конференция
РусКрипто

Ежегодная международная научно-практическая конференция

«РусКрипто’2023»

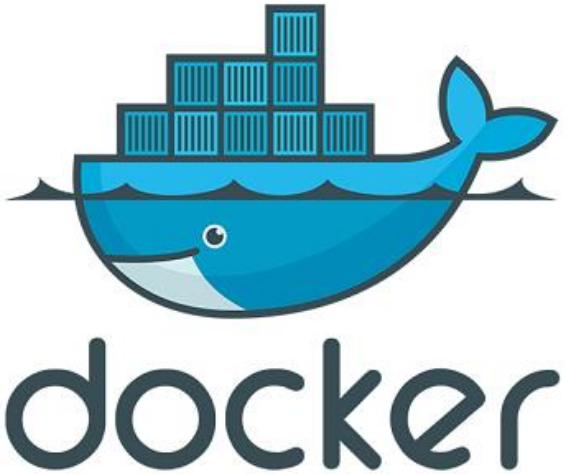
Некоторые вопросы использования СКЗИ с применением средств контейнеризации

Пузырев В.А., зам. начальника отдела анализа криптосредств, КриптоПро
Крапивенцев Д.М., инженер-аналитик, КриптоПро

Актуальность

Средства контейнеризации приобрели популярность по причинам:

- удобство разработки (создание изолированных сред)
- изоляция процессов
- низкоресурсный способ виртуализации
- развитие концепции микросервисов

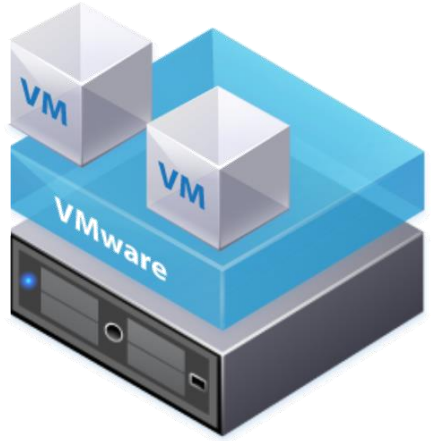


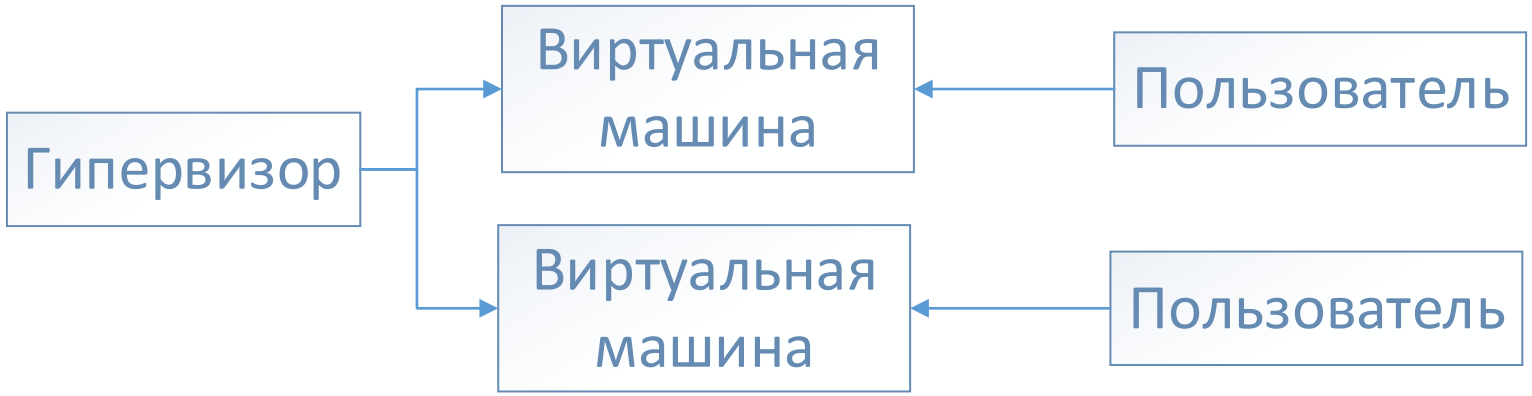
Запрос рынка: прикладное ПО, использующее СКЗИ, помещать в контейнер

