

План вебинара

Расскажем

- какие есть мастер-ключи
- зачем менять мастер-ключи
- как выглядит смена мастер-ключей на временной шкале

Заполним

- чек-лист подготовки сети к смене мастер-ключей

Покажем

- подготовку к смене мастер-ключей
- как контролировать процесс
- смену мастер-ключей

Коротко про мастер-ключи

Создает ключевой центр управляющего ПО для защищенных VPN-соединений между узлами

Срок действия – 1 год

При компрометации мастер-ключей их смена выполняется внепланово

Зачем менять мастер-ключи

Смена мастер-ключей – это регламентная процедура

Безопасность



Администратор повышает степень защищенности своей сети от компрометации

Требования регулятора



В Правилах пользования зафиксирована необходимость регулярно менять мастер-ключи

Какие есть мастер-ключи



МАСТЕР - КЛЮЧИ

МАСТЕР-КЛЮЧИ

Внутрисетевые

Используют узлы своей сети для связи и Prime для защиты этих ключей

Межсетевые

Используют узлы своей сети и узлы доверенной сети для связи между собой

МАСТЕР - КЛЮЧИ

Внутрисетевые

Межсетевые





- *Используют узлы 4 поколения*
- *Всегда на ГОСТ 28147-89*
- *Создаются сразу на всю сеть*
- *Аналогично ключам в УКЦ*

МАСТЕР-КЛЮЧИ

Внутрисетевые

Межсетевые

Сети

- Используют узлы 4 поколения
- Всегда на ГОСТ 28147-89
- Создаются сразу на всю сеть
- Аналогично ключам в УКЦ

Организации

- Используют узлы 5 поколения
- Могут быть как на ГОСТ 28147-89, так и на ГОСТ 34.12-2015
- Влияют на сегмент сети (организацию, пару организаций)
- Ключи появляются только в Prime

МАСТЕР-КЛЮЧИ

Внутрисетевые

Межсетевые

Сети

Организации

v.4

ГОСТ
28147-89

v.5

ГОСТ
28147-89

ГОСТ
34.12-2015

МАСТЕР-КЛЮЧИ

Внутрисетевые

Межсетевые

Сети

v.4

ГОСТ
28147-89

Организации

v.5

ГОСТ
28147-89ГОСТ
34.12-2015

Персональные ключи

Ключи защиты

Ключи обмена

МАСТЕР-КЛЮЧИ

Внутрисетевые

Межсетевые

Сети

v.4

ГОСТ
28147-89

Персональные ключи

Ключи защиты

Ключи обмена

Организации

v.5

ГОСТ
28147-89ГОСТ
34.12-2015

Ключи защиты обновлений

Ключи обмена

Ключи обмена внутри организации

Ключи обмена с узлами Core Network

Технические ключи обмена

Ключи обмена с другой организацией (МОВ)

МАСТЕР-КЛЮЧИ

Внутрисетевые

Межсетевые

Сети

v.4

ГОСТ
28147-89

Персональные ключи

Ключи защиты

Ключи обмена

Организации

v.5

ГОСТ
28147-89

ГОСТ
34.12-2015

Ключи защиты обновлений

Ключи обмена

Ключи обмена внутри организации

Ключи обмена с узлами Core Network

Технические ключи обмена

Ключи обмена с другой организацией (МОВ)

МАСТЕР-КЛЮЧИ

Внутрисетевые

Межсетевые

Сети

v.4

ГОСТ
28147-89

Персональные ключи

Ключи защиты

Ключи обмена

Организации

v.5

ГОСТ
28147-89

ГОСТ
34.12-2015

Ключи защиты обновлений

Ключи обмена

Ключи обмена внутри организации

Ключи обмена с узлами Core Network

Технические ключи обмена

Ключи обмена с другой организацией (МОВ)

МАСТЕР-КЛЮЧИ

Внутрисетевые

Межсетевые

Сети

v.4

ГОСТ
28147-89

Персональные ключи

Ключи защиты

Ключи обмена

Организации

v.5

ГОСТ
28147-89ГОСТ
34.12-2015

Ключи защиты обновлений

Ключи обмена

Ключи обмена внутри организации

Ключи обмена с узлами Core Network

Технические ключи обмена

Ключи обмена с другой организацией (МОВ)

