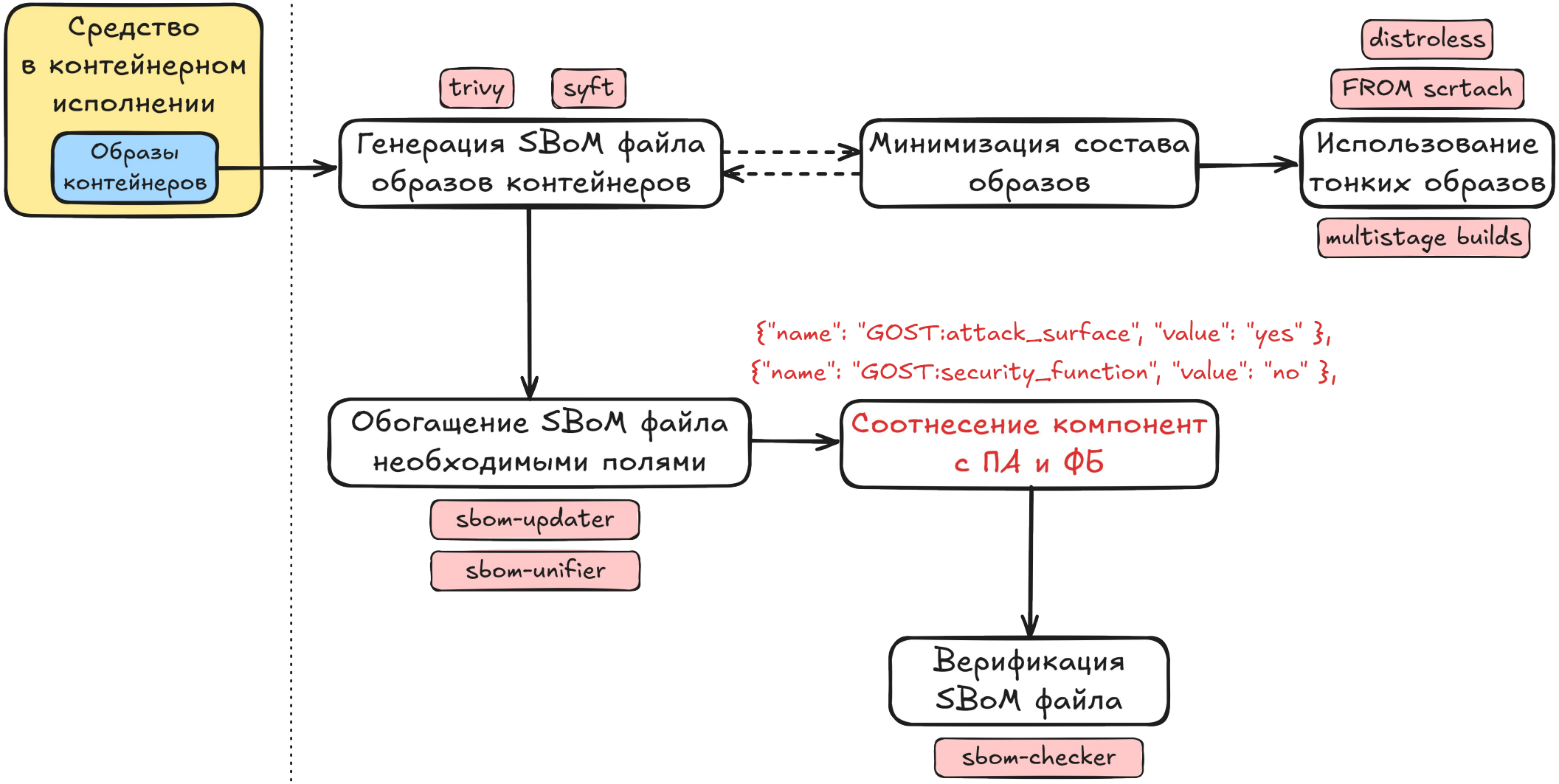
sbom-checker

```
prompt> python sbom-checker.py --help

usage: sbom-checker.py [-h] [-e ERRORS] [--check-vcs] filename

проверка sbom-файлов

positional arguments:
  filename              входной файл в формате CycloneDX JSON для проверки
```

[Ссылка на репозиторий]

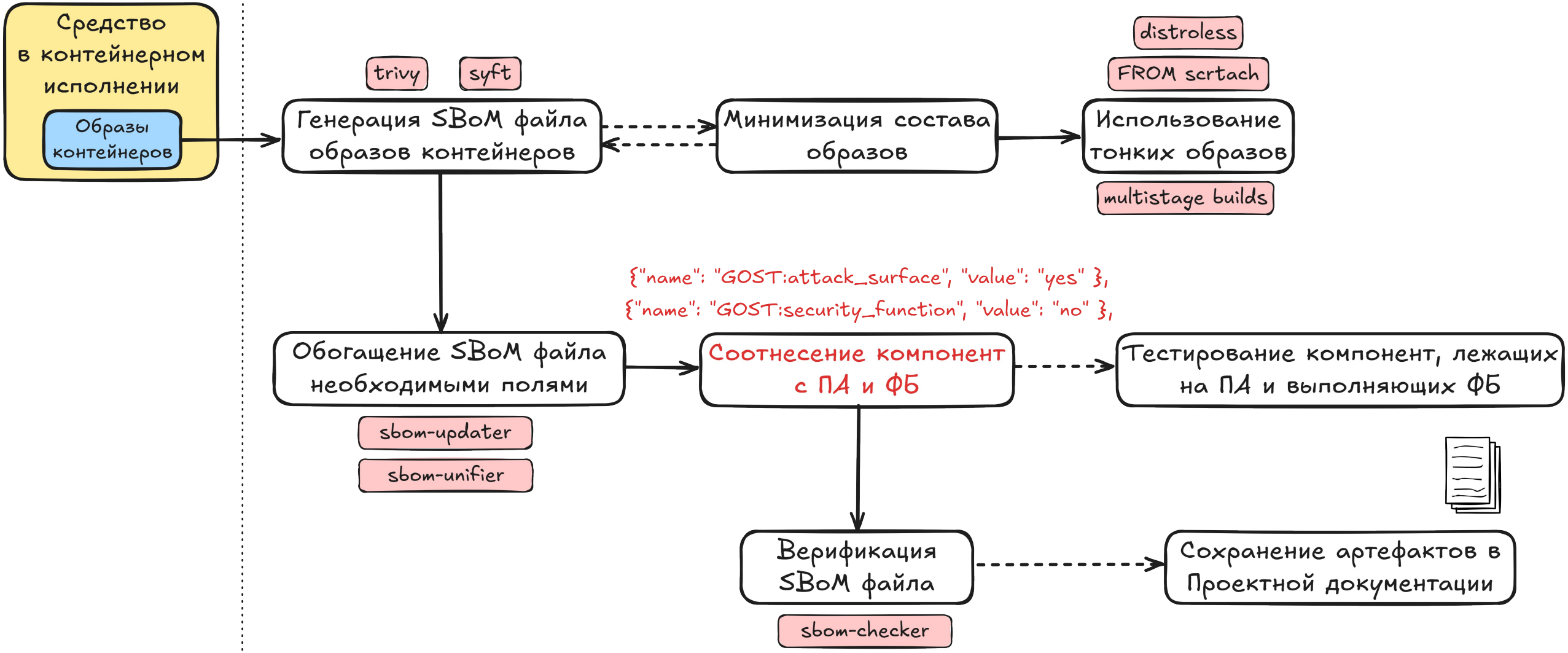
Инвентаризация

БЕКОН



Инвентаризация

БЕКОН



БЕКОН

Контроль целостности

«3. В средстве должна обеспечиваться целостность образов контейнеров и исполняемых файлов, содержащихся в контейнерах средства. При этом как минимум средство должно обеспечить контроль целостности образов контейнеров и исполняемых файлов, содержащихся в контейнерах средства, при установке или по требованию (периодически в ходе эксплуатации средства).

Контроль целостности образов контейнеров и исполняемых файлов, осуществляется средством самостоятельно, с использованием средства контейнеризации или сертифицированного средства контроля целостности. Методика проверки контроля целостности должна быть приведена в эксплуатационной документации средства.»

Контроль целостности

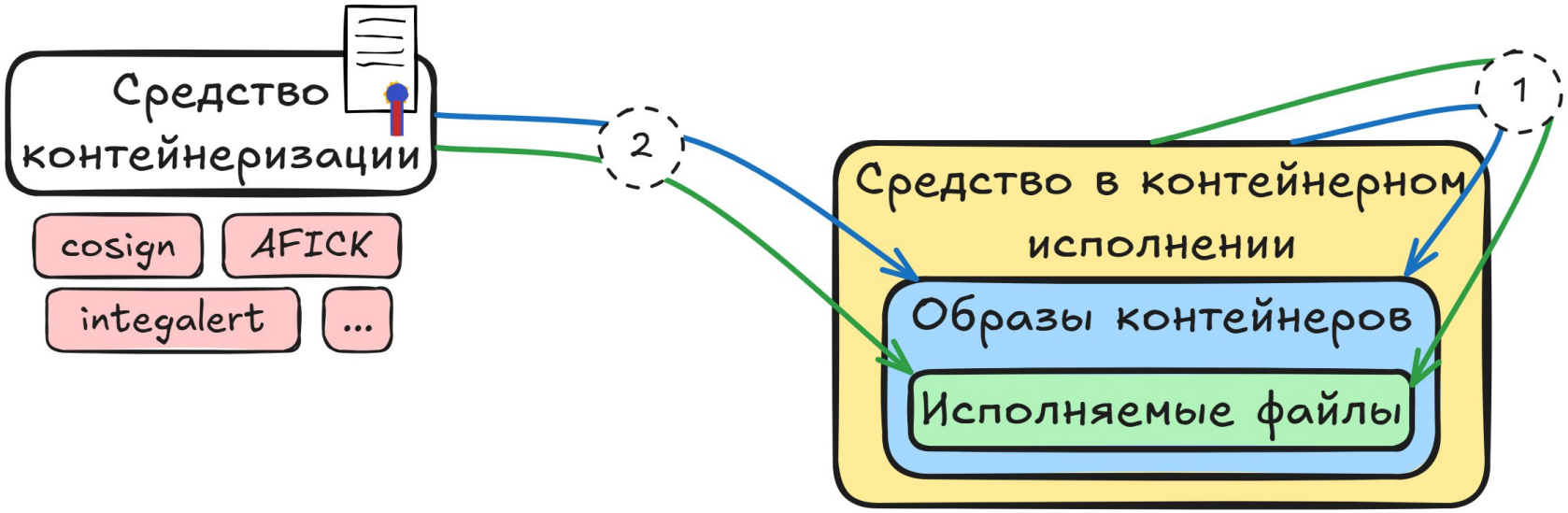
БЕКОН

Контроль целостности

БЕКОН

Контроль целостности

БЕКОН



Контроль целостности

БЕКОН

Реестры ФСТЭК России

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

Государственный реестр сертифицированных средств защиты информации

Обновлено: 12.05.2025 11:26 Просмотры: 1245026

ODS Государственный реестр ССЗИ
Размер: 214 КБ Скачивания: 52153

CSV Государственный реестр ССЗИ
Размер: 1 МБ Скачивания: 22793

Искать в таблице

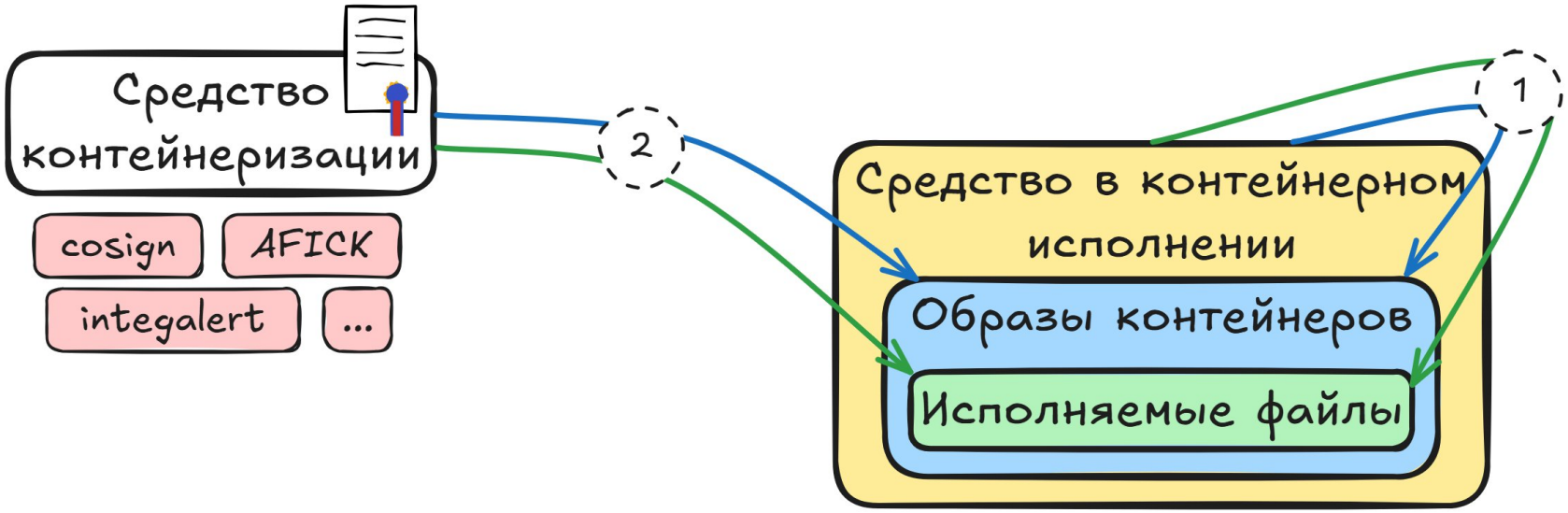
Отображать 10 записей

№ сертификата	Дата внесения в реестр	Срок действия сертификата	Наименование средства (шифр)	Наименования документов, требованиям которых соответствует средство	Схема сертификации	Испытательная лаборатория	Орган по сертификации	Заявитель	Реквизиты заявителя (индекс, адрес, телефон)	Информация об окончании срока технической поддержки, полученная от заявителя
Поиск	Поиск	Поиск	Поиск	Требования к средствам контейнеризации	Поиск	Поиск	Поиск	Поиск	Поиск	Поиск
2557	27.01.2012	27.01.2026	операционная система специального назначения «Astra Linux Special Edition»	Соответствует требованиям документов: Требования доверия(1), Требования доверия(2), Требования к ОС, Профиль защиты ОС(А первого класса защиты. ИТ.ОС.А1.ПЗ), Профиль защиты ОС(А второго класса защиты. ИТ.ОС.А2.ПЗ), Требования к средствам контейнеризации(1), Требования к СУБД(1), Требования к средствам виртуализации(1)	серия	АО «НПО «Эшелон»	ФАУ «ГНИИИ ПТЗИ ФСТЭК России»	ООО «РусБИТех-Астра»	117105, г. Москва, Варшавское шоссе, д. 26, стр. 11, (495) 369-4816	31.12.2050
3866	10.08.2018	10.08.2028	операционная система Альт 8 СП	Соответствует требованиям документов: Требования доверия(4), Требования к ОС, Профиль защиты ОС(А четвертого класса защиты. ИТ.ОС.А4.ПЗ), Требования к средствам контейнеризации(4), Требования к СУБД(4), Требования к средствам виртуализации(4)	серия	АО «НПО «Эшелон»	ФАУ «ГНИИИ ПТЗИ ФСТЭК России»	АО «ИВК»	129110, г. Москва, ул. Гиляровского, д. 57, стр. 1, комн. 73, (495) 221-6580	10.08.2073
4060	12.01.2019	12.01.2029	операционная система «РЕД ОС»	Соответствует требованиям документов: Требования доверия(4), Требования к ОС, Профиль защиты ОС(А четвертого класса защиты. ИТ.ОС.А4.ПЗ), Требования к средствам контейнеризации(4), Требования к средствам виртуализации(4)	серия	ЗАО ГИЦ ПС ВТ	ООО «ЦБИ»	ООО «РЕД СОФТ»	121205, г. Москва, территория Сколково инновационного центра, ул. Нобеля, д. 5, эт. 2, пом. 4, (495) 285-6268	31.12.2030
4381	31.03.2021	31.03.2026	операционная система общего назначения «Основа»	Соответствует требованиям документов: Требования доверия(4), Требования к ОС, Профиль защиты ОС(А четвертого класса защиты. ИТ.ОС.А4.ПЗ), Требования к средствам контейнеризации(4), Требования к средствам виртуализации(4)	серия	ООО «ЦБИ»	ФАУ «ГНИИИ ПТЗИ ФСТЭК России»	АО «НППКТ»	127474, г. Москва, шоссе Дмитровское, д. 60А, помещение XXV, ком. 5, (499)280-0970	

