

ризуется высоким значением параметра a_t и, в соответствии с формулой (5, 6), оказывает значительное влияние на формирование общего решения всей модели в целом. Если такой эксперт плохо справляется с задачей обнаружения некоторого класса атак, то это отрицательно сказывается на результатах совместного решения.

Таблица 4. Результаты тестирования модели AdaBoost

класс	всего	обнаружено	распознано
DoS	391458	389917 (99.61%)	369088 (94.29%)
U2R	52	51 (98.08%)	44 (84.62%)
R2L	1126	1119 (99.37%)	636 (56.48%)
Probe	4107	3908 (95.15%)	3668 (89.31%)
normal	97277	---	77212 (79.37%)
Итого	494020	---	450648 (91,22%)

Для устранения этого недостатка каждому нейрону выходного слоя эксперта ставилось в соответствие определенное значение q_{ty} из диапазона [0..1] (т.н. коэффициент "доверия"). Этот коэффициент рассчитывался для обученной нейронной сети с использованием примеров из обучающей выборки таким образом, чтобы:

- при $q = 1$, этот нейрон реагировал только на образы своего класса;
 - при $q = 0$, на все образы из обучающей выборки.
- Общее решение вычислялось по формуле (8), которая является модификацией формулы (6).

$$H(x) = \operatorname{argmax}_{y \in \{1,2,\dots,k\}} \left[\sum_{t: h_t(x)=y} a_t \cdot q_{ty} \right]. \quad (8)$$

Такая методика применима только в случае ансамбля классификаторов.

Заключение. Как показали эксперименты, применение ансамблей классификаторов позволяет улучшить некоторые показатели эффективности модели. Однако это достигается за счет увеличения в разы количества вычислений. Кроме того, применение алгоритмов усиления не всегда приводит к улучшению распознавания определенных классов атак. Наряду с усилением наблюдаются процессы усреднения результата по ансамблю. Поэтому в каждом конкретном случае нужно решать отдельно, стоит ли применять алгоритм усиления.

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. Web Application Security Consortium. Классификация угроз [Электрон. ресурс]. - Режим доступа: www.webappsec.org.
2. V. Golovko and L. Vaitsekhovich. Neural Network Techniques for Intrusion Detection // In Proceedings of the International Conference on Neural Networks and Artificial Intelligence (ICNNAI-2006) / Brest State Technical University - Brest, 2006. - P. 65-69.
3. Головкин В.А., Войцехович Л.Ю. и Шевеленков В.В. Нейросетевые принципы построения нейронных систем обнаружения атак на компьютерные сети // Вестник БрГТУ. Физика, математика, информатика. - 2006. - №5(41). - С. 14-19.
4. H.Drucker, R.Schapire and P.Simard. Improving performance in neural networks using a boosting algorithm // In S.J.Hanson, J.D.Cowan and C.L.Giles eds., Advanced in Neural Information Processing Systems 5, Denver, CO, Morgan Kaufmann, San Mateo, CA. - 1993. - P. 42-49.
5. Yoav Freund, Robert E. Schapire. A short introduction to boosting // Journal of Japanese Society for Artificial Intelligence. - 1999. - №14(5). - P. 771-780.
6. Головкин В.А. Нейронные сети: обучение, организация и применение. Кн. 4: Учеб. пособие для вузов / Общая ред. А.И. Галушкина. - М.: ИПРЖР, 2001. - 256 с.

Материал поступил в редакцию 13.02.08

VAITSEKHOVICH L.U., GOLOVKO V.A., RUBANOV V.S. Some aspects of applying boosting algorithms in modular neural networks for intrusion detection

In this article the classification task in the domain of intrusion detection is considered. Often a chosen algorithm is not good enough for practical use. So the question arises how it is possible to improve the performance? In this case we can employ so-called Committee Machines that increase accuracy and reliability of the base classification model. These advantages are the result of dividing complex computational problems among several experts. The knowledge of each expert influences on the general conclusion of Committee Machine.

УДК 681.3 + 004.9

Палий И.О., Саченко А.А., Турченко В.А., Куриляк Ю.О., Капура В.А.