МАСТЕР-КЛЮЧИ

Внутрисетевые

Межсетевые

Сети

v.4

ГОСТ
28147-89

Персональные ключи

Ключи защиты

Ключи обмена

Организации

v.5

ГОСТ
28147-89

ГОСТ
34.12-2015

Ключи защиты обновлений

Ключи обмена

МАСТЕР-КЛЮЧИ

Внутрисетевые

Межсетевые

Сети

v.4

ГОСТ
28147-89

Организации

v.5

ГОСТ
28147-89

ГОСТ
34.12-2015

1 **Персональные ключи**

Ключи защиты обновлений

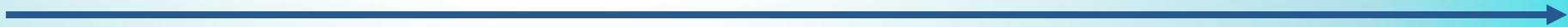
2 Ключи защиты

Ключи обмена

Ключи обмена

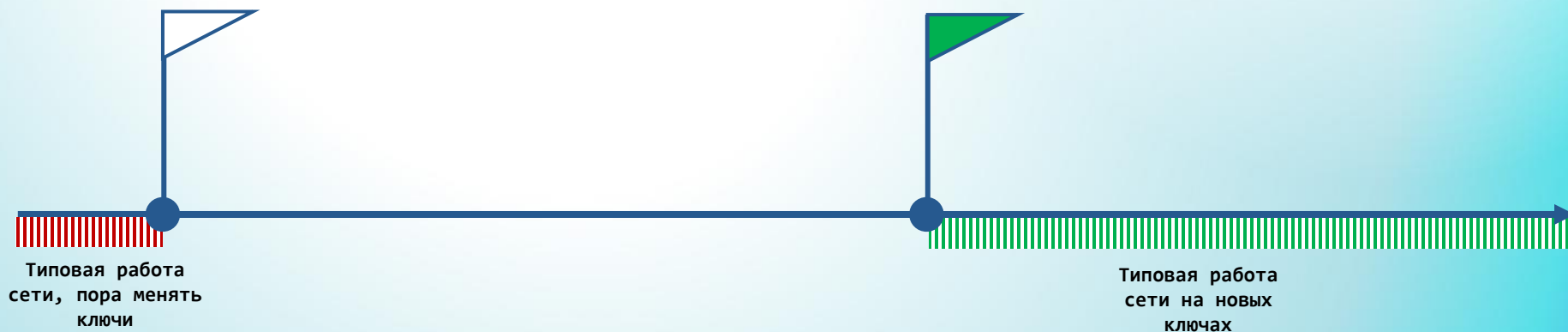
Смена мастер-ключей сети на временной шкале

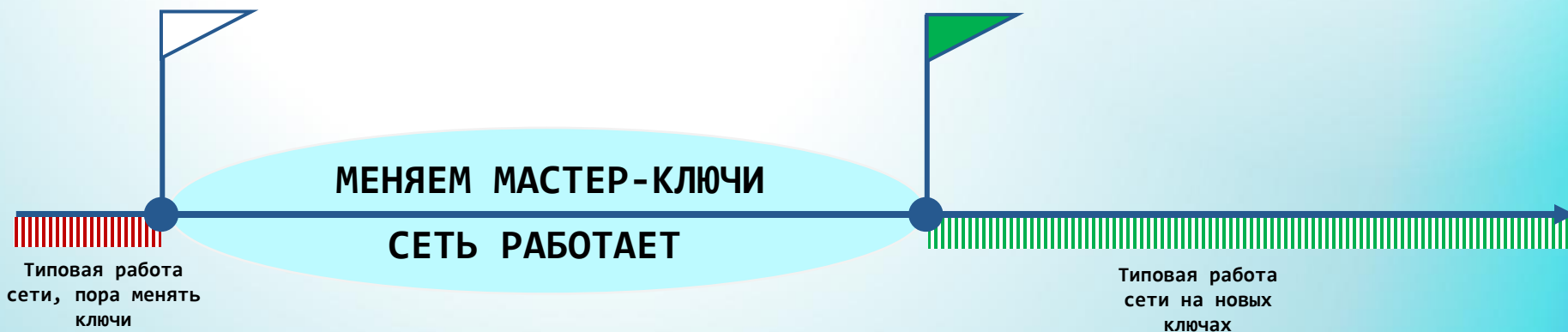






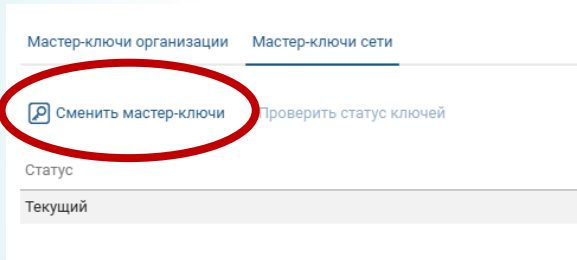
Типовая работа
сети, пора менять
ключи







Типовая работа
сети, пора менять
ключи



ЭТАП 1.
ОТПРАВКА ПЕРСОНАЛЬНЫХ
КЛЮЧЕЙ.



  Отправлено
 Доставлено
 Принято
 Ошибка



A



Начало смены
мастер-ключей







ЭТАП 1.
ОТПРАВКА ПЕРСОНАЛЬНЫХ
КЛЮЧЕЙ



Отправляется в
единственном
экземпляре!

