

# Особенности технической реализации, нормативное регулирование – облик СКЗИ

**Науменко Антон Павлович**

Зам. начальника отдела ООО «СФБ Лаб»

Руководитель направления АО «ИнфоТеКС»

Круглый стол «На пути к экономике данных без экономии данных.  
Практические наблюдения о протоколах конфиденциальных  
вычислений»

**5 июня 2025 года**

**CTCrypt'25**

**[Anton.Naumenko@infotecs.ru](mailto:Anton.Naumenko@infotecs.ru)**

## Специализированное СКЗИ

Разрабатывается для решения конкретной бизнес-задачи

Реализует один или более ПКВ при решении задач

Примеры: кредитный скоринг, отраслевая статистика, реклама

## Многоцелевое СКЗИ

Предназначено для встраивания в пользовательские средства

Реализуют один или более ПКВ, которые могут задействоваться (или не задействоваться) в зависимости от потребности пользователя

# Типовые роли участников

## Клиент



участник, конечным потребителем предоставляющий свои данные и/или являющийся результатом выполнения протокола

## Сервер



участник, выполняющий обслуживание клиентских запросов

## Оператор



участник, который обеспечивает функционирование ИС, в т.ч. синхронизацию работы других участников, а также может выполнять отдельные криптографические функции

❗ В рамках каждого протокола может выделяться подмножество специфичных ролей

# Некоторые особенности



При выполнении функций протоколов производятся вычисления над чужими данными (как правило, в зашифрованном и разделенном представлении), при этом **участники не обязаны доверять друг другу**

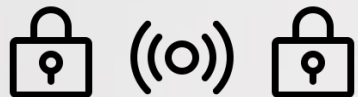


**Допускается работа системы в условиях наличия скомпрометированных узлов**, доля которых не превышает допустимого порога, определяемого по результатам анализа протокола



Сеть представляет собой распределённую систему СКЗИ.  
**Текущие требования определяют принципы защиты в отношении каждого отдельного СКЗИ.** При анализе протоколов конфиденциальных вычислений целесообразно рассматривать сеть в целом

# Некоторые особенности



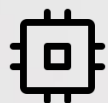
Большинство протоколов конфиденциальных вычислений **по умолчанию** подразумевает наличие **защищенных каналов** передачи данных между участниками

Это требование удовлетворяется при помощи стандартных средств (TLS, IPsec, CRISP и др.)



Таким образом, функционирование системы конфиденциальных вычислений предполагает **развернутую структуру PKI** или наличие **предраспределенных парных ключей**

# Техническая реализация



По сравнению с «классическими» СКЗИ не видится значимых отличий в плане технической реализации

Вместе с тем, в отдельных сценариях могут задействоваться специальные **аппаратные средства**

Доверенная среда исполнения (TEE/TRM)

Многоядерные ускорители (например, графический процессор)

что потенциально приводит к необходимости привлечения дополнительных мер инженерно-криптографической защиты

- ➔ Ключевые системы СКЗИ, реализующих протоколы конфиденциальных вычислений, помимо
  - 🔑 **стандартных типов криптографических ключей** могут включать
  - 🔑 **специальные виды ключевой информации** (например, «вычислительные ключи»), используемой в процессе вычислений
- ➔ Некоторые подходы к конфиденциальным вычислениям предполагают, что СКЗИ вырабатывает и выдает **«вслепую»** часть выработанной ключевой информации
- ➔ Требования к ДСЧ **стандартные**



## Р 1323565.1.012—2017 Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации

**4.2.** СКЗИ должно реализовывать одну или несколько криптографических функций. В зависимости от реализуемых криптографических функций СКЗИ может быть отнесено к одному или нескольким средствам:

- a. средству шифрования;
- b. средству электронной подписи;
- c. средству кодирования;
- d. средству изготовления ключевых документов;
- e. ключевому документу.

