Запрос на внешние инновации

|  |  |  |
| --- | --- | --- |
|  | Организация, ХК | АО «Концерн «Автоматика» |
|  | Наименование ЗВИ,  Обобщенное краткое наименование задачи | Построение защищенных децентрализованных сетей связи. |
|  | Описание ситуации: ЦЕЛЬ, НАДСИСТЕМА,  Проблема верхнего уровня, для решения которой ставится настоящая задача  *(может быть несколько уровней иерархии целей)* | В условиях динамически меняющегося списка абонентов и помех (радио-электронной борьбы) требуется установить доверие в сети не имея возможности обменяться общим секретом. На основе этого доверия построить другие необходимые криптопротоколы (шифрование, подпись, орк, и др.).  1. Существующие сегодня централизованные решения не работают в условиях динамически меняющейся обстановки (например, в услових боя).  2. Нужно связать криптографию с программно-конфигурируемыми сетями  3. Построена модель на мобильных телефонах. Ее надо актуализировать.  4. Это повысит функциональность и стойкость сетей связи. |
|  | Постановка задачи, кто, что и над чем должен сделать  (Субъект– действие–объект) | Алгоритм аутентификации пользователей в децентрализованной сети с частичным доверием |
|  | Объект (устройства, система, техпроцесс) | Сети связи специального и гражданского назначения с распределенной децентрализованной системой аутентификации, шифрования и цифровой подписи. |
|  | Его функция | Позволяет восстановить доверие между клиентами сети в случае, когда между ними нет общей секретной информации. |
|  | Значения ключевых характеристик, которые требуется достичь  Для проблемной ситуации укажите какова ее первопричина и в чем состоит «неразрешимый конфликт (противоречие) в требованиях.  Допускается ли компромисс (оптимизация) | Обеспечить криптографическую стойкость в условиях динамически меняющейся сети, в отсутствии трастового центра. |
|  | Уровень ключевых характеристик мирового лидера | В современных решениях стойкость обеспечивается с помощью централизованных протоколов. |