9. D. R. Stinson. Combinatorial techniques for universal hashing, submitted to J. Comput. System Sci.

10. D. R. Stinson. Combinatorial characterizations of authentication codes, submitted to Designs, Codes and Cryptography (a preliminary version appears elsewhere in these proceedings).

11. M. N. Wegman and J. L. Carter. New hash functions and their use in authentication and set equality, J. Comput. System Sci. 22 (1981), 265-279.

12. Federal Criteria for Information Technology security. – NIST, NSA, US Government, 1993.

13. Cryptrec. Cryptrec liaison report to ISO/IEC 18033-2 and 18033-3. Technical report, ryptography Research and Evaluation Committees, October 2002.

14. Jakob Jonsson and Burt Kaliski. RSA-PSS. Primitive submitted to NESSIE by RSA,September 2000.

*Поступила 23.01.09*

**УДК 681.3.004**

**Петров А.А.**

## ОПРЕДЕЛЕНИЯ ТЕХНИЧЕСКИХ ХАРАКТЕРИСТИК СИСТЕМ АКТИВНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Под техническими характеристиками (ТХ) систем активной защиты будем понимать ряд важнейших качеств данной системы, определяющих эффективность ее применения как средства защиты информации от утечки за счет ПЭМИН. К числу таких характеристик могут быть отнесены:

1) маскировочная способность;
2) защищенность по отношению к методам селекции и компенсации помех;
3) скрытность применения;
4) универсальность;
5) соответствие требованиям электромагнитной совместимости;
6) простота технической реализации.

Маскирующая способность систем активно защиты (САЗ) характеризует степень подавления приемника перехвата искусственной помехой и зависит, в первую очередь, от применяемого класса помех, что определяет потенциальные возможности САЗ, а также от полноты технической реализации предложенной математической модели помехи. Эта характеристика требует качественного описания и должная позволять сравнивать достигнутую за счет применения САЗ защищенность канала утечки с установленными нормами на границе контролируемой зоны.

Естественным количественным показателем, наиболее полно отражающим маскирующую способность помехи, является средняя вероятность ошибки при приеме одного бита информации. Именно эта величина нормируется в качестве первичной в действующей и последующих редакциях норм, поскольку она определяет возможность восстановления перехваченной информации. Вероятность ошибки во многом зависит от способа приема, и для создания гарантированного уровня защищенности принято исходить из предположения, что техническая разведка пользуется оптимальными методами приема и, тем самым, может минимизировать величину средней вероятности ошибки.

Изложенной соображение предполагает метод количественной оценки маскирующей способности помех, заключающейся в следующем:

1. С учетом действующих в канале утечки сигналов и помех формируется математическая

модель взаимодействия сигналов и помех, в соответствии с которой синтезируется оптимальный алгоритм приема сигналов.

2. В результате анализа алгоритма приема сигналов определяется выражение для средней вероятности ошибки приема сигналов на фоне помех.

Такой подход носит универсальный характер, поскольку изменения параметров сигналов и помех влияют на модель и результаты синтеза и анализа, но не приводят к изменению общей процедуры, определяемой схемой: математическая модель – синтез алгоритма – анализ алгоритма. Однако его недостатком является сложность расчета в задачах анализа и синтеза, особенно при использовании негауссовых классов помех[1].

Вторая характеристика – защищенность по отношению к методам селекции и компенсации помех, оказывает большое влияние на эффективность САЗ. Принципиальная возможность снижения эффективности САЗ за счет селекции и компенсации базируется на отличии структуры и закономерностей изменения параметров, свойственных опасным сигналам и мешающим воздействиям.

Селекция помех возможна по различным признаками как раздельно, так и комбинировано [2]. Пространственная селекция обеспечивается антенной приемника перехвата. Чем уже ее диаграмма направленности и меньше уровень боковых лепестков, тем выше пространственная селекция. Поляризационная селекция основывается на различии поляризации принимаемых сигналов и помех, временная – на возможности различать помехи и сигналы по временным параметрам.

При компенсации помех, помимо основного приемного канала, реагирующего на смесь сигнала и помехи, используется дополнительный канал приема, воспринимающий только помехи. Интенсивность помех в компенсационном и основном каналах выбираются одинаковыми, а фазы - противоположными, в результате чего помеха компенсируется.

Количественная оценка защищенности по отношению к методам компенсации помех может быть основана на величине средней вероятности ошибки на один бит, полученной в результате анализа структурной схемы оптимального приемника с компенсацией.

