

УДК 681.3.06

**С.Л. Емельянов**

кандидат технических наук, доцент

## СИСТЕМАТИЗАЦИЯ КРИТЕРИЕВ ОЦЕНКИ ЭФФЕКТИВНОСТИ ПОМЕХ СИСТЕМ АКТИВНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

*Систематизированы возможные критерии оценки эффективности видов и параметров помех в системах активной защиты информации и показаны результаты их применения.*

**Ключевые слова:** активная помеха, система активной защиты, эффективность, критерий.

*Систематизовано можливі критерії оцінки ефективності видів і параметрів перешкод у системах активного захисту інформації й показано результати їх застосування.*

**Ключові слова:** активна перешкода, система активного захисту, ефективність, критерій.

*Possible criterion are systematized for an estimation of the effectiveness noise parameters and its kinds in the systems of the information active protection and the results of their using are shown.*

**Keywords:** active noise, active protection system, effectiveness, criterion.

В целях защиты информации и блокирования разнообразных технических каналов утечки информации широкое применение находят методы активной маскировки [1–3]. Их сущность заключается в создании преднамеренных помех в канале утечки информации, затрудняющих выделение полезных (разведываемых) сигналов и измерение их информативных параметров на фоне помех. Подобные системы активной защиты (САЗ) применяются, например, для защиты от радиомикрофонов, маскировки побочных электромагнитных излучений и наводок (ПЭМИН) средств ЭВТ, маскировки акустических и виброакустических сигналов из выделенных помещений, подавления средств скрытной аудио- и видеозаписи, противодействия системам активной радиолокационной, гидролокационной и лазерной разведки и т.д.

Одной из актуальных проблем при разработке и внедрении любой САЗ является обоснование видов и параметров активных помех, оптимальных по заданному критерию эффективности.

В теории и технике радиоподавления достаточно хорошо исследованы и реализованы практически *информационный* и *энергетический* критерии, позволяющие синтезировать оптимальные помехи и оценить эффективность подавления конкретного средства разведки [4]. В настоящее время большое внимание уделяется также вопросам экономического обоснования эффективности САЗ [5].

Однако ранее *нерешенной частью проблемы* является систематизация существующих критериев оценки эффективности САЗ, их сравнительный анализ

и исследование особенностей практической реализации, что и составляет *цель написания статьи*.

Эффективность средств и способов маскировки можно оценивать по различным критериям (или их совокупности), основные из которых показаны на рис.1.

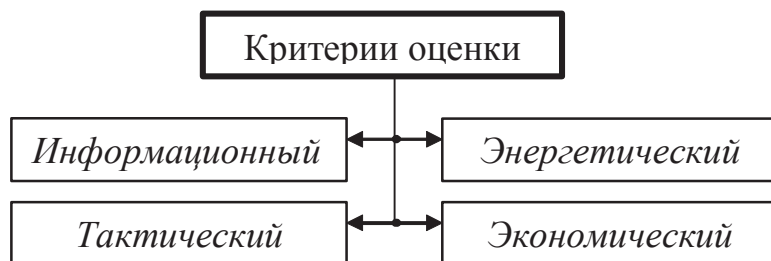


Рис.1. Основные критерии оценки эффективности маскировки

*Информационный критерий* является наиболее универсальным и используется для сравнительной оценки качества помеховых сигналов. Он позволяет определить эффективность заданного помехового сигнала по подавлению средства разведки и его устойчивость к контрмерам противника, направленным для борьбы с помехами.

При использовании данного критерия мерой, маскирующей способности помех, служит их энтропия или энтропийная мощность, уменьшающая количество информации, получаемое противником от данного средства разведки. В рамках данного критерия показано [4, 6], что при наличии ограничения на среднюю мощность шума  $\sigma^2$  наибольшей энтропией  $H_n$  обладает гауссовский шум, для которого

$$H_n(x) = \ln \sqrt{2\pi e \sigma^2} . \quad (1)$$

Заметим, что шумовые помеховые сигналы являются наиболее универсальными среди известных к настоящему времени помеховых сигналов [4, с. 91]. Они обеспечивают принципиальную возможность маскировки разведываемых сигналов любой структуры и формы. Если помеховый сигнал представляет собой белый шум (БШ), то вероятность правильного обнаружения разведываемого сигнала в шумах на выходе даже оптимального приемника определяется только отношением энергии сигнала к спектральной плотности шума и не зависит от формы скрываемого сигнала.

