НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

Подпись ПО в процессах РБПО, обеспечении и эксплуатации доверенного ПО

infotecs

Калугина Анастасия
Руководитель направления безопасной разработки и инфраструктуры

Содержание

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

1. Введение – формулировка цели активности
2. Процессы РБП(О), как база системного подхода
3. Проблематика – причины, следствия и решение (что такое единое пространство доверия – ЕПД)
4. РБПО и использование ЕПД. Эксперимент по проработке и тестированию подхода – **подпись ПО**
5. Системы конструктивной информационной безопасности (СКИБ) в инфраструктуре. Инфраструктурные шаблоны
6. Итоги

№1.
Введение

Проблематика

Отсутствие системного подхода, гарантирующего разработку доверенных продуктов (ПО)

Верхнеуровневая цель

Разработка и регламентация системного подхода,

гарантирующего решение существующих проблем в части обеспечения доверия продуктов российской разработки

№2.
Процессы РБП

Термины и определения

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

Терминология:

- **РБПО** (ГОСТ 56939) – разработка безопасного **ПО**
- **РБП*** (ИнфоТеКС) – разработка безопасных **продуктов** (ПО программных и программно-аппаратных комплексов ViPNet)

- **ЖЦП** – жизненный цикл продуктов

* **РБП**, а не РБПО - это осознанный подход ИнфоТеКС, т.к. использование продуктов потребителями – это про продукт. И необходимо обеспечивать безопасность **конечного продукта**

ГОСТ 56939-2024 (1/2)

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

5.1 Планирование процессов разработки

5.2 Обучение сотрудников

5.3 Формирование требований безопасности продуктов

5.4 Управление конфигурацией продуктов

5.5 Управление недостатками и запросами на изменение

5.6 Безопасность архитектуры продуктов

5.7 Моделирование угроз и разработка описания поверхности атаки

5.8 Формирование правил кодирования

5.9 Экспертиза исходного кода

5.10 Статический анализ

5.11 Динамический анализ

5.12 Безопасная система сборки

5.13 Безопасность сборочной среды

5.14 Обеспечение целостности кода

ГОСТ 56939-2024 (2/2)

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

5.15 Обеспечение безопасности используемых секретов

5.16 Композиционный анализ

5.17 Безопасность цепочки поставок

5.18 Функциональное тестирование

5.19 Нефункциональное тестирование

5.20 Безопасности выпуска версии продукта

5.21 Безопасная доставка продуктов пользователям

5.22 Техническая поддержка продуктов на этапе эксплуатации

5.23 Управление уязвимостями

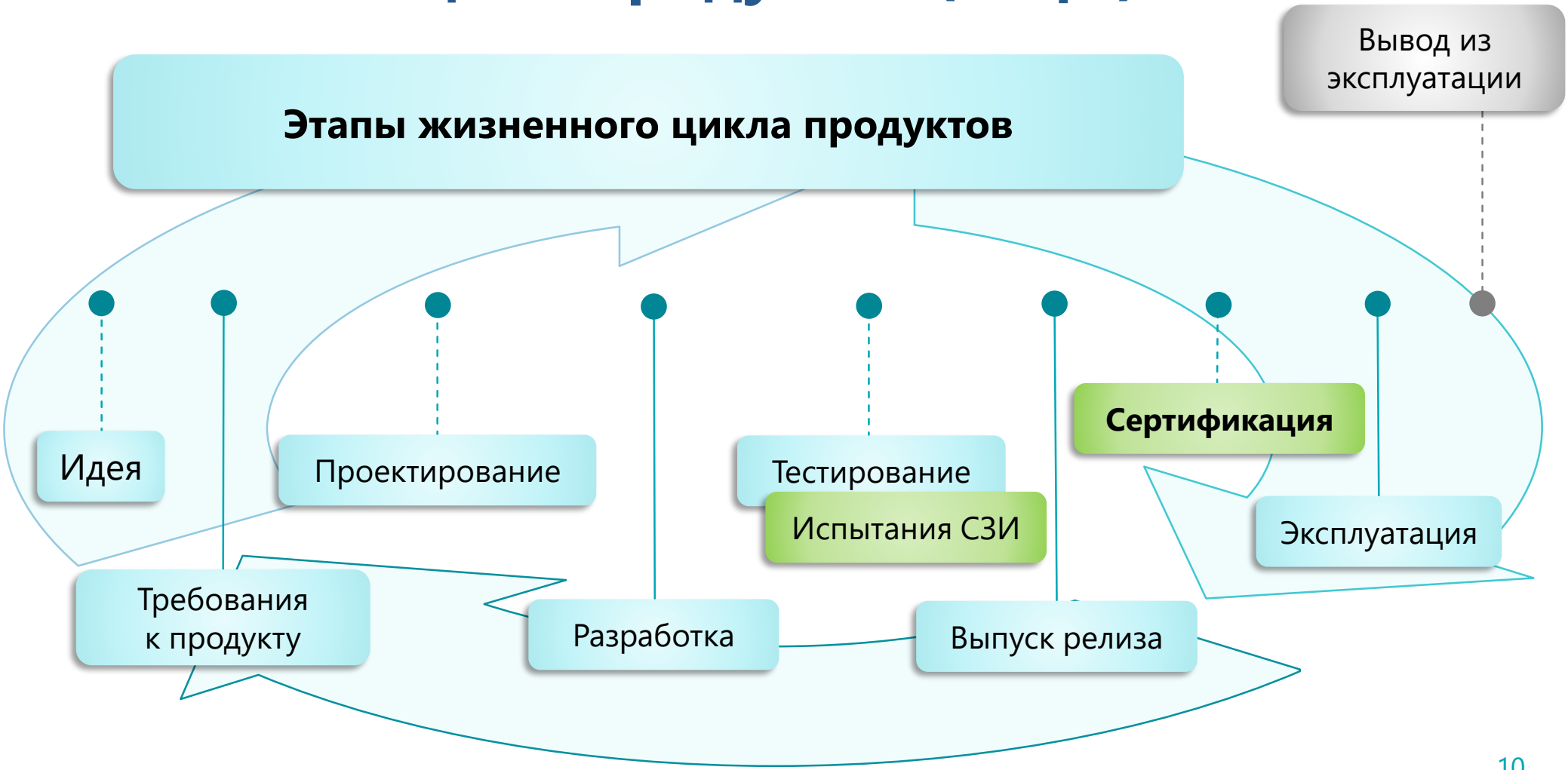
5.24 Поиск уязвимостей в продуктах на этапе эксплуатации

