спектра, или шумоподобных сигналов (ШПС). Применение подобного сигнала подразумевает использование специального кода (в нашем случае, псевдослучайной последовательности) на приемной и передающей стороне. Через использование в системе метода расширения спектра достигается энергетическая эффективность и помехозащищенность сигнально-кодовой конструкции, защита от сосредоточенных помех и сокрытие сигнала под шумами.

Основной задачей проводимых исследований является синтезирование алгоритма, обеспечивающего указанные выше характеристики, если в качестве расширяющей спектр последовательности будет использоваться случайно-подобный бинарный или многоуровневый сигнал, генерируемый системами с нелинейными обратными связями. По результатам проведенного исследования предполагается синтезировать квазиоптимальный алгоритм обработки сигнала на фоне помех и выявить параметры нелинейной системы, при которых обеспечивается приемлемый коэффициент взаимной корреляции сигналов.

Результаты данной работы могут оказать большую помощь в разработке и оптимизации схем и алгоритмов расширения спектра и внести большой вклад в улучшения качества связи.

Литература

1. Чердынцев, В.А. Системы передачи информации с расширением спектра сигналов / В.А. Чердынцев, В.В. Дубровский. – Минск, 2009. – 131 с.

2. Варакин Л.Е. Системы связи с шумоподобными сигналами / Л.Е. Варакин. – М.: Радио и связь, 1985. – 384 с.

ОБЪЕДИНЕНИЕ РЕШЕНИЙ О КЛАССЕ ЦЕЛИ В ИНФОРМАЦИОННОЙ ПОДСИСТЕМЕ КОМПЛЕКСА СРЕДСТВ АВТОМАТИЗАЦИИ ЗЕНИТНОЙ РАКЕТНОЙ БРИГАДЫ

А.Ю. Липлянин, Е.И. Хижняк

В основе эффективного управления боевыми средствами системы войск противовоздушной обороны лежит качественное управление огневыми средствами, решаемое в управляемой подсистеме комплексов средств автоматизации. Одним из факторов успешного функционирования управляющей подсистемы является эффективное решение задачи целераспределения. При этом критерием качества процесса целераспределения определим значение предотвращенного ущерба объекту обороны [1], в котором немаловажный фактор при расчете данного показателя учитывается важность цели, которая в настоящий момент задается оператором вручную. Однако, не вызывает сомнения тот факт, что важность цели неразрывно связана с ее классом и задачей выполняемой в налете [2]. Но в связи с тем, что на средства автоматизации приходят данные о классе цели от различных источников, решения о принадлежности классов источников разнится как качественно, так и количественно. По этой причине возникает задача объединения решений о классе цели.

В современной зарубежной литературе задачи, методы и алгоритмы коллективного распознавания встречаются в различных работах под разными названиями:

– объединение множества классификаторов (combination of multiple classifiers);
– объединение классификаторов (classifier fusion);
– объединение экспертов (mixture of experts);
– комитеты (committees);
– согласованная агрегация (consensus aggregation);
– голосующее объединение классификаторов (voting pool of classifiers);
– динамический выбор классификатора (dynamic classifier selection);
– комбинированные системы классификаторов (composite classifier system);
– комбинирование решений (decision combining);
– классификаторы типа «разделяй и властвуй» (divide-and-conquer classifiers).

В действительности, приведенное разнообразие используемой терминологии отражает также и разнообразие постановок задач, предположений, типы выходов классификаторов, стратегии объединения. [3] Задачей настоящей диссертационной работы является создание метода и алгоритма объединения решений классификаторов для качественного распознавания классов целей, для дальнейшего использования при решении задачи целераспределения. Это позволит решать задачу целераспределения более эффективно.

Литература

1. Кругликов, С.В. Методика решения задачи многофакторного целераспределения в автоматизированной системе управления / С.В. Кругликов // Доклады БГУИР. – 2013. – № 5. – С 93–99.