Вопрос «**Безопасно ли это?**» ранее еще не прорабатывался

Средства виртуализации

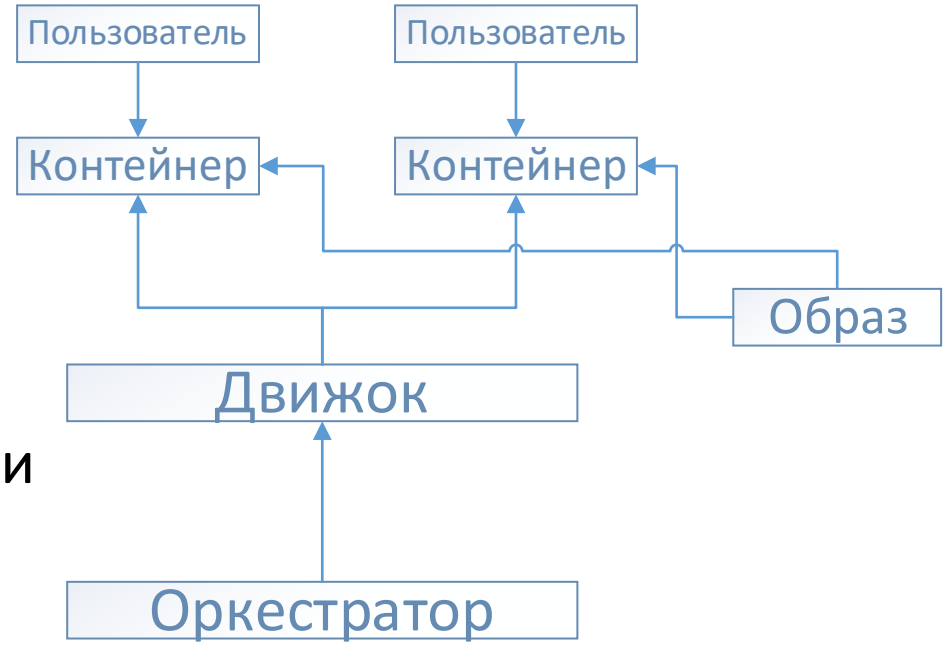
- Виртуальная машина – результат эмуляции аппаратной платформы
- Гипервизор – ПО/АС для работы с виртуальными машинами (ВМ)