Однако формирование помехи типа БШ в широких диапазонах защищаемых (разведываемых) частот требует высокого энергопотенциала САЗ, увеличивает их массогабаритные характеристики, усложняет электромагнитную обстановку на объекте разведки и может приводить к нарушению медикобиологических норм на уровне излучений. Например, многие подавители диктофонов (“Сапфир”, “Буря”, УПД и др.) имеют специальные медицинские сертификаты, в которых указано, на каком расстоянии и сколько по времени может находиться человек в зоне излучения.

Поэтому в ряде практических случаев применения САЗ предлагается формирование отличных от гауссовых помех, что позволяет снизить энергетические требования к ним и упростить их техническую реализацию в широком диапазоне защищаемых частот [4].

Поиск оптимальных помех, отличных от гауссовых, как в радиодиапазоне, так и в речевом диапазоне частот является достаточно актуальной задачей и продолжается до сих пор. Ее успешное решение позволяет добиться энергетического выигрыша в генераторе маскирующих помех, упростить его техническую реализацию, обеспечить защиту более широкого диапазона частот при сохранении заданного качества подавления и т.д.

Например, в качестве шумовых в современных системах акустической и виброакустической маскировки (САВАМ) могут применяться помехи типа БШ, “розовый” шум (РШ), “коричневый” шум (КШ) и “окрашенный” шум (ОШ).

Помеха типа БШ имеет постоянную спектральную плотность мощности в речевом диапазоне частот. Помеха типа РШ ( $1/f$ -шум) – акустический шум со спадом спектральной плотности 3 дБ на октаву в сторону высоких частот. Она может быть создана путем прохождения БШ через фильтр, имеющий скорость спада АЧХ 3 дБ/октаву.

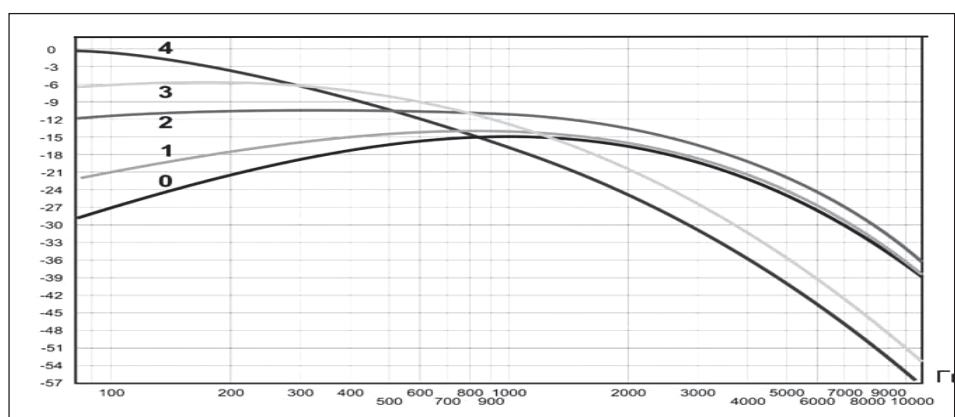


Рис.2. Огибающие интегрального спектра шумовых помех в 5-ти режимах работы САВАМ “Соната-АВ”

Помеха типа КШ ( $1/f^2$ -шум) – акустический шум со спадом спектральной плотности 6 дБ на октаву в сторону высоких частот.

В качестве иллюстрации на рис. 2 приведены спектральные профили шумовых помех, формируемые новой САВАМ российского производства “Соната-АВ” [7].

В работах [8, 9] на основе информационного критерия показано, что спектральная плотность “оптимальной” помехи с точностью до постоянного множителя должна совпадать с амплитудно-частотным спектром разведываемого (защищаемого) сигнала.

Поэтому помеха типа ОШ – акустический шум с огибающей спектра, подобной усредненному речевому сигналу. Для формирования ОШ в основных октавных полосах речевого диапазона частот производится оценка параметров речевого сигнала и осуществляется корректировка уровня шума в тех же полосах, с помощью, например, встроенных эквалайзеров.

Так, САВАМ “Шорох-1” позволяет регулировать не только выходную мощность, но и форму генерируемой помехи пятиполосным октавным эквалайзером, а в САВАМ “Барон” встроен низкочастотный четырехканальный пятиполосный анализатор спектра [7].

