конференция РусКрипто

Ежегодная международная научно-практическая конференция

«РусКрипто'2022»

ГИС или не ГИС: вот в чем вопрос.

О требования к системам ДЭГ

Г.Б. Маршалко А.М. Семенов

Безопасность информационных систем

- Требования регуляторов + федеральное законодательство — централизованная модель:
  - Обязанности заказчика, разработчика, оператора …. — выделенные субъекты
  - … По обеспечению ИБ (конфиденциальности, целостности, доступности, аутентичности …) на всех этапах жизненного цикла криптографическими, организационно-техническими методами

- При голосовании + требования избирательного законодательства:
  - свободное и добровольное голосование (доступность)
  - обеспечение тайны голосования (конфиденциальность/анонимность),
  - открытости и гласности деятельности избирательных комиссий:
    - проверки правильности подсчета голосов (верифицируемость/контроль целостности)
    - возможности наблюдения за процедурой их подсчета (доступность/контроль целостности)

Безопасность информационных систем

- Требования регуляторов + федеральное законодательство — централизованная модель:
  - Обязанности заказчика, разработчика, оператора …. — выделенные субъекты
  - … По обеспечению ИБ (конфиденциальности, целостности, доступности, аутентичности …) на всех этапах жизненного цикла криптографическими, организационно-техническими методами

- При голосовании + требования избирательного законодательства (децентрализованная модель?):
  - свободное и добровольное голосование (доступность/отказуемость)
  - обеспечение тайны голосования (конфиденциальность/анонимность),
  - открытости и гласности деятельности избирательных комиссий:

    проверки правильности подсчета голосов (верифицируемость/контроль целостности)

    возможности наблюдения за процедурой их подсчета (доступность/контроль целостности)

Формализация криптографических задач, решаемых ДЭГ

- отказуемая конфиденциальная анонимная верифицируемая передача данных (от избирателя регистратору)
- конфиденциальное верифицируемое (с контролем целостности) вычисление суммы значений
- ….?

- Если есть четкий перечень решаемых криптографических задач — это СКЗИ?
- В любом случае, развитие криптографии позволяет увеличить долю криптографических мер защиты в ДЭГ

Различные субъекты — различные свойства

Поскольку в процессе голосования участвует большое число субъектов, обладающих различными правами доступа к компонентам и данным: избиратели, наблюдатели, администраторы, члены комиссий, то целесообразно ввести иерархию свойств в зависимости от возможности их реализации относительно тех или иных субъектов на разных этапах

Иерархия свойств

Примеры

Контроль целостности бюллетеня (публичный) - должна существовать возможность проверки корректности всех бюллетеней, принятых в рамках проведения ДЭГ.
Контроль целостности бюллетеня (личный) - у избирателя должна быть возможность убедится в корректности полученного бюллетеня, а также подтвердить его корректность записи в реестре.

Корректность итогов (публичная) - должны быть предусмотрена возможность проверки корректности проведения ДЭГ и подсчета голосов.
Корректность итогов (личная) - должны быть предусмотрена возможность проверки избирателем корректности учета его голоса (бюллетеня).

Аутентификация избирателя (публичная) - должна быть предусмотрена возможность по проверке всех субъектов (избирателей), проходящих процедуру аутентификации.
Аутентификация избирателя (личная) - субъект (избиратель) должен пройти процедуру аутентификации, подтверждающую его избирательное право и право на участие в ДЭГ.

Публичные свойства криптографического контроля целостности и верифицируемости являются новыми, и ранее не рассматривались в ИС