❗ **Проблема:** перечень функциональных возможностей существующих протоколов конфиденциальных вычислений шире перечисленных функций СКЗИ



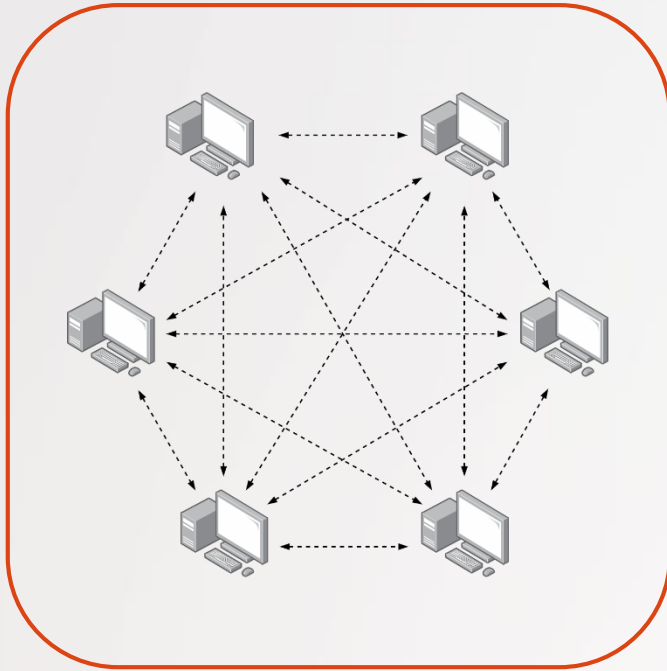
## Р 1323565.1.012—2017 Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации

**5.1.1.** При разработке (модернизации) СКЗИ следует использовать криптографические механизмы, утвержденные в качестве национальных стандартов Российской Федерации или рекомендаций по стандартизации Росстандарта, или криптографические механизмы, имеющие положительное заключение ФСБ России по результатам их экспертных криптографических исследований.

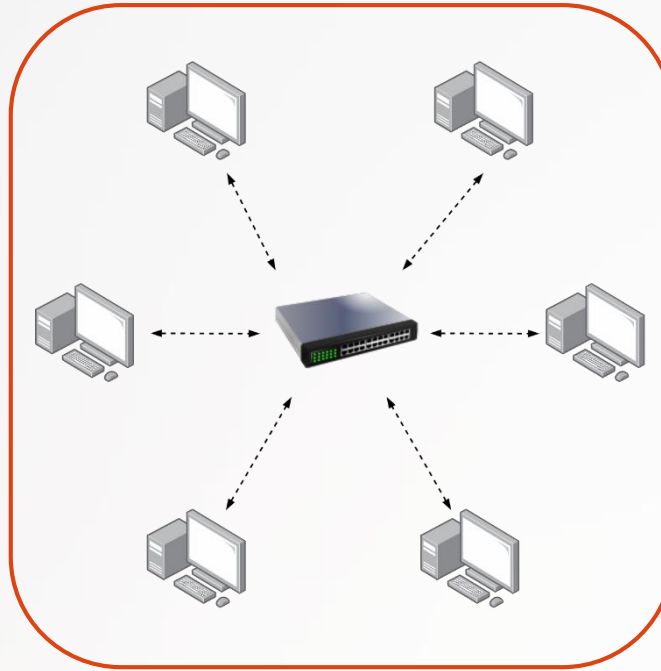
❗ **Проблема:** многие механизмы, широко применяемые в протоколах конфиденциальных вычислений, не стандартизованы