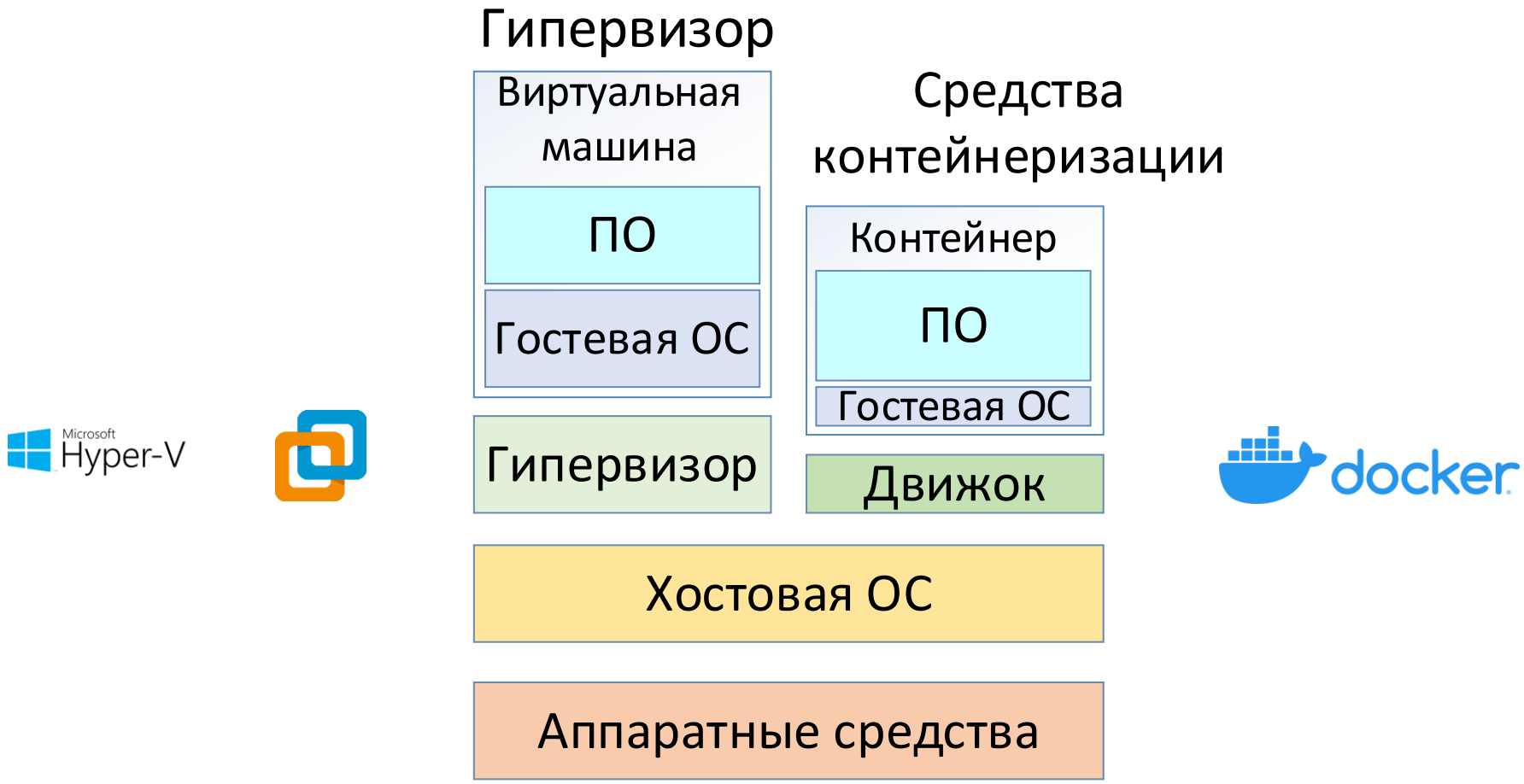


Средства виртуализации

- Образ – неизменяемый шаблон, из которого разворачивается *контейнер*, состоит из нескольких слоев
- Контейнер – исполняемый экземпляр, развернутый из образа
- Средство контейнеризации («Движок») – ПО, обеспечивающее управление работы с контейнерами
- Оркестратор – набор инструментов для управления инфраструктурой контейнеров



Сравнение средств виртуализации



Сравнение средств виртуализации

Признак	Для виртуальных машин	Для контейнеров
Разграничение доступа	Аппаратные средства и гипервизор	Ядро ОС
Уровень изоляции	Полная изоляция	Изоляция файлов внутри контейнеров
Эмулируемая ОС	Любая ОС	Того же семейства ОС, что и у основной ОС
Эмулируемое окружение	Свой набор виртуальных аппаратных средств, дисков и полная ОС	Базовый образ ОС, окружение, изолированное приложение и виртуальный сетевой интерфейс

Сравнение средств виртуализации

Признак	Для виртуальных машин	Для контейнеров
Практическое применение	Разделение крупного сервера для запуска разных ОС на изолированных ВМ	Создание низкоресурсных узлов на базе одной ОС
Средний срок жизни	До необходимости перейти на новую ОС = месяцы/годы	Средний срок жизни контейнера = сутки/недели
Пользовательское взаимодействие	Управление как в ОС, легко и удобно менять настройки внутри после запуска	Интерфейс предоставляется ПО средства контейнеризации, управление сложно и ограничено

Отличительные черты контейнеризации

- Виртуализация на уровне ядра ОС, т.е. **средства изоляции предоставляются операционной системой**
- Может работать только ОС того же семейства, что и у основной ОС
- Как правило, запускается одно приложение с включенными необходимыми библиотеками
- Малый срок жизни контейнера
- Взаимодействие с пользователями ограничено

Результаты опубликованных исследований

Рассматриваемые вопросы безопасности контейнеров

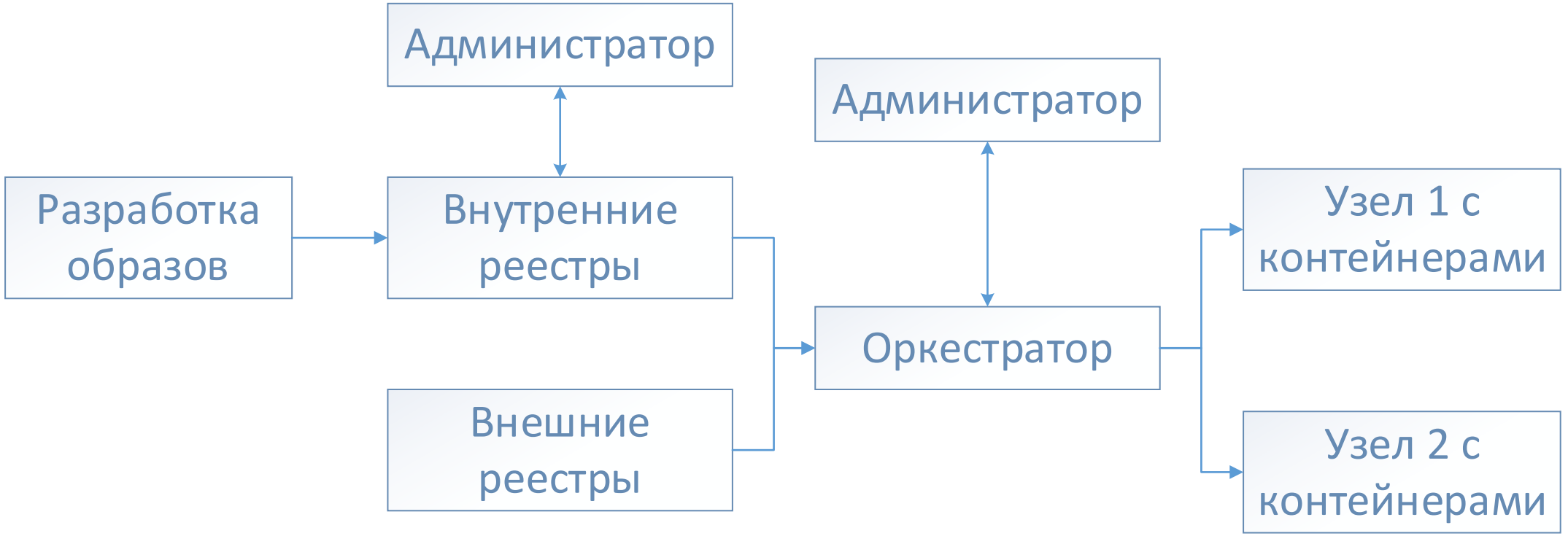
- Уязвимости контейнеров и образов
- Обеспечение целостности
  - Контроль изменения критических данных (например, конфигурационные файлы)
  - Защита критических данных от скомпрометированного узла
  - Сбор неподделываемых доказательств
  - Статический анализ (например, проверка ЭП на образе)
  - Динамический анализ (поведенческая модель, Intel SGX)
  - Удаленная аттестация