A

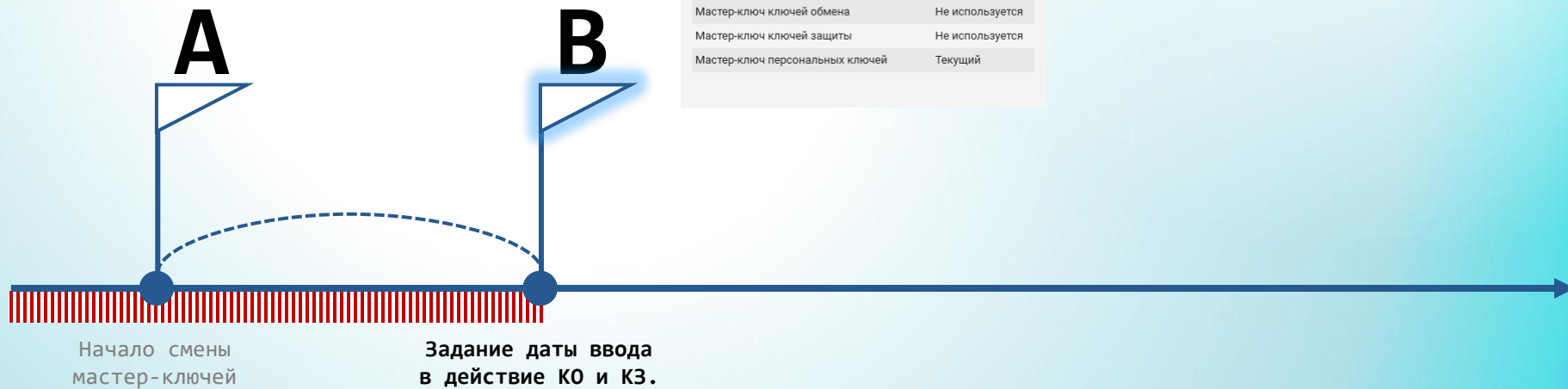
B

Типовая работа сети
сохраняется

Пока ПК не применяются на
всех узлах 4 поколения

Начало смены
мастер-ключей





Мастер-ключи сети



Запланируйте дату и время отложенной установки на узлах новых ключей защиты и новых ключей обмена.

