
АНАЛИЗ ОСНОВНЫХ ТЕХНИЧЕСКИХ ХАРАКТЕРИСТИК СИСТЕМ АКТИВНОЙ ЗАЩИТЫ В СЕТЯХ ОБЩЕГО ПОЛЬЗОВАНИЯ

Петров Антон Александрович¹, канд. техн. наук

Минина Евгения Александровна², канд. экон. наук

¹ Ведущий разработчик систем искусственного интеллекта, ООО «Геомир-Агро»; ул. Колонцова, 5, пом. 302, Мытищи, Россия, 141009; e-mail: petrov@geomir.ru

² Кубанский государственный аграрный университет им. И. Т. Трубилина, ул. Калинина, 13, Краснодар, Россия, 350044; e-mail: minina.e@edu.kubsau.ru

Предмет: одной из основных задач при создании систем активной защиты является многокритериальная оптимизация технических характеристик. *Цель:* решение этой задачи предусматривает, помимо количественного или качественного описания каждой характеристики, их сравнение с аналогичными характеристиками систем активной защиты, использующих другие классы помех. *Дизайн исследования:* системы активной защиты с прицельными параметрами имеют некоторые преимущества перед другими системами активной защиты, поэтому оценка их эффективности произведена путем сравнения соответствующих технических характеристик. В статье рассмотрена маскирующая способность прицельной помехи и ее зависимость от параметров, определяющих схемные и конструктивные особенности генераторов помех; маскирующая способность прицельной помехи по отношению к идеальному параллельному коду. Сравнение маскирующей способности прицельной и имитирующей помех в условиях полного совпадения параметров помехи и сигнала без учета гауссовского компонента сводится к рассмотрению влияния числа уровней квантования помехи m на среднюю вероятность ошибки. Сравнение маскирующей способности прицельной и имитирующей помех в условиях полного совпадения параметров помехи и сигнала без учета гауссовского компонента сводится к рассмотрению влияния числа уровней квантования помехи m на среднюю вероятность ошибки. *Результаты:* авторами представлены обобщенные результаты качественного и количественного анализа основных технических характеристик систем активной защиты, использующих прицельные, имитирующие и гауссовские помехи. По результатам сравнительного анализа наиболее эффективными следует признать САЗ ПП и в несколько в меньшей степени САЗ ГП. САЗ ИП уступает им по общей эффективности и имеет значительно худ-

шие показатели по первым двум важнейшим техническим характеристикам.

Ключевые слова: уровни квантования помехи, вероятность ошибки, разрядность параллельного кода.

DOI: 10.17308/meps/2078-9017/2022/10/34-46

Введение

Одной из основных задач при создании систем активной защиты является многокритериальная оптимизация технических характеристик. Решение этой задачи предусматривает, помимо количественного или качественного описания каждой характеристики, их сравнение с аналогичными характеристиками систем активной защиты (САЗ), использующих другие классы помех. САЗ с прицельными параметрами имеют некоторые преимущества перед другими САЗ, поэтому оценку их эффективности будем производить путем сравнения соответствующих технических характеристик (ТХ).

Методы и результаты исследования

Рассмотрим маскирующую способность прицельной помехи и ее зависимость от параметров, определяющих схемные и конструктивные особенности генераторов помех. Маскирующие свойства прицельной помехи в значительной степени обусловлены таким параметром, как число уровней квантования m . На рис. 1 и 2 приведены результаты расчетов средней вероятности ошибки для последовательных кодов с основанием p и равномерным распределением символов¹. Случай, когда $n=2$, соответствующий двоичному коду, представляет особый интерес. Как видно из рис. 1, нормированная величина вероятности ошибки даже для объектов первой категории ($P_{Ош} = 0,4602$) достигается при относительно небольших величинах параметра m^2 . Для его окончательного выбора при практической реализации необходимо учитывать следующие обстоятельства.

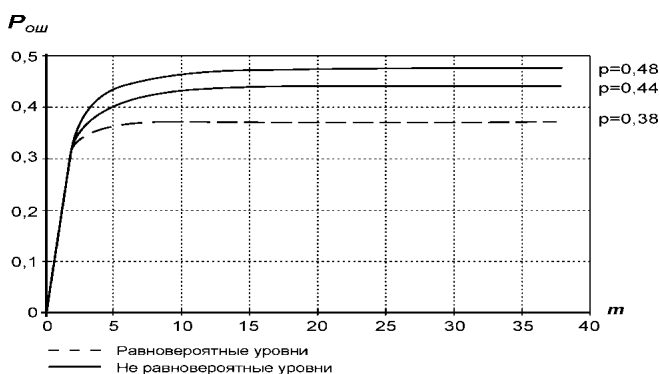


Рис. 1. Зависимость вероятности ошибки от числа уровней квантования помехи

¹ Гуткин Л.С. Теория оптимальных методов радиоприема при флуктуационных помехах: 2-е изд. Москва, Сов. радио, 1972. 448 с.