5.25 Обеспечение безопасности при выводе продуктов из эксплуатации

* Выделенные **жирным** применяются на всех (либо большинстве) этапов ЖЦП

Жизненный цикл продуктов (ЖЦП)

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ



Сопоставление ГОСТ-56939 и ЖЦП

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

infotecs

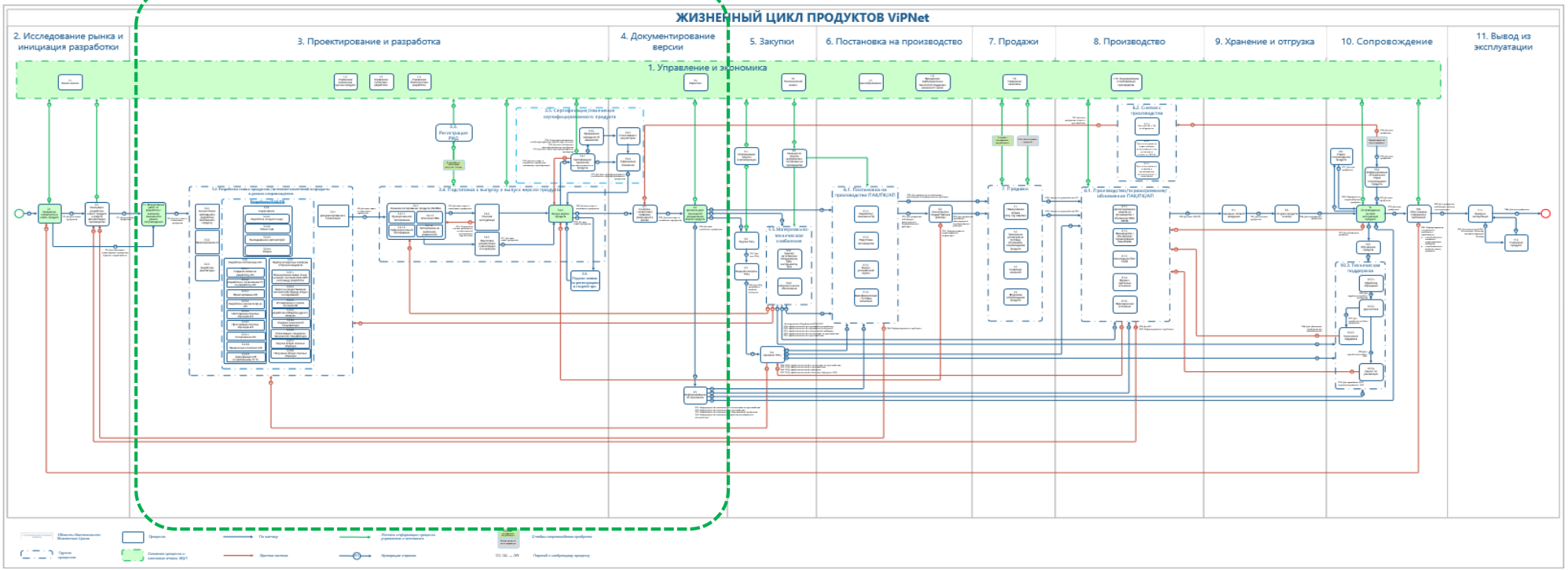
Разработка продукта на практике

Схема ЖЦ продуктов ViPNet в ИнфоТеКС

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

infotecs

Разработка



Для всех разрабатываемых продуктов ViPNet, включая продукты СКЗИ, применяются требования, практики и механизмы РБП

Сертификация процессов РБП

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

Сертификат №4 ФСТЭК России

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4

Выдан: 8 апреля 2025 г.
Действителен до: 8 апреля 2030 г.

Настоящий сертификат удостоверяет, что процессы безопасной разработки, реализованные акционерным обществом «Информационные технологии и коммуникационные системы» (АО «ИнфоТеКС»), соответствуют требованиям национального стандарта ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования», утвержденного и введенного в действие приказом Федерального агентства по техническому регулированию и метрологии от 1 июня 2016 г. № 458-ст.

Сертификат выдан на основании результатов сертификации, проведенной органом по сертификации федерального государственного бюджетного учреждения науки Институт системного программирования им. В.П. Иванникова Российской академии наук (аттестат аккредитации от 24.05.2024 № СЗИ RU.0001.01БИ00.А009) - экспертное заключение от 21.03.2025.

ПЕРВЫЙ ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Подход infotecs комплексный:

- Обеспечиваем безопасность разрабатываемых продуктов
- Выстраиваем процессы РБПО/РБП (требования ФСТЭК)
- Участвуем в работе **Центра исследований безопасности системных ПО** под управлением ИСП РАН

2014
iSDL.v0
(пилот)

2016
ГОСТ 56939-2016
iSDL.v1

2018
iSDL.v2

2023
iSDL.v3

2024
ГОСТ 56939-2024

2025
Сертификат РБП ФСТЭК России

SDL – Secure Development LifeCycle
iSDL – адаптированный под ИнфоТеКС SDL

№3.
Проблематика

Проблемы: причины и следствия

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

- Обеспечение доверенного распространения ПО, его целостности и подлинности невозможно без применения криптографических механизмов. Однако, в России использование для этого средств ЭП не регулируется
- В ГОСТ 56939 РБПО не описаны механизмы обеспечения целостности и подлинности ПО, как в самих процессах, так и конечного результата (ПО)
- Разработчики отечественных ПО/ОС/оборудования используют либо базовые (основанные на зарубежной криптографии механизмы целостности ПО), либо реализуют что-то свое независимо друг от друга
- Отсутствуют стандартизованные в России подходы к реализации концепции аппаратного корня доверия

