КП-0.5	$D[\Delta x(t)]$	$11{,}39D[\Delta x(t)]$
КП-1	$D[\Delta x(t)]$	$69D[\Delta x(t)]$

З табл. 2 видно, що у випадку корельованого шуму ЗВ дисперсія не змінюється. Якщо шум не корельований, то дисперсія значно збільшується, причому збільшення залежить від ступеня алгоритму прогнозу та від кроку прогнозу. Лише для алгоритму КС2-0,5 дисперсія не корельованого шуму зменшується.

IV Висновки

Таким чином завдяки ПЗВ виникає можливість захистити інформацію від штучних або природних перешкод.

Використання алгоритмів прогнозу спричиняє зміну дисперсії не корельованого шуму, причому вона залежить не тільки від рівня шуму, але й від алгоритму прогнозу. У більшості випадків дисперсія збільшується. Тільки для КС2-0.5 вона має максимальне зменшення у 2 рази.

Для збільшення точності вимірювання складних процесів використовуються складні алгоритми прогнозу, такі як А3Т та А4Т, але при цьому значно збільшується дисперсія шумів. Тому при виборі алгоритму прогнозу треба порівнювати вплив шумів з похибкою методу вимірювання ПЗВ [2], і домагатися зменшення шумової складової для збільшення точності прогнозу. Для цього треба використовувати більш прості алгоритми або збільшувати коефіцієнт кореляції.

Література: 1. Губарь В. И. "Метод последовательного накопления корректирующих поправок результатов измерений". – "Метрология" – 1981., - № 2, – С. 3-9. 2. К. Б. Скочеляс "Дослідження похибок прогнозуючих засобів вимірювання". - Наукові вісті НТУУ "КПІ". – 2000. - № 6. – С 101-105.

УДК 654.924

ОЦЕНКА ВЕРОЯТНОСТИ ПЕРЕДАЧИ СООБЩЕНИЙ В СИСТЕМЕ БЕЗОПАСНОСТИ

Владимир Волхонский
Санкт-Петербургский Государственный университет аэрокосмического приборостроения

Аннотация: **Анализируются основные факторы снижения вероятности выполнения задачи системой передачи извещений в составе централизованной системы безопасности. Рассматриваются обобщенная структура многоканальной системы передачи, ее вероятностные характеристики, предлагается способ оценки вероятности передачи сообщения.**

Summary: **Analysis of general decreasing reasons of transmission signal probability in monitoring security systems. Based on offered general structure of multi channel communication system, estimation of transmission signal probability is accomplised.**

Ключевые слова: **Система безопасности, передача сообщений, помехозащищенность, вероятность.**

Один из основных элементов системы безопасности (СБ) с передачей сообщений на пункт централизованной охраны (ПЦО), то есть в системах централизованного наблюдения (СЦН) - это система передачи извещений (СПИ). В качестве каналов связи в таких системах используются главным образом телефонные и радиоканалы. Общие принципы построения таких систем достаточно широко и подробно рассмотрены в опубликованных за последнее время работах, например в [1].

Построение любой системы безопасности, как объектовой, так и централизованного наблюдения в значительной мере определяется системой передачи извещений от датчиков контроля состояния объекта (извещателей) к приемно-контрольному прибору (контрольной панели) в объектовой части СЦН и в автономных системах сигнализации или от объектовых систем на пункт централизованной охраны в СЦН. А это предполагает, в первую очередь, организацию соответствующей проводной или радио канальной системы передачи информации или извещений. Наличие достаточно большого количества абонентов (источников извещений) в обоих случаях требует создания многоканальной системы. Образование многоканальной системы может быть реализовано двумя методами объединения – централизованным или автономным [2]. В первом случае обмен информацией между абонентами происходит через центральные

станции (ЦС). Кроме того, возможен обмен и между центральными станциями – ретрансляторами (например, при передаче информации на большие расстояния). При обмене внутри одной зоны обычно достаточно одной ЦС. Такие системы называются многоканальными централизованными радиальными системами (МЦРС). Примерами МЦРС являются городские телефонные сети и ряд систем радиосвязи, которые главным образом используются в СПИ рассматриваемого класса.

