где $\frac{d}{\sqrt{2N_0}} = \sqrt{\frac{h_m^2}{(\sqrt{M}-1)^2}} = \sqrt{\frac{3h_c^2}{M-1}}, h_m^2 = \frac{E_m}{N_0}, h_c^2 = \frac{E_c}{N_0}$

Сравним характеристики качества КАМ и ФМ для заданного объема сигналов М. Оба типа сигналов являются двухмерными.

Аппроксимация вероятности ошибки на символ М-позиционной ФМ выглядит следующим образом [7]

$$P_{\sqrt{m}\text{ФМн}} \approx 2Q\left(\sqrt{2\gamma_s}\sin\frac{\pi}{m}\right),$$

Аппроксимация вероятности ошибки на символ М-позиционной КАМ представлена в виде [7]

$$P_{m\text{КАМ}} = 2\left(1-\frac{1}{\sqrt{m}}\right)Q\left(\sqrt{\frac{3}{m-1}\frac{E_{cp}}{N_0}}\right)$$

Отношение двух аргументов Q-функции [7]

$$K_m = P_{m\text{КАМ}} / P_{\sqrt{m}\text{ФМн}} = \frac{3/(M-1)}{2\sin^2(\pi/M)}$$

Заключение

В ходе работы предложено для оценки защищенности цифровых каналов утечки информации использовать в качестве измерительных двоичные ортогональные когерентные и некогерентные сигналы, зависимости вероятности ошибки от отношения мощности сигнала к мощности шума которых находятся вблизи границы Шеннона. Установлены зависимости для сигналов сложной формы КАМ, АФМ, а также зависимости для двоичных и многопозиционных сигналов. Это позволяет оценивать защищенность систем передачи информации по единому нормированному показателю – вероятности ошибки на бит информации.

Литература:

1. Железняк, В.К. Защита информации от утечки по техническим каналам: учебное пособие / В.К. Железняк; ГУАП. – СПб., 2006. – 188 с.

2. Зюко, А.Г. Помехоустойчивость и эффективность систем связи / А.Г. Зюко. – М.: Связьиздат, 1963. – 320 с.

3. Клюев, Н.И. Информационные основы передачи сообщений / Н.И. Клюев. – М.: Московская типография № 10 Главполиграфпрома, 1966. – 360 с.

4. Стейн, С. Принципы современной теории связи и их применение к передаче дискретных сообщений / С. Стейн, Дж. Джонс, отв. редактор Л.М. Финк. – М.: «Связь», 1971. – 376 с.

5. Дядюнов, А.Н. Адаптивные системы сбора и передачи аналоговой информации. Основа теории / А.Н. Дядюнов, Ю.А. Онищенко, А.И. Сенин – М.: Машиностроение, 1988. – 288 с.

6. Варакин, Л.Е. Теория систем сигналов / Л.Е. Варакин. – М.: «Сов.радио», 1978. – 304 с.

7. Савищенко, Н.В. Многомерные сигнальные конструкции: их частотная эффективность и потенциальная помехоустойчивость приема / Н.В. Савищенко, под ред. Д.Л. Бураченко. – СПб.: Изд-во Политехн. ун-та, 2005. – 420 с.

Abstract

The optimum signal for an estimation of security of digital channels of information leakage is investigated. The technology of technical protection of the information forms the generalized requirements to the theory and techniques of transfer of systems of signals. The system of signals used for an information transfer as set of signals, united by a uniform rule of construction is considered. It is known, that a noise stability – one of the basic requirements to transfer system. The optimum system of signals providing the maximum noise stability at the minimum relations of energy of bit to spectral density of capacity of noise in channels of information leakage, methods of an estimation of security of discrete systems of signals in information leakage channels are offered at influence of noise of high level of type white Gaussian noise, and also a choice and a substantiation of an optimum signal which will allow to estimate security of digital channels of information leakage.

Поступила в редакцию 18.05.2013 г.