Проблемы: причины и следствия

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

- «Стихийная» реализация подписи ПО может создать иллюзию безопасности и дискредитировать общую полезную идею
- Потребители не будут заниматься организацией проверки подписи ПО для множества независимых вендорских реализаций
- В промышленных ИС и IoT ручные проверки практически не применимы

Проблематика в механизмах

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

Отсутствуют:

- Системный подход при разработке ПО/АП в части обеспечения:
  - целостности и подлинности разрабатываемого ПО/АП;
  - шифрования TLS соединений;
  - аутентификации субъектов и объектов взаимодействия
- **Типовые** решения с использованием российских криптоалгоритмов
- Корневой доверенный УЦ
- Нормативное регулирование по каждой проблеме
- Технологическая независимость

Что делать?

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

Формировать технологическую основу на базе российских средств PKI и СКЗИ с единым центром выработки технических и организационных мер с требованиями ко всем участникам взаимодействия различных цифровых платформ и сервисов, реализующих **единое пространство доверия (ЕПД)**.

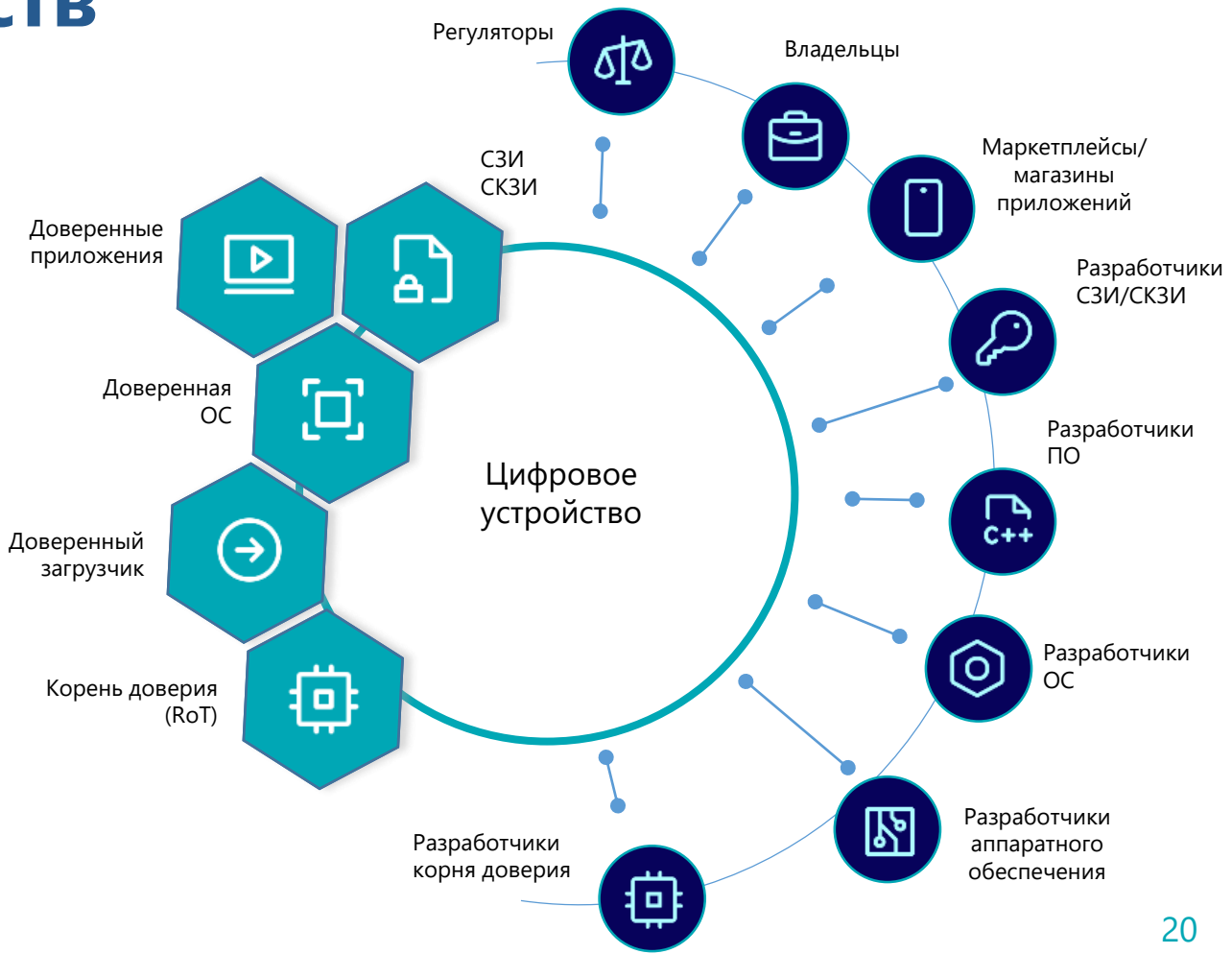
Суть подхода – возможность построение криптографически верифицируемых цепочек выполнения доверенного российского ПО на доверенных российских ОС и доверенном российском оборудовании. Цель – обеспечение надежной идентификации всех участников взаимодействия и повышения общего уровня безопасности функционирования тех или иных ИС (в первую очередь ГИС и КИИ) **на всех этапах их жизненного цикла**.

Подход должен применяться к любому ПО и ПАК, которые должны быть доверенными, а не только к СКЗИ/СЗИ!