² Ризкин А.А. Основы теории усилительных схем. Москва, Сов. радио, 1954. 420 с.

Во-первых, увеличение числа элементов, используемых в схеме генератора помехи, происходит скачком пропорционально целой части $\log(m+1)$. Так, количество элементов, используемых в генераторах помехи на 5-8 уровней, практически одинаково, тогда как маскирующая способность таких помех различна.

Во-вторых, при снижении требований к точности параметров помехи приходится увеличивать или число уровней квантования помехи, или мощность помехи.

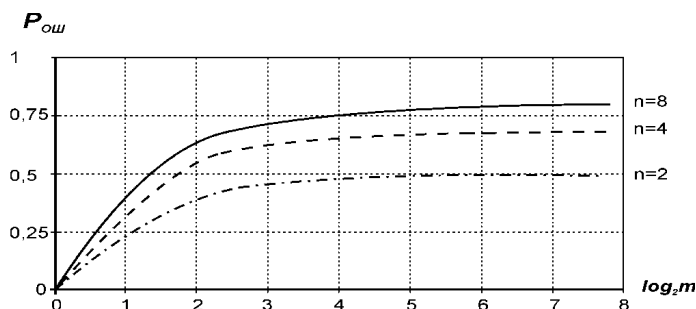


Рис. 2. Зависимость вероятности ошибки от числа уровней квантования помехи для n -разрядного последовательного кода с биномиальным распределением уровней

Следовательно, для обеспечения заданной маскирующей способности число уровней квантования помехи m должно выбираться с некоторым запасом в соответствии с таблицей 1 путем округления в большую сторону до тех пор, пока $\log(m+1)$ не примет ближайшее целое значение.

Таблица 1

Зависимость значения параметра m для различных категорий объектов при представлении информации в последовательном коде

Категория объекта	1	2	3
Число уровней квантования	15	7	3

Рассмотрим маскирующую способность прицельной помехи по отношению к идеальному параллельному коду. Его особенностью является то, что при приеме даже в отсутствии помех возникают ошибки, вероятность которых увеличивается с увеличением разрядности кода. Так, например, как видно из рис. 3, уже 8-разрядный параллельный код удовлетворяет требованиям норм по третьей категории^{3,4}. Кроме того, необходимое число уровней квантования помехи в значительной степени зависит от разрядно-

³ Ванштейн Т.Г. Теория обработки сигналов автоматического управления в радиоэлектронных системах. Л., МО, 1992. 245 с.

⁴ Котоусов А.С. Различение детерминированных сигналов в квазидетерминированном потоке импульсов // Проблемы передачи информации, 1976, т. 12. вып. 1, с. 41-47.

сти параллельного кода, однако для вероятности ошибки, соответствующей нормам для объектов первой категории, такая зависимость проявляется в меньшей степени.

Выбор значений параметра m для различных категорий объектов при представлении информации в параллельном коде осуществляется с учетом ранее сделанных замечаний в соответствии с таблицей 2.

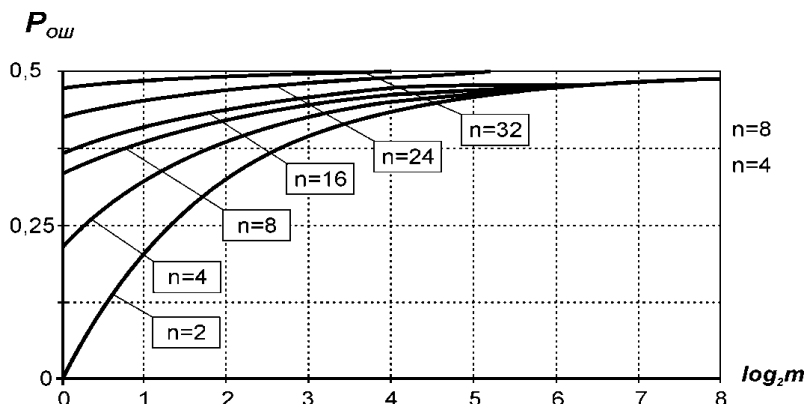


Рис. 3. Зависимость вероятности ошибки от числа уровней квантования помехи для двоичного равновероятного параллельного кода