СПОСОБ ПОДАВЛЕНИЯ ЗАШУМЛЕННЫХ ИМПУЛЬСНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ПУТЕМ КОМПЕНСАЦИИ

УДК 621.397.7:004.056.57

В.К. Железняк, А.В. Барков,
ПГУ, г. Полоцк

Аннотация

Рассматривается обнаружение периодических импульсных последовательностей и их подавление путем компенсации в канале утечки информации. Задачей является обнаружение периодической импульсной последовательности из аддитивных шумов высокого уровня с целью последующего её подавления. Обнаружение основано на быстром преобразовании Фурье и накоплении сигнала в частотной области. Сравнение и оценку обнаружения производят при помощи оптимального приема и порогового детектирования. Выбор порога осуществляют по известным критериям оптимальности в задачах обнаружения сигналов. Подавление импульсных последовательностей в канале утечки информации решается их компенсацией воспроизведением противофазного обнаруженного сигнала. Эксперименты проведены моделированием периодической импульсной последовательности с добавлением аддитивных шумов, таких как белый шум, хаотическая импульсная последовательность, телеграфный сигнал. Предложен способ обнаружения и компенсация зашумленных импульсных последовательностей. Проанализированы известные

способы, что позволило выявить ряд преимуществ предложенного способа.

Введение

Основные информационные процессы – передача, прием, распространение, преобразование, запоминание – были интересны всегда, на современном этапе развития техники и информационных технологий возросла видимая (открытая) часть интересов к вопросам добычи, утечки, сохранности и защиты информации. На расстояние информация передается в подавляющем преимуществе по каналам электро- и радиосистем в виде сообщений в аналоговой или цифровой форме. Многообразие существующих способов обеспечения информационной безопасности показывает возможность различных подходов к вопросу обеспечения защиты информации и необходимость разработки более совершенных способов защиты информации от утечки. [1]. Синхронизация используется при передаче цифровых сообщений, которые имеют логическую форму двоичных единиц и нулей [2, с. 84].

Проанализированы известные решения [3, 4], данные способы не рассматривают возможность обнаружения сигнала в шумах высокого уровня, в маскирующих помехах в виде белого шума, учитывают только влияния мешающих импульсных последовательностей.

В работе [5] предложен способ измерения и подавления физических полей самонастраивающимся опорным полем. Недостатками способа является невозможность обнаружения сигнала в шумах высокого уровня.

Задачей предлагаемого способа является обеспечение обнаружения и компенсации зашумленных импульсных последовательностей в канале утечки информации (КУИ) в шумах высокого уровня.

Обнаружения периодической импульсной последовательности

Обнаружение сигналов в шумах может быть основано на накоплении сигнала с целью выделения его из шума. В работе [3] представлен принцип выделения сигналов, основанный на совпадении сигналов, и реализуется с применением накопителей на линиях задержки с положительной обратной связью. В [3] показано накопление сигнала во временной форме. Сигнал по линии обратной связи поступает на вход приемного устройства с квазипериодом T. Таким образом, для накопления сигнала и улучшения отношения сигнал-шум в [3] требуются априорные данные о сигнале – период повторения сигнала.

Предложен способ обнаружения периодических импульсных последовательностей и оценки их периода, который измеряет и оценивает параметры зашумленного сигнала, выделяет сигнал из шума без априорных данных о сигнале.

Периодическая импульсная последовательность $x(t)$, смешанная с аддитивным шумом $n(t)$ в КУИ, моделирует сигнал в КУИ $s(t)$:

$$s(t) = x(t) + n(t), \quad (1)$$

Произведем разделение сигнала на отрезки равной длительности и преобразование Фурье каждого отрезка, суммируют результаты преобразования по формуле:

$$S = \sum_{0}^{N-1} FFT(S_n), \quad (2)$$

где N – количество отрезков сигнала равной длины, S_n – сигнал указанной длины, FFT – быстрое Фурье-преобразование сигнала, S – накопленное Фурье преобразование отрезков сигнала.