Запланировать

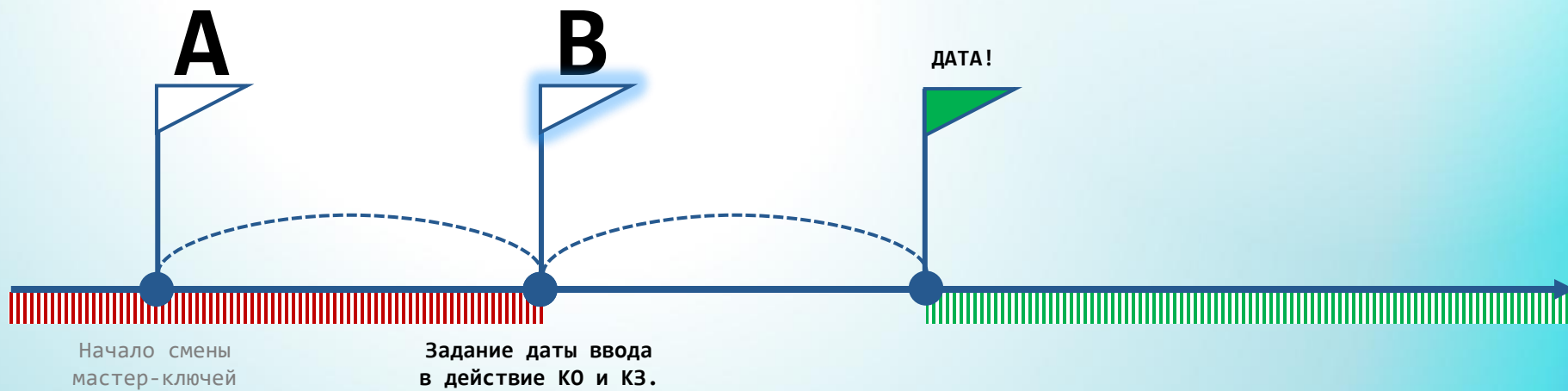
Срок действия 08.05.2026-08.05.2027

Статус Ввод в действие

Состав набора мастер-ключей сети

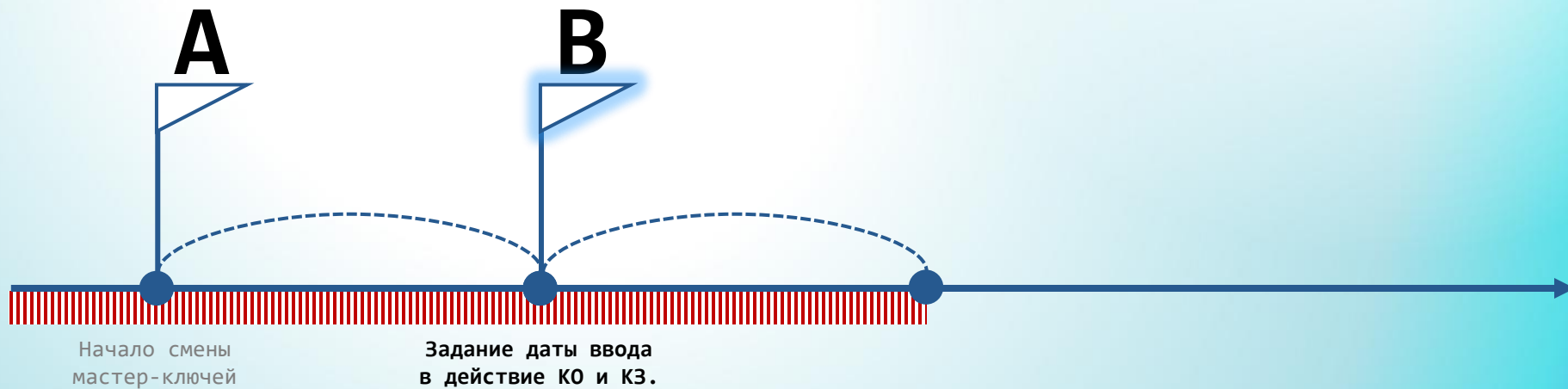
Мастер-ключ	Статус
Мастер-ключ ключей обмена	Не используется
Мастер-ключ ключей защиты	Не используется
Мастер-ключ персональных ключей	Текущий