Таблица 2

Соответствие числа уровней квантования помехи для 8-, 16- и 32-разрядного параллельного кода

Категория объекта	1			2			3		
	Разрядность параллельного кода	8	16	32	8	16	32	8	16
Число уровней квантования	15	7	3	3	1	0	1	0	0

Сравнение маскирующей способности прицельной и имитирующей помех в условиях полного совпадения параметров помехи и сигнала без учета гауссовского компонента сводится к рассмотрению влияния числа уровней квантования помехи m на среднюю вероятность ошибки.

Предельно допустимая маскирующая способность имитирующей помехи несколько выше, чем у прицельных помех. Так, например, в симметричном канале, в котором присутствует опасный сигнал, представленный в последовательном коде, и имитирующая помеха, вероятность ошибки равна 0,5, в то время как для прицельной помехи с $m=15$ вероятность ошибки уменьшается лишь на 0,03. С другой стороны, маскирующая способность имитирующих помех снижается за счет того, что генератор помех в процессе ее формирования сам становится источником опасного инверсного сигнала и должен проходить специальные исследования. Указанное об-

стоятельство ограничивает применимость САЗ с имитирующими помехами.

Остановимся подробнее на сравнении сигналоподобных помех по величине параметра m . Как уже отмечалось, значение t прицельной помехи для сигналов последовательного кода выбирается в соответствии с таблицей 1 и лежит в пределах от 15 до 3 в зависимости от категории объекта. В случае имитирующей помехи параметр $m=1$, то есть имеется некоторый выигрыш. Несколько иная картина наблюдается для сигналов двоичного параллельного кода. Значение m в этом случае колеблется: в пределах от 15 до 0 в зависимости от категории объекта и разрядности кода. Для имитирующей помехи параметр m должен выбираться из условия обеспечения постоянного уровня излучения в соответствии с максимальным весом Хемминга, который для двоичного TV-разрядного параллельного кода равен N .

Отсюда следует, что чем выше разрядность кода, тем больше максимальное число уровней квантования имитирующей помехи m . Для прицельных помех имеет место обратная зависимость числа уровней квантования m от разрядности кода N (рис. 4). Учитывая, что параллельный способ передачи информации является наиболее распространенным в ЭВМ, можно утверждать, что по величине параметра m прицельные помехи дают в общем случае выигрыш по сравнению с имитирующими помехами.

Таким образом, сравнение прицельных и имитирующих помех по величине маскирующей способности оказывается в пользу первого класса помех. Следует отметить, что прицельные помехи по величине маскирующей способности имеют некоторое преимущество и перед гауссовскими помехами за счет того, что одна и та же средняя вероятность ошибки достигается при меньшей мощности помехи [9].

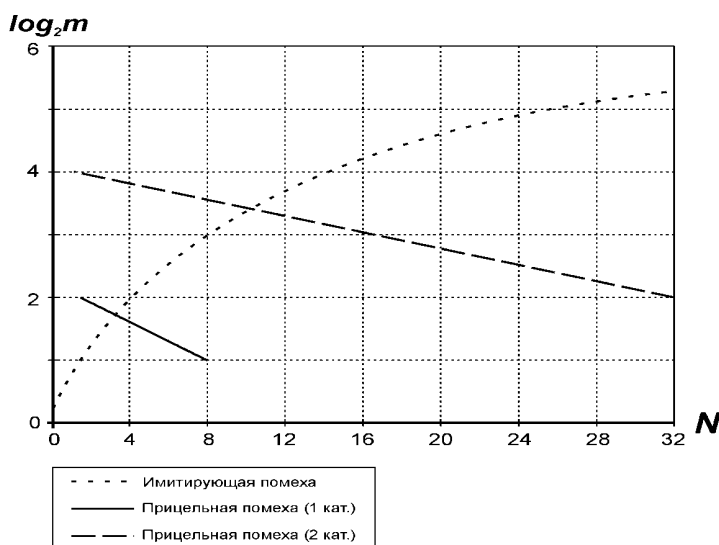


Рис. 4. Зависимость $\log_2 m$ от разрядности параллельного кода для имитирующей и прицельной помех

Рассмотрим количественные показатели защищенности по отношению к методам селекции и компенсации САЗ, использующих сигналоподобные помехи, поскольку для них эта проблема наиболее актуальна. Степень возможной компенсации помех определяется величиной взаимной энергии E или производного от нее параметра – отношения сигнал-помеха/шум q .