Результаты опубликованных исследований

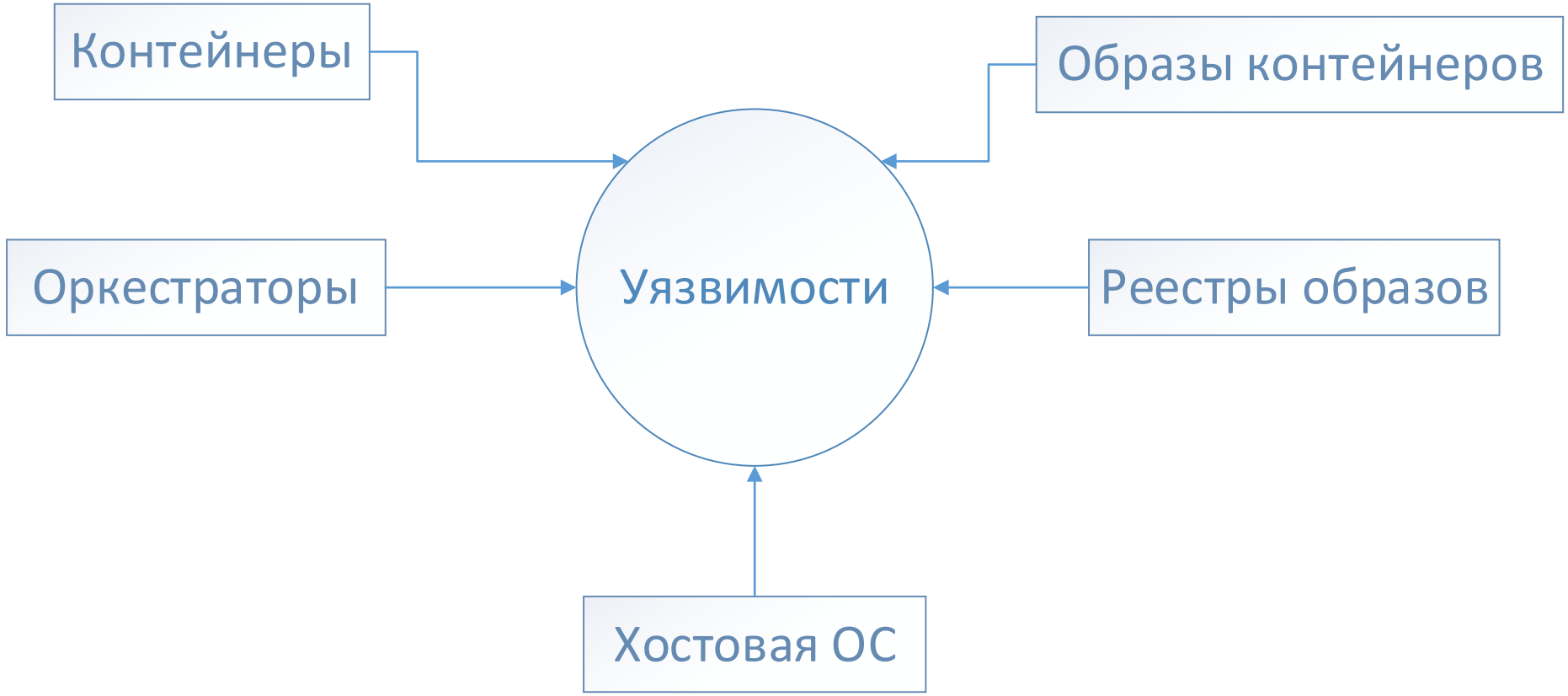
Рассматриваемые вопросы безопасности контейнеров