По данным преобразования Фурье, которое получили в результате накопления, формируют спектр амплитуд зашумленного сигнала, по которому определяют гармонику с наибольшей амплитудой A_{max}, не учитывая значения нулевой гармоники. Частоту гармоники с наибольшей амплитудой f_{max} принимаем за период следования импульсов. Обнуляем в спектре амплитуд составляющие, не кратные частоте следования импульсов f_{max} и нулевую гармонику, получаем:

$$A_k = \begin{cases} 0, для k \neq M \cdot m, m = (1..K-1); \\ A_k, для k = M \cdot m, m = (1..K-1) \end{cases} \quad (3)$$

где A_k – k-ая гармоника Фурье-преобразования, K – количество гармоник Фурье-преобразования, M – номер гармоники с частотой $f_{A\max}$.

Получаем спектр сигнала $S`$, состоящий из отфильтрованных по формуле (4) гармоник A_k без шума, т.е. остались только гармоники периодической импульсной последовательности.

Производим обратное дискретное преобразование Фурье IFFT обработанного (после обнуления) сигнала, получаем восстановленный сигнал $x`(t)$:

$$x`(t) = IFFT(S`), \quad (4)$$

Сравниваем полученный сигнал с исходным, из которого удалена его постоянная составляющая. Сравнение и оценку обнаружения производят при помощи оптимального приема и порогового устройства, выбор порога осуществляем по известным критериям оптимальности решений в задачах обнаружения сигналов, а за оценку периодов обнаруженных импульсных последовательностей принимают частоту $f_{A\max}$ гармоники спектра амплитуд с наибольшей амплитудой A_{max}, частота которой соответствует частоте следования импульсов.

Компенсация периодических импульсных последовательностей в канале утечки информации

Ряд сигналов (например, видео, цифровой) являются синхронными. При наличии информации о периоде сигнала есть возможность его синхронного накопления и улучшения отношения сигнал-шум. Для невозможности синхронного накопления требуется решить задачу по разрушению сигналов синхронизации.

Компенсация периодических импульсных последовательностей происходит после их обнаружения в шумах представленным выше способом.

Если определили наличие сигнала в шумах, то необходимо его разрушить.

Сигнал восстанавливается способом представленным ранее. Компенсацию осуществляем поворот восстановленного сигнала в противофазе, который при сложении с зашумленным сигналом разрушит посредством компенсации периодическою импульсную последовательность, которая была в зашумленном сигнале.

Покажем результаты моделирования обнаружения и компенсации.

Входным параметром является зашумленный сигнал, который может содержать периодическую импульсную

последовательность $x(t)$ с неизвестными параметрами (рисунок 1).

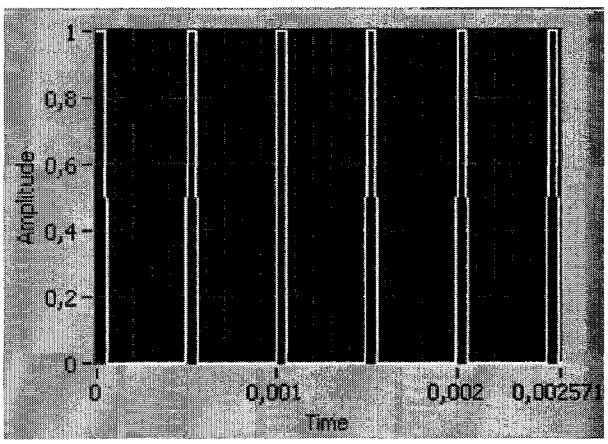

Рисунок 1 – Последовательность прямоугольных импульсов

Формируем аддитивную смесь сигнала с белым гауссовым шумом. Задача заключается в том, чтобы принять решение о наличие или отсутствии периодической импульсной последовательности с неизвестными параметрами в шумах (рисунок 2).