Известно также, что основная доля энергии видеосигнала дисплея ПК заключена в строчной структуре. Поэтому оптимальным условием для обнаружения видеосигнала в шумах будет устройство, имеющее передаточную характеристику, определяемую спектром последовательности строчных гасящих импульсов. Применение для активной защиты помехового сигнала, имеющего нормальный закон распределения в видимой части строки и распределение спектральной плотности, подобное строчной структуре защищаемого видеосигнала, обеспечивает выигрыш в энергии помехи более чем в 20 раз, по сравнению с применением для этой цели помехи типа БШ [10, с. 265].

*Энергетический критерий* отличается от информационного тем, что он требует знания конкретных характеристик (например, энергопотенциала) подавляемых средств разведки.

Для сравнения вводится коэффициент подавления  $K_n = (P_{\text{пех}}/P_{\text{свх}})_{\text{мин}}$ , определяющий минимальное отношение мощности помехи  $P_n$  к мощности сигнала  $P_c$  на входе подавляемого приемника в пределах его полосы пропускания, при котором имеет место заданная эффективность подавления.

Заранее известная система разведки может быть подавлена с меньшими энергетическими затратами помеховым сигналом, неоптимальным по информационному критерию. Однако если помеховый сигнал выбран и имеется возможность изменения какого-либо его параметра, то наилучшая степень подавления соответствует минимальному коэффициенту подавления и наибольшей энтропии этого помехового сигнала.

*Тактический критерий* позволяет оценивать полноту выполнения задачи различными САЗ и обеспечивает их сравнение между собой. Наиболее полной количественной характеристикой тактического критерия является вероятность выполнения противником конкретной задачи, например, обнаружения заданного объекта. Другими показателями тактической эффективности могут быть: увеличение ошибок местоопределения координат разведываемых объектов, увеличение времени обнаружения объекта на фоне помех и др.

Например, о точности измерения параметров сигналов средствами радиотехнической разведки можно судить по апостериорному распределению вероятностей  $P_{ps}(\lambda_c)$ , которое известным образом связано с их априорным для разведки распределением вероятности параметров  $P_{pr}(\lambda_c)$  и функционалом правдоподобия [3]:

$$P_{ps}(\lambda_c) = \kappa P_{pr}(\lambda_c) F(\lambda_c, \lambda_n), \quad (2)$$

где:  $\kappa$  – нормирующий множитель, а  $F(\lambda_c, \lambda_n)$  – функционал правдоподобия параметров сигнала  $\lambda_c$ , наблюдаемого средством разведки на фоне созданной САЗ маскирующей помехи с параметрами  $\lambda_n$ .

Сигнал с помехой принимается на фоне аддитивного нормального шума (внутреннего шума разведприемника) и маскирующих помех, поэтому [3, 11]:

$$F(\lambda_c, \lambda_n) = \exp \left\{ -\frac{1}{N_0} \int_0^T [x(t) - C(t, \lambda_c) - \Pi(t, \lambda_n)]^2 dt \right\}, \quad (3)$$

где:  $x(t)$  – наблюдаемое приемником разведки колебание – аддитивная смесь сигнала, маскирующей помехи и шума;  $C(t, \lambda_c)$  – скрываемый от разведки (информативный) сигнал;  $\Pi(t, \lambda_n)$  – маскирующая помеха;  $N_0$  – спектральная плотность мощности шума;  $T$  – длительность времени наблюдения сигнала приемником средства РТР.

Минимизация апостериорного распределения вероятностей  $P_{ps}(\lambda_c)$  с помощью САЗ достигается за счет снижения уровня максимума функционала правдоподобия  $F(\lambda_c, \lambda_n)$  (3), т.е. за счет такого выбора помехи  $\Pi(t, \lambda_n)$ , при котором

$$\frac{1}{N_0} \int_0^T [x(t) - C(t, \lambda_c) - \Pi(t, \lambda_n)]^2 dt \rightarrow \max. \quad (4)$$

Заметим, что в (4) входят слагаемые, не зависящие от  $\Pi(t, \lambda_n)$ . Их можно исключить из рассмотрения, подобрав соответствующим образом нормирующий коэффициент  $\kappa$  в (2). Поэтому подлежащее максимизации значение показателя степени при экспоненте в функционале правдоподобия (3) будет иметь вид

$$\frac{1}{N_0} \int_0^T \Pi(t, \lambda_n)^2 dt - \frac{1}{N_0} \int_0^T x(t) \Pi(t, \lambda_n) dt + \frac{1}{N_0} \int_0^T C(t, \lambda_c) \Pi(t, \lambda_n) dt. \quad (5)$$

Форму (5) можно максимизировать в результате следующих действий.