МЦС позволяет организовать более эффективный обмен информацией между многими абонентами. Однако это делает их и более уязвимыми. Так как выход (или вывод) из строя ЦС приводит к выходу из строя всей системы передачи извещений в целом, и, соответственно, система безопасности не решает своей задачи.

Обычно каждой системе передачи информации выделяется свой канал связи или своя полоса частот. Использование общей полосы частот абонентами определяется методами уплотнения (размещением спектров сигналов в общей полосе частот) и разделением (выделением сигналов абонентов). Заметим, что метод уплотнения определяет и метод разделения (и наоборот).

Известны три метода разделения информации разных абонентов [2]. При методе частотного разделения (ЧР) каждому абоненту выделяется свой частотный канал (полоса частот). Полосы частот сигналов не перекрываются, но сами сигналы передаются во времени одновременно. При использовании метода временного разделения (ВР) каждый абонент работает в своем строго определенном временном интервале. Полоса частот при этом общая. Метод кодового разделения (КР) предполагает разделение по форме сигналов абонентов, работающих в одно и то же время и в одной полосе частот. В последнем случае структура СПИ и ее характеристики определяются главным образом сигналами и их свойствами (см. например, [1–2]). Системы с КР являются адресными системами и могут быть синхронными или асинхронными. Помехоустойчивость СПИ будет зависеть также от вида модуляции.

Важнейшим требованием к СПИ является надежность передачи извещений по каналу связи. Количественно это можно оценить вероятностью выполнения системой своих функций, то есть вероятностью передачи сообщения.

Обобщенная структурная схема СЦН с одним каналом передачи извещений на ПЦО представлена на рис. 1. В общем случае она включает в себя пульт централизованного наблюдения (ПЦН), СПИ и объектовую систему сигнализации (ОСС). В состав СПИ, в свою очередь, входят пультовое оконечное устройство (ПОУ), ретрансляторы (Р) и объектовое устройство (ОУ).

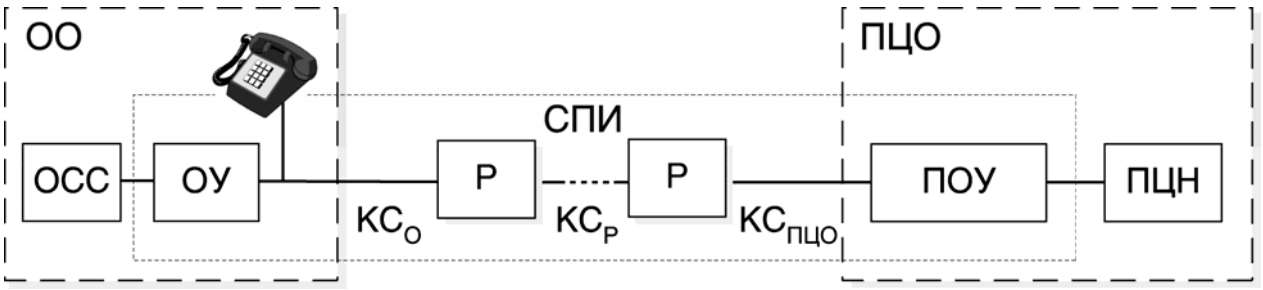

Рисунок 1 – Структурная схема СЦН

ПЦН и пультовое объектовое устройство ПОУ (приемник СПИ) устанавливаются на пункте централизованной охраны. Ретрансляторы (которые в частном случае могут и отсутствовать) расположены в определенных точках каналов связи (КС$_i$), ОУ и ОСС – на охраняемом объекте (ОО). В зависимости от конкретной технической реализации возможно конструктивное совмещение ПЦН и ПОУ, а также частичное совмещение ОУ и ОСС. В подавляющем большинстве случаев современные СЦН используют в качестве каналов связи телефонные линии (ТЛ) или радиоканал (РК).

Одним из основных методов повышения надежности передачи извещения на ПЦО является дублирование каналов связи. Естественно, что это должны быть каналы разной физической природы. Например, практически не имеет смысла использовать два передатчика одного частотного диапазона. Одновременное подавление их помехой не составит труда. В то же время использование дополнительного телефонного (проводного) или телефонного радио канала другого частотного диапазона может заметно повысить надежность СПИ.

