Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации

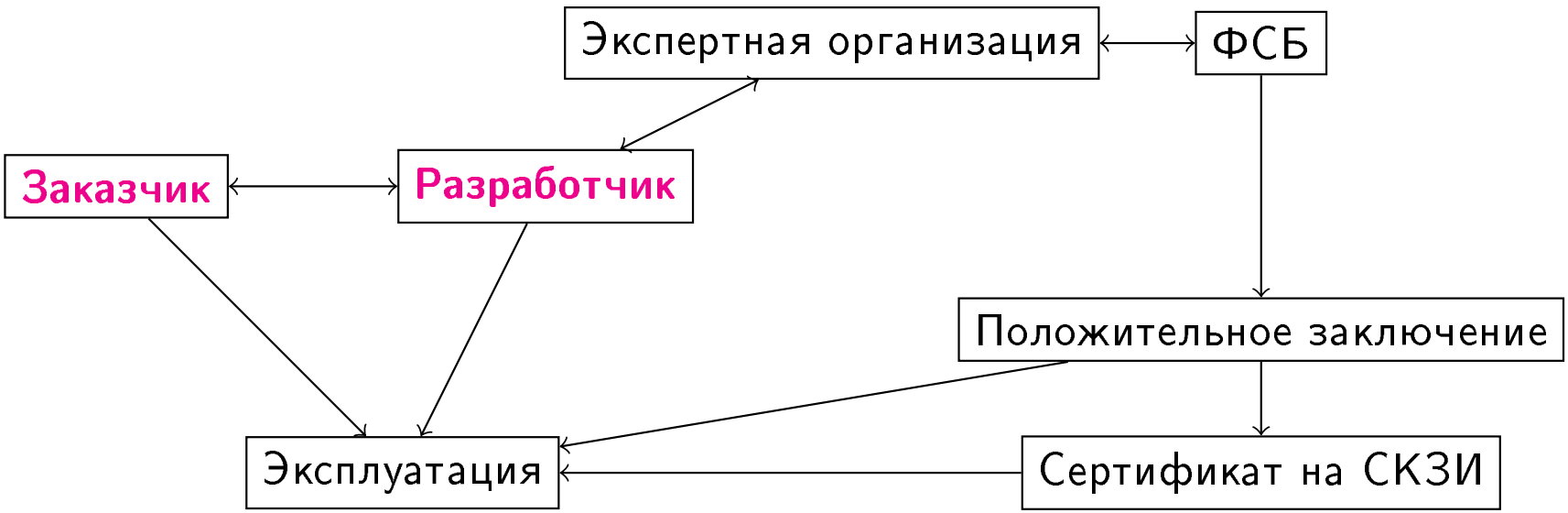
Бондаренко А.И., Нестеренко А.Ю.

Технический комитет №26 «Криптографическая защита информации»

22 марта 2017 г.

Основные этапы разработки СКЗИ

Порядок разработки СКЗИ в свете «Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации» [Положение ПКЗ-2005]



Принципы разработки СКЗИ: классификация

1. Классификация по криптографическим функциям
2. Классификация средств (по ПКЗ-2005)
   (см. также Постановление Правительства РФ №313 от 16.04.2012 «О лицензировании деятельности по разработке средств, информационных систем . . . »)
3. Классы СКЗИ: КС1, КС2, КС3, КВ, КА.
4. Класс СКЗИ определяет перечень необходимых для разработки мер защиты

Принципы разработки СКЗИ: классификация

1. Классификация по криптографическим функциям
2. Классификация средств (по ПКЗ-2005)
   (см. также Постановление Правительства РФ №313 от 16.04.2012 «О лицензировании деятельности по разработке средств, информационных систем . . . »)
3. Классы СКЗИ: КС1, КС2, КС3, КВ, КА.
   - Класс средства определяется **заказчиком**
   - Для определения класса необходимо:
     - Определить перечень подлежащих защите объектов
     - Определить совокупность возможностей при проведении атаки (перечень сведений, перечень технических средств, место проведения атаки)
   - Принципы содержат **базовую совокупность возможностей** с учетом «Требований к ЭП» (Приказ ФСБ 796) и «Состава и содержания оргштатных мер по обеспечению защиты ПД» (Приказ ФСБ 378).
4. Класс СКЗИ определяет перечень необходимых для разработки мер защиты