Ссылка на реестр

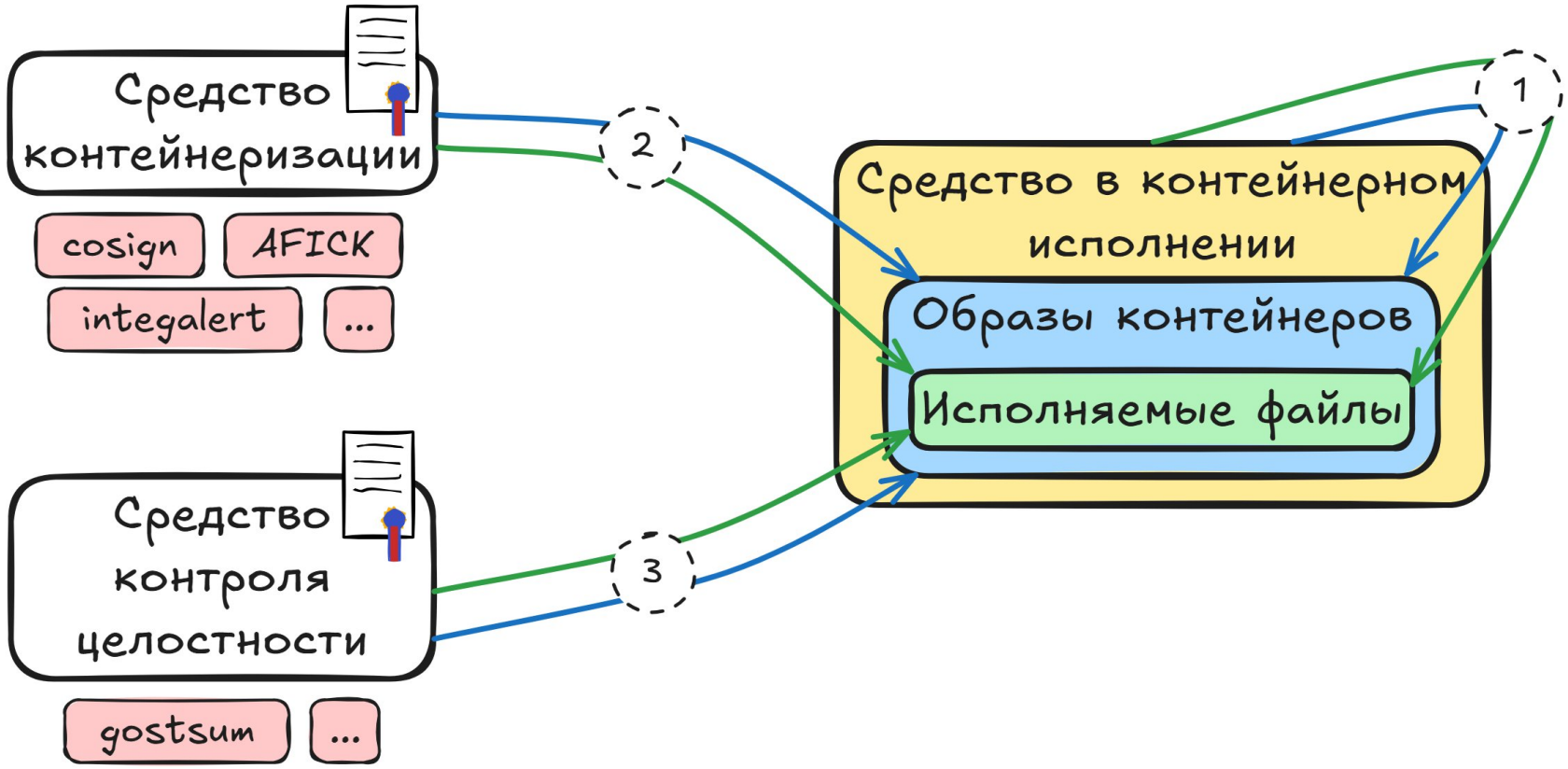
Контроль целостности

БЕКОН



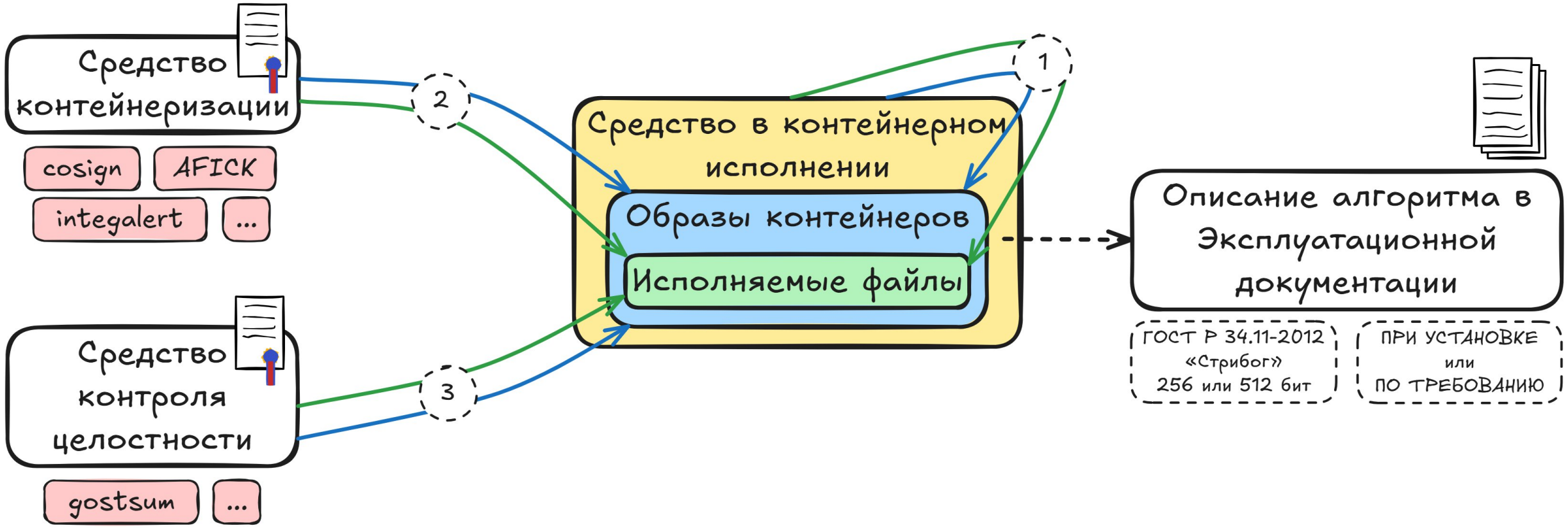
Контроль целостности

БЕКОН



Контроль целостности

БЕКОН



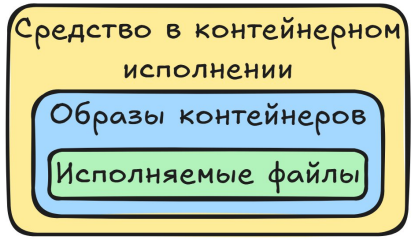
БЕКОН

Обеспечение совместимости

«4. Разработчик средства в контейнерном исполнении должен обеспечить **совместимость программного обеспечения, входящего в состав образов контейнеров, с хостовыми операционными системами,** указанными в эксплуатационной документации средства в качестве среды функционирования.»