Во-первых, можно увеличить мощность активной помехи на входе развед-приемника, или, точнее, увеличить энергетическое соотношение

$$\frac{1}{N_0} \int_0^T \Pi(t, \lambda_n)^2 dt = \frac{E_n(T)}{N_0} \rightarrow \max, \quad (6)$$

где  $\frac{E_n(T)}{N_0}$  – энергия маскирующей помехи, наблюдаемой средством разведки в сеансе продолжительностью  $T$ . Однако величину энергии помехи, как отмечалось ранее, ограничивают требования электромагнитной совместимости, медико-биологические нормы, применяемая в САЗ элементная база и т.д.

Во-вторых, для уменьшения уровня главного максимума функционала правдоподобия можно увеличить значение функции

$$r_{cn} = \frac{1}{N_0} \int_0^T C(t, \lambda_c) \Pi(t, \lambda_n) dt \rightarrow \max, \quad (7)$$

по определению совпадающей с функцией взаимной корреляции между сигналом и маскирующей его помехой.

Содержательное условие (7) означает, что сигнал и помеха должны быть максимально похожими друг на друга, трудноразличимыми для разведывательного

приемника. Иначе говоря, маскирующая помеха должна имитировать сигнал по форме и по значениям параметров. Утверждение об имитирующем характере активной помехи следует понимать в том смысле, что она должна совпадать с сигналом по неинформативным для разведки параметрам, но максимально отличаться по значениям параметров информативных. Например, в современных САВАМ широко используются не только шумовые помехи, описанные ранее, но и речеподобные помехи, синтезированные из речевых фрагментов защищаемой речи с помощью специальных фонемных клонеров. Показано, что речеподобные помехи позволяют достичь заданного тактического показателя – коэффициента неразборчивости речи при меньших на порядок мощностях помехи, по сравнению с шумовой помехой типа БШ [12].

В-третьих, повышение эффективности противодействия разведке достигается за счет уменьшения взаимной корреляции между активной помехой и наблюдаемым разведприемником, результирующим колебанием  $x(t)$

$$r_{nn} = \frac{1}{N_0} \int_0^T x(t) \Pi(t, \lambda_n) dt \rightarrow \min. \quad (8)$$

На содержательном уровне это условие означает, что при маскировке параметров сигнала нужно затруднять для средств разведки определение как самого факта активного противодействия, так и параметров маскирующей помехи. В противном случае маскирующее действие помех может быть, в свою очередь, минимизировано (скомпенсировано) на стороне разведприемника.

*Экономический критерий* служит для оценки САЗ с точки зрения их эффективности и стоимости и широко используется при разработке САЗ. Оптимизация САЗ по экономическому критерию заключается в определении оптимальных параметров помеховых сигналов, мощности передатчика помех, диаграммы направленности и других характеристик САЗ при наличии ряда ограничений, основным из которых является стоимость системы САЗ и ее основных компонентов, а также их масса, объем, габариты и т. д.

Ущерб от утраты защищаемой информации может быть гораздо меньше стоимости САЗ. Поэтому уровень финансовых средств, выделяемых на создание и эксплуатацию САЗ, должен быть сбалансированным и соответствовать масштабу возможных угроз. Если стоимость САЗ, по сравнению с предполагаемым ущербом, мала, то основным фактором риска собственника являются экономические потери от несанкционированных действий с принадлежащей ему информацией. В противоположной ситуации основные потери связаны с чрезмерно высокой стоимостью САЗ. Такой качественный анализ позволяет предполагать, что существует область экономически оптимальных САЗ, обеспечивающих наименьший риск собственника информации (рис. 3). В качестве меры риска понимаются ожидаемые суммарные потери в процессе защиты информации от утечки в течение определенного периода времени.