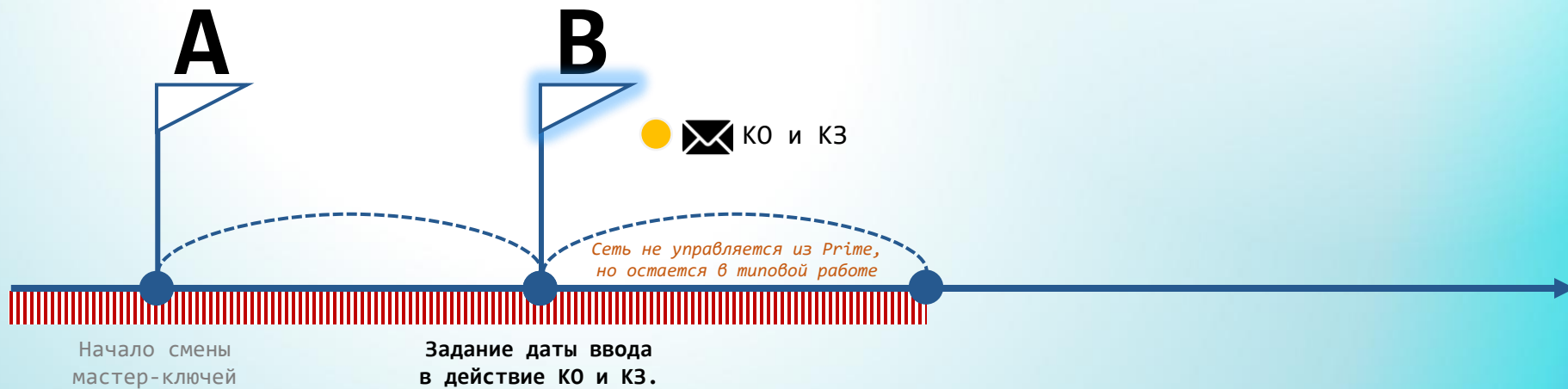


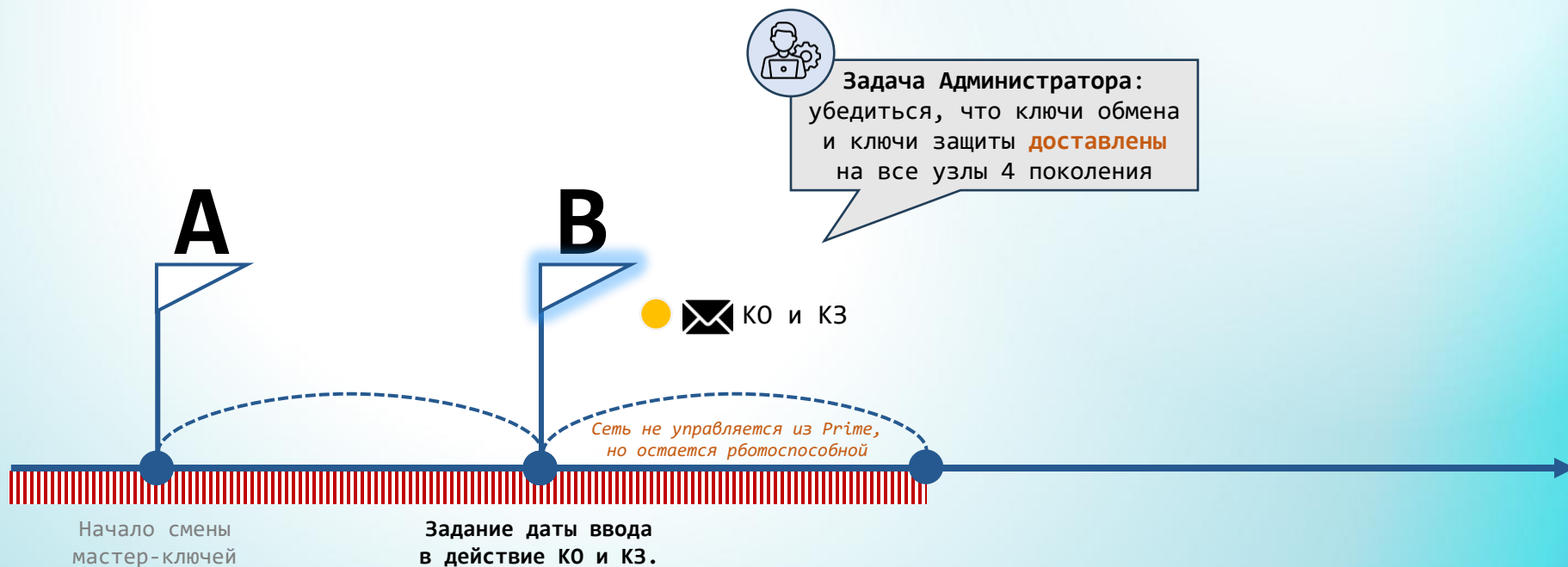
ЭТАП 2.
ОТПРАВКА КЛЮЧЕЙ ЗАЩИТЫ
И КЛЮЧЕЙ ОБМЕНА.

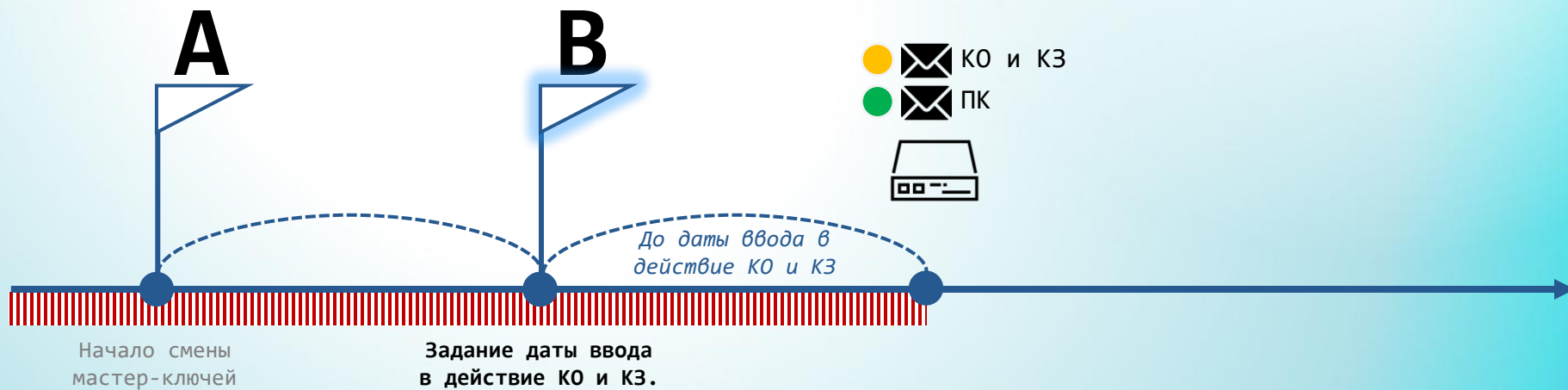
● ✉ КО и КЗ



ЭТАП 2.
ОТПРАВКА КЛЮЧЕЙ ЗАЩИТЫ
И КЛЮЧЕЙ ОБМЕНА.







ЭТАП 1.
ОТПРАВКА ПЕРСОНАЛЬНЫХ
КЛЮЧЕЙ



Отправляется в
единственном
экземпляре!