Иногда удобно пользоваться более сложным параметром η , равным

$$\eta = \frac{E_{Si}}{\sqrt{E_s \cdot E_i}} = \frac{q_{Si}}{\sqrt{q_s \cdot q_i}}. \quad (1)$$

Для прицельных помех параметр η представляет собой коэффициент корреляции случайного процесса на выходах линейных частей тракта обработки сигнала и канала компенсации помехи.

Воспользуемся результатами, которые дают возможность проанализировать влияние параметра η на вероятность ошибки. На рис. 5 приведены зависимость вероятности ошибки в канале с последовательным кодом прицельной или имитирующей помехи от параметра η .

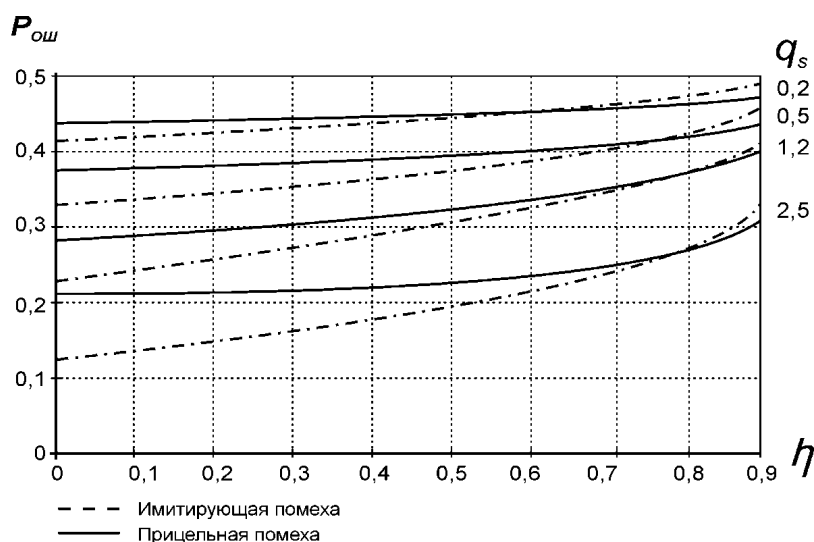


Рис. 5. Влияние точности параметров сигналоподобных помех на вероятность ошибки

Для прицельных ($m=15$) и имитирующих помех в качестве дополнительного параметра в семействе кривых фигурирует отношение сигнал/шум q . Предполагается, что отношение сигнал/шум q_s и помеха/шум q_i равны. Такое предположение вполне корректно, поскольку при практической реализации САЗ стремятся добиться максимального совпадения параметров разряда помехи и сигнала, а имеющиеся несовпадения в основном вызваны незначительными временными задержками и другими различиями временных параметров.

Из графиков, приведенных на рис. 5, становится очевидно, что наличие гауссовского компонента, интенсивность которого характеризуется величиной q_s , снижает степень компенсации сигналоподобной помехи. Таким образом, величина отношения сигнал/шум в канале утечки определяет своеобразный допуск на точность параметров как прицельной, так и имитирующей помехи. Параметр m в основном влияет на максимальную величину вероятности ошибки.

Кроме того, полученные графики, представленные на рис. 6, 7, показывают имеющиеся существенные различия между прицельной и имитирующей помехами. В области значений параметра $0,7 < \eta < 0,9$ происходит снижение эффективности обеих помех тем интенсивнее, чем больше величина отношения сигнал/шум. Однако возможность компенсации имитирующей помехи возрастает заметно быстрее. При значении параметра $\eta < 0,5$ средняя вероятность ошибки для имитирующей помехи становится даже ниже, чем при наличии только гауссовского компонента. Это свидетельствует о том, что при $\eta < 0,5$ имитирующая помеха не только не обеспечивает защищенность канала, а даже приводит к ее снижению. Причины, ухудшающие маскирующие свойства прицельных помех, отличаются от тех, которые приводят к уменьшению средней вероятности ошибки в канале с имитирующими помехами. Снижение средней вероятности ошибки для прицельных помех происходит в результате того, что при приближении значений параметра η к нулю происходит все более полная их компенсация, и, наконец, при $\eta = 0$ прицельная помеха компенсируется полностью. Однако при этом вероятность ошибки остается равной величине, обусловленной присутствием в канале гауссовского компонента. При отрицательных значениях параметра η будет наблюдаться рост величины средней вероятности ошибки, поскольку условия для компенсации ухудшаются, и при $\eta = -1$ средняя вероятность ошибки вновь достигает максимального значения.