Принципы разработки СКЗИ: замкнутость

Замкнутость (функциональная законченность)

$$\text{СКЗИ} = \begin{cases} \text{Криптографические механизмы защиты} \\ \text{Датчики случайных чисел} \\ \text{Ключевая система} \\ \text{Аутентификация субъектов доступа} \\ \text{Инженерно-криптографические механизмы} \\ \text{Взаимодействие со средой функционирования} \\ \text{Документация} \end{cases}$$

$\uparrow$

Терминология (**область ТК №26**)

Криптографические механизмы

1. Криптографические механизмы
   1. Национальные стандарты Российской Федерации
      - ГОСТ Р 34.10/34.11-2012
      - ГОСТ Р 34.12/34.13-2015 + ГОСТ 28147-89
   2. Рекомендации по стандартизации (**область ТК №26**)
      - рекомендации Росстандарта Р 50.1-111/113/114/115
      - разработка с учетом классификации СКЗИ
      - согласование подкомитетов ТК
   3. Механизмы, получившие положительное заключение ФСБ России
   4. Рекомендации по выбору параметров криптографических механизмов (**область ФСБ России**)

Криптографические механизмы

1. Криптографические механизмы
   1. Национальные стандарты Российской Федерации
      - ГОСТ Р 34.10/34.11-2012
      - ГОСТ Р 34.12/34.13-2015 + ГОСТ 28147-89
   2. Рекомендации по стандартизации (**область ТК №26**)
      - рекомендации Росстандарта Р 50.1-111/113/114/115
      - разработка с учетом классификации СКЗИ
      - согласование подкомитетов ТК
   3. Механизмы, получившие положительное заключение ФСБ России
   4. Рекомендации по выбору параметров криптографических механизмов (**область ФСБ России**)
2. Датчики случайных чисел
   - Физические, программные, биологические
   - Статистическая проверка качества (регламентный/динамический контроль)
   - Базовая методика проверки (**область ТК №26**)

Ключевая система

1. Принципы выработки ключевой информации
2. Принципы использования ключевой информации
    1. Хранение ключевой информации в СКЗИ
       за рамками - организационно штатные меры
        - Инструкция ... (Приказ ФАПСИ 152, 2001)
        - Состав мер по обеспечению защиты ПД (Приказ ФСБ 378)
    2. Протоколы передачи ключевой информации (транспортные/выработки общего ключа)
    3. Использование асимметричных ключей
        - "криптографическо-юридический дуализм" ЭП (ФЗ-63)
        - Требования к форме квалифицированного сертификата (Приказ ФСБ 795)
        - Неквалифицированный сертификат (**область ТК №26**)
    4. Криптографическая аутентификация субъектов доступа

Инженерно-криптографические механизмы

- Инженерно-криптографическая защита
  - опасные события и сбои,
  - несанкционированный доступ (**область ФСТЭК**)
  - контроль целостности (СКЗИ, среда функционирования, ключевая информация, документация),
  - экстренное удаление ключевой информации,
  - аудит (регистрация событий),
  - блокировка работы,
  - очистка памяти
- Технические характеристики
  - влияние на разработку рекомендаций (**область ТК №26**)
  - "Допустимые объемы материала для обработки на одном ключе ..."(утверждены ТК 26) contra "Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования"(проект)
- Базовые положения для ПО и аппаратных средств СКЗИ
- Взаимодействие со средой функционирования
- Принципы построения документации (ЕСПД)

Спасибо за внимание

утвержденная ТК 26 версия документа

www.tc26.ru/standard/draft/Принципы_14.11.2016.pdf