Обобщим модель одноканальной СПИ на систему с произвольным числом каналов передачи извещений для передачи извещения от объектового оборудования на ПЦН. Структурная схема такой многоканальной системы приведена на рис. 2.

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

Мы не будем здесь рассматривать непосредственно надежность элементов системы (наработка на отказ), полагая их достаточно высокими, чтобы они не влияли на оценки вероятности выполнения системой задачи. Уделим основное внимание воздействию на СПИ различного вида помех, способных препятствовать передаче извещения.

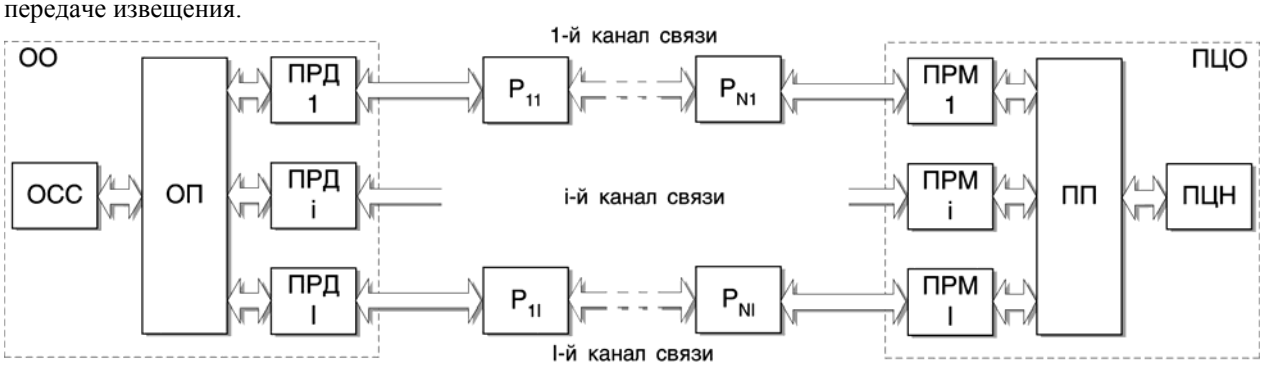

Рисунок 2 – Обобщенная структурная схема многоканальной СЦН

Обычно при оценке возможности использования какой-либо СПИ прежде всего задается вопрос о возможности контроля канала связи. В радио канальных СПИ это может быть реализовано реально только периодически с интервалом от единиц и десятков минут до нескольких часов. Реально это проверка главным образом работоспособности оборудования. При использовании современного высоконадежного оборудования эта проблема решается достаточно просто как в дуплексных системах (приемопередатчики на объектах), так и в симплексных (на объектах приемники). В последнем случае тестовые сигналы инициируются объектовым оборудованием с заданной периодичностью. В принципе это то же самое, что и инициирование теста посылкой сигнала запроса с ПЦН. Последний также должен посылаться с определенной периодичностью. Однако сам по себе контроль канала связи не обеспечивает выполнения системой своей задачи.

Наиболее опасно воздействие помех на канал связи, выводящий СПИ из строя на время постановки помехи, например, постановкой помехи в виде сигнала несущей, сформированного стандартным передатчиком с программируемой частотой вблизи ПЦО. При этом отношение сигнал/шум будет много меньше единицы и вероятность правильного приема будет близка к нулю. Сначала выделим несколько основных групп помех, влияющих прежде всего на рассматриваемый вопрос.

Помехи естественного происхождения (в первую очередь атмосферные помехи, вызываемые грозовыми разрядами).

Индустриальные помехи, создаваемые работой различного электро- и радиооборудования (электросварочными аппаратами, системами зажигания автомашин, коммутирующими устройствами мощных потребителей электроэнергии и т.д.).

Активные помехи, специально организованные для подавления СПИ (как шумовые, так и имитационные, подобные рабочим сигналам СПИ).

Структурные взаимные помехи в асинхронных системах связи, то есть сигналы разных передатчиков одной и той же системы, совпадающие во времени полностью или частично.