- Разграничение доступа к контейнерам
- Изоляция

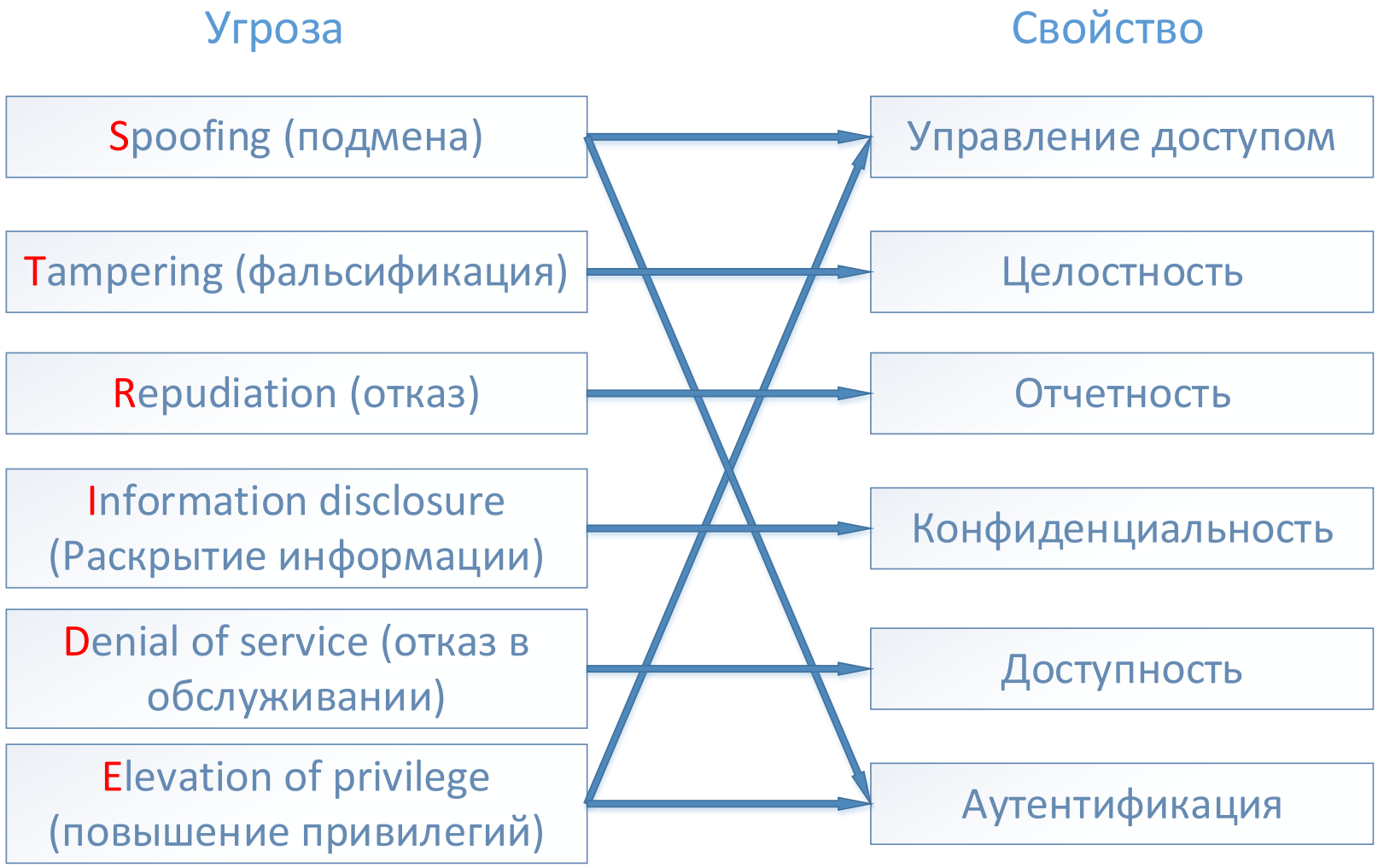
Модель NIST (SP.800-190)



Модель NIST (SP.800-190)



Организационные меры (модель STRIDE)



ФСТЭК

Функции безопасности по требованиям

- изоляция контейнеров
- выявление уязвимостей в образах контейнеров
- проверка корректности конфигурации контейнеров
- **контроль целостности контейнеров и их образов**
- **регистрация событий безопасности**