Единое пространство доверия цифровых устройств

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

- Доверенные цифровые устройства и базовые аппаратные/программные элементы доверия безопасности (корни доверия)
- Доверенная среда исполнения ПО на цифровых устройствах
- Доверенная среда взаимодействия участников цифровых платформ и сервисов



№4.
РБПО и ЕПД

ГОСТ 56939 – безопасность инфраструктуры

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

5.1 Планирование процессов разработки

5.2 Обучение сотрудников

5.3 Формирование требований безопасности продуктов

5.4 Управление конфигурацией продуктов

5.5 Управление недостатками и запросами на изменение

5.6 Безопасность архитектуры продуктов

5.7 Моделирование угроз и разработка описания поверхности атаки

5.8 Формирование правил кодирования

5.9 Экспертиза исходного кода

5.10 Статический анализ

5.11 Динамический анализ

5.12 Безопасная система сборки

5.13 Безопасность сборочной среды

5.14 Обеспечение целостности кода

ГОСТ 56939 – безопасность инфраструктуры

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

5.15 Обеспечение безопасности используемых секретов в коде и конфигурации

5.16 Композиционный анализ

5.17 Безопасность цепочки поставок

5.18 Функциональное тестирование

5.19 Нефункциональное тестирование

5.20 Безопасности выпуска версии продукта

5.21 Безопасная доставка продуктов пользователям

5.22 Техническая поддержка продуктов на этапе эксплуатации

5.23 Управление уязвимостями

5.24 Поиск уязвимостей в продуктах на этапе эксплуатации

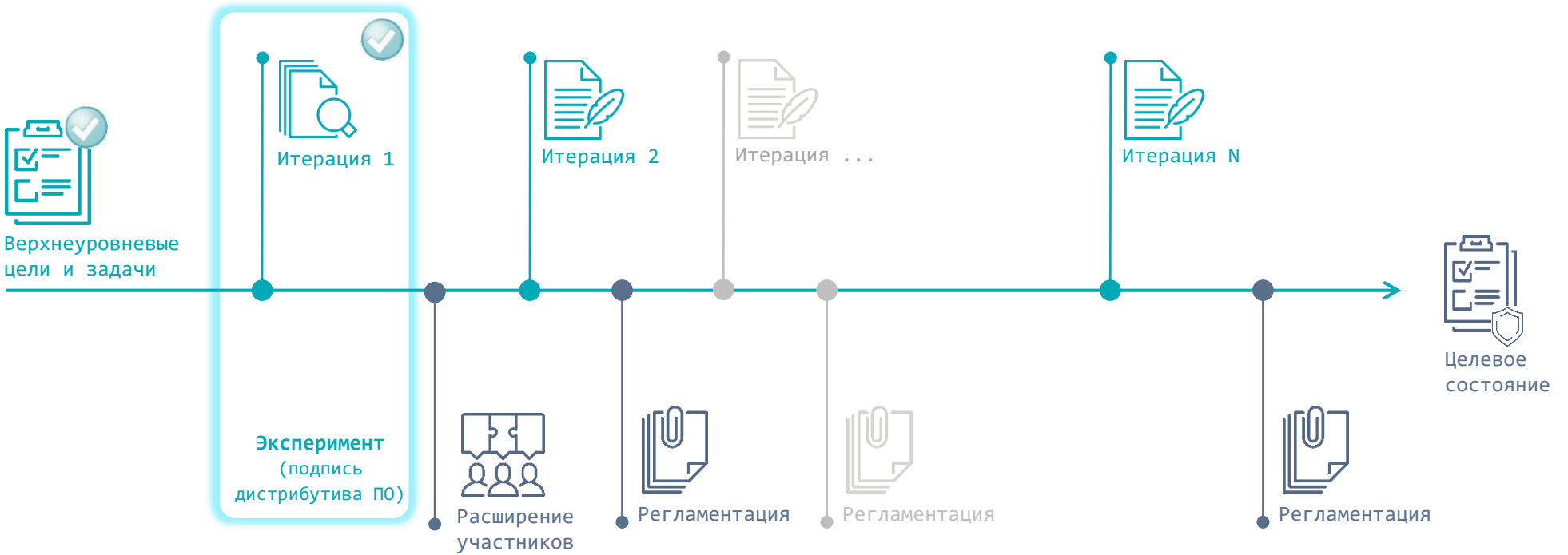
5.25 Обеспечение безопасности при выводе продуктов из эксплуатации

* Выделенные **жирным** применяются на всех (либо большинстве) этапов ЖЦП

РБПО + ЕПД – стихийная РГ вендоров

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

Подход прорабатываем итерационно:
Фиксируем верхнеуровневые цели и задачи, проводим первичную оценку, формируем дорожную карту планируемых работ



Подпись дистрибутива ПО

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

Выравнивание формулировки объекта управления:

- **Code Sign*** (короткая формулировка) – подписание кода
- **Code Sign** (полная формулировка) – это процесс цифровой подписи **исполняемого кода** (т.е. дистрибутива конечного продукта) и ее последующей проверки потребителем

На 1 итерации рассматриваем 1 объект, для которого на финальном этапе разработки необходимо гарантировать целостность и подлинность – этим объектом является **дистрибутив ПО**

* **Code Sign** (подписание кода) многими разработчиками прикладного ПО термин некорректно воспринимается, как подпись «исходного кода»

№5.
СКИБ в инфраструктуре

Подпись дистрибутива и СКИБ

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

Конструктивная безопасность в инфраструктуре организации-разработчика с использованием механизмов PKI для обеспечения целостности и подлинности **дистрибутивов ПО**