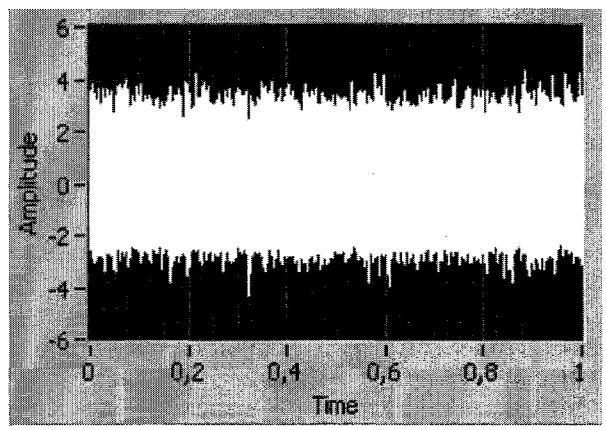

Рисунок 2 – Зашумленная периодическая импульсная последовательность

Последовательность (пачка) прямоугольных импульсов характеризуется длительностью импульса, периодом следования импульсов и общим числом импульсов в пачке. [6, с. 316]

Обнаружение периодической импульсной последовательности производим способом, описанным ранее.

При моделировании периодической импульсной последовательности исходные параметры эксперимента: частота следования импульсов 2000 Гц, амплитуда импульсов 1В, скважность 10.

Представим зашумленную импульсную последовательность в частотной области F{x}. Спектр амплитуд зашумленного сигнала представлен на рисунке 3.

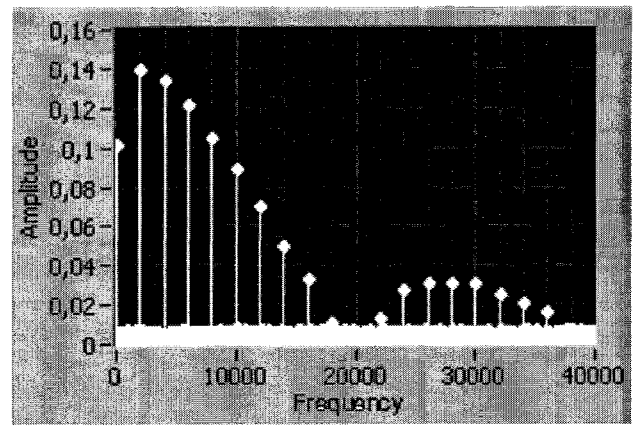

Рисунок 3 – Спектр зашумленного сигнала

По спектру амплитуд определяют гармонику с наибольшей амплитудой. Рисунок 4 показывает, что будет выделена гармоника с амплитудой 0,14 и частотой 2000 Гц. За частоты следования импульсов f обнаруженной периодической импульсной последовательности принимают частоту гармоники спектра амплитуд с наибольшей амплитудой, производим выделение этой гармоники в данном случае это гармоника на частоте 2000 Гц. Этот параметр носит информативный характер, при правильном обнаружении данная частота соответствует частоте следования импульсов f.

Производим фильтрацию спектра, обнуляя составляющие, не кратные основной частоте следования импульсов f (значение этой частоты определили по спектру амплитуд ранее). Кратность частот определяем по формуле:

$$fk=f^*k, \qquad (5)$$

где $k = 0, 1, 2 \ldots N$ – номер гармоники, f – частота следования импульсов.

Спектр амплитуд после фильтрации представлен на рисунке 4.

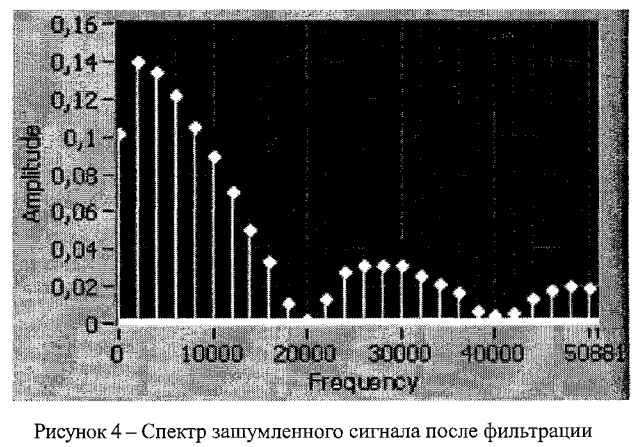

Рисунок 4 – Спектр зашумленного сигнала после фильтрации

Спектр амплитуд периодической импульсной последовательности исходного сигнала $x(t)$ и восстановленного сигнала после фильтрации незначительно отличаются амплитудами.