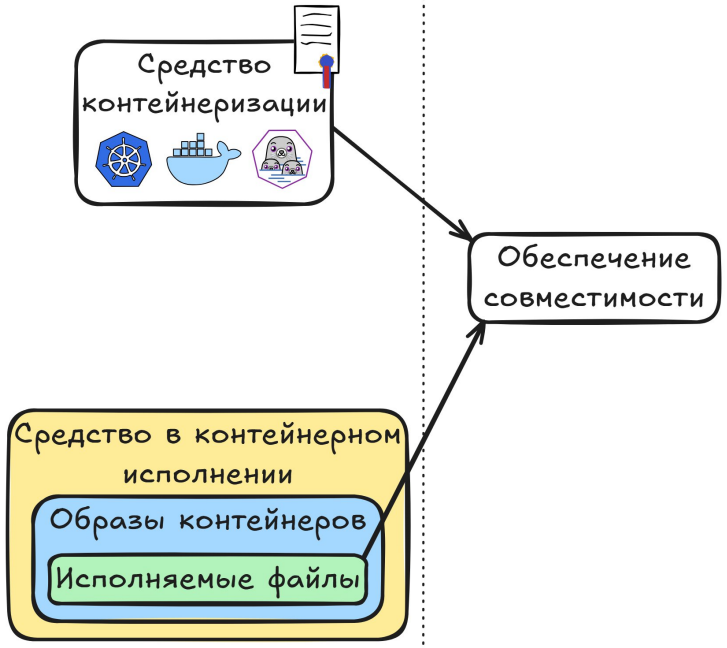
Обеспечение совместимости

БЕКОН



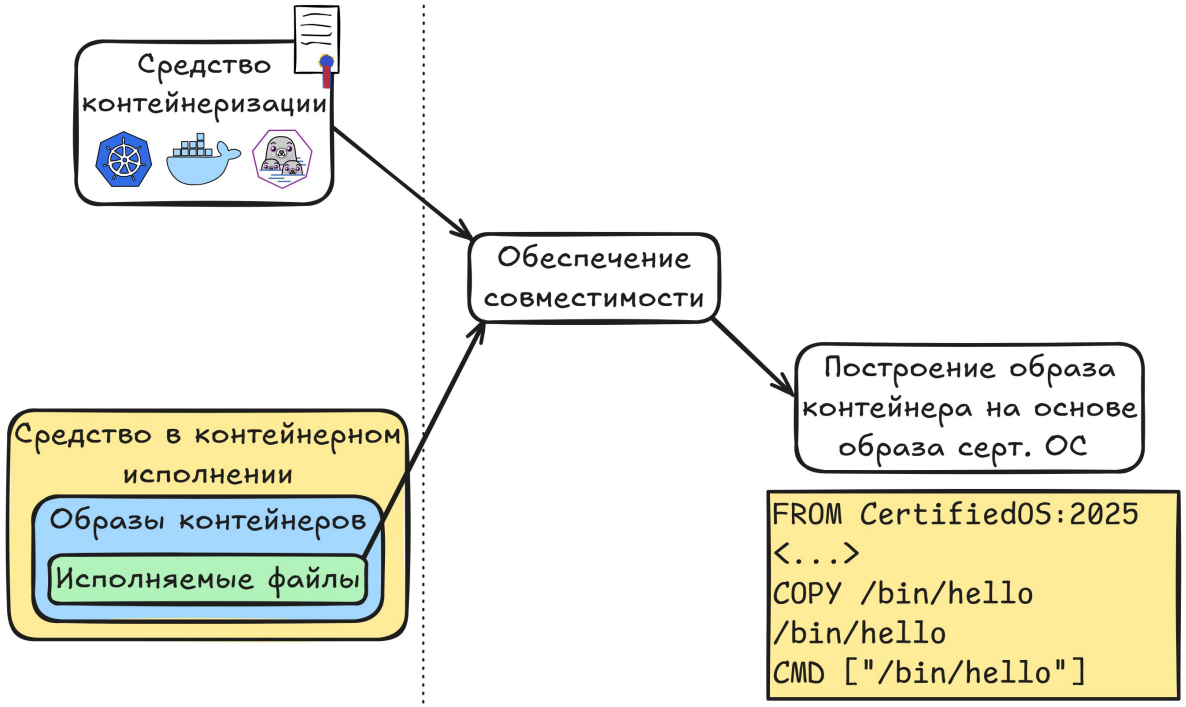
Обеспечение совместимости

БЕКОН



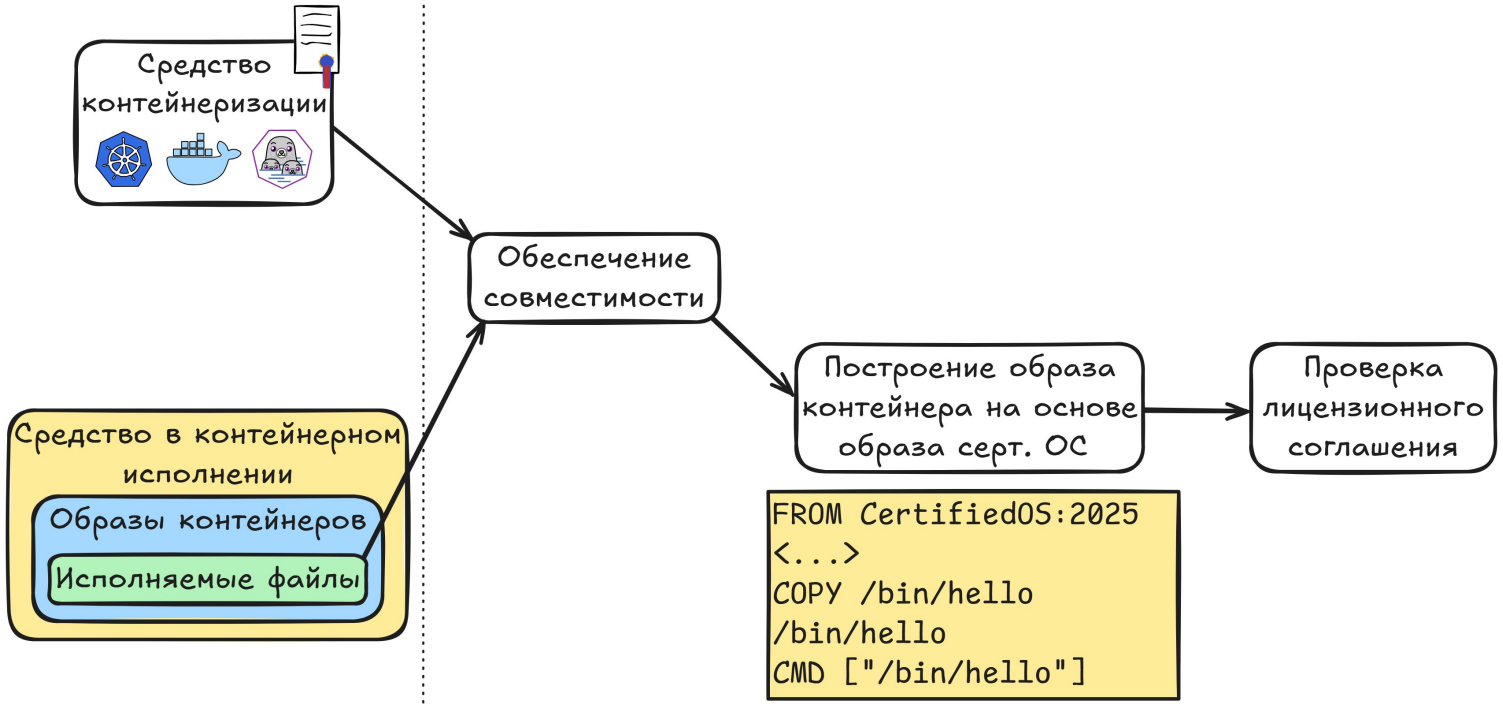
Обеспечение совместимости

БЕКОН



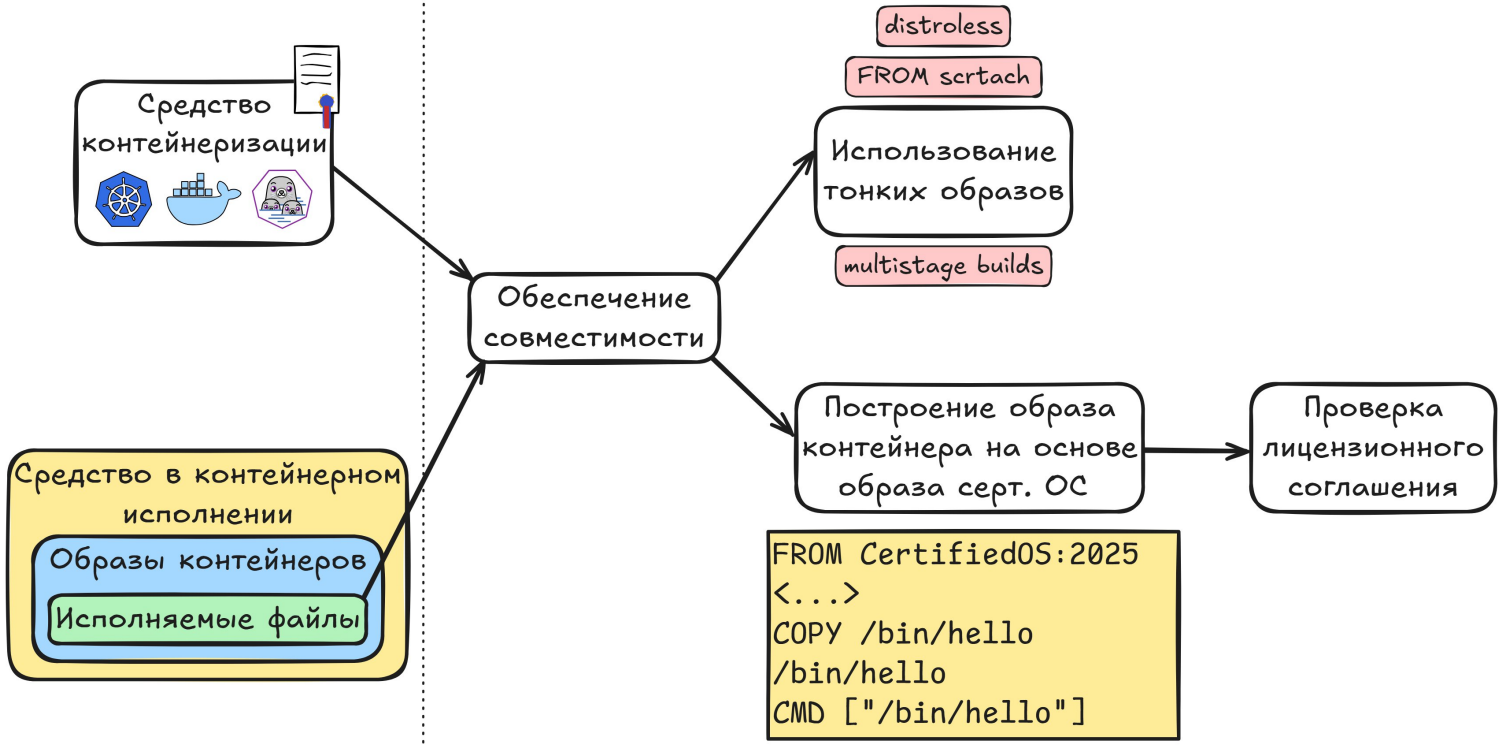
Обеспечение совместимости

БЕКОН



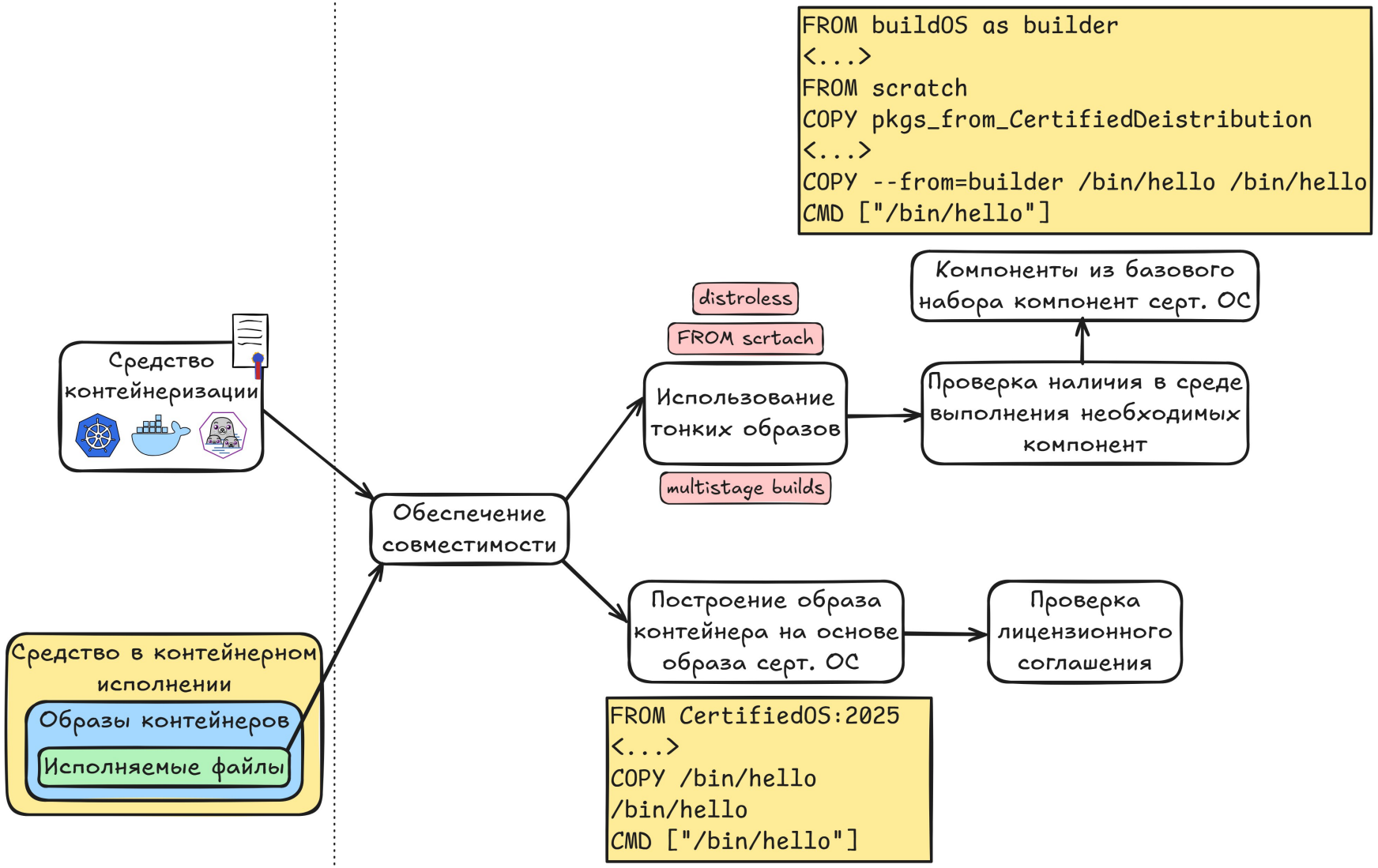
Обеспечение совместимости

БЕКОН



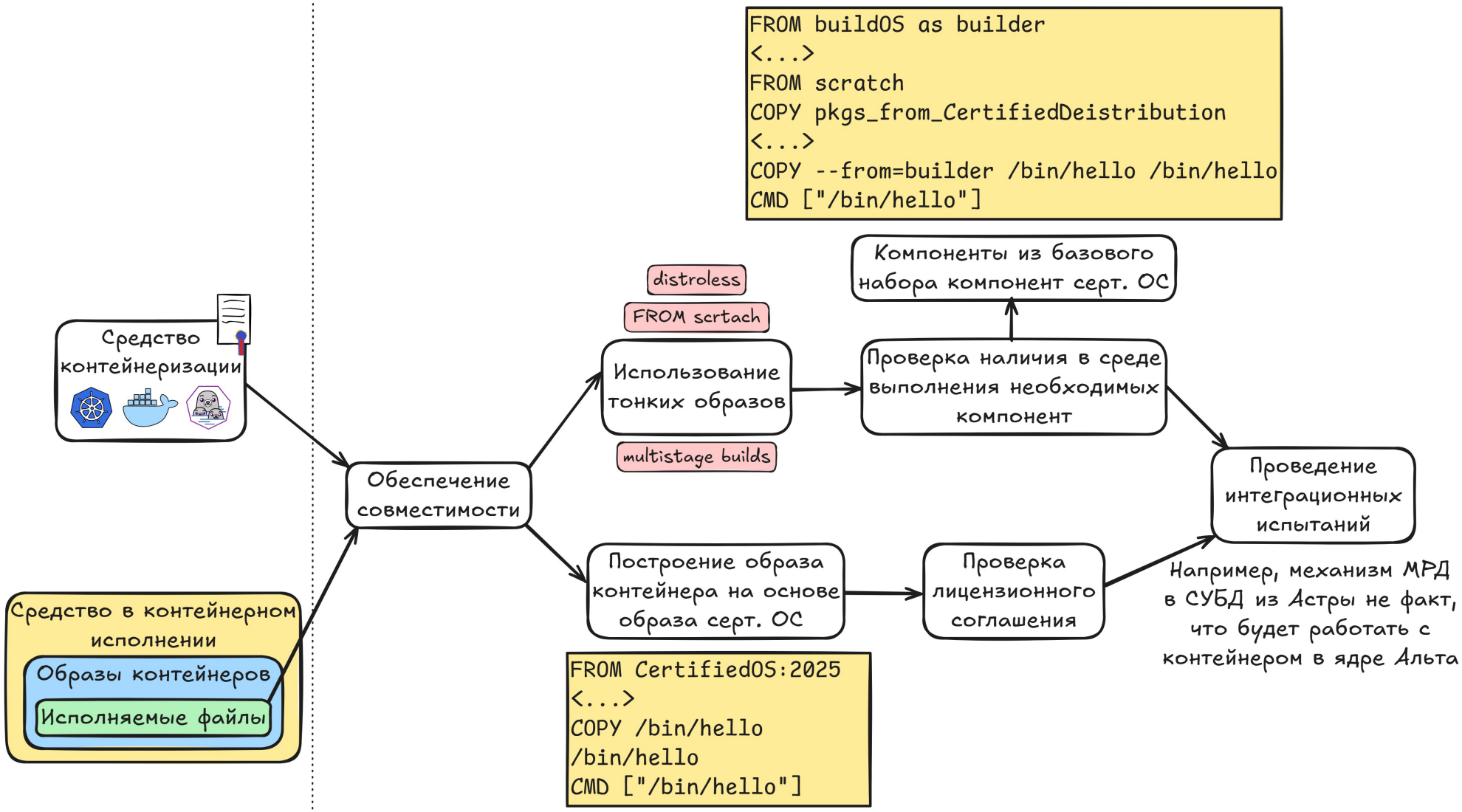
Обеспечение совместимости

БЕКОН



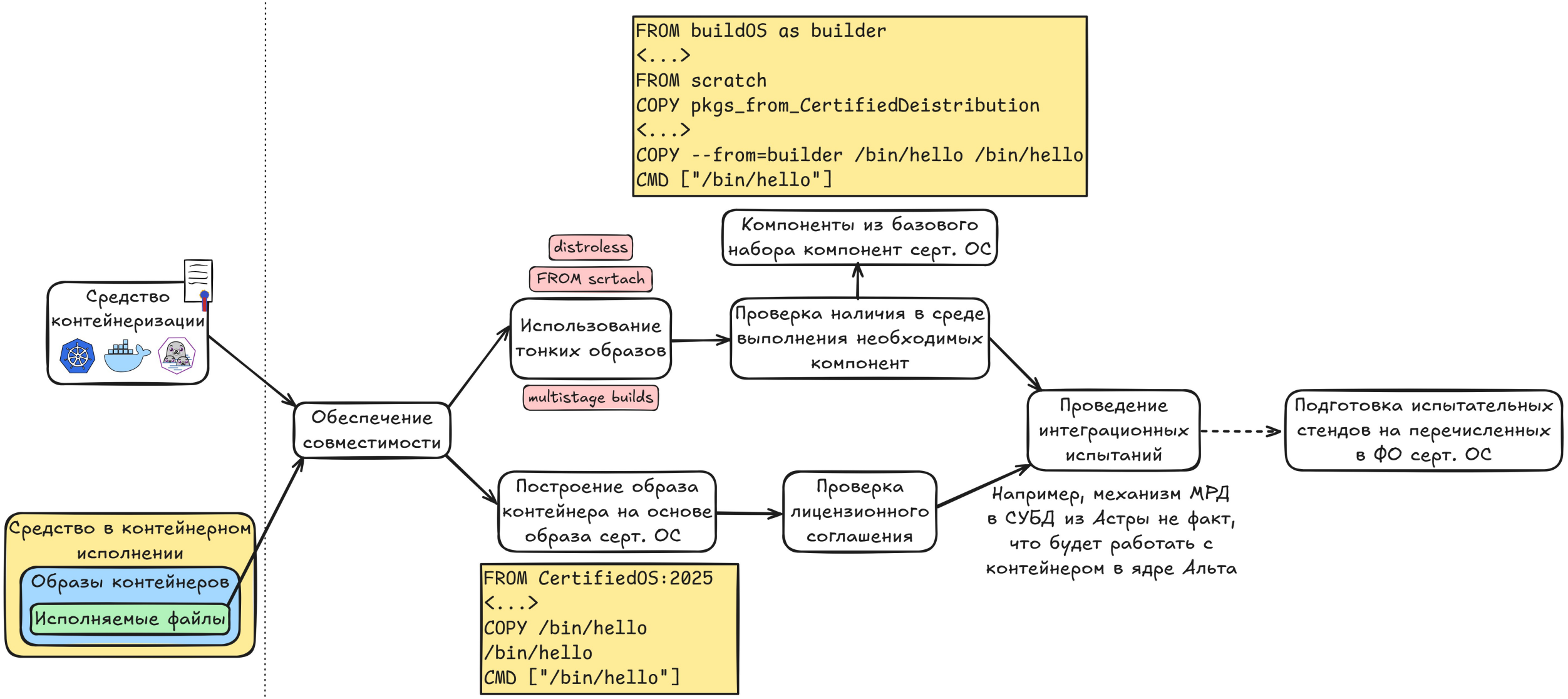
Обеспечение совместимости

БЕКОН



Обеспечение совместимости

БЕКОН



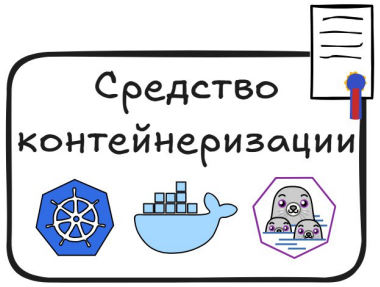
БЕКОН

Минимизация привилегий

«5. Средство в контейнерном исполнении должно обеспечивать запуск контейнеров с полномочиями, минимально необходимыми для функционирования средства на уровне процессов хостовой операционной системы. Избыточные полномочия компонентов, выявленные при проведении сертификации средства должны быть устранены.»