A

Типовая работа сети
сохраняется

Пока ПК не применяются на
всех узлах 4 поколения

Начало смены
мастер-ключей



ЭТАП 2.
ОТПРАВКА КЛЮЧЕЙ ЗАЩИТЫ
И КЛЮЧЕЙ ОБМЕНА



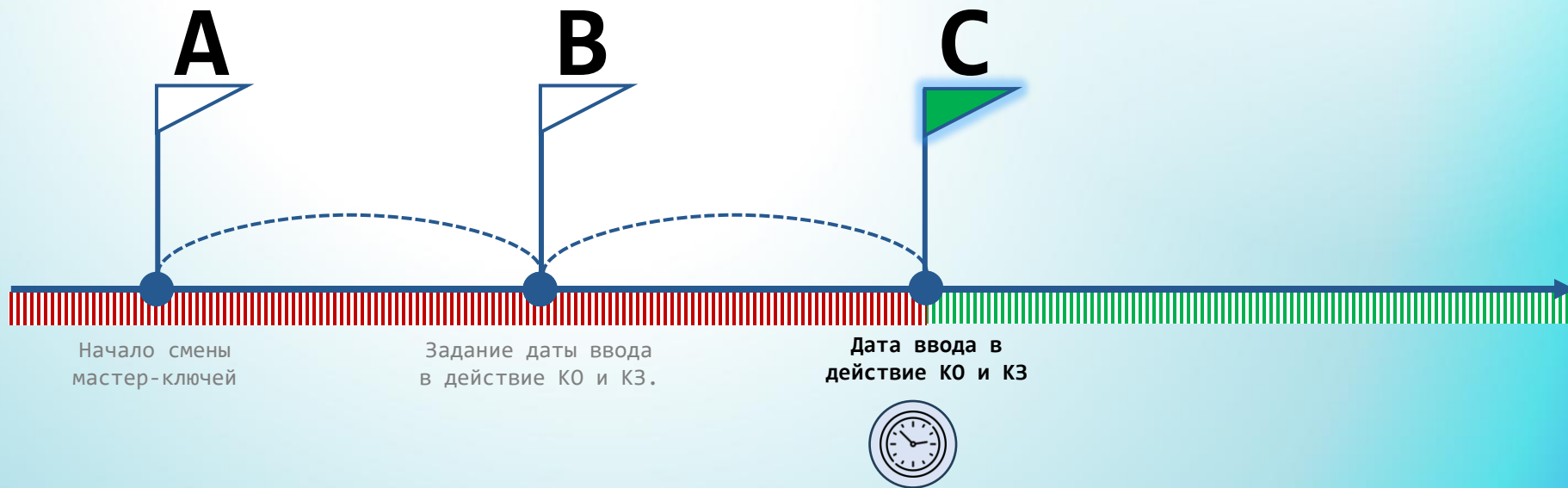