Выполняем ОДПФ (обратное дискретное преобразование Фурье) и производят нормирование амплитуд восстановленной импульсной последовательности по формуле

$$Sig = InvFFT\{S\} / N, \quad (6)$$

где $InvFFT\{S\}$ – обратное дискретное преобразованием Фурье; N – количество отрезков сигнала равной длины, получаем восстановленный сигнал $x1(t)$.

Получаем восстановленную импульсную последовательность. Если сравнить импульсную последовательность из исходного сигнала (рисунок 1) и восстановленную импульсную последовательность после обратного дискретного преобразования Фурье (рисунок 5), видно, что импульсная последовательность восстановлена с некоторыми искажениями по форме, однако значительно отличается от зашумленного сигнала (рисунок 2).

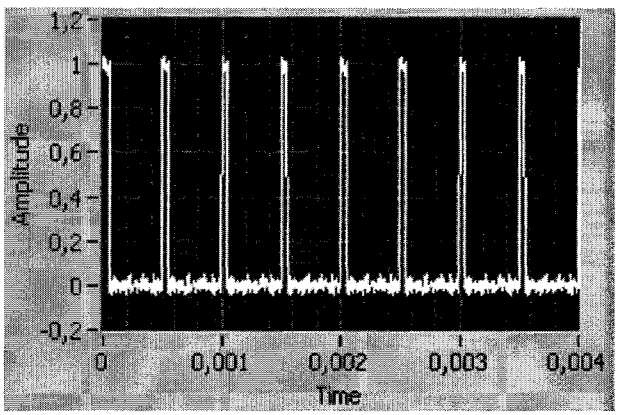

Рисунок 5 – Импульсная последовательность после ОДПФ

Сравниваем импульсные последовательности рисунок 1, принимаем решение о соответствии восстановленной импульсной последовательности и исходной. Соответствие сигнала исходному определяем с помощью оптимального приема и порогового устройства. Выбор порога осуществляется по известным критериям оптимальности решений в задачах обнаружения сигналов [7, с. 33]. За оценку частоты следования периодической импульсной последовательности принимаем значение равное 2000 Гц, что соответствует значению частоты следования импульсов в исходном сигнале.

Осуществляем поворот восстановленного сигнала $x1(t)$ (рисунок 5) в противофазе, получаем сигнал $x1r(t)$, таким образом, при сложении с зашумленным сигналом $x(t)$ этот сигнал разрушит посредством компенсации периодическою импульсную последовательность, которая была в зашумленном сигнале.

Если определили наличие сигнала в шумах, то необходимо его разрушить. Производим сложение сигналов $x(t)$ и $x1r(t)$, на выходе получаем разрушенный сигнал $x2(t)$, в котором скомпенсирована периодическая импульсная последовательность. Рисунок 6 представляет спектр разрушенного сигнала, который значительно отличается от спектра зашумленного сигнала (рисунок 3) и в нем отсутствуют признаки наличия сигнала в шумах, что говорит об успешном разрушении сигнала.