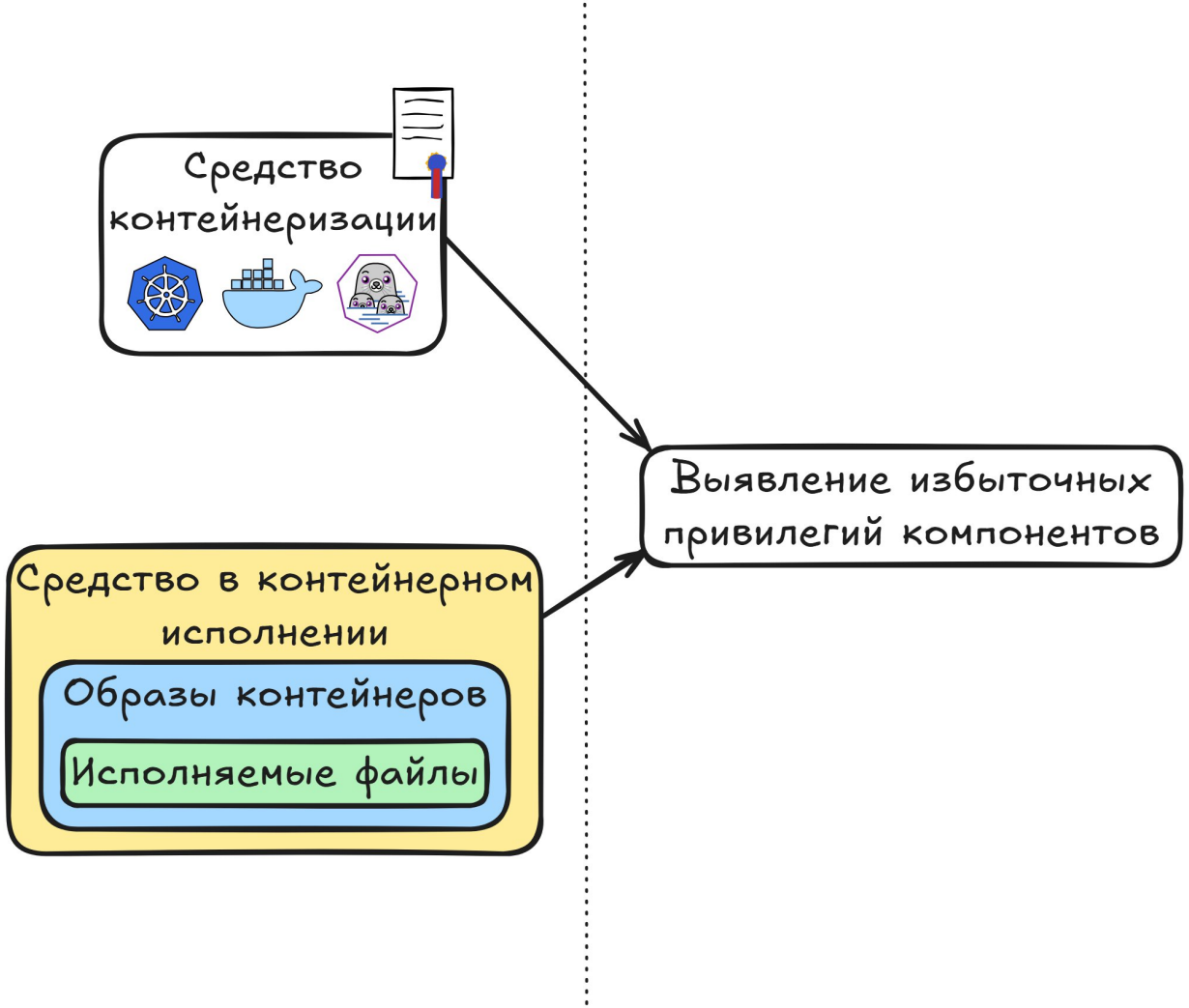
Минимизация привилегий

БЕКОН



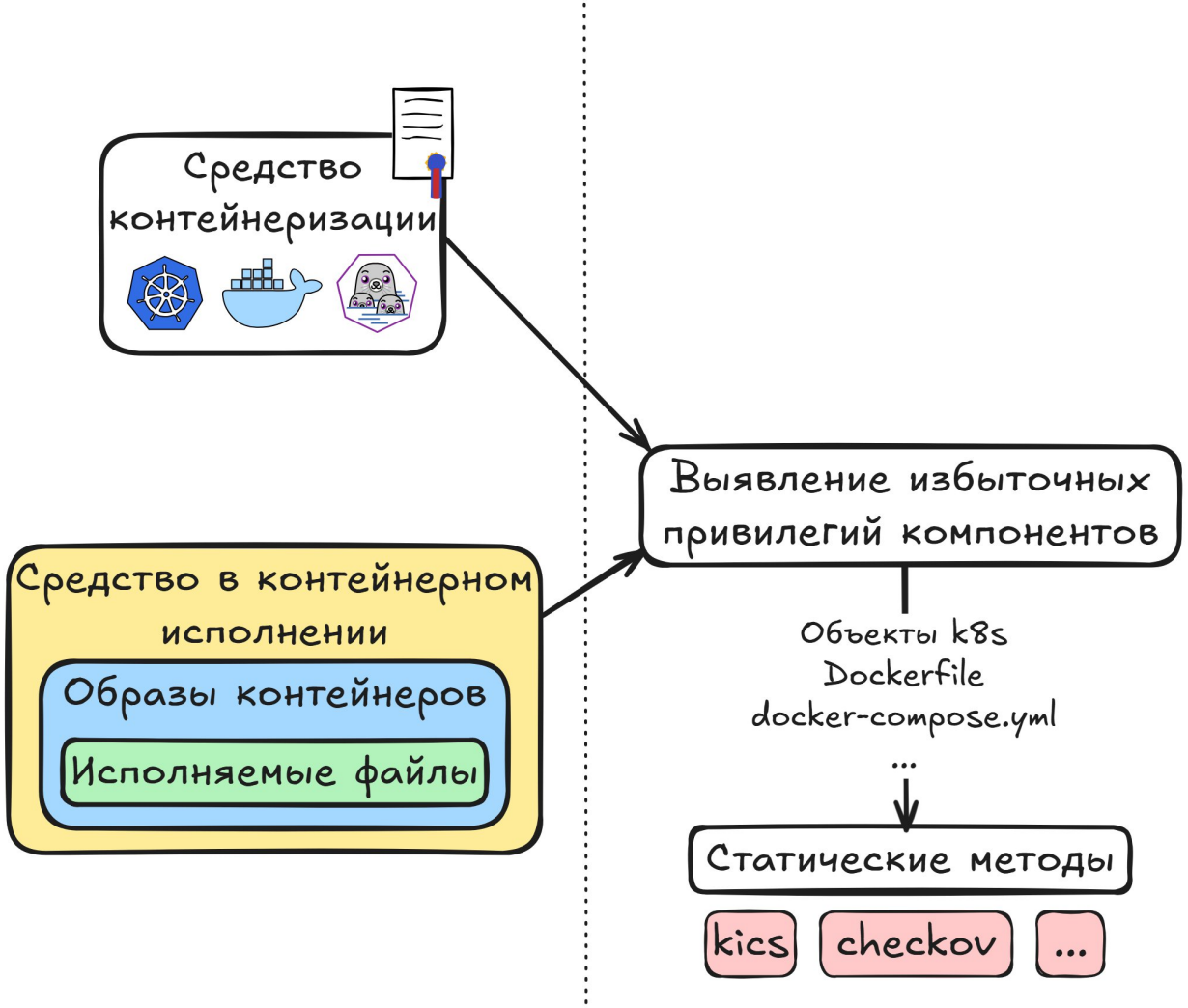
Минимизация привилегий

БЕКОН



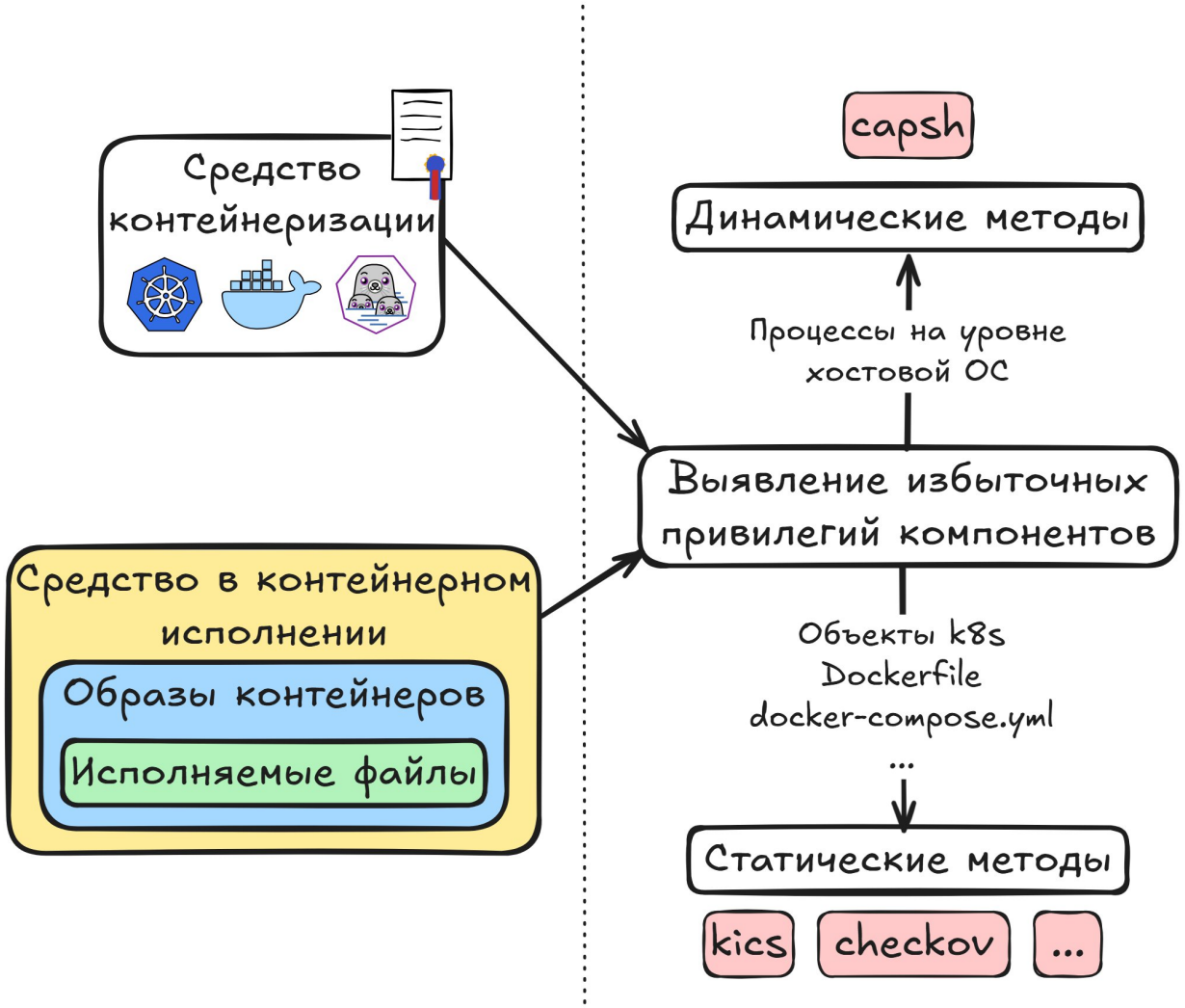
Минимизация привилегий

БЕКОН



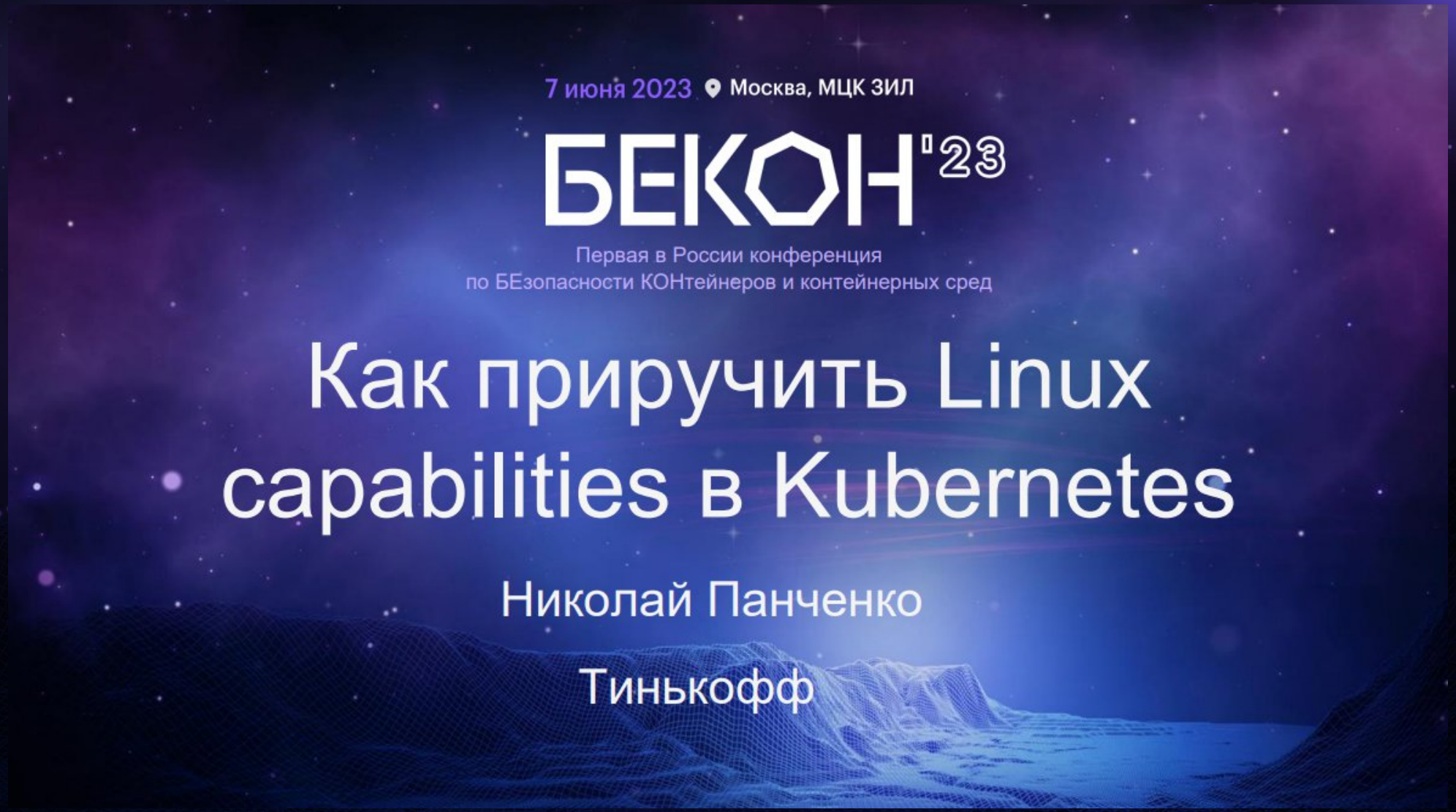
Минимизация привилегий

БЕКОН



Минимизация привилегий

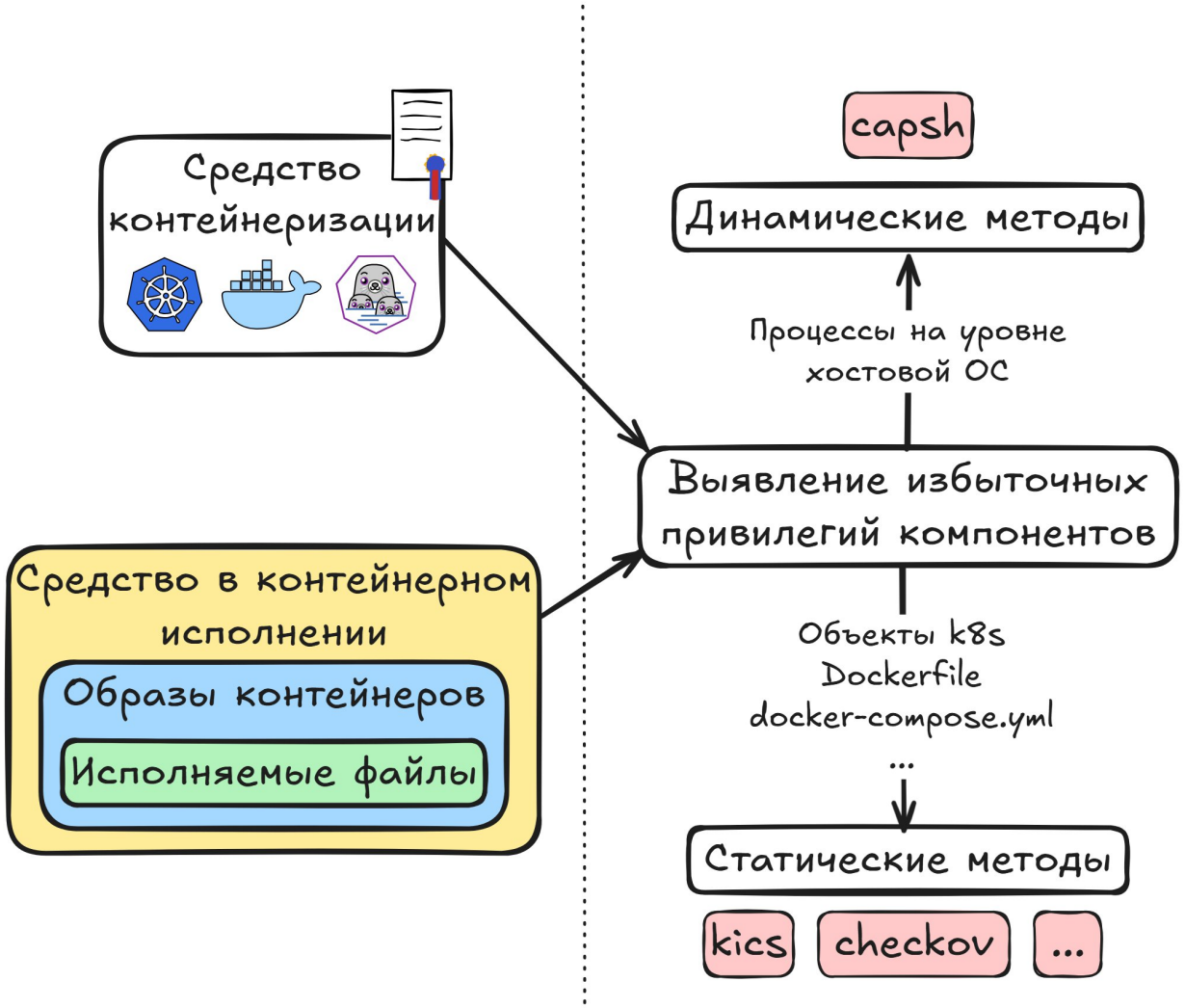
БЕКОН



Ссылка на доклад

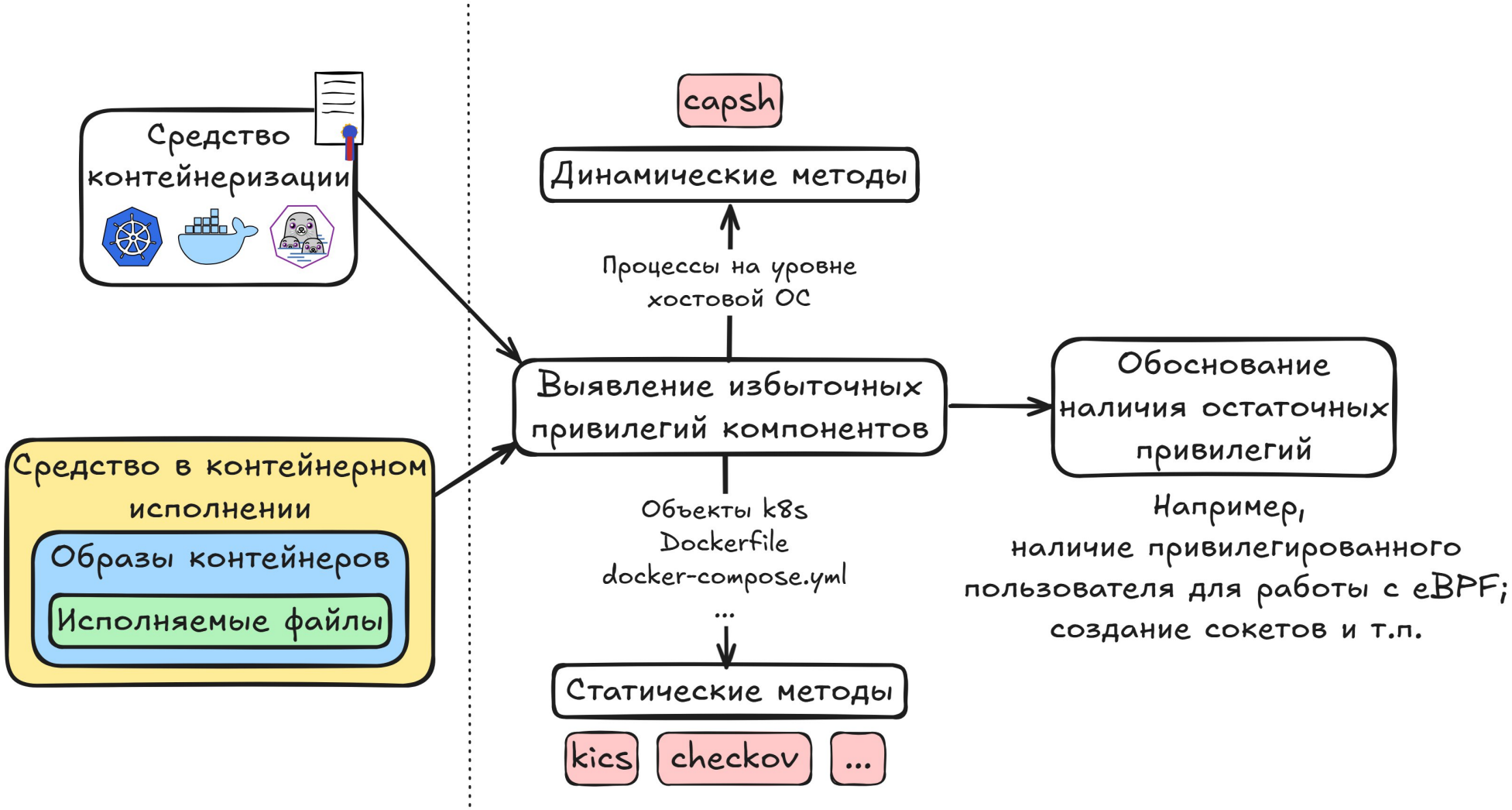
Минимизация привилегий

БЕКОН



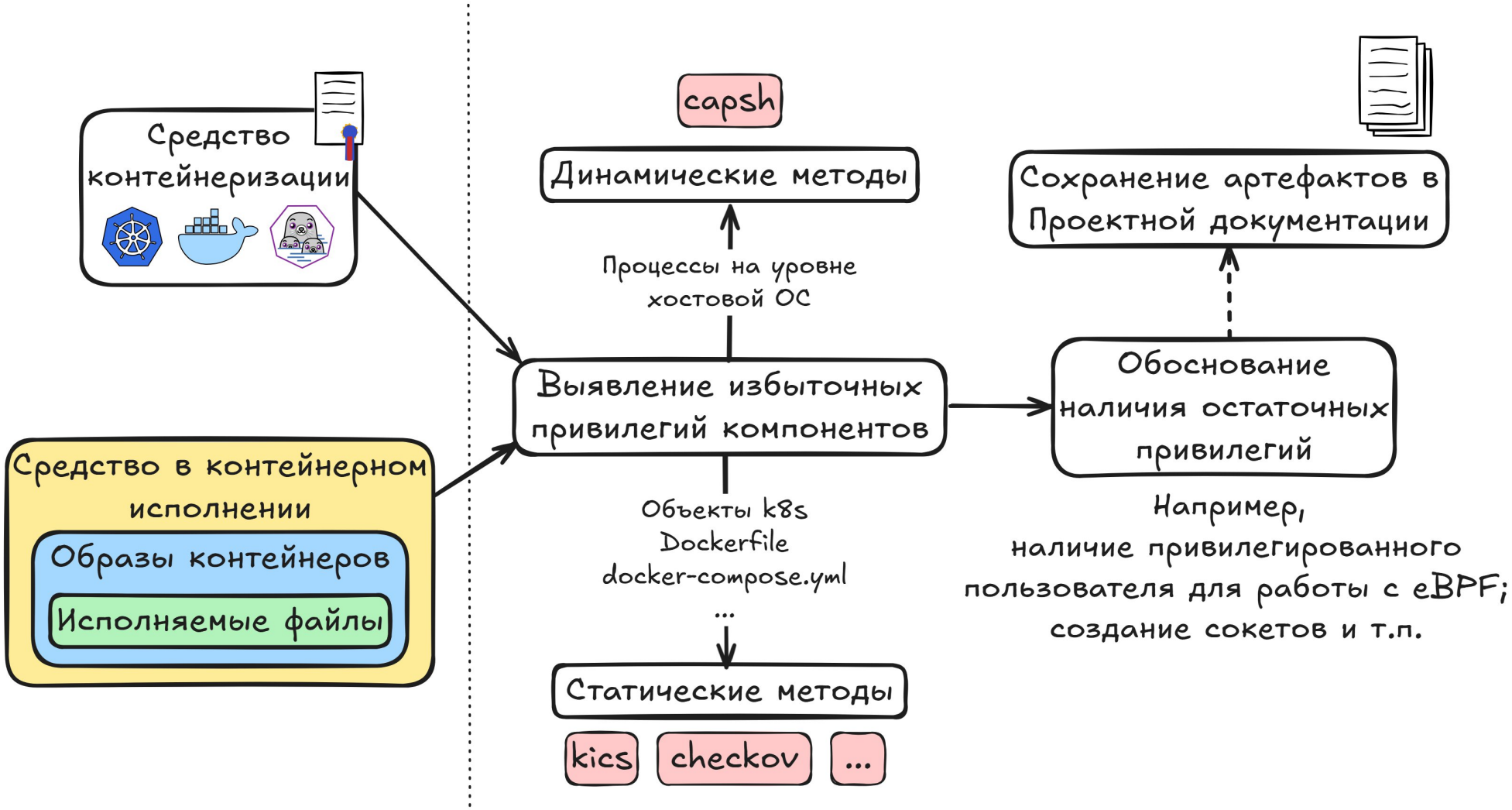
Минимизация привилегий

БЕКОН



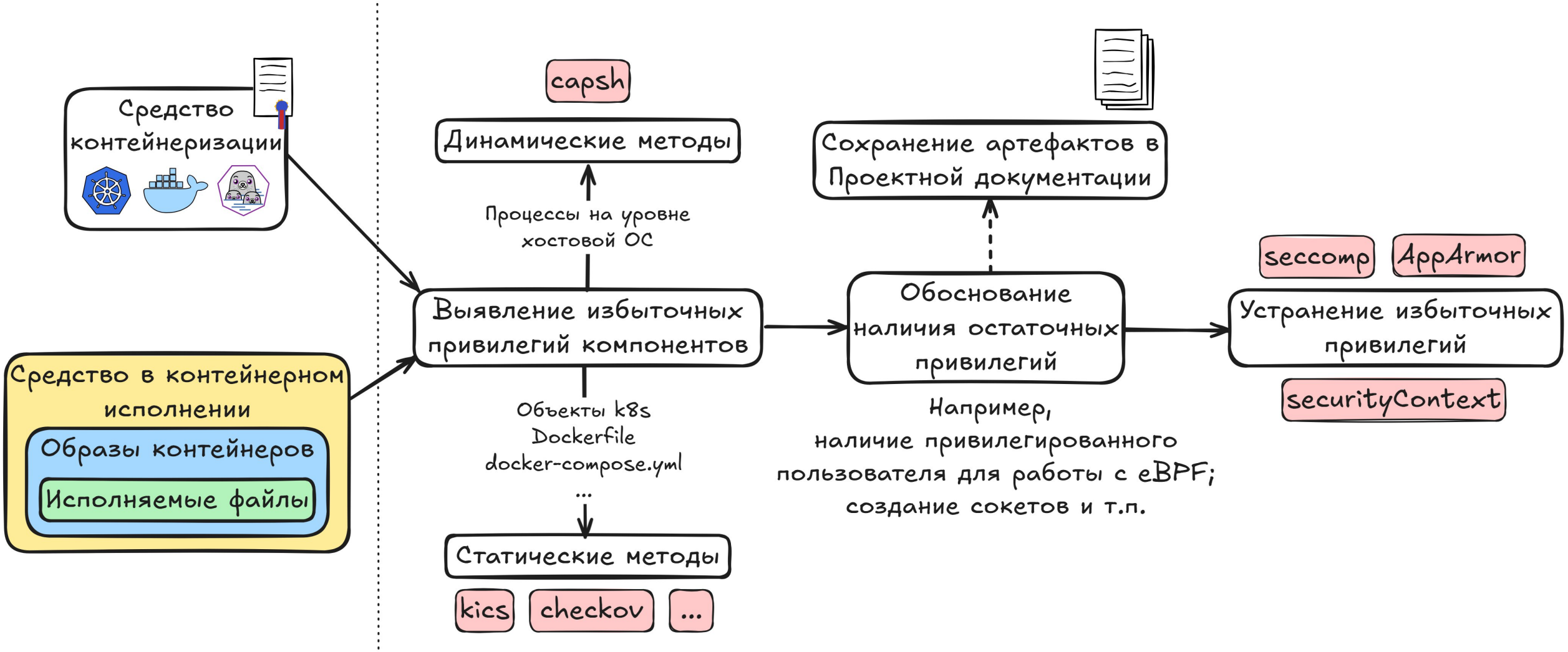
Минимизация привилегий

БЕКОН



Минимизация привилегий

БЕКОН



БЕКОН

Управление доступом

«6. Средство контейнеризации с функцией централизованного управления контейнерами (далее — оркестратор) должно обеспечивать управление доступом между компонентами средства (контейнерами, микросервисами, иными ресурсами, характерными для выбранного типа оркестратора), компонентами среды функционирования, внешними по отношению к средству компонентами в соответствии с заданными разработчиком средства правилами.

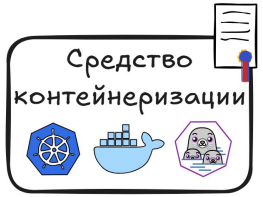
Заданные разработчиками средства правила должны содержать список действий, разрешенных при взаимодействии компонентов средства между собой, компонентами среды функционирования, внешними по отношению к средству компонентами.

Избыточные разрешающие правила доступа к компонентам средства, выявленные при проведении сертификации средства, должны быть устранены.

Правила доступа, содержащие список действий, разрешенных при взаимодействии компонентов средства между собой и компонентами среды функционирования, должны быть описаны в документации средства.»

