

Поиск устройств негласного получения информации, использующих шумоподобные сигналы

В статье рассмотрены вопросы обнаружения сигналов с шумоподобным спектром техническими средствами радионаблюдения (далее – поисковым приемником) при проведении мероприятий по контролю эффективности защиты информации. Основной ее целью является ознакомление специалистов с демаскирующими признаками шумоподобных сигналов, методами и средствами обнаружения электронных устройств негласного получения информации (ЭУНПИ), использующих шумоподобные сигналы.

Д. И. Белорусов, генеральный директор ООО «РИКОМ»

Е. И. Кубов, начальник Управления разработки и производства ЗАО «НПЦ Фирма «НЕЛК»

Основным признаком, по которому сигналы, рассматриваемые в настоящей статье, выделяются в отдельный класс шумоподобных сигналов (сигналов с шумоподобным спектром), является то, что спектральная мощность таких сигналов в занимаемой полосе на длительном интервале наблюдения сопоставима с мощностью шума в этой полосе или ниже.

Хотя сам по себе этот факт еще ничего не говорит о потенциальной сложности обнаружения таких сигналов, поскольку спектральная плотность мощности сигнала может быть достаточно высокой, но позволяет выделить шумоподобные сигналы в отдельный класс. Как будет показано ниже, шумоподобные сигналы обладают рядом «замечательных» свойств, которые, в свою очередь, могут существенно затруднить их

обнаружение и различение обычными средствами радионаблюдения, основанными на спектральном анализе сигналов, а именно – энергетическую и структурную скрытность.

Кроме того, как правило, шумоподобные сигналы имеют достаточно широкую полосу, существенно превышающую ширину спектра переносимого ими сообщения, а зачастую – и полосу пропускания поисковых приемников, что также снижает качество их обнаружения.

Задача поиска шумоподобных сигналов состоит из двух взаимосвязанных частей: обнаружения сигнала и различения сигнала. В общем виде решением задачи является метод, который позволит определить признак(и) отсутствия или наличия шумоподобного сигнала в смеси с шумом и отличить его от истинного шума в анализируемой выборке.

Под «обнаружением» в данном случае понимается фиксирование с заданной вероятностью наличия признаков искомого сигнала на фоне аддитивного шума по некоторому признаку. Для фиксирования

признака необходимо выбрать проекцию признака (например, гистограмму), которая позволит зафиксировать наличие признака пороговой схемой обнаружения. При наличии четко фиксируемой количественной оценки данного признака (статистики) возможно исследование обнаруженного сигнала с целью уточнения параметров, например несущей частоты и полосы, которое понадобится для повышения качества следующей стадии поиска – различения.

Для шумоподобных сигналов стадия обнаружения является необходимой, но не может считаться достаточной. Следующей не менее важной стадией поиска шумоподобных сигналов является «различение» обнаруженного сигнала. Как следует из названия шумоподобных сигналов, при их обнаружении возможны ложные результаты, связанные с обнаружением шумовых сигналов или помех, сходных по признакам с искомым. Поэтому на этапе различения результат обнаружения следует подвергнуть дополнительной вери-

фикации, исследовав свойства обнаруженного сигнала и сопоставив их со свойствами известных шумоподобных сигналов.

В данной статье качество обнаружения шумоподобных сигналов будет оцениваться по совокупности двух критериев:

- вероятности обнаружения (p_o) – величины обратной вероятности пропуска искомого сигнала ($1 - p_{п}$), которая характеризует *точность* метода обнаружения;
- вероятности ложной тревоги ($p_{л}$) – вероятности ошибочного обнаружения помехового сигнала, которая характеризует *помехоустойчивость* системы обнаружения.

Если в качестве критерия качества обнаружения сигналов использовать не только вероятность обнаружения, но и вероятность ложной тревоги, то понятие «обнаружение» необходимо рассматривать несколько шире, чем для узкополосных сигналов. Для нормирования вероятности ложной тревоги не достаточно обнаружить сигнал, необходимо убедиться, что обнаруженный сигнал не является помехой, то есть доследовать сигнал процедурой различения.