Общая схема ЕПД в организации

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

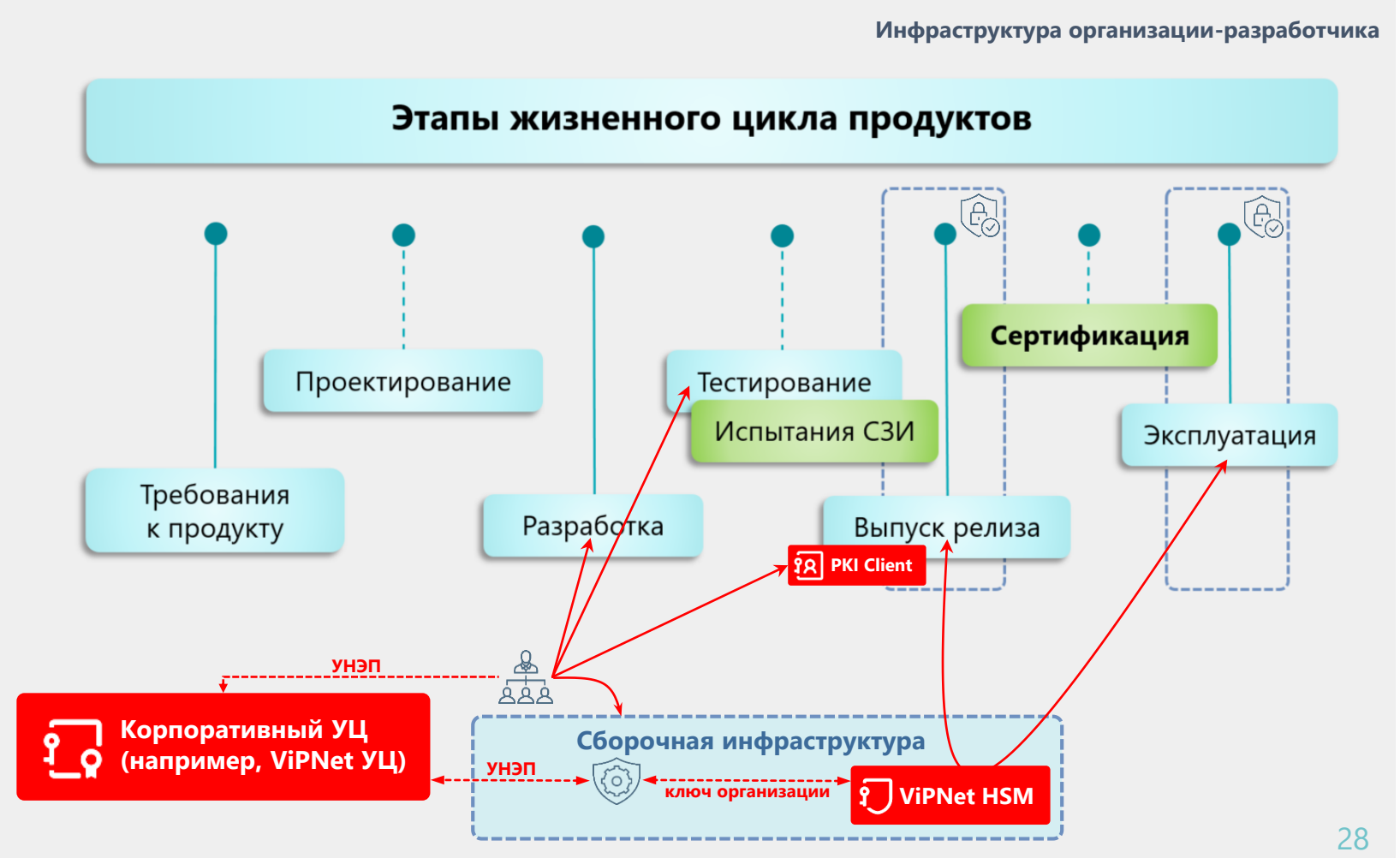
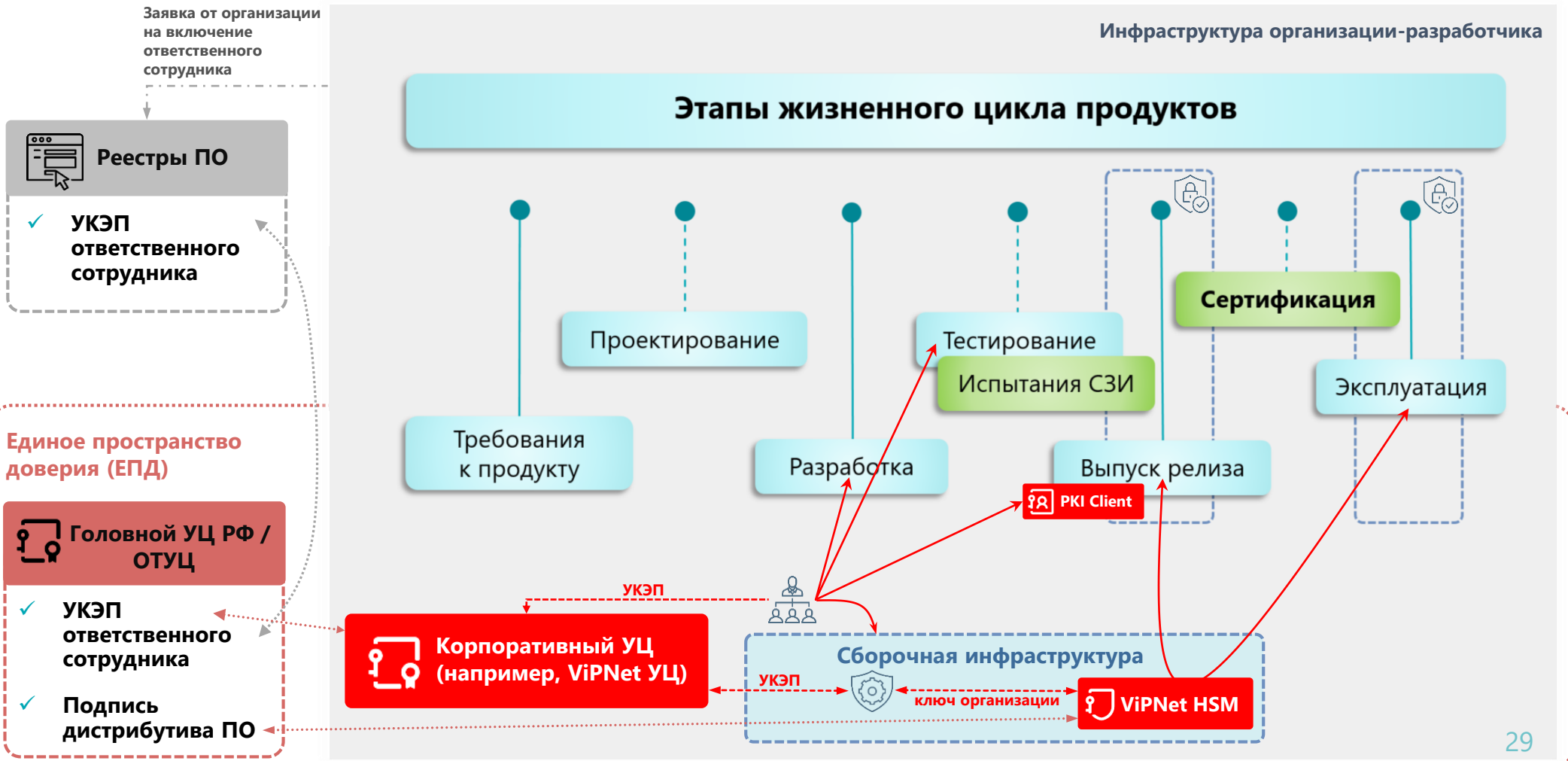