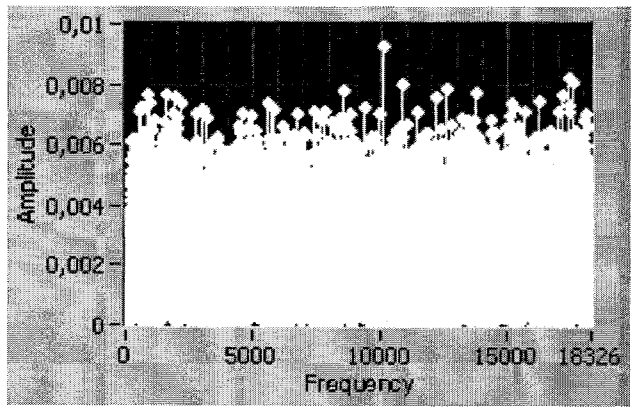

Рисунок 6 – Спектр разрушенного сигнала в канале утечки информации

Моделирование отсутствия периодической импульсной последовательности с неизвестными параметрами в шумах производится после ее разрушения.

Обнаружение синхросигналов в шумах при оценке защищенности информации представляет признак, по которому принимают решение о наличие канала утечки. Считается, что цифровое сообщение имеет логическую форму двоичных единиц и нулей и с целью передачи проходят этап импульсной модуляции, в результате чего преобразуются в низкочастотные (импульсные) сигналы, или видеоимпульсы. Видеоинформацию накапливают, используя полученные данные о параметрах синхронизации, так же накопление информации позволяет улучшить отношение сигнал/шум. Выделение синхронизирующих импульсов позволяет проводить синхронное накопление информации, например в виде видеокадров.

Предложенный способ является универсальным, так как при различных структурах маскирующих сигналов результаты обработки аналогичны.

Заключение

Исследовано обнаружение и компенсация периодических импульсных последовательностей и импульсов синхронизации в шумах высокого уровня при воздействии различных помех и выделение их из аддитивной смеси с шумом.

Показана возможность обнаружения периодических импульсных последовательностей из шумов, принимать решение о соответствии восстановленного сигнала исходному сигналу, разрушение сигнала в канале утечки информации путем компенсации исходного сигнала восстановленной импульсной последовательностью.

Предложенный способ обладает следующими преимуществами: обнаружение и компенсация периодических импульсных последовательностей в шумах высокого уровня без априорных данных о сигнале при воздействии факторов помех, таких как белый шум, хаотическая импульсная последовательность, телеграфный сигнал, возможность накопления сигнала с неизвестными параметрами в частотной области, обнаружение импульсных последовательностей в аддитивной смеси с шумом, в которой может меняться амплитуда сигнала за счет наложения шума.

Литература:

1. Домарев, В.В. Безопасность информационных технологий. Методология создания систем защиты. – К.: ТИД Диа Софт, 2002. – 688 с.

2. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение. Изд. 2-е, испр.: Пер. с англ. – М.: Издательский дом «Вильямс», 2003. – 1104 с.

3. Лезин, Ю.С. Оптимальные фильтры и накопители импульсных сигналов. – М.: «Сов.радио», 1969. – 320 с.

4. Патент Российской Федерации 2251704, МПК G01R23/02, опубл. 10.05.2005

5. Патент Российской Федерации 2391678, МПК G01R29/08, опубл. 27.01.2010

6. Ван Трис Г. Теория обнаружения, оценок и модуляции. Том III. Обработка сигналов в радио- и гидролокации и прием случайных гуссовых сигналов на фоне помех. Нью-Йорк, 1971. Пер. с англ. Проф. В.Т. Горяинова. М.: «Сов.радио», 1977. – 664 с.

7. Помехоустойчивость информационных радиосистем управления: Учеб. пособие / А.Г. Охонский, А.А. Елисеев, Н.В. Каплунова, А.Н. Кулин, Э.В. Минько. – М.: МГАП «Мир книги», 1993. – 216 с.

Abstract

We consider the detection of periodic pulse sequences and their suppression by compensation in the channel information leakage. The task is to detect the periodic pulse sequence of high level of additive noise to its subsequent suppression. The detection is based on a fast Fourier transform and the accumulation of a signal in the frequency domain. Comparison and evaluation of the detection is carried out with the best reception and the threshold of detection. Thresholding performed by well-known criteria of optimality in problems of signal detection. Suppression pulse sequences in the channel leak solved their compensation playback antiphase signal detection. Experiments were carried out simulations of the periodic pulse sequence with the addition of additive noise such as white noise, chaotic pulse sequence, telegraph signal. We propose a method of detecting and compensating for noisy pulse sequences. The known methods, which revealed a number of advantages of the proposed method.