Заметим, что атмосферные и индустриальные помехи представляют собой кратковременные импульсы (выбросы) с широкой спектральной плотностью. При этом вопрос о влиянии структурных взаимных помех в асинхронных системах связи, создаваемых друг другу разными передатчиками одной и той же системы, связан, прежде всего, с количеством используемых передатчиков в системе, количеством передаваемых сигналов, распределением их во времени.

Основная характеристика, определяющая способность СПИ эффективно работать в составе СЦН в условиях воздействия помех – это помехозащищенность. Понятие помехозащищенности включает в себя, во-первых, скрытность СПИ и, во-вторых, ее помехоустойчивость. В свою очередь скрытность – это способность СПИ противостоять обнаружению и измерению параметров системы.

Будем рассматривать наиболее распространенные, с практической точки зрения, СПИ. К ним можно отнести асинхронно адресные системы. Это в полной мере относится к широко используемому современному способу передачи сообщений методом автодозвона по стандартным линиям телефонной сети. Кроме того, сюда же надо отнести и широкий класс систем с радиоканалом.

Будем рассматривать в качестве основной характеристики вероятность $p_З$ выполнения системой своей задачи – передачи извещения и приема его пультом. С точки зрения выполнения системой своих функций наиболее опасна постановка активных помех.

Введем следующие обозначения:

$p_З^E$ – вероятность выполнения задачи при условии воздействия только естественных помех;

$p_З^{ПЕ}$ – вероятность выполнения задачи при условии воздействия естественных помех и радиопротиводействия – постановки организованных помех;

$p_П$ – вероятность противодействия СПИ (повреждения проводного канала связи, постановка специально организованных помех и т. п.);

$p_З^{СЕ}$ – вероятность выполнения задачи при условии воздействия естественных и взаимных структурных помех.

Вероятность $p_З^{СЕ}$, как отмечалась выше, зависит от загрузки канала связи. Практически для систем, имеющих до нескольких сотен контролируемых объектов, $p_З^{СЕ}$ и $p_З^E$ близки. Поэтому сначала будем полагать $p_З^{СЕ} \approx p_З^E$ и не будем учитывать взаимные помехи.

Вероятность противодействия СПИ $p_П$ характеризует, во-первых, скрытность работы СПИ, сложность обнаружения ее работы; во-вторых, возможность эффективной разведки ее параметров; и, в-третьих, важность объекта, привлекательность его с точки зрения несанкционированных действий (проникновения, кражи, ...). Так, например, в синхронно адресных системах с постоянным опросом объектовых передатчиков легче как обнаружить работу системы, так и определить ее параметры, необходимые для эффективной постановки активной помехи. И, тем самым, существенно облегчить задачу подавления СПИ.

Два других параметра $p_З^{ПЕ}$ и $p_З^E$ являются основными количественными показателями СПИ, определяемыми при разработке системы. Исходные параметры СПИ обеспечивают определенную величину $p_З^E$. Для профессиональных радио канальных систем порядок значения этого параметра обычно составляет порядка 0.999. Для оценки сравнительных характеристик можно использовать соотношение $p_З^{ПЕ} / p_З^E$.

Вероятность выполнения одноканальной системой (рис. 1) своей задачи в условиях противодействия определяется следующей формулой

$$p_З = p_П\, p_З^{ПЕ} + (1 - p_П)\, p_З^E . \qquad (1)$$

Проанализируем это выражение. При пренебрежимо малой вероятности $p_П \approx 0$ противодействия СПИ вероятность выполнения задачи $p_З$ определяется исходными параметрами системы и, как и следовало ожидать, равна $p_З$.

При вероятности противодействия $p_П$, близкой к единице, работоспособность СПИ определяется значением $p_З^{ПЕ}$. Учитывая, что реально подавление узкополосной радиосистемы передачи извещений технически не представляет особого труда, можно считать, что $p_З^{ПЕ} \approx 0$. То есть система становится неработоспособной и, следовательно, $p_З \approx 0$. Поэтому основным способом решения этой проблемы является дублирование каналов связи (рис. 2).