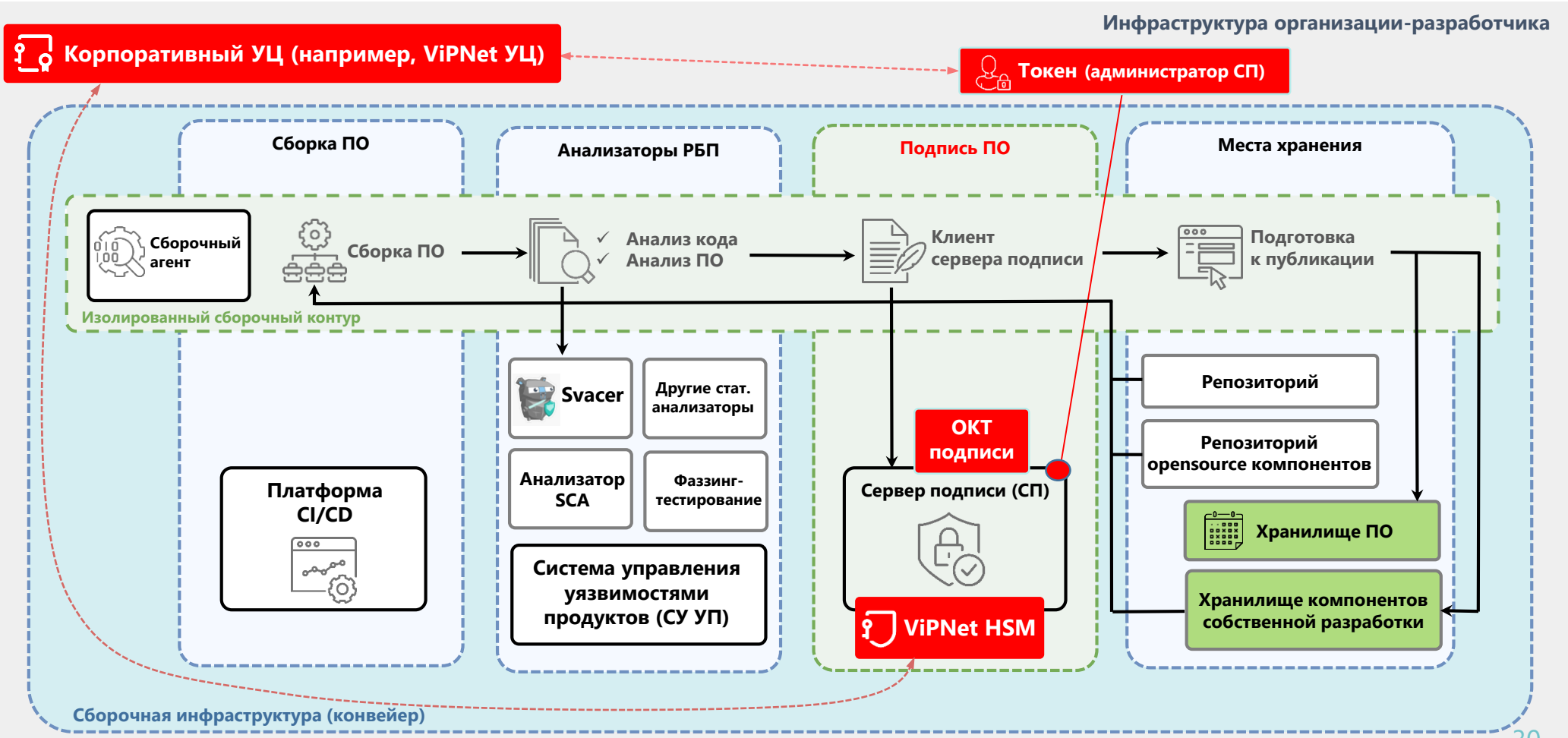
Схема ЕПД в границах страны

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ



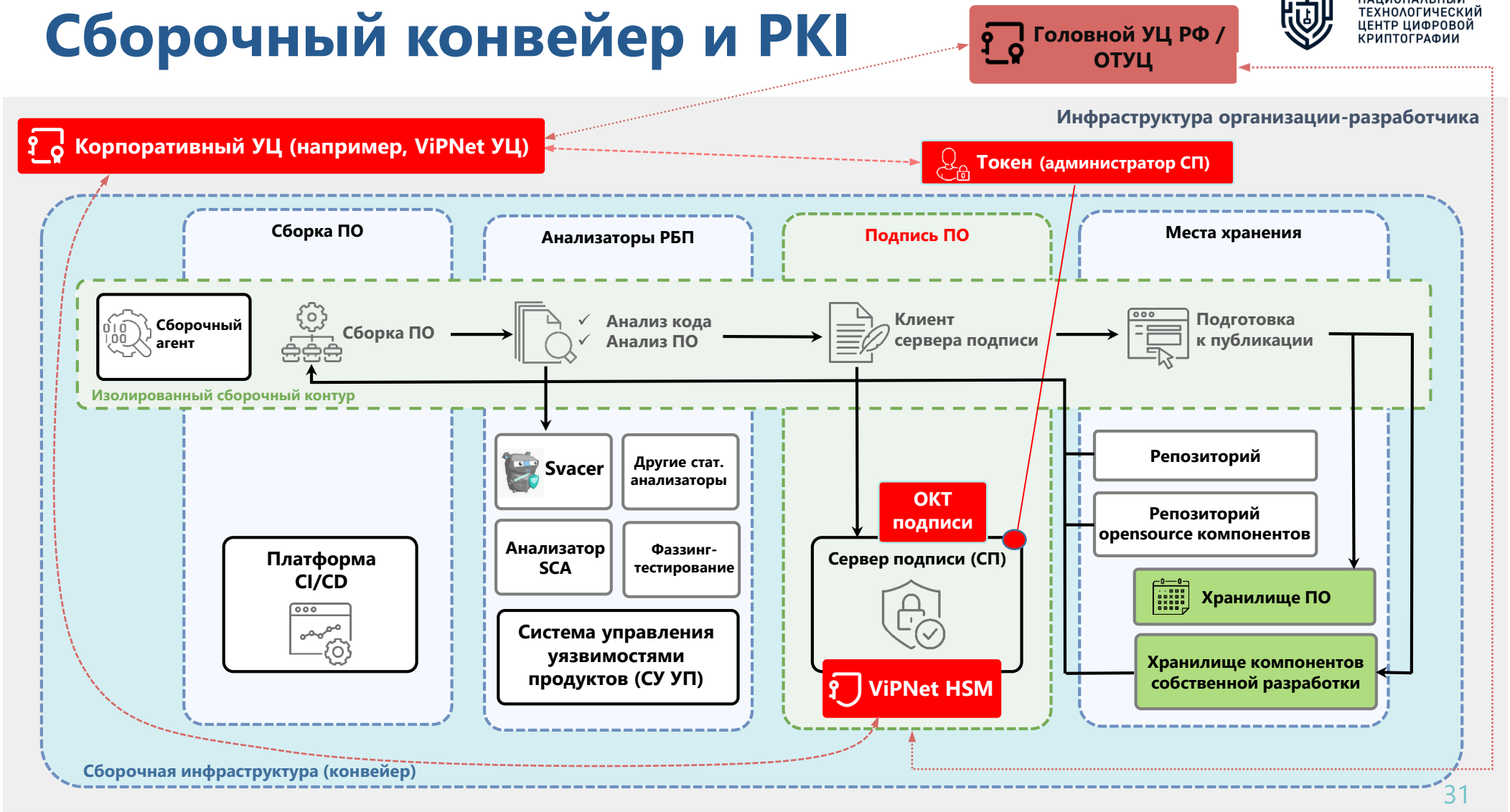
Сборочный конвейер и PKI

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ



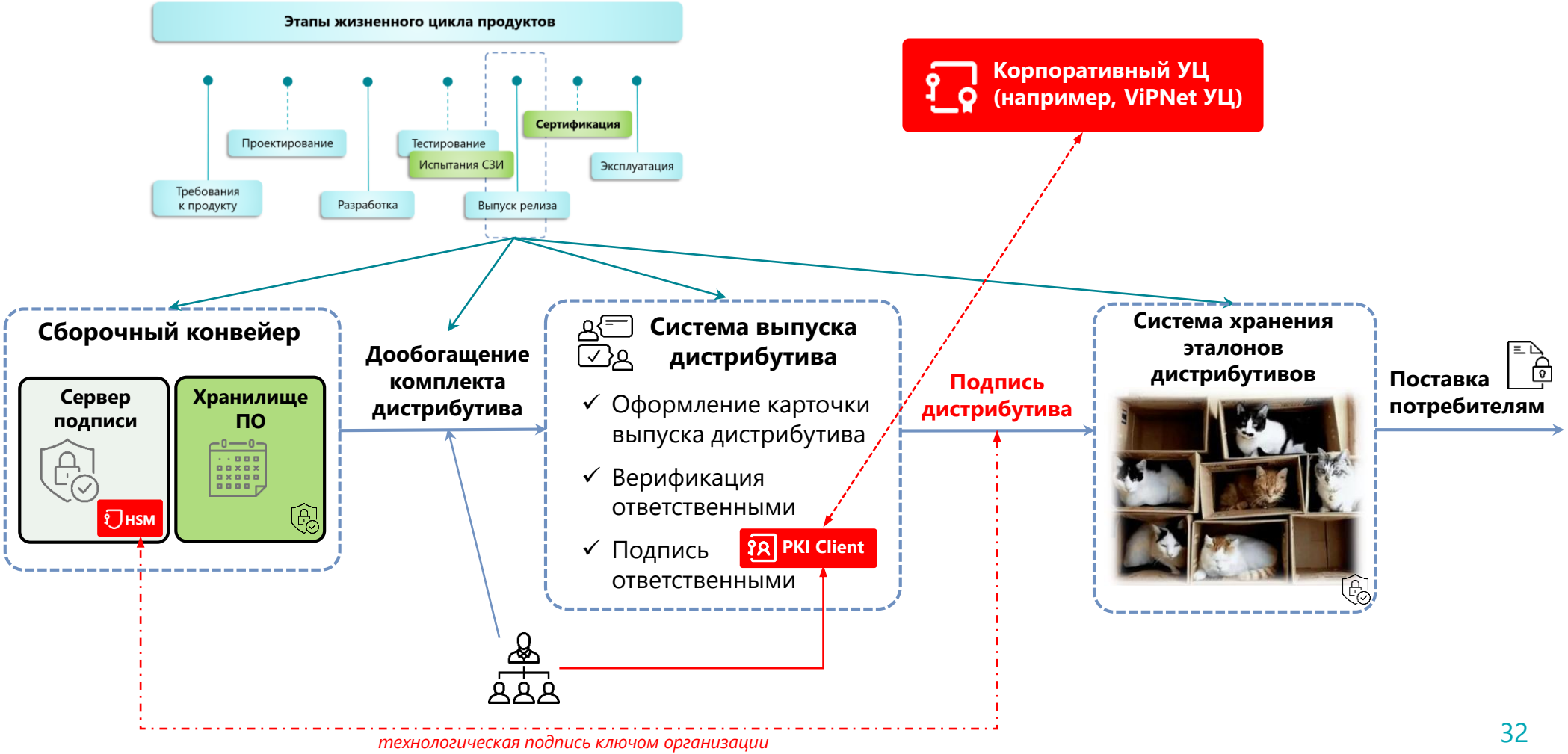
Сборочный конвейер и PKI

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ



Выпуск дистрибутива продукта

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ



Проверка подписи потребителями

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

- **Варианты проверки подписи потребителями**
  - Ручная проверка
  - Автоматизированная проверка
  - Проверка средствами ОС (аппаратный корень доверия)
- **Верификация подписи ПО в реестрах**