Третья характеристика – скрытность применения, отражает способность САЗ функционировать, не привлекая дополнительного внимания ТСР к особо важным объектам, на которых ведется обработка секретной информации. Строгая количественная оценка данной характеристики затруднена, поскольку ей соответствует достаточно сложная математическая модель, однако вполне возможна объективная качественная оценка.

Поскольку в самом принципе действия САЗ заложено создание активных помех, то весьма важной ее характеристикой является электромагнитная совместимость (ЭМС) с защищаемым техническим средством сети общего пользования и окружающими радиоэлектронными средствами. На эту характеристику влияют следующие факторы:

- энергетические и вероятностные характеристики помехи;
- применяемая элементная база;
- конструкция устройства, компоновка узлов и блоков, восприимчивых к воздействию помехой т.п.

Все это приводит к тому, что довольно трудно дать однозначную количественную оценку ЭМС САЗ, и в значительной мере эти свойства могут быть определены лишь экспериментальным путем [3, 2, 4]. Тем не менее, очевидно, что, добиваясь одних и тех же маскирующих свойств помехи при меньшей ее мощности, обеспечивается лучшая ЭМС САЗ. Поэтому одним из количественных показателей ЭМС САЗ может служить величина средней мощности помехи (в абсолютном или относительном выражении), необходимая для определения заданной средней вероятности ошибки приема одного бита информации.

Смысл такой качественной характеристики как простота технической реализации очевиден и не требует дополнительных комментариев.

Имеет смысл на базе описанных ТХ провести анализ используемых в настоящее время САЗ, определить их слабые стороны и наметить пути совершенствования. Рассмотрение ТХ в совокупности показывает, что для детального количественного описания необходимо использовать величину средней вероятности ошибки приема сигналов на фоне помех, полученной в результате решения задач синтеза и анализа соответствующих оптимальных алгоритмов, а качественные оценки могут быть получены путем анализа математической модели помехи и способов ее практической реализации.

**Выводы**

Таким образом, можно сделать вывод, что эффективность любой САЗ определяется совокупностью ее основных ТХ. С учетом этого должен проводиться анализ существующих систем и определяться направления их совершенствования.

**Список литературы**

1. Новиков А.А. Анализ отношения сигнал/маскирующая помеха в системах пространственного зашумления при произвольном расположении источников помехи и опасного сигнала: отчет НИИ "Квант", 1981.-33С.

2. Защита от радиопомех/Под ред. М.В. Максимова.- М.: Сов. радио, 1967.-496 с.

3. Захаров Е.К. Активное противодействие перехвату ПЭМИН дисплеев ЭВМ и персональных компьютеров// Тезисы докладов Межведомственной конференции по безопасности информации, обрабатываемой в АСУ, СВТ и ТСПИ.- М., 1990.- с.132-133.

4. Ордынский А.Б. Методология пространственного зашумления // Тезисы докладов Межведомственной конференции по безопасности информации, обрабатываемой в АСУ, СВТ и ТСПИ.- М., 1990.-с.115-116.

*Поступила 23.01.09*

**УДК 004.681.3**

**Бартків Н.І., Коротєєв І.М.**

## МЕТОДИ ВИЯВЛЕННЯ ТА ЛОКАЛІЗАЦІЇ ДЖЕРЕЛ НЕСАНКЦІОНОВАНОГО ВИПРОМІНЮВАННЯ

Необізнаний громадянин тільки з журналів та газет отримує сенсаційну інформацію, що десь у владних структурах виявлено «жучок». Різноманітність пристроїв витоку інформації викликана не тільки попитом починаючи з пересічних громадян що бажають слідкувати за своїми родичами, але й «професійною» потребою кримінальних елементів.

Все частіше з метою заволодіння важкодоступної інформації використовуються електронні пристрої перехоплення інформації (закладні пристрої), що скрито встановлюються в технічні засоби обробки, збереження і передачі інформації, подарунки, а також в будівельних конструкціях службових приміщень.

Одним зі шляхів передачі інформації є використання радіоканалу (радіозакладок). Тому виявлення на об'єкті інформаційної діяльності технічних засобів передачі інформації є одним із напрямків забезпечення інформаційної безпеки підприємств, установ і організацій незалежно від їх форм власності.

Зараз на вітчизняному ринку представлено широкий асортимент засобів пошуку та локалізації закладних пристроїв, серед яких значну роль відводиться комплексам радіомоніторингу (далі - КРМ), які побудовані на базі сучасних скануючих приймачів. Це