Обозначим для СПИ с несколькими каналами передачи извещений между объектом и ПЦО $p_{Зi}$ - вероятность выполнения задачи i-м каналом; $p_{Пi}$ - вероятность противодействия i-му каналу СПИ. При правильном выборе основных характеристик и параметров каналов связи и обеспечении достаточно высокой скрытности вероятность организации противодействия каналам связи и вероятность выполнения задачи каждым из каналов $p_{Зi}$ можно считать независимыми, поскольку они будут определяться возможностями

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

обнаружения этого канала, определения его параметров и создания и применения соответствующих средств противодействия. Тогда, к примеру, для двухканальной системы вероятность передачи извещения хотя бы одним каналом СПИ будет определяться выражением

$$p_з^{II} = p_{з1} + p_{з2} - p_{з1} p_{з2} \ . \tag{2}$$

Подставляя значения $p_{з1}$ и $p_{з2}$ в последнюю формулу нетрудно убедиться, что $p_з^{II} >> p_з$.

Таким образом, основными путями повышения вероятности выполнения СПИ своей задачи являются повышение помехозащищенности (как помехоустойчивости, так и скрытности) и правильное структурное построение системы, дублирование не только каналов связи, но и ПЦО (территориально разнесенных).

С точки зрения дублирования каналов связи наиболее распространенный вариант – это использование радиоканала и проводного телефонного. В последнее время перспективным и достаточно легко реализуемым становится применение телефонного радиоканала. При этом телефонный канал использует другой частотный диапазон, обладает достаточно высокой скрытностью и помехоустойчивостью. А это делает его применение весьма эффективным. Кроме того, регулярный обмен информацией радиотелефона с базовой станцией может служить основой для организации регулярного контроля канала связи уже имеющимися средствами.

Оценим влияние взаимных структурных помех в асинхронно-адресной СПИ, имеющей на объектах только передатчики. Рассмотрим ситуацию с передачей источником сообщения одного сигнала о событии в СБ в течении суток. Обозначим длительность сигнала t_c . Будем полагать, что любое перекрытие двух сигналов во времени ведет к тому, что ни один из них не будет принят.

Можно говорить о двух типичных вариантах плотности распределения вероятности $p(t)$ передачи сигнала в системе. Это, во-первых, равномерное распределение (рис. 3) на интервале 24 часа, типичное, к примеру для систем пожарной сигнализации. В таких случаях количество служебных сообщений мало (обычно это сигналы авто теста объектового оборудования), тревожные сообщения достаточно редки, чтобы не учитывать их влияние на $p_1(t)$.

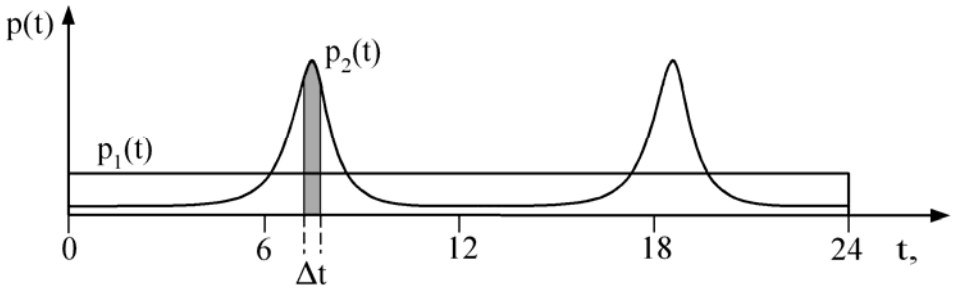

Рисунок 3 – Плотность распределения вероятности передачи сигналов во времени

Во-вторых, это многомодальные распределения, свойственные, например, системам охранной сигнализации $p_2(t)$ (рис. 3). В таких системах передается достаточно много служебных сообщений, которые неравномерно распределены по времени. Примером могут служить сигналы постановки на охрану и снятия с охраны, передаваемые в основном в утренние часы и в конце рабочего дня. Соответственно вероятности совпадения сигналов в эти периоды времени совпадают.