ОБНАРУЖЕНИЕ ЛИЦ С ПОМОЩЬЮ КОМБИНИРОВАННОГО КАСКАДА КЛАССИФИКАТОРОВ ДЛЯ ВИДЕОНАБЛЮДЕНИЯ

Введение. Обнаружение человеческих лиц (ОЛ) – это очень важная и быстроразвивающаяся область исследований, которая всегда является первым этапом к любой обработке лиц и имеет следующие приложения: распознавание лиц, видеоконференции, поиск изображений за содержанием, видеонаблюдение и др. ОЛ также является сложной задачей благодаря таким факторам, как масштаб, размещение, ориентация в пространстве, степень поворо-

та и условия освещения лиц. Много разных подходов ОЛ [1] представлено в последние годы, которые базируются на знаниях, инвариантных признаках, сравнении с шаблоном и внешнем виде.

Сан и Поджио [2] разработали первый точный метод ОЛ, который базируется на внешнем виде. Они предложили несколько алгоритмов, которые потом были использованы во многих других системах ОЛ: нормализация входных изображений, генерация виртуаль-

Палий И.О., научный сотрудник НИИ интеллектуальных компьютерных систем (НИИ ИКС) Тернопольского национального экономического университета (ТНЭУ), г. Тернополь, Украина.

Саченко А.А., доктор технических наук, профессор и зав. кафедрой информационно-вычислительных систем и управления факультета компьютерных информационных технологий и директор Американско-украинской программы по компьютерным наукам, Тернопольского национального экономического университета (ТНЭУ), г. Тернополь, Украина.

Турченко В.А., кандидат технических наук, доцент кафедры информационно-вычислительных систем и управления факультета компьютерных информационных технологий ТНЭУ, глава группы нейронных сетей и параллельных вычислений в НИИ ИКС при ТНЭУ, г. Тернополь, Украина.

Куриляк Ю.О., младший научный сотрудник НИИ ИКС, ТНЭУ, г. Тернополь, Украина.

Капура В.А., младший научный сотрудник НИИ ИКС, ТНЭУ, г. Тернополь, Украина.

Физика, математика, информатика

ных примеров, выбор нелиц (bootstrapping), поиск лиц по масштабу и размещению фиксированным окном и др.

Роули и др. [3] предложили нейросетевой подход, продемонстрировавший хорошие результаты на большом и тяжелом тестовом наборе. Их система использует нейронную сеть с несколькими группами локальных рецепторных полей (retinally connected neural network). Каждое входное окно изображения проходит предварительную обработку, как и в [2]. Для уменьшения количества ложных позитивных обнаружений (ЛПО) использован ансамбль нейронных сетей с разными стратегиями принятия решений. Быстрая версия системы ОЛ имеет каскадную структуру и использует дополнительную нейронную сеть, которая сканирует изображения с большим шагом. Найденные кандидаты верифицируются с помощью базового классификатора.

Очень быстрый метод ОЛ представлен Виолой и Джонсом [4], который использует AdaBoost для выбора важных Хаар подобных признаков и каскад простых классификаторов (КПК).

Гарсиа и Делакис [5] предложили новую схему ОЛ с помощью сверточной нейронной сети (СНС), разработанной ЛеКуном и др. [6]. Их система автоматически в процессе обучения настраивает оптимальные сверточные фильтры, которые работают в качестве экстракторов признаков. В отличие от предыдущих методов, которые сканируют входное изображение с помощью окна, СНС обрабатывает изображение за раз при каждом уровне масштабирования.

Современные подходы все еще имеют некоторые недостатки. Например, системы ОЛ на основе "сильных" монолитных классификаторов [2, 3, 5] являются точными, дают очень мало ЛПО, но они слишком медленные для работы с видеопотоком. Даже система, представленная в [5], наиболее быстрая в этой группе, требует дополнительное время для верификации найденных лиц. Стадия верификации в данном случае обусловлена неточностью проекции результатов обнаружения с выходного слоя СНС на входное изображение. Система ОЛ на основе КПК [4] является очень быстрой, но пропускает частично закрытые или затененные лица, а также дает больше ЛПО.

В статье представлен гибридный подход к ОЛ, использующий комбинированный каскад классификаторов, который состоит из КПК [4] для выделения лиц-кандидатов и СНС [5] для их верификации. Подход сохраняет высокую скорость работы и дает очень низкий уровень ЛПО.

Статья организована следующим образом: в разделе 2 проанализировано обнаружение лиц-кандидатов, этап верификации подан в разделе 3, экспериментальные результаты представлены в разделе 4, заключение и будущие направления исследований даны в последнем разделе.