➔ Разделяются по **типу топологии** и **ролям участников**

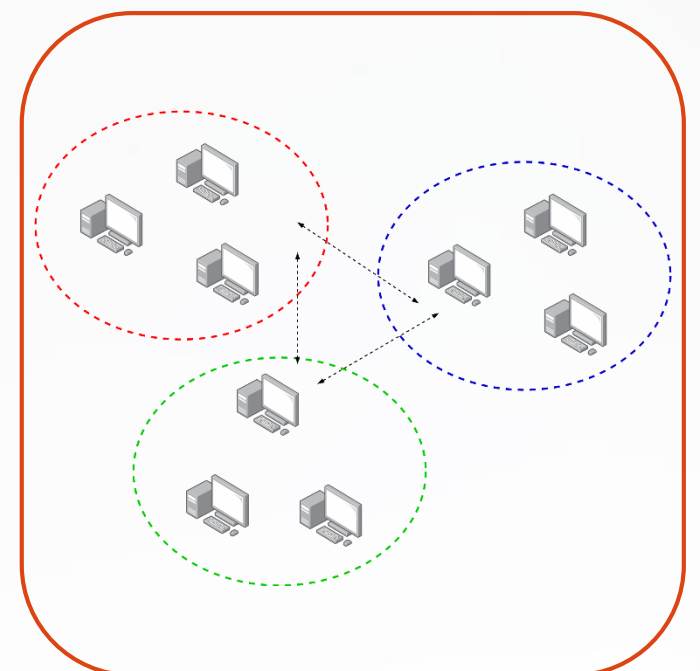
Некоторые примеры:



Равноправные участники



Участники и оператор

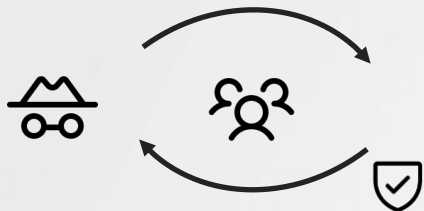


Разные группы  
участников

# Модели нарушителя

Формальный анализ стойкости протоколов проводится относительно следующих категорий нарушителя:

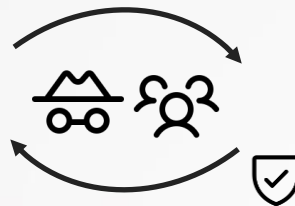
## Внешний



нарушитель, не  
являющийся участником  
протокола

## Пассивный

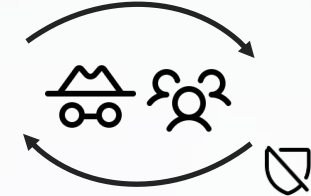
(«получестный»/«честный, но любопытный»)



внутренний нарушитель  
(участник), который следует  
спецификации протокола, но  
может проводить атаки на  
защищаемую информацию

## Активный

(«злонамеренный»)



внутренний нарушитель  
(участник), который может  
произвольно отклоняться от  
спецификации протокола  
(вносить намеренные  
искажения, задержки,  
навязывать слабые параметры  
и т.д.)

# Модели нарушителя

❗ Модель **пассивного нарушителя** –  
**слабое** предположение о возможностях противника

💡 Требование к «доверенному функционированию»  
реализуется за счет контроля за соблюдением  
комплекса организационно-технических мер

Ограничение возможностей пользователя по  
влиянию на криптографические функции СКЗИ

## **Динамический состав участников**

Влечет дополнительные требования к порядку использования выходных данных протокола, реализованного в СКЗИ: невозможность вывода данных за пределы СКЗИ, удаление предыстории при изменении состава участников, обязательства о неразглашении данных сотрудниками

-  **Проблема:** добавление/удаление новых участников в систему с предысторией может приводить к потере конфиденциальности данных в прямую/обратную сторону



Существующие нормативные документы по разработке СКЗИ (по нашему мнению) **не противоречат** концепциям известных нам протоколов конфиденциальных вычислений, но каждый отдельный сценарий может потребовать проработку новых подходов к анализу



Целесообразно поставить вопрос о разработке специальных требований для СКЗИ, реализующих многосторонние вычисления для широкого класса протоколов

# СПАСИБО ЗА ВНИМАНИЕ!

**Науменко Антон Павлович**

Зам. начальника отдела ООО «СФБ Лаб»

Руководитель направления АО «ИнфоТеКС»

**[Anton.Naumenko@infotecs.ru](mailto:Anton.Naumenko@infotecs.ru)**