Проверка дистрибутива у потребителя

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

Дистрибутив продукта

- ✓ Открытый ключ ИнфоТеКС
- ✓ Открепленная подпись дистрибутива

Система проверки целостности и подлинности продукта при установке и эксплуатации

- ✓ Ручная проверка — **PKI Client**
- ✓ Проверка при установке, обновлении и функционировании
- ✓ Проверка средствами ОС — **Аппаратный корень доверия(!)**

Целостность и подлинность в реестрах

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

Открытые реестры ПО

✓ Внесение дистрибутива ПО в реестр ответственным сотрудником

Механизмы проверки целостности и подлинности релиза

PKI Client

№6. Подход: Итог

Верхнеуровневая цель

Разработка и регламентация системного подхода,
гарантирующего решение существующих проблем в части обеспечения доверия продуктов российской разработки

Задачи

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

Разработать
(направления)

- Требования к механизмам и технологиям
- Требования по типовому конфигурированию инфраструктуры
- Требования к жизненному циклу сертификатов
- Требования к организации процессов взаимодействия (всех участников взаимодействия)

Регламентация

- Определение корневых доверенных УЦ
- Нормативное регулирование по каждому направлению

Единое пространство доверия

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

ЕПД

Цель

Задачи

РБПО

Выполнение задач

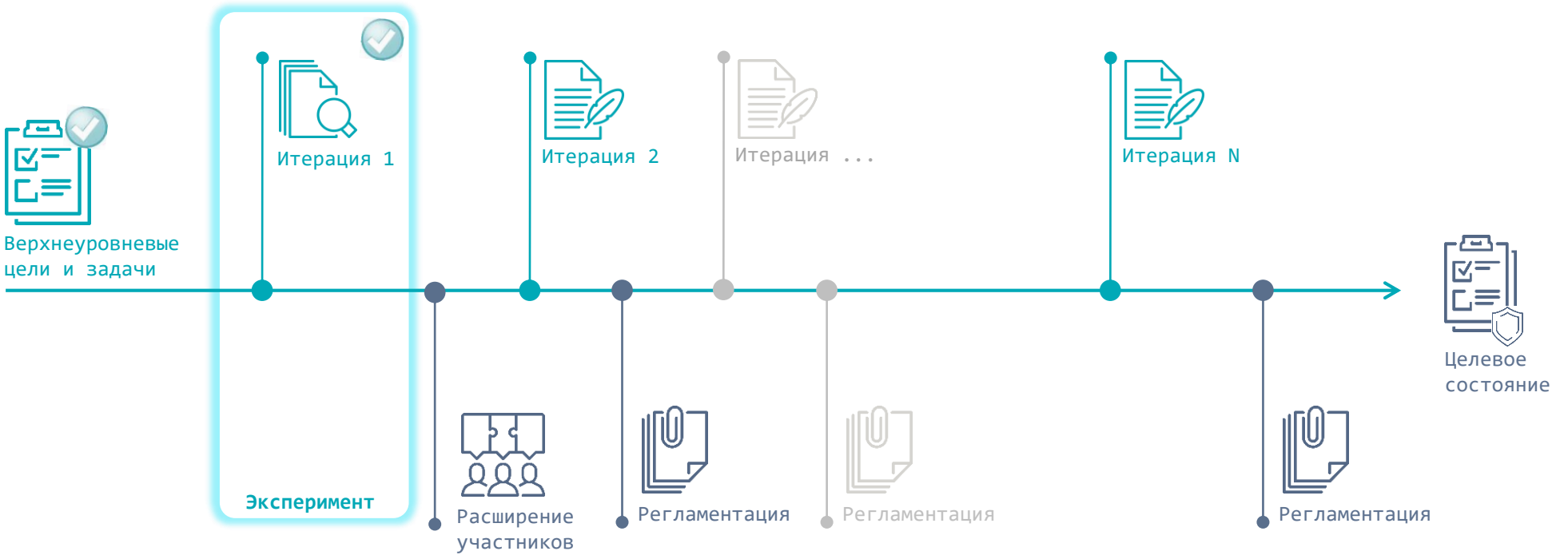
- Технические и организационные меры на базе требований ко всем участникам взаимодействия
- На всех этапах жизненного цикла ПО
- С использованием механизмов PKI

Позволяют сформировать **единое пространство доверия (ЕПД)**

Итерационный подход

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

Подход прорабатываем итерационно:
Фиксируем верхнеуровневые цели и задачи, проводим первичную оценку, формируем дорожную карту планируемых работ



Итоги эксперимента

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

Первая итерация в виде эксперимента по подписи дистрибутива ПО находится в статусе завершения

Достигнуты цели

- ✓ Разработан проект подхода на примере решения проблемы обеспечения целостности и подлинности дистрибутива ПО
- ✓ ОТУЦ использовался в качестве корневого доверенного УЦ
- ✓ Протестировано использование системы ОТУЦ при кросс-верификации целостности и подлинности дистрибутивов ПО
- ⚑ Привлечь более широкий круг заинтересованных организаций к проработке и регламентации системного подхода

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

Спасибо за внимание!

Москва
info@ntc-cc.ru