Снижение вероятности ошибки в канале с имитирующими помехами вызвано тем, что по мере уменьшения взаимной энергии, как известно, фактически улучшается различение сигнала и помехи. Так, например, при $\eta = 0$ сигнал и помеха становятся ортогональными, а при $\eta = -1$ противофазными, что значительно улучшает их различение. Снижение эффективности имитирующих помех в области отрицательных значений параметра η по сравнению с каналом, в котором присутствует только гауссовский компонент, показано на графиках рис. 6, из которых видно, что снижение может быть значительным.

Минимальный выигрыш в энергетическом отношении сигнал/помеха, получаемый за счет применения прицельных помех, при корректном выборе параметра η ($\eta > 0,8$) колеблется в пределах от 2,2 до 1,6 раза в зависимости от категории объекта. За счет применения многоканальных схем величина выигрыша может быть увеличена в несколько раз. Применение многоканальных схем в САЗ с имитирующими помехами из-за жесткой связи

сигнала и помехи не дает положительного результата, так как при приеме помехи одного из каналов проникновение помех из других каналов способствует ухудшению совпадения сигнала и помехи (параметр η уменьшается).

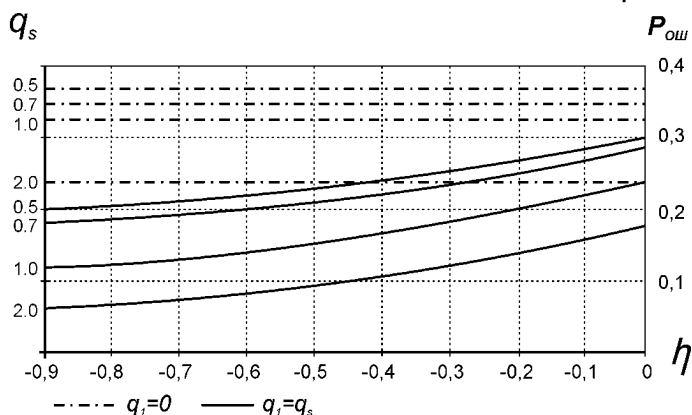


Рис. 6. Снижение эффективности имитирующей помехи относительно гауссовской в области отрицательных значений параметра η

Таким образом, САЗ прицельной помехи превосходят САЗ имитирующей помехи по защищенности по отношению к методам селекции и компенсации помех, но несколько уступают по этому показателю САЗ гауссовской помехи. Область применения САЗ имитирующей помехи должна быть ограниченной и включать в себя те случаи, когда величина параметра η с достаточной гарантией поддерживается на уровне 0,8-0,9. Очевидно, что сюда относится область низких частот и те ситуации, когда достаточно просто моделируется излучатель опасного сигнала.

Сравнение параметров САЗ, характеризующих ЭМС, целесообразно проводить путем анализа влияния относительных энергозатрат (отношения сигнал/помеха q) на величину средней вероятности ошибки. На рис. 7 приведен график, характеризующий зависимость средней вероятности ошибки от отношения сигнал/помеха для канала с $\lambda = 1$.

Кривая, соответствующая прицельной помехе с компенсированной постоянной составляющей, проходит выше кривых, соответствующих как гауссовской, так к прицельной помехе без компенсации постоянной составляющей. Это свидетельствует о том, что прицельная помеха позволяет получать в канале большую вероятность ошибки по сравнению с другими помехами при одинаковой с ними мощности помех. Однако разница в затратах энергии на получение определенной вероятности ошибки для всех трех типов помех неодинакова в различных условиях: для области относительно больших значений $P_{ош}$, соответствующих требованиям норм для объектов первой категории, эта разница невелика, но она становится существенной для области, соответствующей нормам для объектов второй и третьей категорий.

При рассмотрении канала с неравновероятным появлением единиц и

нулей, что менее характерно для опасных сигналов корпоративных сетей, можно отметить те же тенденции. В этом случае придельные помехи с равновероятными и неравновероятными уровнями практически на всей шкале измерений отношения сигнал/помеха превосходят гауссовские помехи.