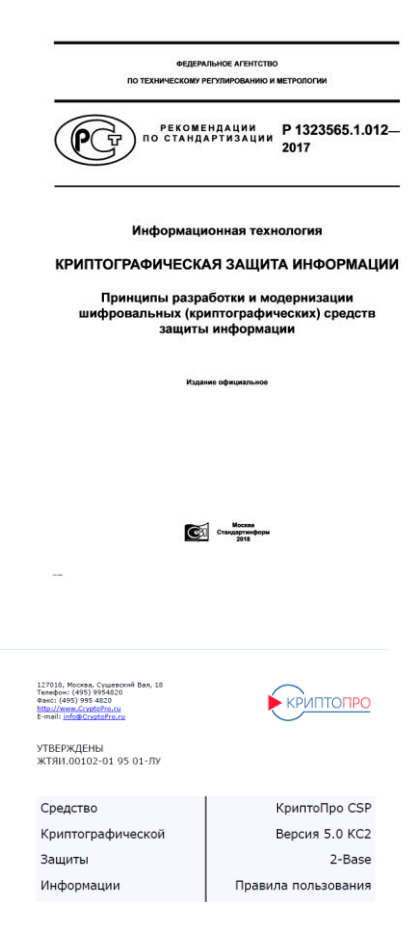
Дополнительные функции безопасности

- **управление доступом**
- **идентификация и аутентификация пользователей**
- централизованное управление образами контейнеров и контейнерами

Нормативная база по СКЗИ

1) Р 1323565.1.012-2017. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации.

2) Требования к средствам электронной подписи (Приказ ФСБ России № 796).


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ Р 1323565.1.012— 2017

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации

Издание официальное

Москва
Стандартинформ
2018

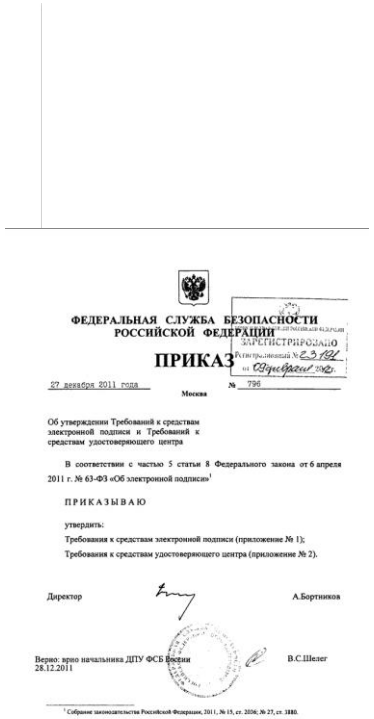
127018, Москва, Сущевский Вал, 18
Телефон: (495) 9954820
Факс: (495) 995 4820
http://www.CryptoPro.ru
E-mail: info@CryptoPro.ru

КРИПТОПРО

УТВЕРЖДЕНЫ
ЖТЯИ.00102-01 95 01-ЛУ

Средство Криптографической Защиты Информации	КриптоПро CSP Версия 5.0 KC2 2-Base Правила пользования

ЖТЯИ.00102-01 95 01
Листов 60


ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ЗАРЕГИСТРИРОВАНО

ПРИКАЗ

27 декабря 2011 года — Москва — № 796

Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра

В соответствии с частью 5 статьи 8 Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»[1]

ПРИКАЗЫВАЮ

утвердить:

Требования к средствам электронной подписи (приложение № 1);

Требования к средствам удостоверяющего центра (приложение № 2).

Директор А.Бортников

Верно: врио начальника ДПУ ФСБ России В.С.Шелег
28.12.2011

[1] Собрание законодательства Российской Федерации, 2011, № 15, ст. 2036; № 27, ст. 3880.

Дополнительные материалы

Общеприменительные требования к порядку эксплуатации, содержащиеся в Формулярах и Правилах пользования на СКЗИ.

Средства контейнеризации

Контейнеры рассматриваются только как **среда функционирования СКЗИ**.

Использование средств контейнеризации **в качестве средства защиты информации не рассматривается**.