Примером может служить обнаружение сигнала с псевдослучайной перестройкой рабочей частоты (ППРЧ). Обнаружение отдельных составляющих само по себе не будет являться обнаружением ППРЧ-сигнала, пока не удастся, например, установить, что частоты появления составляющих имеют детерминированную структуру, отличающую его от стохастических сигналов узкополосных помех.

Шумоподобные сигналы (рис. 1) можно разделить на две основные группы: постояннодействующие и пакетные (англ. – burst) сигналы.

Постоянно действующие сигналы характеризуются в общем случае достаточно стабильной во времени спектральной плотностью мощности, в то время как сигналы, передающиеся в пакетном режиме, излучаются в эфир не постоянно, и поэтому спектральная плотность мощности таких сигналов может меняться во времени от нулевого до пикового значения. Этим, собственно, и обуславливается их близость к шуму

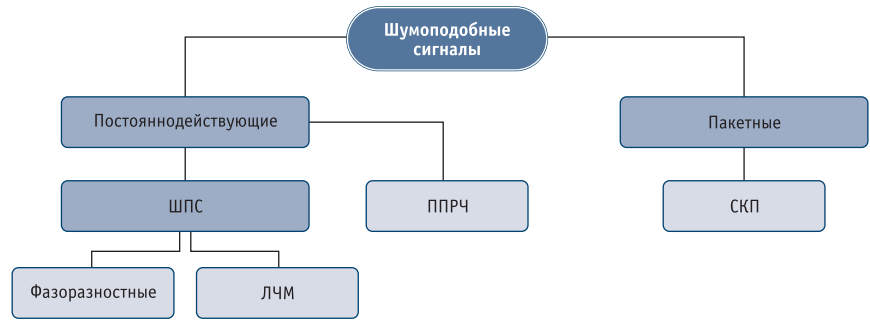


Рис. 1. Классификация шумоподобных сигналов

му средней спектральной мощности. Для постояннодействующих сигналов близость спектральной мощности сигнала к спектральной мощности шума может достигаться различными способами. Для ШПС-сигналов это возможно благодаря малой собственно спектральной мощности сигнала. Для ППРЧ сигнала это обусловлено тем, что в каждый момент времени сигнал излучается в полосе во много раз более узкой, чем та, в которой может перестраиваться рабочая частота сигнала. Для пакетных сигналов, в частности СКП, это обусловлено сверхкороткими длительностями посылок (порядка сотен наносекунд).

Дополнительные сложности при обнаружении СКП-сигналов могут возникнуть, если скважность следования посылок не постоянная и изменяется по псевдослучайному закону. При этом СКП-сигналы по определению сложными не являются, а лишь подчиняются требованиям теоремы Шеннона.

Сформулируем основные определения, которые понадобятся для понимания природы шумоподобных сигналов.

Базой сигнала называется произведение:

$$B = \Delta F \times T, \quad (1)$$

где ΔF – ширина спектра сигнала; T – длительность символа информационного сообщения, которое несет в себе этот сигнал.

Сложными называются сигналы, у которых значение $B \gg 1$, в отличие от простых сигналов, где $B = 1$. Другими словами, сложные сигналы несут в себе избыточность, которая определяет их замечательные свойства, не увеличивая при этом информационной емкости сигнала.

Повышенная скрытность сложных сигналов обеспечивается тем, что при равных мощностях и длительностях сигнала, то есть при равных энергиях, спектральная плотность сложных сигналов в B раз меньше, чем у узкополосных сигналов.

База сигнала (иногда называемая информационной емкостью сигнала) также прямо пропорциональна числу признаков сигнала, которые должен иметь для сравнения поисковый приемник, чтобы отличить этот сигнал от любого другого после установления факта наличия сигнала в смеси с шумом на входе (структурная скрытность).