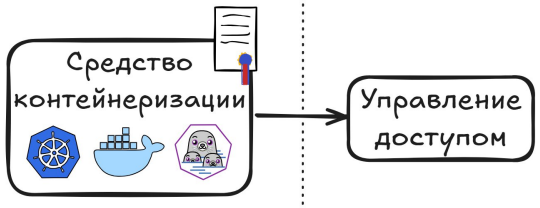
Управление доступом

БЕКОН



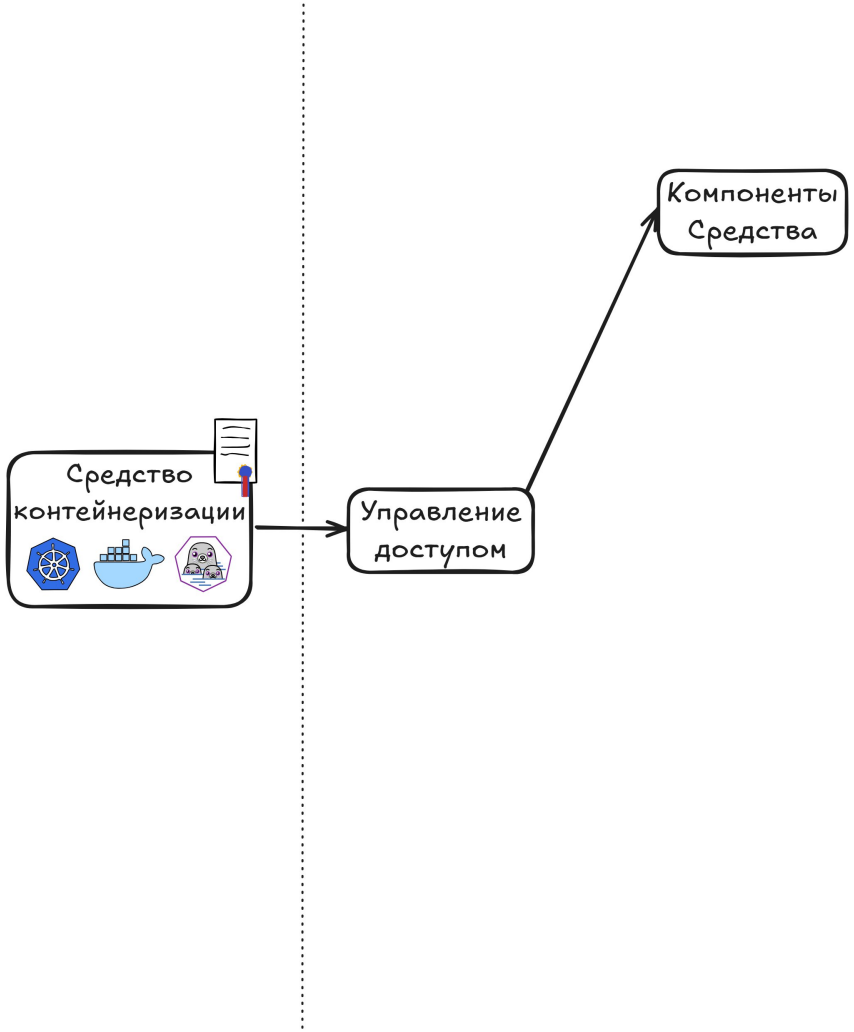
Управление доступом

БЕКОН



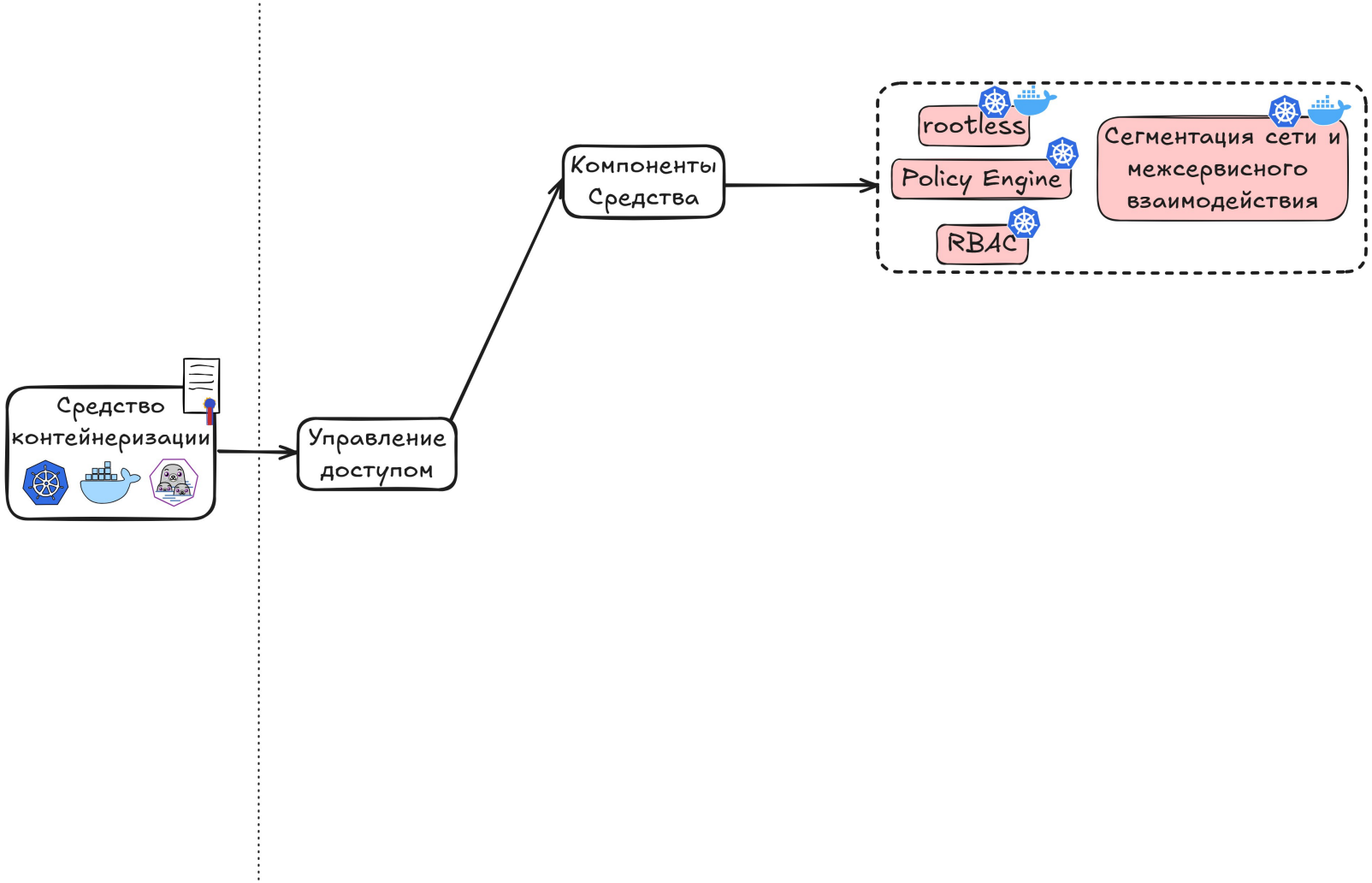
Управление доступом

БЕКОН



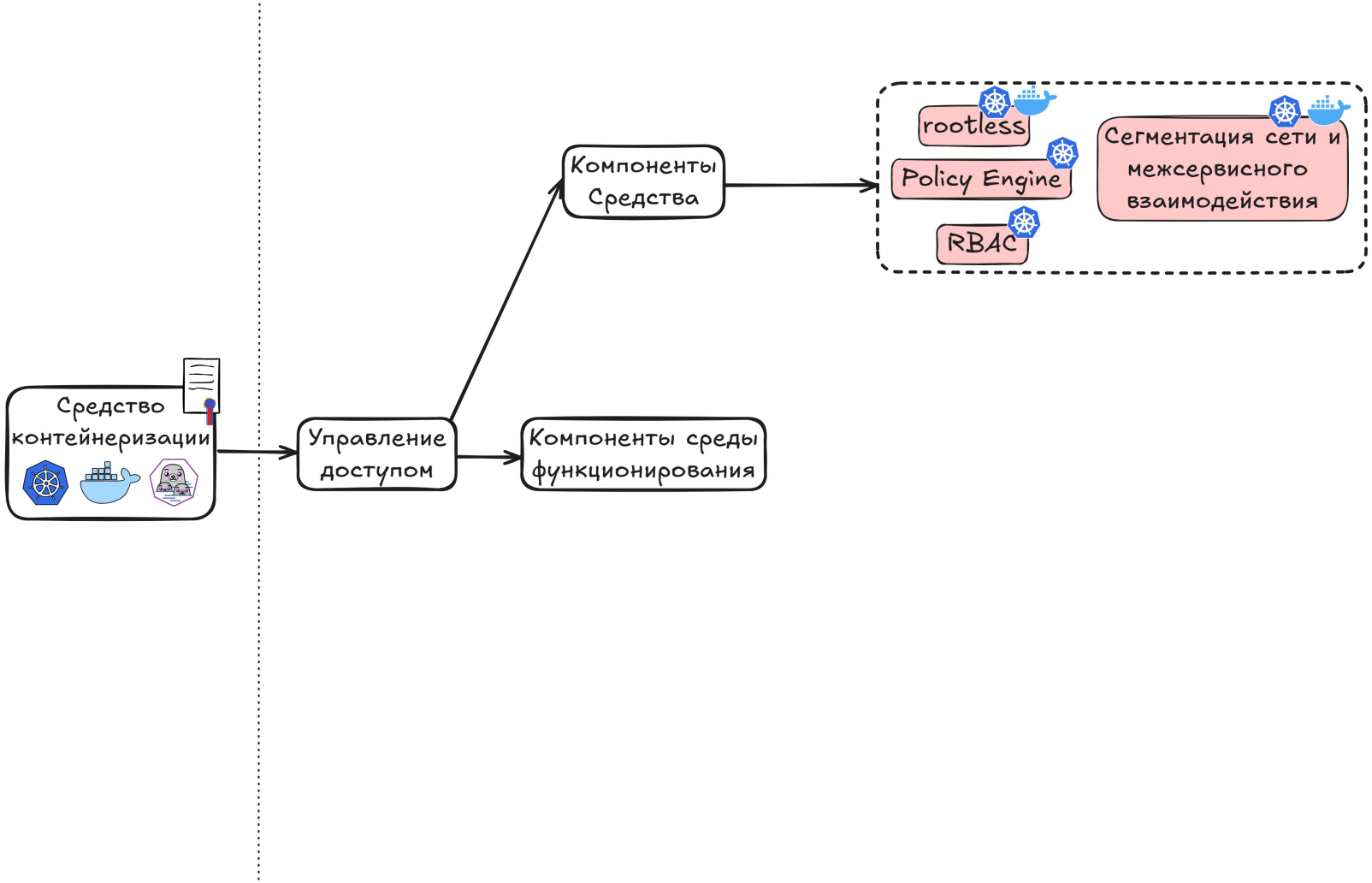
Управление доступом

БЕКОН



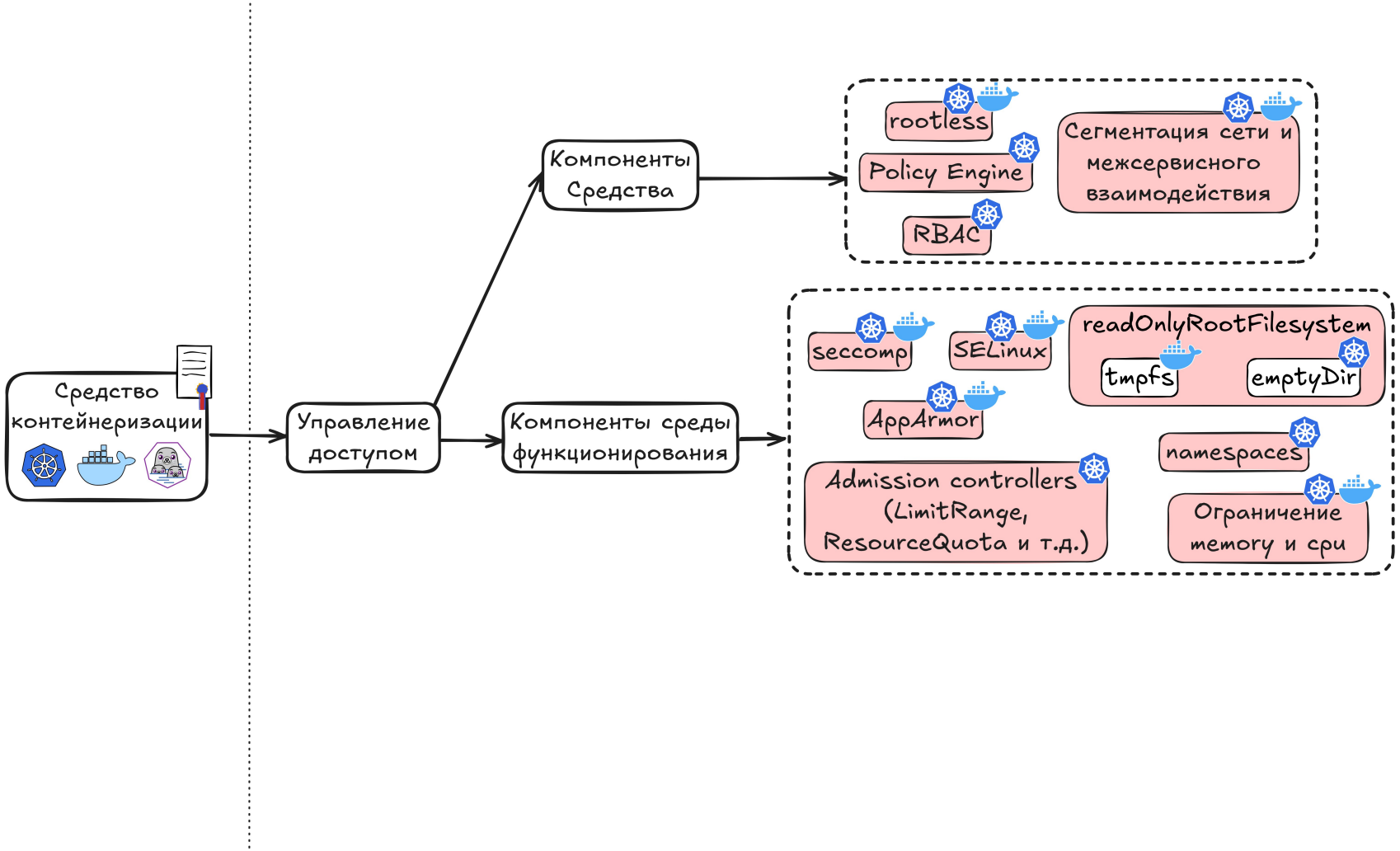
Управление доступом

БЕКОН



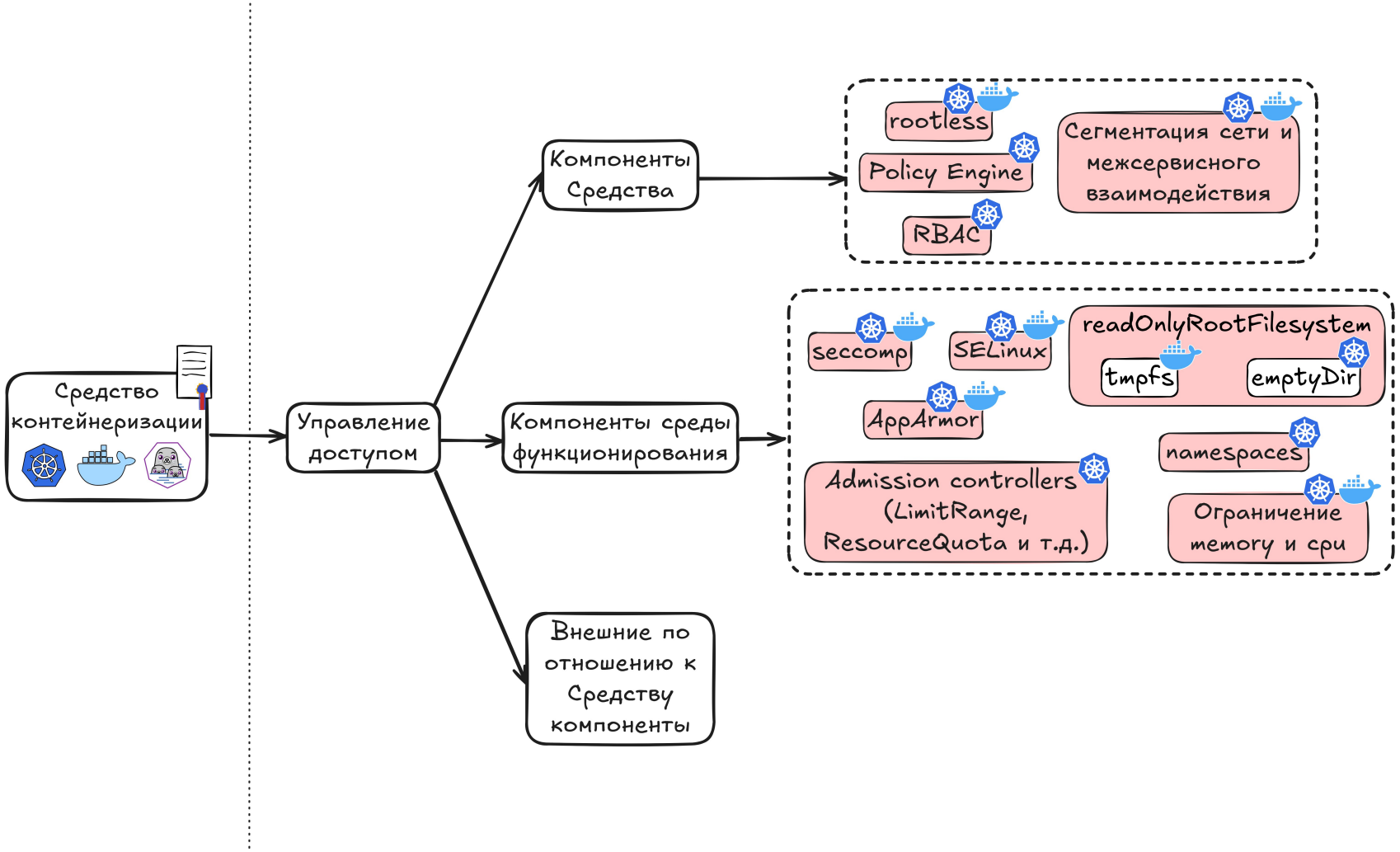
Управление доступом

БЕКОН



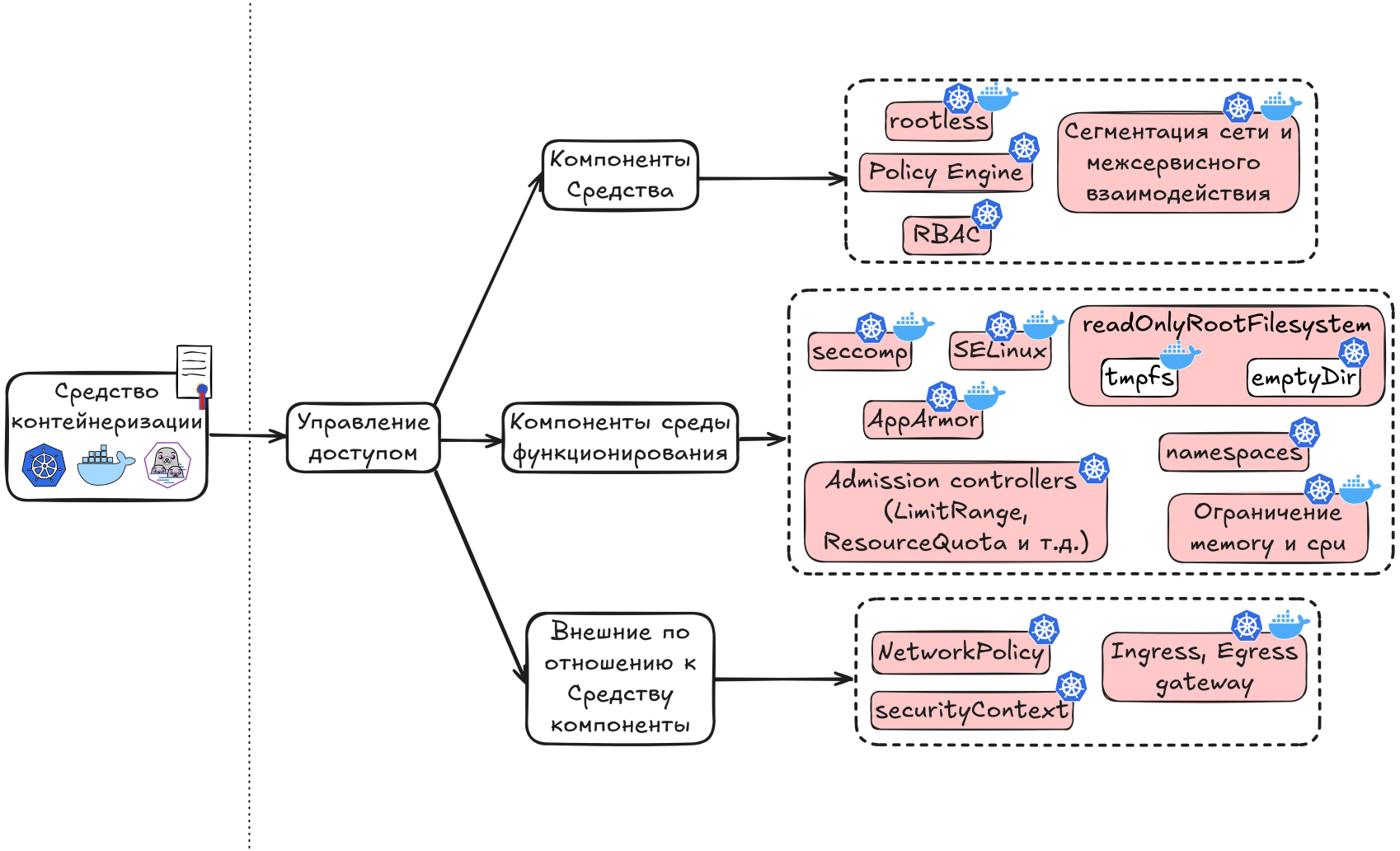
Управление доступом