B

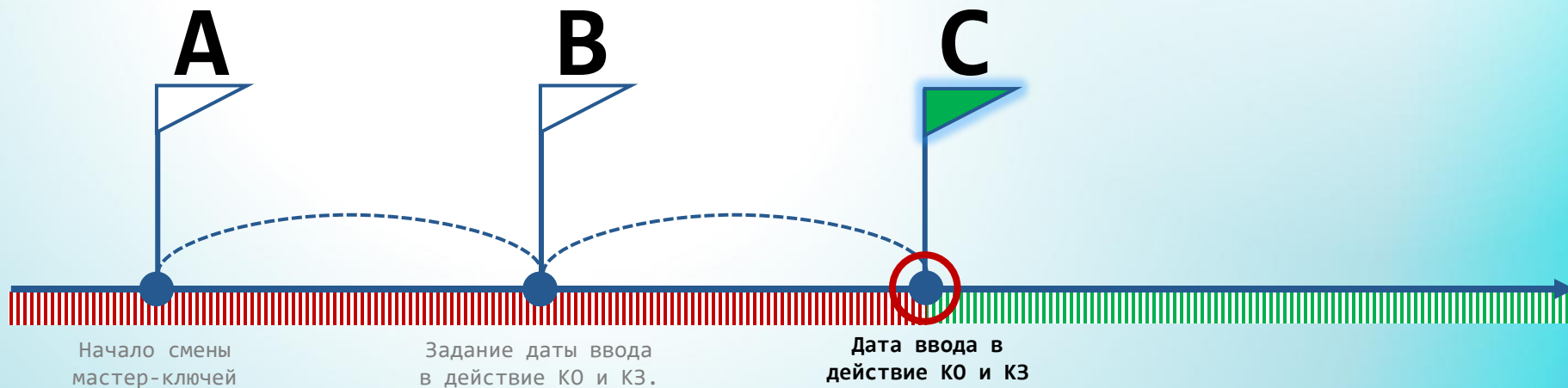
Смена мастер-ключей

До даты ввода в действие
КО и КЗ

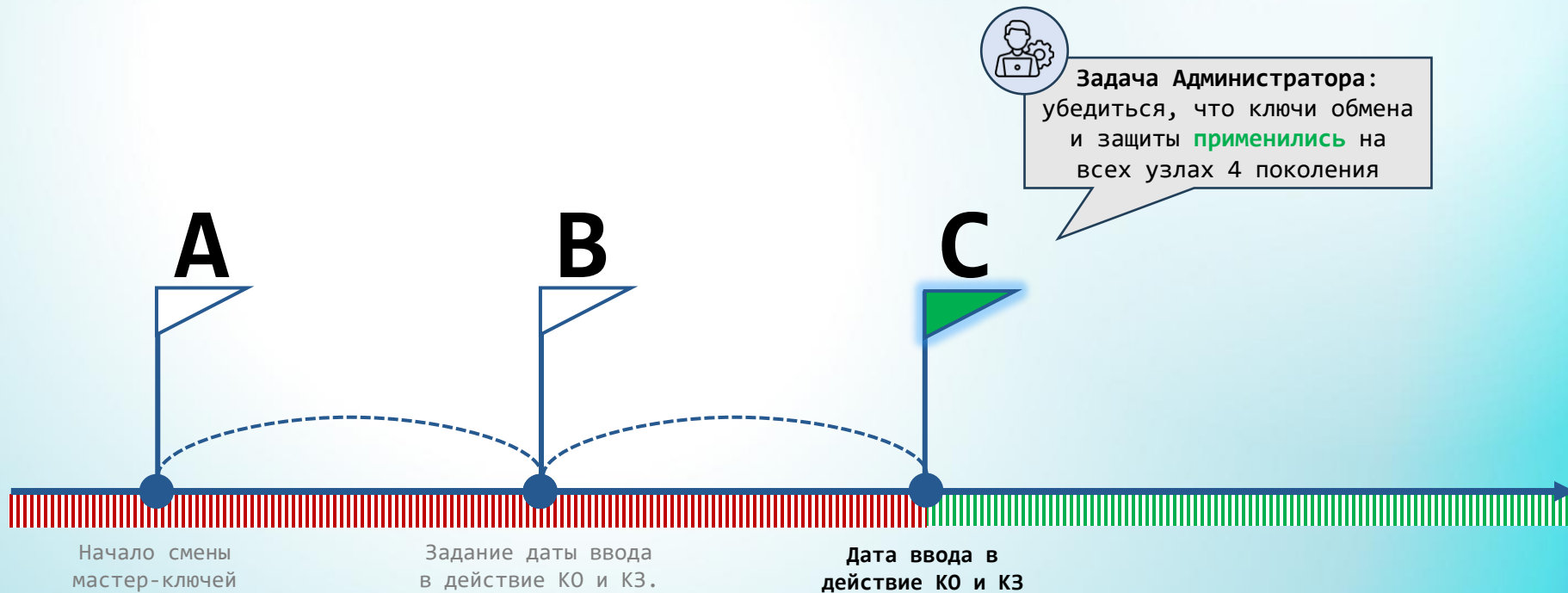
Задание даты ввода
в действие КО и КЗ.