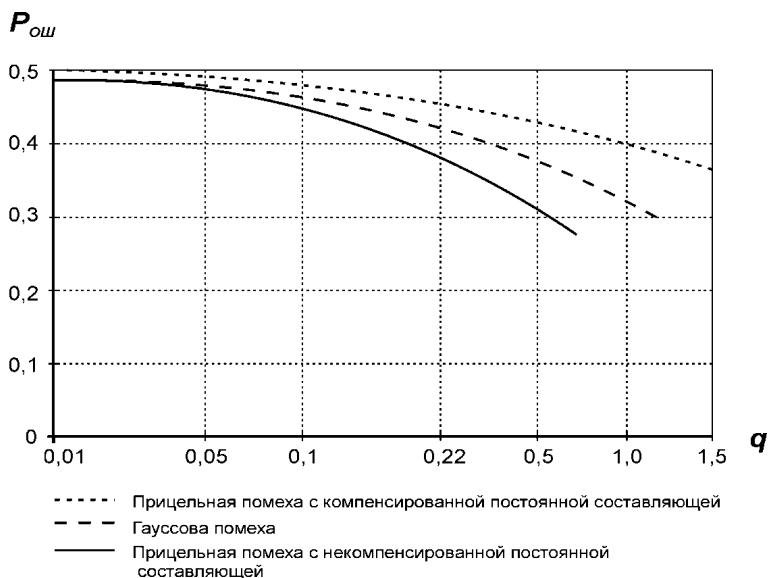


Рис. 7. Вероятностно-энергетические характеристики прицельных и гауссовских помех для $\lambda = 1$

Представляет определенный интерес сравнение прицельных помех с равновероятными и неравновероятными уровнями квантования друг с другом. Прицельные помехи с неравновероятными уровнями даже при больших t имеют ограниченную мощность, вызванную тем, что вероятность больших уровней стремится к нулю. Однако и вероятность ошибки для этих помех стремится к некоторому пределу, связанному с величиной λ , который меньше соответствующего предела вероятности ошибки в канале с помехой, имеющей равновероятные уровни. Это объясняется особенностью работы оптимального приемного устройства для прицельных помех с неравновероятными уровнями⁵. Таким образом, прицельная помеха с равновероятными уровнями превосходит аналогичную помеху с неравновероятными уровнями квантования по всем показателям, включая простоту реализации.

Заключение

Обобщенные результаты качественного и количественного анализа основных технических характеристик САЗ, использующих прицельные, имитирующие и гауссовские помехи, проведенного в данном исследовании, приведены в таблице 3.

⁵ Конторович В.Я., Ляндерс В.Е. Оптимальный прием сигналов дискретных сообщений на фоне аддитивных помех // Известия вузов. Серия Радиоэлектроника, 1973, т. 16, по. 3, с. 49-53.

Таблица 3

Сравнительная таблица основных технических характеристик САЗ

Технические характеристики	САЗ имитирующей помехи	САЗ прицельной помехи	САЗ гауссовской помехи
Маскирующая способность	2	3	3
Защищенность по отношению к методам селекции и компенсации помех	1	2	3
Скрытность	2	3	1
ЭМС	3	3	1
Универсальность	1	1	3
Простота реализации для нескольких опасных сигналов	2	2	3
Простота реализации для одного-двух опасных сигналов	3	3	2

Экспертная оценка отдельных показателей осуществлялась по 3-балльной ранжированной системе. В таблице 3 маскирующая способность имитирующих помех оценена несколько ниже, чем для других помех, из-за ухудшения специальных свойств вследствие наличия жесткой связи их с информационным сигналом. Скрытность САЗ прицельной помехи признана максимальной потому, что, помимо сигналоподобного характера помехи, учитывается сложность алгоритма перехвата.

Таким образом, по результатам сравнительного анализа наиболее эффективными следует признать САЗ прицельной помехи и в несколько в меньшей степени САЗ гауссовской помехи. САЗ имитирующей помехи уступает им по общей эффективности и имеет значительно худшие показатели по первым двум важнейшим техническим характеристикам.