БЕКОН



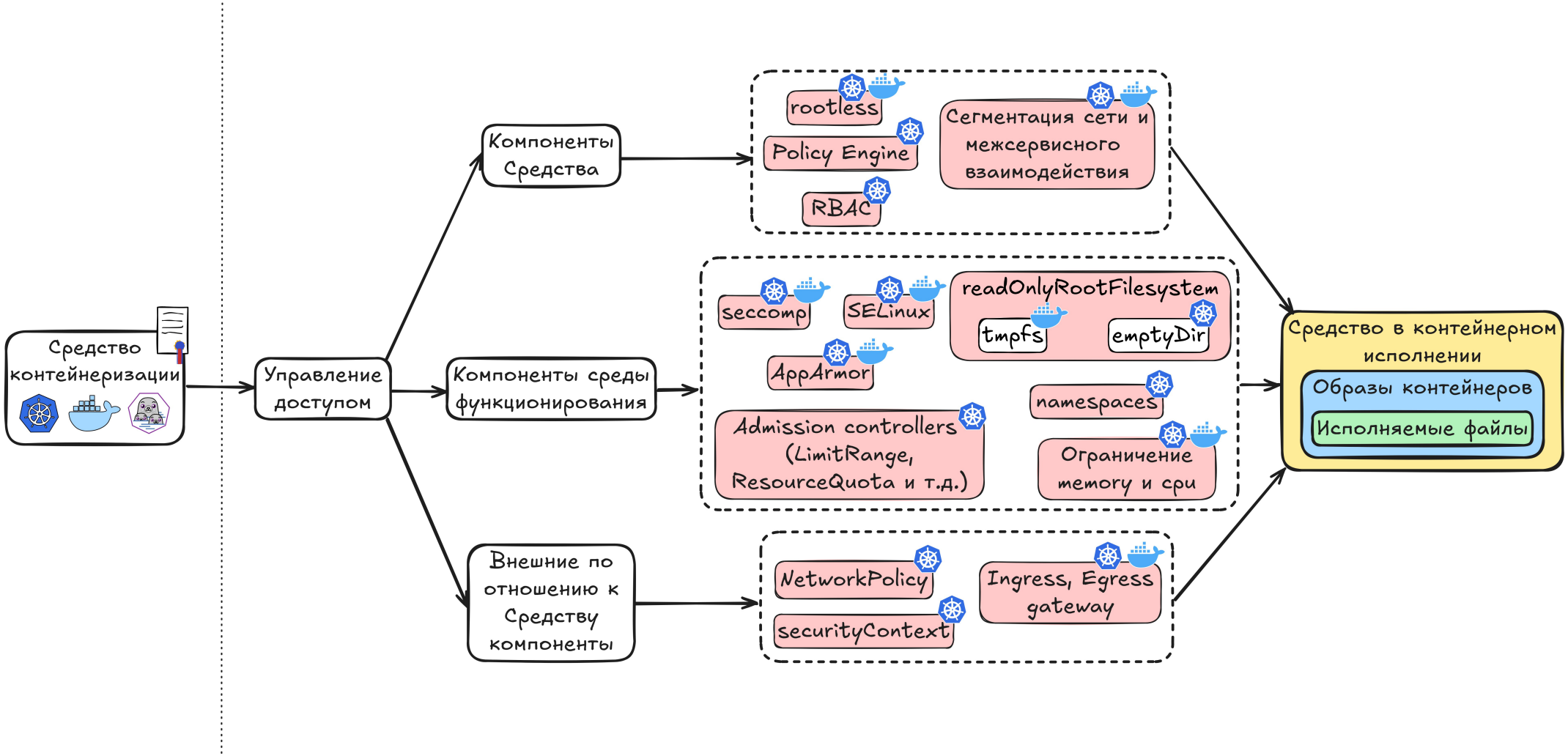
Управление доступом

БЕКОН



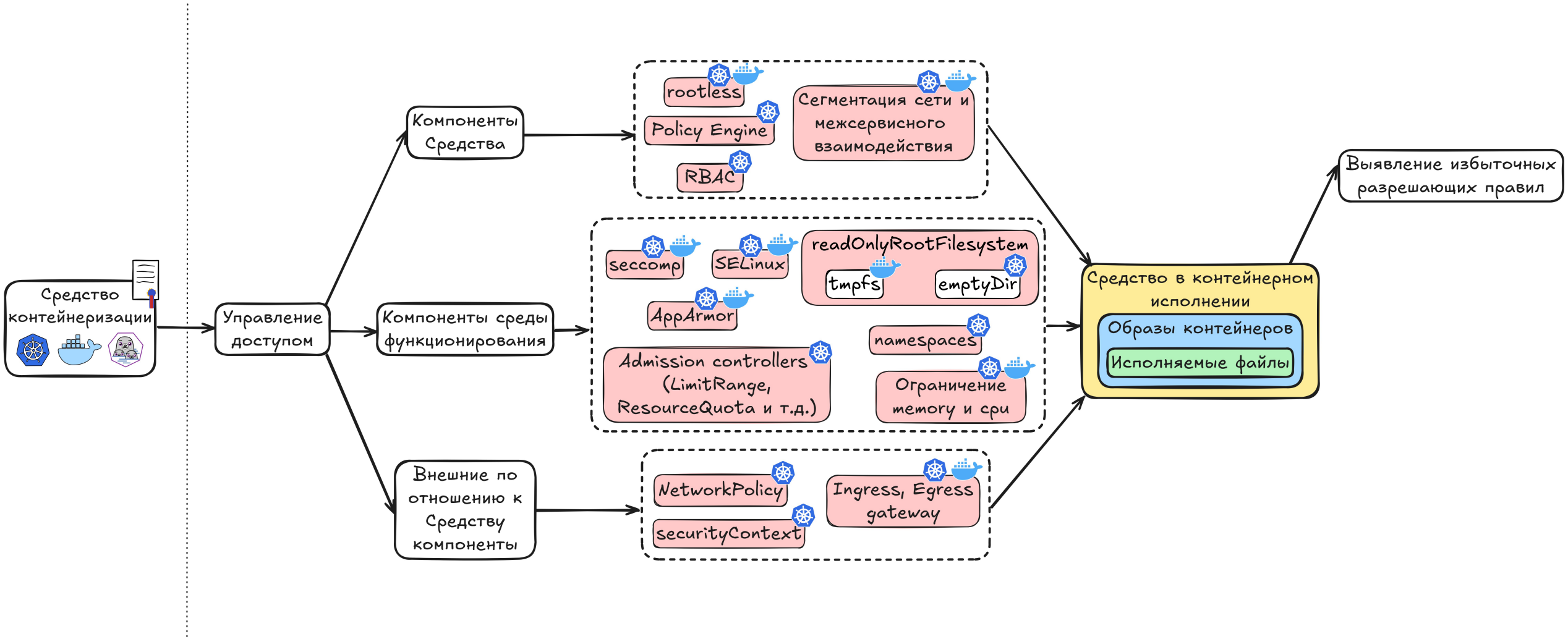
Управление доступом

БЕКОН



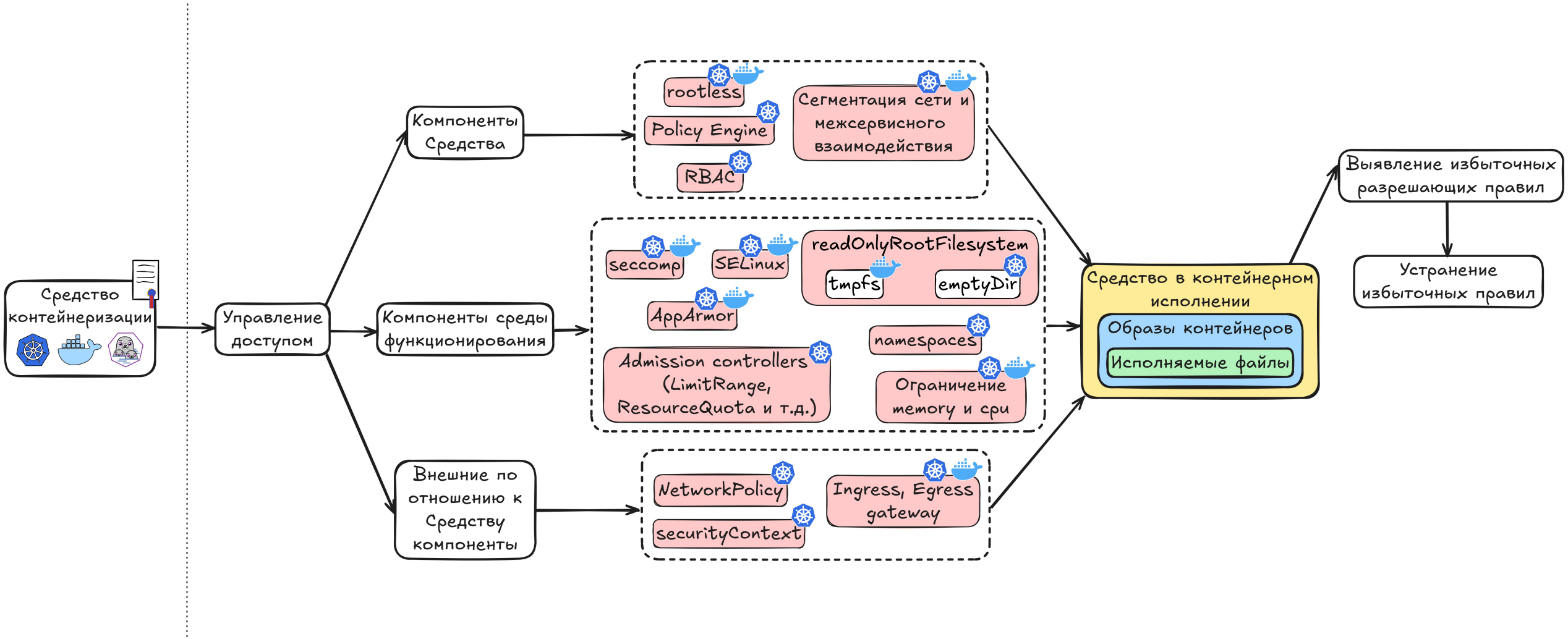
Управление доступом

БЕКОН



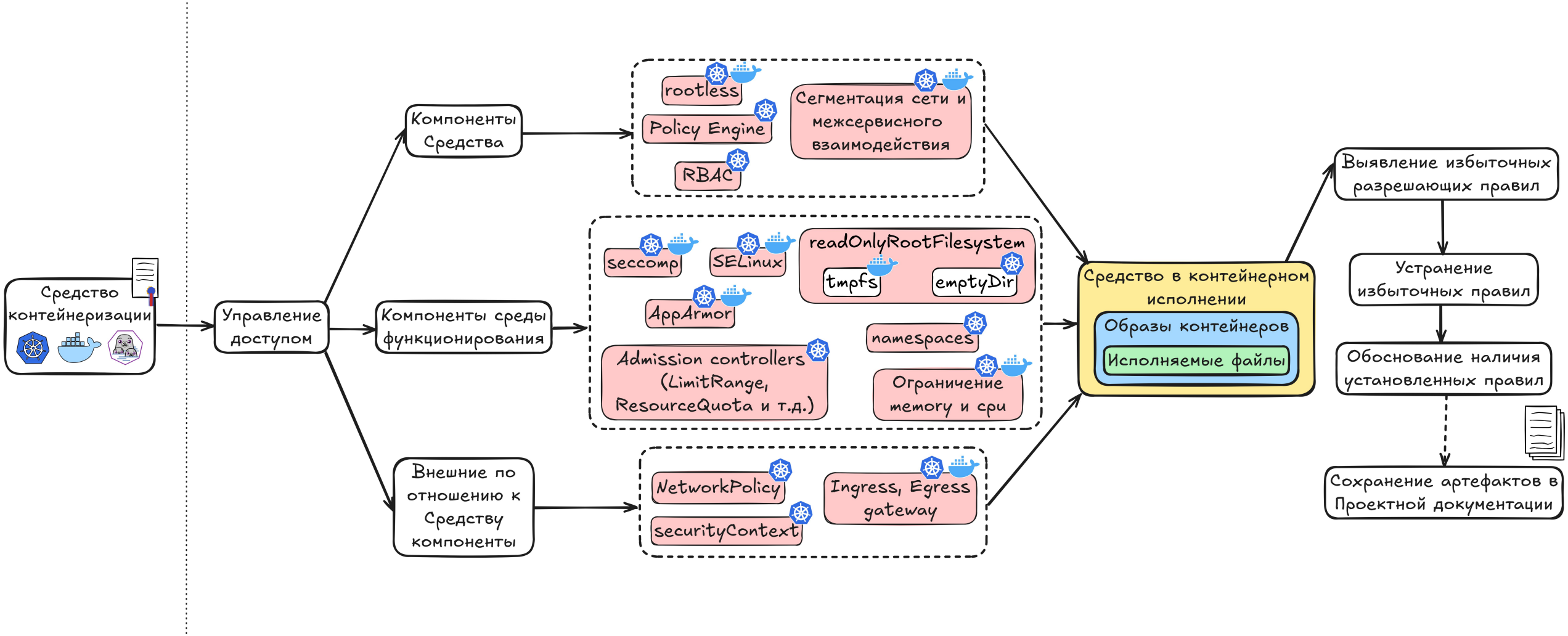
Управление доступом

БЕКОН



Управление доступом

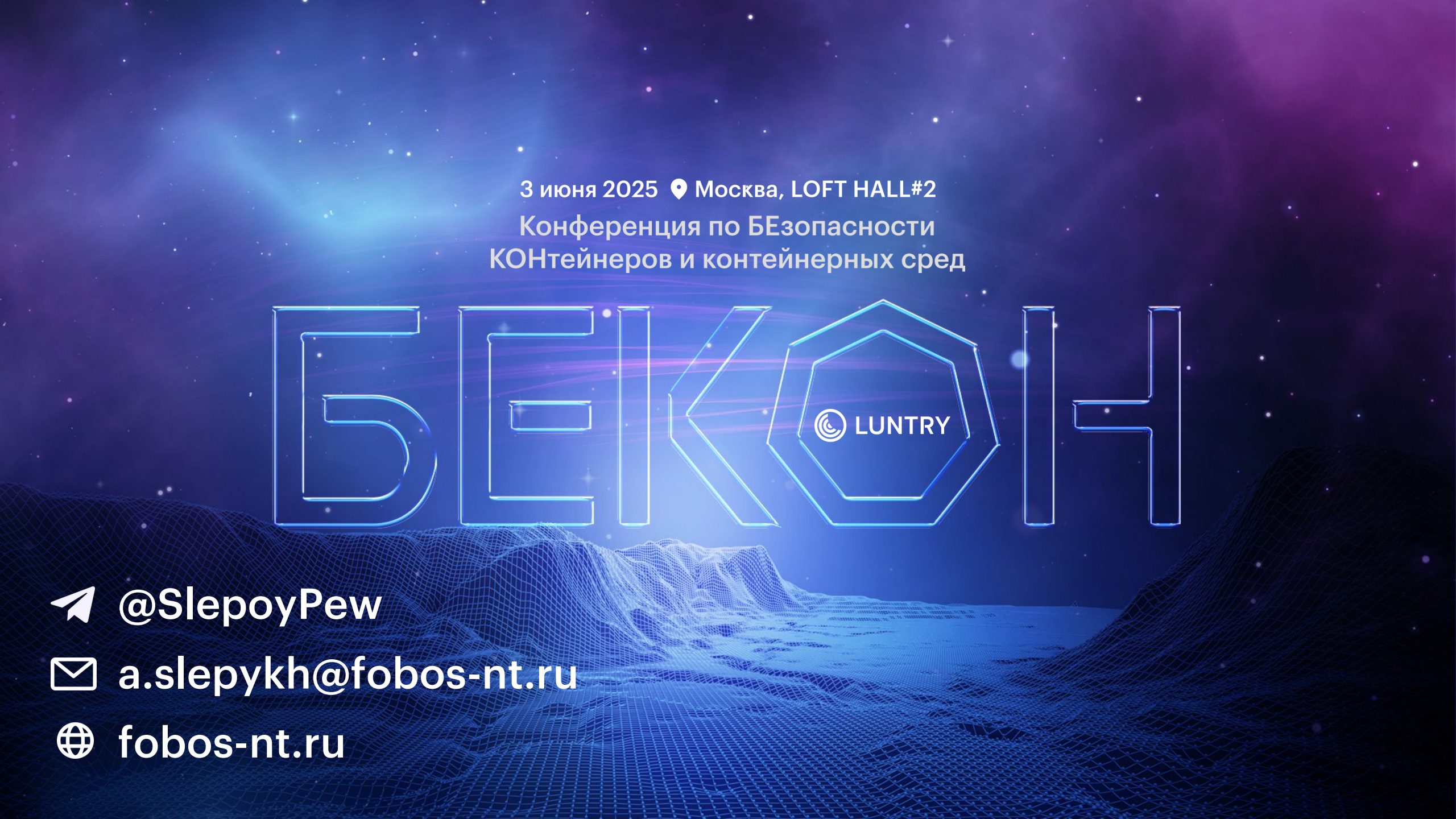
БЕКОН



Выводы

БЕКОН

- Виден интерес Регулятора к вопросам обеспечения безопасности контейнеров
- Взаимодействие представителей промышленности с Регулятором ведет к прозрачности и повышению эффективности процесса сертификации
- ИС ФСТЭК России 240/24/38 дает «первый шаг» к обеспечению безопасности контейнеров
- Требования применительны не только в рамках сертификации
- Если вы уже занимались безопасностью ваших контейнеров, то проблем с сертификацией быть не должно


3 июня 2025 Москва, LOFT HALL#2
Конференция по БЕзопасности
КОНтейнеров и контейнерных сред
БЕКОН
LUNTRY
@SlepoyPew
a.slepykh@fobos-nt.ru
fobos-nt.ru