Поступила в редакцию 18.05.2013 г.

40-ЛЕТНИЙ ЮБИЛЕЙ ПД ИТР

УДК 519.6

В.К. Железняк,
ПГУ, г. Полоцк

В статье рассматриваются этапы развития и пути совершенствования государственной системы защиты информации противодействия иностранным техническим разведкам (ПД ИТР). Уровень развития этого направления по праву позволяет отнести его к научному направлению информатики. Эффективность применения разработанных в предвоенный период отечественных радиолокационных станций позволило во время Великой Отечественной войны принять Постановление о развитии радиолокации, в послевоенный (1952) – о создании НИИ Автоматики для развития науки и техники, криптографических методов безопасности, включающих наряду с военной, научной, экономической, политической и другие виды информации. И наконец, в 1973 году принято важнейшее постановление о развитии ПД ИТР.

Научное направление деятельности формировалось в ЦНИРТИ, созданном Постановлением ГКО 4 июля 1943 г. №ГОКО-368сс «О радиолокации», подписанным И.В. Сталиным. Главный инициатор подготовки и принятия постановления ГКО выдающийся ученый Герой Социалистического Труда инженер-адмирал академик Аксель Иванович Берг – первый директор ордена Ленина ЦНИИ 108 МО [1]. В лаборатории радиоприемных устройств разрабатывал УПЧ и УНЧ для самолетной ОКР «Ласточка» (главный конструктор Ю.Н. Мажоров в дальнейшем зам. директора по науке и директор ЦНИРТИ) ОПЧ и УНЧ для космической ОКР К8 (главный конструктор Плешаков П.С. директор ЦНИРТИ и в дальнейшем Министр радиопромышленности СССР).

Опыт разработки самолетной, космической аппаратуры радиотехнической разведки повысил научный потенциал. Опыт по созданию РЭА пригодился в дальнейшем, работая по переводу в НИИ 110 г. Киев. Проработав в филиале ЦНИИ 108 (ВЧ 25757) 4 года инженером, старшим инженером, начал работать по космической тематике, через короткое время назначен ведущим инженером и заместителем главного конструктора двух ОКР «Пион 2» и «Пион 4» по морской тематике. Пригодился опыт предыдущей работы по летным экспериментальным работам в интересах космической тематики (ОКР «Кортик» гл. конструктор В.Л. Гречка Лауреат Ленинской премии за эту разработку).

Далее работал начальником НИЛ и начальником НИО, разрабатывая специальную измерительную аппаратуру.

После выхода Постановления ЦК КПСС и Совмина СССР от февраля 1973 г № 903-903 и приказа МПСС СССР назначен в марте 1973 г. начальником головной НИЛ специальных исследований. Это определило второй и последний этап деятельности по ПД ИТР.

Новая эра началась выступлением в Москве Председателя Гостехкомиссии СССР Маршала Огаркова Н.В., который обосновал важность Постановления, исходя из возможностей и намерений предполагаемых противников. Стройное построение единой общегосударственной системы ПД ИТР дало положительный результаты в разработке В и ВТ. Эти работы базировались на научной основе, оснащении разработчиков самой современной аппаратурой контроля. Ежеквартальные семинары по научным вопросам в НИИ Автоматики г. Москва давали возможность внедрять в разработки самые современные научные достижения. В период работы по этой тематике в НИИ 110 выполнено более 20 фундаментальных НИОКР, что позволяло прогнозировать наши возможности и предполагаемых противников. Выполнен ряд работ по формированию маскирующих сигналов, слабым магнитным полям, разработаны ОКР «Гранит XVI», а «Гранит IV» с Вильнюсским КБ магнитной записи, ряд работ непосредственно для эксплуатации