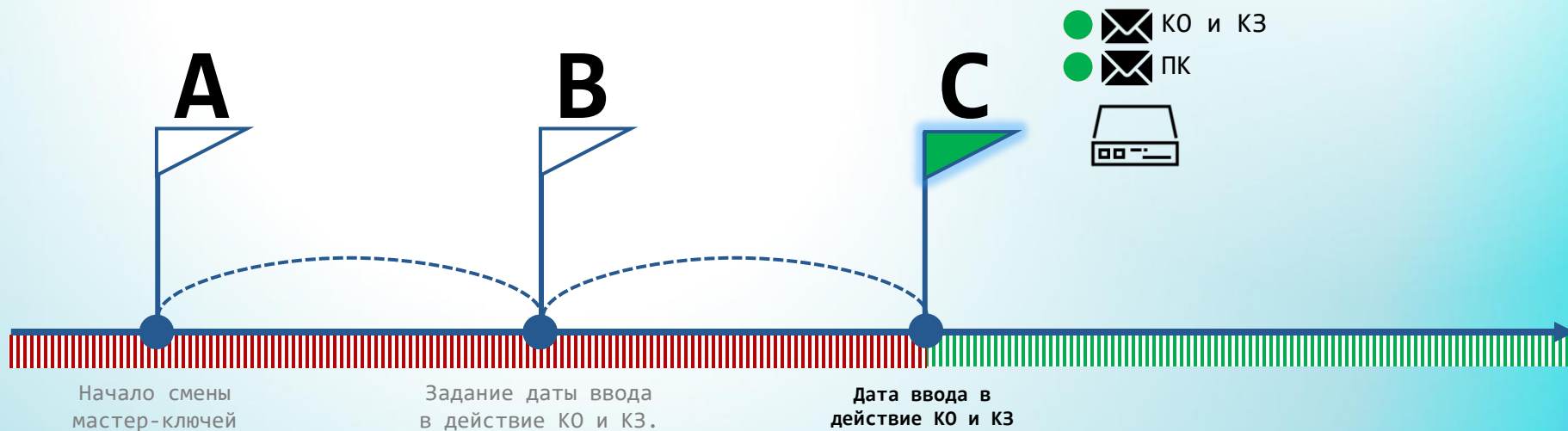


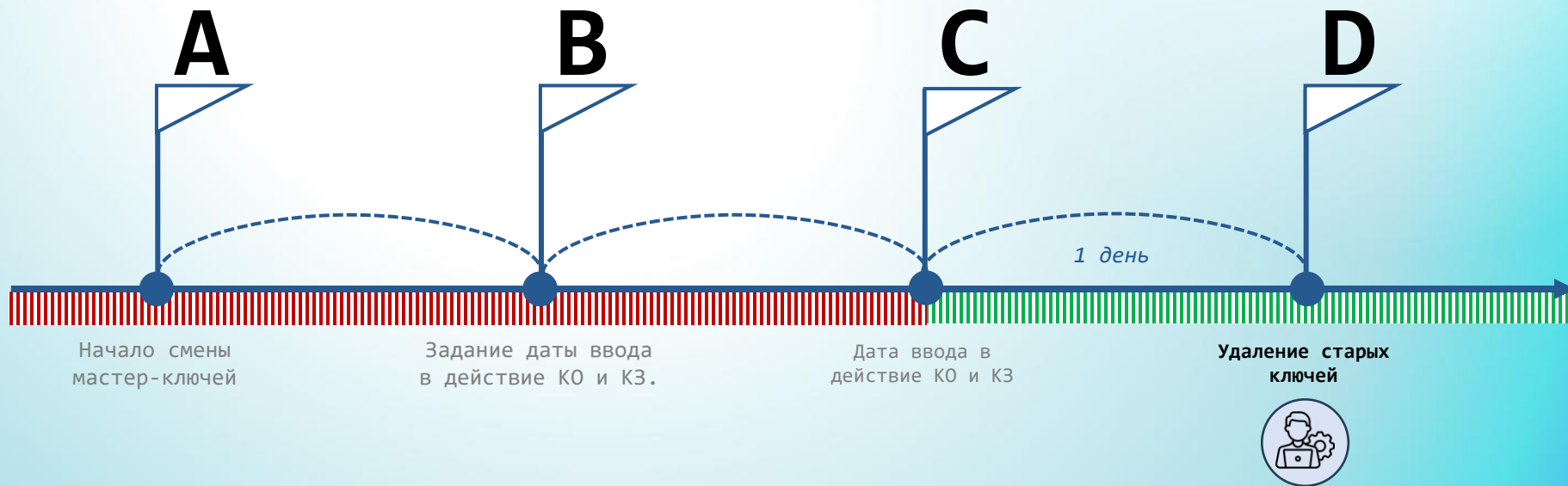




Единственный узкий момент, в котором возможны разрывы связи





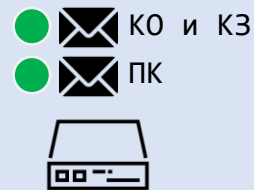
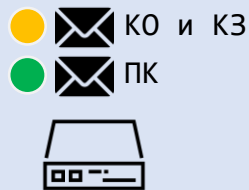


ЭТАП 1. ОТПРАВКА ПЕРСОНАЛЬНЫХ КЛЮЧЕЙ



Отправляется в единственном экземпляре!

ЭТАП 2. ОТПРАВКА КЛЮЧЕЙ ЗАЩИТЫ И КЛЮЧЕЙ ОБМЕНА



A

B

C

D

Типовая работа сети, пора менять ключи

Типовая работа сети сохраняется

Смена мастер-ключей

Типовая работа сети на новых ключах

Типовая работа сети на новых ключах

Пока ПК не применяются на всех узлах 4 поколения

До даты ввода в действие КО и КЗ

1 день

Начало смены мастер-ключей

Задание даты ввода в действие КО и КЗ.





Дата ввода в действие КО и КЗ

Удаление старых ключей



Единственный узкий момент, в котором возможны разрывы связи на секунды-минуты

Чек-лист по подготовке сети к смене мастер-ключей

-  На управляемых узлах совместимые версии ПО
-  На узлах есть РНПК (резервный набор персональных ключей)
-  Оповещаем Администраторов и пользователей узлов о сроках проведения работ
-  Проверяем, что сеть работоспособна и управляема

Переход к демонстрации



Подписывайтесь
на наши соцсети,
там много интересного




инфотекс

Присылайте ваши вопросы по темам
вебинара по адресу:

Ivan.Doroshenko@infotecs.ru

