Уважаемый Максим Викторович!

Войсковая часть 43753-А рассмотрела представленные Вами «Отчет по контрольным специальным исследованиям и исследованиям линейной передачи изделия М-661А» (№ 2993с) в части анализа линейной передачи (АЛП).  
 По мнению экспертов в указанных отчетных материалах имеется ряд недостатков. Отчет оформлен как результаты специальных исследований, включающие в себя исследования канала связи. При этом представление полученных результатов не позволяет экспертизе провести их качественный анализ. Напоминаем, что «Методические указания по проведению анализа линейной передачи шифровальной техники» (ТА -38951) содержат раздел «Требования к отчетам по анализу линейной передачи, представляемым в экспертную организацию», которого следует придерживаться при оформлении результатов АЛП и обосновании защищенности канала связи. В вышеуказанных отчетных материалах отсутствуют описание измерительных каналов ИВК (п.4.1 «Требований к отчетам…»), временной диаграммы экспериментов (п.4.3), табличных значений измеренных сигналов в электронном виде (п.4.5, 4.6), описание метода расчета сигнал/помеха (п.5). Особое внимание следует обратить на необходимость представления результатов измерения сигналов-откликов (их временных форм и спектральных плотностей) в электронном табличном виде. Наличие таких материалов существенно упрощает проведение экспертизы – позволяет провести выборочные встречные расчеты и тем самым снять вопросы к корректности полученных результатов.  
 Конкретные недостатки, замечания и рекомендации по «Отчету…» в части АЛП приводятся в Приложении. Считаем необходимым устранить их, и результаты выслать в наш адрес в виде дополнительных отчетных материалов по АЛП.  
  
Приложение: 1. Замечания к отчету по контрольным СИ и АЛП изделия М-661А в части исследований линейной передачи,149/3/3/1/1703, секретно, на 3 листах, экз.№ 1-в адрес

В ходе экспертизы анализа линейной передачи изделия М-661А экспертами в/ч 43753А рассмотрен «Отчет по контрольным специальным исследованиям и исследованиям линейной передачи изделия М-661А» (№ 2993с, ЗАО «Эврика», вх.3145 от 08.11.18). В результате отмечены следующие недостатки.  
   
 1. Общие замечания.  
 Рассмотренный в отчете список ОС является не полным. Не рассмотрен источник опасного сигнала (ИОС) ОИ – сигнал на входе передающего оптического модуля 100Base-FX. Тактовая частота передачи данных – 125 МГц. При установке сетевого протокола в режим IDLE возможно исследование спектральным методом с основной гармоникой теста 62.5 МГц  
  
 2. Замечания к результатам, полученным спектральным методом.  
 В соответствии с «Методическими указаниями по АЛП…», рекомендуется применение метода синхронного накопления во временной области. Применение спектрального метода допустимо, а иногда и предпочтительно, но с точки зрения эксперта по АЛП чаще требует пояснений по корректности при постановке эксперимента и проведенным расчетам. Например, без приведения временных диаграмм тестов для отдельных источников опасного сигнала, эксперт не может дать оценку полученным результатам.  
 2.1. В частности, сомнения вызывает корректность периодического теста для сигналов протоколов USB1.1 (ОС1.2) и USB2.0 (ОС2). Предлагаемое заполнение пакетов USB нулевыми данными 00h действительно превращает сигнал в меандр, но только на интервале заполнения данными. При этом нет информации, что отменена пакетная структура передачи, а следовательно, помимо данных во временном протоколе будут служебные заголовки пакетов, длительные «пустоты» между пунктами, пакеты с другой структурой (неинформативные для теста) и т.д. Соотношение времен между периодической структурой (интервалов заполнения данными) и суммарной длительности бездействия шины и передачи служебной информации, как правило, не в пользу периодического тестового сигнала. Эксперту не понятно, каким образом с помощью анализатора спектра FSV40 учитывается такая структура пакетной передачи.  
 По данным тестам требуются пояснения, в частности временные диаграммы теста и метод учета нерегулярной пакетной передачи.

2.2. ИОС ОС1.1 заявлен как последовательная шина от РИК к считывателю, протокол ISO7816. Данная шина имеет частоту CLK 4МГц, а частоту следования данных на линии I/O в 273 раза меньше. Как следует из отчета, тестовый сигнал сформирован на I/O путем передачи данных 55h (меандр для последовательного потенциального кода). Почему тогда спектральный метод применен для базовой частоты (1 гармоника) = 4МГц? Заметим, что ожидаемый на I/O меандр (от передачи 55h) будет нарушен дополнительными служебными битами для каждого передаваемого байта 55h, и базовая частота теста становится уже частотой следования байтов что ниже частоты исследования бит и тем более CLK.  
 По мнению эксперта, применения спектральных методов для АЛП с базовыми частотами нижа 100кГц вообще не имеет смысла, т.к. уровень измеряемых гармоник не выделяется в исследуемых цепях над шумом.  
 По данному тесту необходимы разъяснения, почему оценка дана для импульса CLK. Кроме того, обращаем внимание, что для считывателя РИК характерна модуляция побочного сигнала CLK (4МГц и ее высшие гармоники) информативным сигналом I/O, имеющим значительно большую длительность. При наличии такой модуляции энергия опасного отклика от I/O возрастает на несколько порядков по сравнению с энергией отклика от фронта I/O или CLK.  
  
2.3. Расчеты экспериментального отношения сигнал/помеха приводятся в табличной форме. Проведенный расчет не соответствует формуле расчета для спектрального метода из «Методических указаний по АЛП…». Если рассмотреть каждую строку таблицы, эксперту абсолютно не понятно, как из ячеек с измеренными данными и введенными параметрами получаются результаты расчета. Формулы расчета не приведены. Исходные данные (Uс+ш и Uш) в дБ – относительно какой величины? Что такое «К» для линии связи, почему пересчет идет к токовым величинам, хотя норматив шума в линии связи дается как спектральная плотность напряжения.  
 По методике расчета требуются разъяснения.

2.4. Диапазон частот измерений сигналов линейной передачи, в соответствии с Требованиями, в том числе при измерении спектральным методом – до 1ГГц. Почему измерения сигналов выполнены в ограниченном диапазоне? Для ОС1.1 – это 40МГц, ОС1.2 – 125МГц, ОС2 – 480 МГц, ОС5 – 400 МГц и т.д. все сигналы без исключения.

Требуется обоснование

3. Замечания к результатам, полученным методом синхронного накопления.

3.1. Данным методом исследовано два вида ОС. Для пояснения поставленного эксперимента необходимо привести временную диаграмму теста, на которой отобразить взаимное расположение синхроимпульса, измеряемого тестового сигнала и опорного сигнала. Интересует, прежде всего, расположение фронтов на интервале измерения и привязка их к той временной сетке, которая приводится на диаграммах отчета. Необходима также информация о частоте следования синхроимпульсов, т.к. тестовые сигналы являются внутренними, достаточно указать предполагаемое расположение их фронтов на диаграммах. Кроме того, для подтверждения корректности теста целесообразно провести накопление в ближнем поле (антенна в нескольких мм от ПЛИС), где сигнал может быть выделен.  
  
 3.2. Формула для расчета экспериментального отношения сигнал/помеха не указана. Необходимо ее привести с учетом коэффициента входного съемника. Для проверки проведенных расчетов эксперту необходимы вектора сигналов, измеренных в питании (например в формате \*.xls или \*.txt).