Список источников

1. Ажмухамедов И.М., Марьенков А.Н. Повышение безопасности компьютерных систем и сетей на основе анализа сетевого трафика // *Инфокоммуникационные технологии*, 2010, т. 8, по. 3, с. 106-108.
2. Барановская Т.П., Попова Е.В., Замотайлова Д.А. Подходы к многокритериальному анализу деятельности управляющих организаций жилищно-коммунального комплекса // *Материалы Международной научно-практической конференции «Национальные экономики в условиях глобальных и локальных трансформаций»*, 2018, с. 10-14.
3. Волокитина Т.С. Устройства активной защиты телефонных линий // *Проблемы и перспективы развития России: молодежный взгляд в будущее: сборник научных статей 4-й Всероссийской научной конференции*, Курск, 14-15 октября 2021 года. Курск, Юго-Западный государственный университет, 2021, с. 294-296.
4. Глушков А.Н. и др. Анализ современных технических средств защиты информации в проводных линиях связи // *Вестник Воронежского института МВД России*, 2007, по. 1.
5. Иванов В.П. Активная защита информативных наводок средств вычислительной техники // *Вопросы защиты информации*, 2009, по. 3, с. 31-34.
6. Ле Куанг Минь. Оценка эффективности применения методов активной защиты от отказов в иерархических вычислительных системах / Ле Куанг Минь,

А.С. Романовский // *Вестник МГТУ им. Н.Э. Баумана: Сер. «Приборостроение»*, 2007, no. 4, с. 62-74.

7. Лойко В.И. Проектирование автоматизированных систем в защищенном исполнении военного назначения / В.И. Лойко, Ф.Г. Хисамов, Р.С. Шерстобитов // *Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета*, 2017, no. 126, с. 519-532.

8. Нехайчук Д.В. Формирование информационной модели затрат предприятия в системе стратегического управления затратами (ССУЗ) / Д.В. Нехайчук, Ю.С. Нехайчук, Е.А. Минина // *Азимут научных исследований: экономика и управление*, 2019, т. 8, no. 2(27), с. 263-267.

9. Савилова У.А. и др. Система активной защиты информации от утечки по акустоэлектрическому каналу // *Security: Information, Technology, Behavior*, 2020, с. 19-20.

10. Хисамов Ф.Г. Математическая модель оценки защищенности информации от несанкционированного доступа при проектировании автоматизированных систем в защищенном исполнении / Ф.Г. Хисамов, А.С. Жук, Р.С. Шерстобитов // *Известия ЮФУ. Технические науки*, 2017, no. 9 (194), с. 91-102.

11. Petrov A.A., Savinskaya D.N., Minina E.A., Dunskey L.K. Mathematical modeling of corporate network tolerance troubleshooting methods // *Modern Economics: Problems and Solutions*, 2020, no. 12(132), pp. 35-45.

12. Petrov A., Karpinski M., Petrov O. Development of methodological basis of management of information protection in the segment of corporate information systems // *International Multidisciplinary Scientific GeoConference Surveying Geology and Mining Ecology Management, SGEM*, 2018, no. 18(2.1), pp. 317-324.

ANALYSIS OF THE MAIN TECHNICAL CHARACTERISTICS OF ACTIVE PROTECTION SYSTEMS IN PUBLIC NETWORKS

Petrov Anton Alexandrovich¹, Cand. Sci. (Eng.)

Minina Evgeniya Ale[androvna², Cand. Sci. (Econ.)

¹ Leading developer of artificial intelligence systems, LLC «Geomir-Agro», st. Kolontsova, 5, room 302, Mytishchi, Russia, 141009; e-mail: petrov@geomir.ru

² Kuban State Agrarian university, Kalinina st., 13, Krasnodar, Russia, 350044; e-mail: minina.e@edu.kubsau.ru

Importance: one of the main tasks in creating active protection systems is the multicriteria optimization of technical characteristics. *Purpose:* the solution to this problem involves, in addition to a quantitative or qualitative description of each characteristic, their comparison with similar characteristics of active protection systems using other classes of interference. *Research design:* active protection systems with impact parameters have some advantages over other active protection systems; therefore, their effectiveness was assessed by comparing the corresponding technical characteristics. The article considers the masking ability of targeted interference and its dependence on the parameters that determine the circuit and design features of interference generators; masking ability of targeted interference with respect to an ideal parallel code. Comparison of the masking ability of targeted and simulating interference under conditions of complete coincidence of the parameters of the interference and the signal without taking into account the Gaussian component is reduced to considering the influence of the number of interference quantization levels m on the average error probability. Comparison of the masking ability of targeted and simulating interference under conditions of complete coincidence of the parameters of the interference and the signal without taking into account the Gaussian component is reduced to considering the influence of the number of interference quantization levels m on the average error probability. *Results:* the authors present generalized results of a qualitative and quantitative analysis of the main technical characteristics of active protection systems using targeted, simulating and Gaussian interference. According to the results of a comparative analysis, the most effective are the SAZ PP and, to a somewhat lesser extent, the SAZ GP. SAZ IP is inferior to them in terms of overall efficiency and has significantly worse performance in the first two most important technical characteristics.