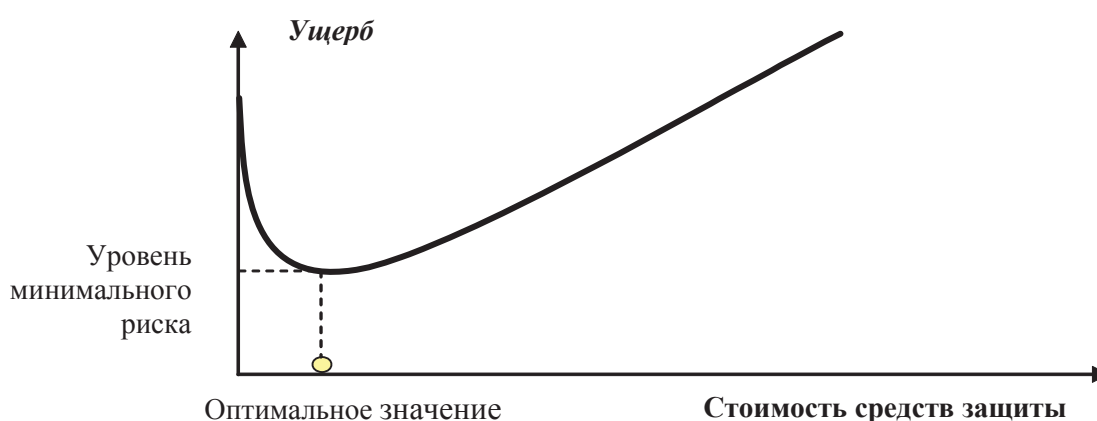


Рис. 3. Экономический критерий

Анализ рис. 3 показывает, что применение даже недорогих способов и средств защиты информации резко снижает суммарные потери собственника. Таким образом, вложение средств в САЗ уже в сравнительно небольших размерах является весьма эффективным. При некоторой стоимости САЗ риск имеет наименьшее значение. Эта стоимость является оптимальной. Дальнейший, сверх оптимального значения, рост затрат на САЗ будет вести к увеличению экономических потерь собственника информации. Поэтому наилучшей стратегией собственника информации будет, очевидно, использование САЗ, обеспечивающих минимум риска. Чем больше оценка размера вероятного ущерба, тем выше и оптимальная стоимость САЗ, однако эта зависимость достаточно гладкая, особенно в диапазоне больших значений ожидаемого ущерба.

Таким образом, основными критериями, позволяющими оценивать эффективность маскировки разведываемых сигналов, являются информационный, энергетический, тактический и экономический. Каждый из них обладает собственными преимуществами и недостатками, а также особенностями технической реализации и используется в современных САЗ.

#### СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Хорошко В.А. Методы и средства защиты информации / В.А. Хорошко, А.А. Чекатков. — Юниор. — 2003. — 504 с.
2. Энциклопедия промышленного шпионажа / Ю.Ф. Каторин, Е.В. Куренков, А.В. Лысов, А.Н. Остапенко ; под общ. ред. Е.В. Куренкова. — С.-Петербург : ООО "Изд-во Полигон", 1999. — 512 с.
3. Демин В.П. Радиоэлектронная разведка и радиомаскировка / В.П. Демин, А.И. Куприянов, А.В. Сахаров. — М. : Изд-во МАИ, 1997. — 156 с.
4. Вакин С.А. Основы радиопротиводействия и радиотехнической разведки / С.А. Вакин, Л.Н. Шустов. — М. : Изд-во "Советское радио", 1968. — 448 с.
5. Баутов А. Экономический взгляд на проблемы информационной безопасности / А. Баутов // Открытые системы. — 2002. — № 2.
6. Тихонов В.И. Оптимальный прием сигналов / В.И. Тихонов. — М. : Радио и связь, 1983. — 320 с.
7. Емельянов С.Л. Систематизация методов и средств защиты акустики помещений / С.Л. Емельянов // Системи обробки інформації. — 2012. — Вип. 4 (102). — С. 31–36.
8. Емельянов С.Л. Некоторые аспекты оптимизации помех в системах активной защиты информации / С.Л. Емельянов // Приладобудування і радіотехніка. — Вісник ЧДТУ. — 2009. — № 1. — С. 63–65.

9. *Емельянов С.Л.* Альтернативные подходы к оптимизации помех в системах активной защиты информации / С.Л. Емельянов // Наукові записки Українського науково-дослідного інституту зв'язку. – 2007. – № 2. – С. 97–100.
10. *Домарев В.В.* Защита информации и безопасность компьютерных систем / В.В. Домарев. – К. : Изд-во “Диа Софт”, 1999. – 480 с.
11. *Ширман Я.Д.* Теория и техника обработки радиолокационной информации на фоне помех / Я. Ширман, В. Манжос. – Радио и связь, 1981. – 416 с.
12. *Болдырев А.А.* Ступени эффективности : речеподобная помеха и непрерывный контроль / А.А. Болдырев, В.В. Бондаренко // Защита информации. INSIDE. – 2005. – № 2. – С. 40–44.

Отримано 10.08.2013