Сложные сигналы, как правило, являются постоянно действующими сигналами, то есть они имеют постоянную временную структуру. Можно считать, что постоянно действующий сигнал гарантировано присутствует в течение всего времени наблюдения.

Из (1) очевидно, что для простых сигналов при условии равенства базы сигнала единице существует жесткая взаимосвязь между полосой сигнала и количеством передаваемой информации. Эта связь описывается теоремой Шеннона. Другими словами, при необходимости передать некоторый объем информации за меньшее время необходимо расширить полосу сигнала. Такое расширение спектра имеет место, например, если передатчик работает в пакетном режиме, то есть чередует режим передачи сообщения с режимом радиомолчания, и чем короче время передачи, тем более широкую полосу будет иметь такой сигнал. Как крайний случай такого сигнала можно рассматривать так называемые сигналы сверхкоротких посылок (СКП), передающие накопленную инфор-

мацию за очень короткий промежуток времени (порядка сотен наносекунд, занимая при этом полосу в сотни мегагерц).

Если на вход поискового приемника, который имеет значительно меньшую полосу пропускания, чем полоса сигнала, поступает смесь СКП-сигнала с шумом, то приемник примет лишь ограниченную своей полосой часть мощности сигнала (*неопределенность по несущей*). При этом плотность шума не изменится, так как шум имеет бесконечный спектр. Как следствие, спектральная плотность принятого сигнала в полосе пропускания поискового приемника будет стремиться к спектральной плотности шума (*энергетическая скрытность*).

Очевидно, приемник не может принимать сигнал постоянно, поскольку вынужден перестраиваться, а если скважность СКП-сигнала меняется по псевдослучайному закону, неизвестному приемнику, то вероятность обнаружения такого сигнала еще более значительно сокращается из-за несовпадения времени наблюдения и посылки СКП (*неопределенность по времени*).

Как и в случае со сложными сигналами, расширение полосы в сигналах СКП не приводит к увеличению информационной емкости, а лишь позволяет сохранить пропускную способность канала передачи.

Допустим, поисковый приемник является классическим энергетическим обнаружителем. Решение о наличии сигнала в аддитивной смеси с шумом в нем принимается на основе сравнения мощности принятого сигнала P_c с некоторым порогом h_0 (*пороговая схема обнаружения*).

При любом пороге обнаружения h_0 вероятность правильного обнаружения будет зависеть от отношения мощности сигнала (P_c) к мощности шумов ($P_{ш}$) на выходе приемника в полосе пропускания, называемого *отношением «сигнал/шум»*:

$$q = P_c / P_{ш}. \quad (2)$$

Очевидно, что для шумоподобных сигналов мощность сигнала P_c будет стремиться к мощности шума $P_{ш}$, уменьшая вероятность обнаружения.

Для простых сигналов с аналоговыми видами модуляций уверенный прием сигнала (с нормированием вероятности обнаружения и вероятности ложной тревоги) возможен при значениях «сигнал/шум» $q \gg 1$. Например, одноканальное обнаружение без усреднения постояннодействующего узкополосного сигнала с вероятностью 0,99 и вероятностью ложной тревоги 5×10^{-2} возможно при $q = 22$.

Отношение «сигнал/шум» на выходе приемника q пропорционально произведению отношения «сигнал/шум» на входе приемника $q_{вх}$ и коэффициента шума ($K_{ш}$) приемника:

$$q = q_{вх} K_{ш}. \quad (3)$$

Если предположить, что соотношение «сигнал/шум» на входе разведывательного (принимающего сигнал УЭНПИ) и поискового приемников равны, то, скорее всего, соотношение «сигнал/шум» на выходе разведывательного приемника будет несколько выше, чем у поискового. Связано это с тем, что $K_{ш}$ разведывательного приемника будет меньше $K_{ш}$ поискового приемника, поскольку последний строится по более сложной схеме из-за необходимости сканирования в широкой полосе частот.