2. Липлянин, А.Ю. Методика учета важности цели при решении задачи распределения летательных аппаратов между огневыми средствами / А.Ю. Липлянин, А.С. Шеин, А.В. Хижняк // Доклады БГУИР. – 2017. – № 2. – С 77–84.

3. Городецкий, В.И.Методы и алгоритмы коллективного распознавания: обзор / В.И. Городецкий, С.В. Серебряков // Труды СПИИРАН. – 2006. – Вып. 3, т. 1. – С. 139 – 171.

АЛГЕБРАИЧЕСКИЕ УРАВНЕНИЯ В АЛГОРИТМАХ ЗАЩИТЫ ИНФОРМАЦИИ

В.А. Липницкий, Л.В. Михайловская

Различные аспекты, связанные с решением алгебраических уравнений, часто и довольно неожиданно возникают при практической реализации тех или иных криптографических систем. Так, криптосистема Рабина своим базовым алгоритмом дешифрования ставит проблему решения квадратного уравнения в кольце классов вычетов по составному модулю – произведению двух простых нечетных чисел. Как ни странно, такие квадратные уравнения в общем случае имеют четыре, а не два корня.

Решение уравнения легальными пользователями сводит задачу по китайской теореме об остатках в минимальных полях Z/pZ и Z/qZ. Если p и q относятся к классу простых чисел Блюма, т.е. имеют вид $4t+3$, t – натуральное число, то задача легко решается возведением дискриминанта в строго определенную степень. Если же $p = 4t+1$, то при нечетных t существуют аналогичные формулы, а при четных t поиск квадратных корней осуществляется процедурой перебора, хотя и достаточно ограниченного перебора. Поэтому реальные пользователи криптосистемы Рабина стараются брать простые числа вида, рассмотренного в первом случае. Хакер вынужден вначале факторизовать модуль n в произведение простых множителей, т.е. решить ту же проблему, что и в криптосистеме *RSA*. Глубокое владение теорией чисел позволяет строить совершенные криптографические системы, удобные и практичные в применении.

ГРУППА АВТОМОРФИЗМОВ БЧХ-КОДА И ЕЕ ПОЛИНОМИАЛЬНЫЕ ИНВАРИАНТЫ

В.А. Липницкий, Е.В. Середа

По сути дела, группа автоморфизмов G любого БЧХ-кода порождена циклической и циклотомической подстановками, а потому является некоммутативной. Нормы синдромов – основной объект, разработанный белорусскими кодировщиками ТНС – теории норм синдромов – явились эффективными инвариантами группы Γ циклических сдвигов: норма синдрома так специфично определена через компоненты синдрома, что является одинаковой для всех векторов каждой Γ-орбиты ошибок, поэтому данный уникальный параметр и назван нормой Γ-орбиты. Выяснялось, что нормы Γ-орбит любой корректируемой совокупности векторов-ошибок попарно различны. Практическим следствием данной теории явилось семейство перестановочных норменных методов и алгоритмов коррекции ошибок БЧХ-кодами, на порядок ускоряющих работу декодеров по сравнению с традиционными синдромными алгоритмами.

В докладе рассматриваются полиномиальные инварианты всей группы G автоморфизмов БЧХ-кодов. Каждая G-орбита представляет собой объединение строго определенного ряда Γ-орбит, связанных друг с другом посредством циклотомической подстановки и ее степеней. Нормы циклотомически связанных Γ-орбит являются сопряженными элементами в конечном поле – поле определения соответствующего БЧХ-кода. Семейство взаимно сопряженных элементов поля Галуа составляет полную группу корней неприводимого полинома любого из элементов этого семейства. Согласно формулам Виета, всякий полином однозначно определяется своими корнями. Таким образом, полное семейство попарно сопряженных норм Γ-орбит, составляющих данную G-орбиту, задают однозначно определенный полином, корнями которого они являются. Это и есть полиномиальный