Аспекты безопасности

1. Датчики случайных чисел
2. Аутентификация
3. Целостность
4. Дополнительные СЗИ
5. Разграничение доступа
6. Очистка памяти
7. Регистрация событий
8. Использование ключевой информации

1. ДСЧ

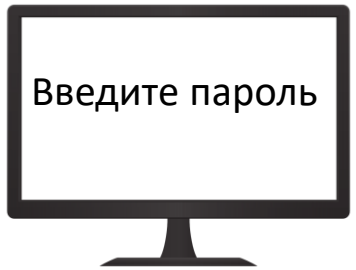
Проблема	Возможное решение
Необходимость инициализации ДСЧ без повторов	Инициализация ДСЧ с нуля для контейнеров
Биологический ДСЧ – нет интерфейса	Использование ФДСЧ или гаммы

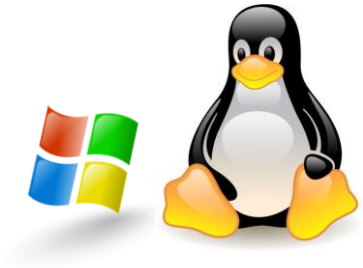
1. ДСЧ

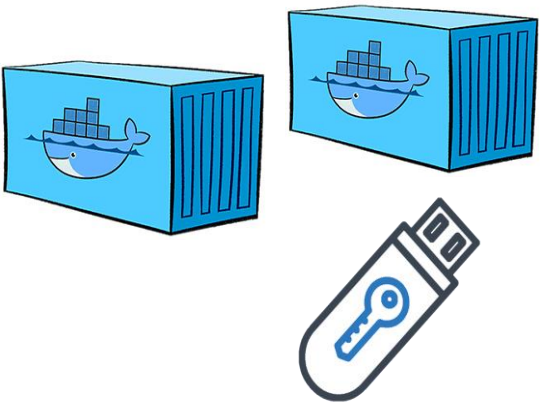
Проблема	Возможное решение
Блокировка доступа к физическому устройству	Использование гибридной инициализации (ФДСЧ + гамма)
Обращение к гамме многих контейнеров	Контроль расхода гаммы и разграничение доступа к ней

2. Аутентификация

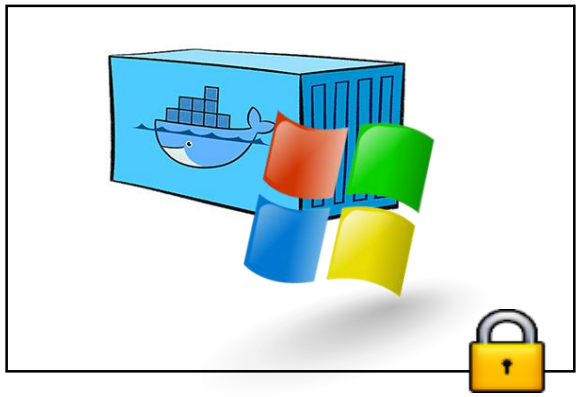
Проблема	Возможное решение
Нет возможности вручную ввести пароль доступа к ключу	Решение на уровне ППО или основной ОС Неактуально для серверов
Сложность подключения нескольких контейнеров к одному токену	Разграничение доступа к токену по времени на уровне основной ОС







3. Целостность

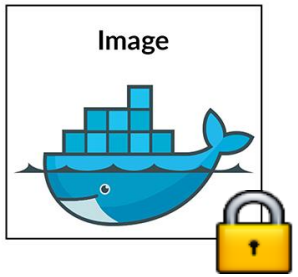


Проблема

Контроль целостности полной среды функционирования

Возможное решение

Контроль целостности с помощью СКЗИ как в основной, так и в гостевой ОС



Контроль целостности образов

Комплекс организационно-технических мер

3. Целостность

Проблема

В СКЗИ класса КС2+ используются АПМДЗ. Для файлов внутри контейнеров АПМДЗ не работает.

Возможное решение

Контроль целостности средствами АПМДЗ ядра ОС, движка, контейнеров (полностью)

Контроль целостности с помощью АПМДЗ ядра ОС, движка и с помощью отдельного средства КЦ (например, ППО или внутри ядра ОС) - файлов внутри контейнеров

4. Дополнительные СЗИ

Проблема

Совместно с СКЗИ класса КС3+ применяются дополнительные СЗИ (например, Secure Pack Rus, Замкнутая программная среда Astra Linux SE и т.д.)

Возможное решение

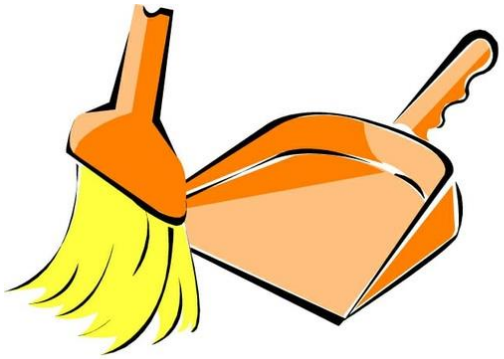
Требуется доказательство корректности работы «движков» и данных СЗИ для каждой пары «движка» и СЗИ

5. Разграничение доступа

Проблема	Возможное решение
В КСЗ атаки проводятся пользователем ИС	Корректное разграничение доступа в «движке» и в оркестраторе
Внутри ИС можно создать вредоносный образ	Сборка образов и подготовка контейнеров только администратором

