О проекте открытых Требований к шифровальным (криптографическим) средствам защиты информации

Бондаренко А.И.

Нестеренко А.Ю.

Нормативная база

- Федеральный закон Российской Федерации от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
- Постановление Правительства Российской Федерации от 16.04.2012 № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств…»;
- Приказ ФСБ России от 09.02.2005 г. № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
- Приказ ФСБ России от 27.12.2011 г. № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра»;
- Приказ ФСБ России от 10.07.2014 г. № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации…».

Назначение открытых Требований

Открытые Требования предназначены в первую очередь **для заказчиков СКЗИ** при их взаимодействии:

- с разработчиками СКЗИ при модернизации и разработке СКЗИ;
- с организациями, проводящими тематические исследования (специализированными организациями);
- с ФСБ России, осуществляющей экспертизу результатов тематических исследований СКЗИ.

Назначение открытых Требований

Открытые Требования призваны обеспечить заказчика СКЗИ необходимой информацией с целью определения:

- **класса** разрабатываемого (модернизируемого) СКЗИ;
- **набора** механизмов защиты информации;
- некоторых количественных и качественных **показателей** механизмов защиты информации;
- **трудоемкости** (объема финансирования) проводимых работ и т. д.

Терминология в области криптографической защиты информации

Использование **единой терминологии** в области криптографической защиты информации (приведение терминологии к единому «стандарту») является актуальной задачей.

- «Рекомендации по стандартизации Р 50.1.053-2005. Информационная технология. Основные термины и определения в области технической защиты информации»
- «Рекомендации по стандартизации Р 50.1.056-2005. Техническая защита информации. Основные термины и определения».

Совокупность предъявляемых требований

Совокупность предъявляемых к разрабатываемому (модернизируемому) СКЗИ требований определяется:

- **классом** СКЗИ;
- **составом** криптографических функций, которые должны быть реализованы в СКЗИ.

Базовая совокупность возможностей, которые могут быть использованы при создании способов, подготовке и проведении атак

Атака, проводимая с целью нарушения безопасности защищаемой информации или создания условий для этого, задается следующими характеристиками:

- **объектом** проведения атаки, безопасность которого должна обеспечиваться в течение определенного периода времени и/или определенного этапа жизненного цикла СКЗИ;
- **возможностями**, которые могут быть использованы при создании способов, подготовке и проведении атак, каждая возможность определяется:
  - **сведениями**, используемыми при создании способов, подготовке и проведении атак;
  - **техническими средствами**, используемыми при создании способов, подготовке и проведении атак;
- **местом** проведения атаки.

Структура открытых Требований

- **криптографические требования**:
  - требования к криптографическим механизмам;
  - требования к датчикам случайных чисел;
  - требования к выработке ключевой информации;
  - требования к использованию ключевой информации;
  - требования к аутентификации;
  - требования к средствам имитозащиты;
- **инженерно-криптографические требования**:
  - требования к инженерно-криптографическим механизмам;
  - требования к программному обеспечению;
  - требования к аппаратным средствам;
  - требования к среде функционирования;
  - требования к документации.

Ввод в действие открытых Требований

Ориентировочные сроки:

- апрель 2016 г. – презентация на весеннем заседании ТК26;
- май 2016 г. – публикация в открытом доступе и проведение процедуры обсуждения с привлечением заинтересованых специалистов и организаций в области защиты информации;
- июнь 2016 г. - доработка по результатам обсуждения.

Спасибо за внимание