Keywords: interference quantization levels, error probability, bit depth of the parallel code.

References

1. Azhmuamedov I.M., Mar'enzov A.N. Povyshenie bezopasnosti komp'yuternyh sistem i setej na osnove analiza setevogo trafika. *Infokommunikacionnye tekhnologii*, 2010, t. 8, no. 3, pp. 106-108. (In Russ.)
2. Baranovskaya T.P., Popova E.V., Zamotajlova D.A. Podhody k mnogokriterial'nomu analizu deyatel'nosti upravlyayushchih organizacij zhilishchno-kommunal'nogo kompleksa. *Materialy Mezhdunarodnoj nauchno-prakticheskoy konferencii «Natsional'nye ekonomiki v usloviyah global'nyh i lokal'nyh transformacij»*, 2018, pp. 10-14. (In Russ.)
3. Volokitina T.S. Ustrojstva aktivnoj zashchity telefonnyh linij. *Problemy i perspektivy razvitiya Rossii: molodezhnyj vzglyad v budushchee : sbornik nauchnyh statej 4-j Vserossijskoj nauchnoj konferencii*, Kursk, 14-15 oktyabrya 2021 goda. Kursk, YUgo-Zapadnyj gosudarstvennyj universitet, 2021, pp. 294-296. (In Russ.)
4. Glushkov A.N. i dr. Analiz sovremennyh tekhnicheskikh sredstv zashchity informacii v provodnyh liniyah svyazi. *Vestnik Voronezhskogo instituta MVD Rossii*, 2007, no. 1. (In Russ.)
5. Ivanov V.P. Aktivnaya zashchita informativnyh navodok sredstv vychislitel'noj tekhniki. *Voprosy zashchity informacii*, 2009, no. 3, pp. 31-34. (In Russ.)
6. Le Kuang Min. Ocenka effektivnosti primeneniya metodov aktivnoj zashchity ot otkazov v ierarhicheskikh vychislitel'nyh sistemah / Le Kuang Min, A.S. Romanovskii. *Vestnik MGTU im. N.E. Bauman. Ser. «Priborostroenie»*, 2007, no. 4, pp. 62-74. (In Russ.)
7. Lojko V.I. Proektirovanie avtomatizirovannyh sistem v zashishennom ispolnenii voennogo naznacheniya / V.I. Lojko, F.G. Hisamov, R.S. Sherstobitov. *Polite-maticheskij setevoy elektronnyj nauchnyj zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta*, 2017, no. 126, pp. 519-532. (In Russ.)
8. Nekhajchuk D.V. Formirovanie informacionnoj modeli zatrat predpriyatiya v sisteme strategicheskogo upravleniya zatratami (CCUZ) / D. V. Nekhajchuk, YU. S. Nekhajchuk, E. A. Minina. *Azimuth nauchnyh issledovanij: ekonomika i upravlenie*, 2019, t. 8, no. 2(27), pp. 263-267. (In Russ.)
9. Savilova U.A. et al. Sistema aktivnoj zashchity informacii ot utechki po akustoelektricheskomu kanalu. *Security: Information, Technology, Behavior*, 2020, pp. 19-20. (In Russ.)
10. Hisamov F.G. Matematicheskaya model ocenki zashishennosti informacii ot nesankcionirovannogo dostupa pri proektirovanii avtomatizirovannyh sistem v zashishennom ispolnenii / F.G. Hisamov, A.S. Zhuk, R.S. Sherstobitov. *Izvestiya YuFU. Tehnicheskie nauki*, 2017, no. 9 (194), pp. 91-102. (In Russ.)
11. Petrov A.A., Savinskaya D.N., Minina E.A., Dunskey L.K. Mathematical modeling of corporate network tolerance troubleshooting methods. *Modern Economics: Problems and Solutions*, 2020, no. 12(132), pp. 35-45.
12. Petrov A., Karpinski M. & Petrov O. Development of methodological basis of management of information protection in the segment of corporate information systems. *International Multidisciplinary Scientific GeoConference Surveying Geology and Mining Ecology Management, SGEM*, 2018, no. 18(2.1), pp. 317-324.