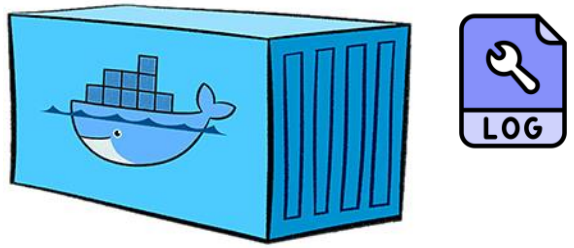
6. Очистка памяти

Проблема	Возможное решение
Завершение работы ОС внутри контейнера должно выполняться так же, как и вне контейнера	В Docker так работает, в других «движках» требуется дополнительное исследование

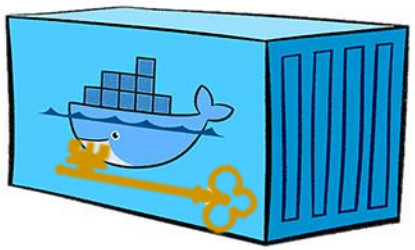


7. Регистрация событий

Проблема	Возможное решение
Короткий жизненный цикл контейнера	Сохраняем логи вне контейнеров
Для КСЗ требуется целостность логов	Контроль целостности средствами СКЗИ внутри и/или вне контейнера



8. Использование ключевой информации



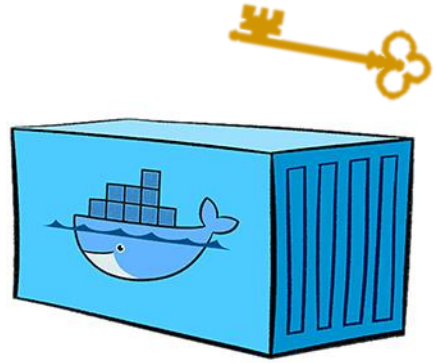
Проблема

Исследование возможности сохранения КИ в контейнерах и их последующего дублирования

Возможное решение

Хранение долговременной КИ вне контейнера

Ограничение количества контейнеров по результатам дополнительных исследований в рамках ТИ СКЗИ



Заключение

- Рассмотрена сфера применения средств контейнеризации
- Рассмотрены аспекты безопасности при функционировании прикладного ПО, использующего СКЗИ, в контейнерах
- Возникающие проблемы решаемы

Список литературы

- Рекомендации по стандартизации Р 1323565.1.012-2017. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации.
- Требования к средствам электронной подписи. Приложение №1 к приказу ФСБ России от 27 декабря 2011 г. № 796.
- Выписка из Требований по безопасности информации, утвержденных приказом ФСТЭК России от 4 июля 2022 г. № 118. Требования по безопасности информации к средствам контейнеризации (выписка).
- NIST Special Publication 800-190. Application Container Security Guide.
- M. De Benedictis, A. Lioy. Integrity verification of Docker containers for a lightweight cloud environment. Future Generation Computer Systems, vol. 97, 2019, pp. 236-246.
- Ahmadvand, M., Pretschner, A., Ball, K., Eyring, D. (2018). Integrity Protection Against Insiders in Microservice-Based Infrastructures: From Threats to a Security Framework. In: Mazzara, M., Ober, I., Salaün, G. (eds) Software Technologies: Applications and Foundations. STAF 2018. Lecture Notes in Computer Science(), vol 11176. Springer, Cham.

Список литературы

- Mullinix, Samuel P. et al. “On Security Measures for Containerized Applications Imaged with Docker.” arXiv: Cryptography and Security (2020).
- C. Munoz, F. Montoto, F. Cifuentes and J. Bustos-Jiménez, "Building a threshold cryptographic distributed HSM with docker containers," 2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON), Pucon, Chile, 2017, pp. 1-5.
- Wong, Annika et al. “Threat Modeling and Security Analysis of Containers: A Survey.” ArXiv abs/2111.11475 (2021).
- Vipin Jain, Baldev Singh, Medha Khenwar1 and Milind Sharma. Static Vulnerability Analysis of Docker Images. IOP Conference Series: Materials Science and Engineering, Volume 1131, 4th International Conference on Emerging Technologies in Computer Engineering: Data Science & Blockchain Technology (ICETCE 2021) 3rd-4th February 2021, Jaipur, India.
- A. Modak, S. D. Chaudhary, P. S. Paygude and S. R. Ldate, "Techniques to Secure Data on Cloud: Docker Swarm or Kubernetes?," 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, India, 2018, pp. 7-12

Вопросы ???

Контактная информация

Электронная почта:

puzyrev@cryptopro.ru

kdm@cryptopro.ru

Сайт:

www.cryptopro.ru