Обнаружение лиц-кандидатов. КПК [4], улучшенный Линхартром [7], использован для обнаружения лиц-кандидатов. Сначала каскад учится на нескольких тысячах позитивных и негативных примерах (лицах и нелицах). После обучения он может быть применен к области интереса входного изображения. КПК выдает "1", если область похожа на лицо, и "0" – в противном случае. Окно поиска двигается по всему изображению для поиска лиц в каждой позиции. Конструкция классификатора такова, что он может легко масштабировать входное окно для обнаружения лиц любых размеров, что является более эффективным, чем масштабирование входного изображения, как это происходит в методах на основе монолитных классификаторов. Процедура сканирования должна быть выполнена несколько раз при разных масштабах для детектирования лиц неизвестных размеров.

КПК состоит из нескольких простых классификаторов (уровней), которые последовательно применяются к области интереса пока кандидат не будет откинут каким-либо уровнем или не будет принят всеми. Структура КПК отображает тот факт, что подавляющее большинство подокон изображения являются негативными примерами. Поэтому каскад стремится откинуть как можно больше фона на ранних уровнях и уделить больше внимания областям, похожим на лица (рис. 1).

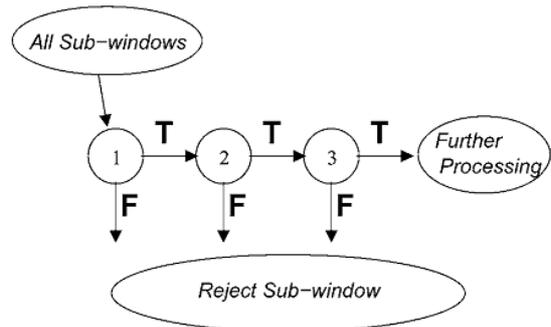


Рис. 1. Процесс обнаружения лиц-кандидатов с помощью КПК [4]

Классификаторы каждого уровня каскада являются сложными сами по себе и построены на основе простых классификаторов с использованием алгоритма Gentle AdaBoost [8]. Простой классификатор – это дерево решений, по крайней мере, с двумя разветвлениями. Входом для простых классификаторов служат Хаар подобные признаки с расширенного набора (рис. 2) [7].

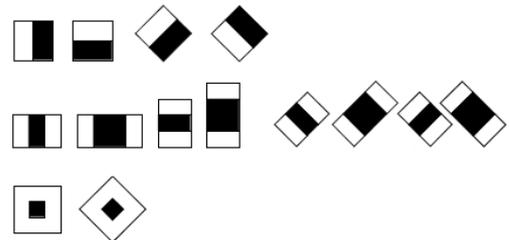


Рис. 2. Расширенный набор Хаар подобных признаков

Признак определяется своей формой, позицией в области интереса и масштабом. Сумы значений пикселей признаков вычисляются с помощью интегральных изображений.

Каскадная структура классификатора и использование интегрального изображения обеспечивают очень высокую скорость работы блока обнаружения лиц-кандидатов (до 15 кадров за сек.).

Верификация лиц-кандидатов. СНС использована для верификации найденных лиц-кандидатов благодаря ее стойкости к шуму, сдвигам, масштабу, углу поворота и формы входных образов [5]. Она представляет собой многослойную нейронную сеть прямого распространения сигнала с архитектурой, которая повторяет принципы строения головного мозга и специализируется на задачах компьютерного зрения. Каждый уровень СНС состоит из плоскостей, извлекающих разные признаки в процессе обучения. Каждый нейрон плоскости получает входной сигнал с небольшого участка плоскости(тей) предыдущего уровня (биологические локальные рецепторные поля). Значения синапсов (ядро свертки) формируют рецепторное поле, которое является одним для всех нейронов плоскости. Каждая плоскость может быть рассмотрена как карта признаков. Каждый уровень состоит из множества плоскостей, поэтому происходит выделения множества признаков.

ЛеКун [6] выделяет два типа уровней СНС: сверточный (convolutional) и усредняющий (subsampling), – но в статье используется структура сети, предложенная Симардом и др. [9]. Она объединяет два типа уровней в один, уменьшая при этом количество уровней и делая за счет этого сеть намного быстрее (рис. 3).