Для радиоканальной СПИ, с учетом соотношения реальных длительностей сигнала и продолжительности суток, можно рассматривать попадание сигнала на дискретный интервал, равный его длительности t_c . Соответственно вероятность попадания сигнала в этот интервал, равномерно распределенный на протяжении суток, будет определяться выражением

$$p = \frac{t_c}{24 \cdot 60 \cdot 60} . \tag{3}$$

Вероятность совпадения *n* сигналов из *N* передаваемых определится формулой

$$p_c = p_n^n q^{N-n} C_N^n \text{, где } q = 1 - p \ . \tag{4}$$

Если в качестве примера взять систему, имеющую 1000 абонентов, каждый из которых передает в сутки один сигнал с длительностью t_c =0,1с, то вероятность совпадения можно вычислить по формуле

$$p_c = p_n^2 q^{998} C_{1000}^2 \text{, где } C_{1000}^2 = \frac{1000!}{2!\cdot(1000-2)!}. \quad (5)$$

После подстановки значений в выражение (5) и вычислений получим численное значение p_c порядка 10^{-6}.

Широко используемый способ повышения надежности СПИ (в нашей задаче – повышения вероятности правильного приема сообщения на ПЦО) – это дублирование (неоднократный повтор) сообщения. При этом целесообразно использовать не просто повтор сообщения через определенный интервал времени, а повтор со случайным временным сдвигом. Тогда вероятность полного совпадения двух сигналов будет практически равна нулю. Чтобы полностью подавить сигнал в этом случае необходимо, чтобы каждый из сигналов пачки совпадал с разными сигналами взаимных помех.

Приведенная выше методика расчета соответствуют первому случаю (равномерному распределению $p_1(t)$). Для второго примера допущение, сделанное выше, становится некорректным. В этом случае необходимо либо оценивать плотность распределения вероятности $p_2(t)$ и вероятность попадания в интервалы времени Δt максимальной загрузки канала, а также аппарат теории массового обслуживания.

Литература: 1. В. В. Волхонский. Системы охранной сигнализации. Экополис и культура. СПб., 2000, 160 с. 2. Варакин Л. Е. Системы связи с шумоподобными сигналами. –М., Радио и связь, 1985, 384 с. 3. Защита от радиопомех. – М., под ред. Максимова М. В., Сов. радио, 1976, 496 с. 4. В. В. Волхонский Оценка помехоустойчивости нелинейных алгоритмов обработки сигналов. Радиоэлектроника". Известия МВ и ССО СССР, т. 30, № 4, 1987.

УДК 621.96

ПРОБЛЕМНЫЕ АСПЕКТЫ РЕАЛИЗАЦИИ ПРОСТРАНСТВЕННОГО И ЛИНЕЙНОГО ЗАШУМЛЕНИЯ В СИСТЕМАХ АКТИВНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Сергей Емельянов, Николай Логвиненко, Виталий Носов, Владимир Писаревский
Национальный университет внутренних дел, г. Харьков

Аннотация: **Обоснована необходимость разработки генераторов шума, реализующих пространственное и линейное зашумление опасных сигналов в электромагнитном и электрическом каналах утечки информации. Приведены результаты экспериментальных исследований макетов разработанных генераторов шума, оценена эффективность их применения.**

Summary: **Necessity of creation of generators of noise is proved. Generators create a radio noise in space and in an electric network. Results of experiments are given. Efficiency of application of the developed generators is appreciated.**

Ключевые слова: **Генератор шума, радио закладка , сетевая закладка.**

I Введение

Одним из путей реализации угроз конфиденциальности информации, обрабатываемой средствами электронно-вычислительной техники (ЭВТ), являются технические каналы утечки информации (КУИ) [1–3]. Среди технических КУИ большую опасность для компьютерной информации представляют электромагнитный и электрический каналы. Первый из них может быть образован побочными электромагнитными излучениями (ПЭМИ) средств ЭВТ, а также за счет скрытно установленных закладных устройств с передачей информации по радиоканалу – радио закладка (РЗ). Источниками опасных сигналов во втором канале могут быть наводки ПЭМИ на цепи электропитания, просачивающиеся в них информационные сигналы средств ЭВТ, а также закладные устройства с передачей информации по электросети – сетевая закладка (СЗ) [2, 3].

Для блокировки указанных КУИ в системах активной защиты информации используют методы

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.