Однако, вероятнее всего, соотношение «сигнал/шум» на входе поискового приемника будет значительно превышать аналогичный показатель на входе разведывательного из-за близкого расположения поискового приемника к источнику искомого сигнала по сравнению с разведывательным. И это преимущество будет пропорционально квадрату расстояния по мощности.

Таким образом, можно утверждать следующее: при обнаружении постояннодействующего узкополосного сигнала на выходе поискового энергетического приемника соотношение «сигнал/шум» всегда будет достаточным для уверенного обнаружения сигнала при условии уверенного обнаружения этого же сигнала в разведывательном приемнике.

При переходе к обнаружению шумоподобных сигналов утверждение, изложенное выше, будет, скорее всего, неверно.

Если считать, что энергетическая скрытность сигнала – это способность противостоять обнаружению, то основным признаком, позволяющим поисковому приемнику судить о наличии сигнала в условиях априорной неопределенности параметров сигнала, является энергия, которую имеет входной процесс (сумма сигнала с шумом) на интервале времени наблюдения единичного символа сообщения, несущего в себе сигнал:

$$E = (P_c + P_{ш}) T_H. \quad (4)$$

где P_c – средняя мощность сигнала в интервале времени наблюдения T_H ; $P_{ш}$ – мощность шума.

Тогда соотношение «сигнал/шум» можно выразить как:

$$q = E_c / E_{ш} = E_c / N_{ш} \Delta f T_H, \quad (5)$$

где E_c – энергия сигнала; $E_{ш}$ – энергия шума.

Как видно, $E_{ш}$ определяется спектральной плотностью шума $N_{ш}$, полосой пропускания приемника Δf и временем наблюдения T_H .

Если разведывательный приемник является оптимальным для искомого сигнала, то есть полоса пропускания приемника Δf равна полосе сигнала (приемник использует всю мощность сигнала, распределенную по спектру), а время наблюдения равно длительности сигнала (приемник не теряет энергию, распределенную во времени), то преимущество в соотношении «сигнал/шум» по сравнению с входом поискового приемника увеличивается, а вероятность обнаружения сигнала поисковым приемником снижается с ростом базы сигнала $B = \Delta f T_H$.

Детальный анализ [1] показывает, что имеет место преимущество оптимального разведывательного приемника по сравнению с неоптимальным поисковым приемником при пороговом обнаружении в корень квадратный раз от базы сигнала $\sqrt{\Delta f T_H}$.

Разведывательный приемник может располагать информацией о структуре сигнала, в том числе о фазовой структуре. Использование фазовой информации позволяет организовать в разведывательном приемнике когерентный прием сигнала.

При когерентном приеме суммирование аддитивной смеси на входе приемника, состоящей из когерентных сигналов и некоррелированных шумовых колебаний, приведет к тому, что пиковое значение сигнала возрастает в n^2 раз по мощности, а значение некоррелированного шума – в n раз по мощности. Таким образом, итоговое соотношение «сигнал/шум» возрастает в n раз, где n – количество накопленных когерентных реализаций сигнала. Соответственно, поисковый приемник в условиях априорной неопределенности параметров сигналов лишен такой возможности.

Изложенное выше, при условии когерентного приема (фазовой синхронизации) с соотношением энергий сигнала и шума на входе приемника до минус 20 дБ по мощности, позволяет организовывать в разведывательном приемнике прием и обработку сигналов большой базы (сложных сигналов) с фазоразностными видами модуляций. Очевидно, что при таком или любом другом достаточно малом соотношении «сигнал/шум» на входе энергетического поискового приемника пороговое обнаружение и спектральный анализ не эффективны. Их применение возможно лишь при использовании корреляционного поискового приемника.

Как было показано выше, в условиях априорной неопределенности по частоте, полосе, времени, фазе искомого сигнала и неизвестном местоположении источника сигнала пространственное преимущество поискового приемника, актуальное для простых сигналов, для шумоподобных сигналов ничтожно по сравнению с возможностями разведывательного приемника по оптимальному приему сигнала. Другими словами, в условиях априорной параметрической неопределенности поисковый приемник, построенный по классической схеме с использованием в качестве основного демаскирующего признака превышение сигнала над шумом, практически не имеет шансов обнаружить сигнал с приемлемым качеством, а спектральный анализ сигнала бесполезен для различения последнего, по-

скольку в таком приемнике невозможно отличить шумоподобный сигнал от помехи или шума.

Может показаться, что обнаружение шумоподобных сигналов поисковыми приемниками на фоне помех при плохой осведомленности о параметрах сигнала невозможно. Но это не так. Шумоподобные сигналы имеют несколько демаскирующих признаков.

Энергетический признак. Как уже упоминалось ранее, спектральная плотность мощности шумоподобного сигнала может быть достаточно высокой на коротком интервале времени. При условии совпадения времени наблюдения полосы пропускания приемника со временем появления и полосой сигнала полностью или частично, реализации некоторых типов шумоподобных сигналов могут быть обнаружены, в том числе могут наблюдаться на энергетическом спектре в БПФ представлении (например, ППРЧ-сигнал).

Статистический признак. Шумоподобные сигналы, генерируемые радиопередающими устройствами, обязательно являются детерминированными (не случайными). Это свойство необходимо для восстановления сигнала на приемной стороне в разведывательном приемнике и оно же может быть использовано в поисковом приемнике для различения шумоподобного сигнала, например от случайных шумовых выбросов или сигналов узкополосных помех.

Корреляционный признак. Сложные сигналы, в силу некоторых особенностей формирования, имеют ряд специфических характеристик, отражающих изменения сигнала во времени, а именно узкую автокорреляционную функцию с малыми боковыми выбросами (для когерентных сигналов).

Временной признак. Ввиду особенности построения задающих генераторов тактовой частоты сложные сигналы, как правило, являются периодическими, то есть имеют выраженный период повторения, который может быть достаточно большим и не всегда укладываться в длительность T_n – время наблюдения в поисковом приемнике.

Таким образом, мы приходим к необходимости формулирования требований к поисковому приемнику, способному обнаруживать и различать шумоподобные сигналы:

- широкая полоса пропускания с обработкой в режиме реального времени (на текущем уровне развития телекоммуникационных технологий – от 50 МГц и более);
- высокая *производительность*: процедуры обнаружения, уточнения параметров и различения должны быть выполнены независимо (по крайней мере, обнаружение и уточнение параметров должны выполняться параллельно);
- в приемнике должны применяться алгоритмы анализа сигналов, способные обнаруживать демаскирующие признаки шумоподобных сигналов с низким и отрицательным соотношением «сигнал/шум»;
- в приемнике должно быть использовано такое представление искомого сигнала, проекции которого были бы достаточно чувствительны к изменению признака, позволяющего отличить шумоподобный сигнал от шума или отличить сигналы с различными видами модуляции между собой.

Указанным критериям удовлетворяет приемник, в основе которого лежит модель корреляционного обнаружителя с некогерентными каналами и широкой полосой пропускания. Как было показано, такая модель обнаружителя уступает идеальному когерентному обнаружителю (в данном случае – разведывательному приемнику) по энергетическому критерию не более чем на 2,5 дБ, что, безусловно, приемлемо в условиях, когда поисковый приемник обладает по сравнению с разведывательным приемником преимуществом в пространственном расположении.

В качестве примера практической реализации указанных выше требований к эффективному обнаружителю шумоподобных сигналов можно привести поисковый приемник, применяемый в программно-аппаратных комплексах выявления электронных устройств негласного получения информации «Крона-А» и «Бастион».