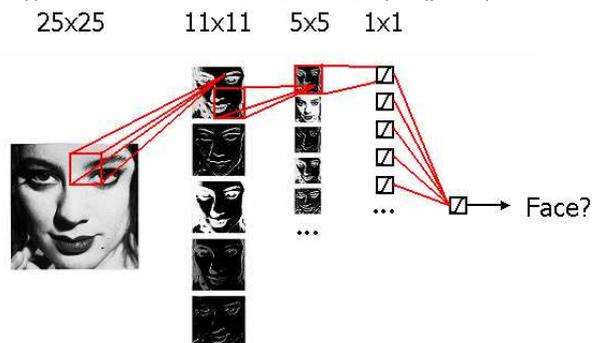


Рис. 3. Структура сверточной нейронной сети

Существует несколько стратегий связывания уровней сети: полная, Тьерплитц, бинарная и ручная. В статье использована стратегия связывания на основе бинарной с заданным коэффициентом связывания, так как ее легко запрограммировать.

Для обучения СНС использован улучшенный алгоритм активного обучения с процедурой bootstrapping [3]. Он состоит из следующих шагов:

1. Создать начальный тренировочный набор путем случайного выбора 1000 позитивных примеров и генерации 1000 негативных.
2. Обучить СНС выдавать 0.6 для позитивных примеров и -0.6 для негативных. Использован алгоритм обратного распространения ошибки с адаптивным шагом обучения (on-line версия) [11]. Если среднеквадратическая ошибка сети слишком большая, то найти тренировочный пример с наибольшей ошибкой и исключить его из тренировочного набора. Повторить шаг 2.
3. Подать на вход сети изображения, не содержащие лица. Случайно выбрать заданное количество подокон, которые сеть ошибочно классифицировала как лица, и добавить их в тренировочный набор в качестве негативных примеров.
4. Случайно выбрать заданное количество позитивных примеров из всего набора лиц и занести их в тренировочный набор.
5. Если не выполняется условие окончания обучения, то перейти к шагу 2.

Количество примеров, выбираемых на шагах 3 и 4, равно 500. Соотношение позитивных/негативных примеров является адаптивным, и на каждой итерации обучения оно зависит от ошибки СНС на всем наборе лиц. Это сделано с целью обеспечения высокого уровня ОЛ. Сеть становится слишком "строгой" и пропускает больше лиц, когда обучение проходит с фиксированным равным соотношением позитивных/негативных примеров.

Результаты экспериментальных исследований. Программное обеспечение для ОЛ разработано в среде С++ с использованием библиотеки OpenCV (Open Computer Vision Library) [12]. В качестве детектора лиц-кандидатов использован один из обученных КПК ("data\haarcascades\haarcascade_frontalface_default.xml"). Он состоит из 25 уровней, обученных достигать на тренировочном наборе уровня ЛПО 50% и уровня ОЛ 99.9%. Каскад обрабатывает входное изображение и передает все найденные лица на вход СНС для верификации без выполнения группировки многократных обнаружений. В процессе работы окно КПК масштабируется с коэффициентом 1.2 для обнаружения лиц разных размеров.

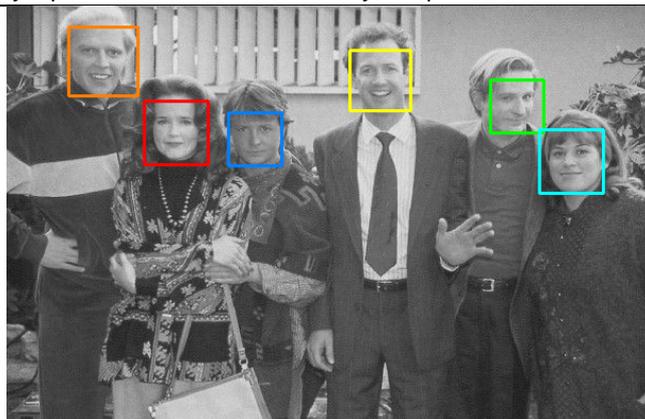
СНС обучена на наборе из 16965 лиц размером 25x25 пикселей каждое, собранном с Интернет и ряда общедоступных баз: BioID [13], CVL [14], UMIST [15] и Yale [16]. Негативные примеры накапливаются в процессе bootstrapping из 170 изображений, не содержащих лица. Оценочный набор состоит из 1000 позитивных и 1000 случайно выбранных негативных примеров, которые не входят в тренировочный набор. СНС, обученная на 40 итерациях, достигает ошибки 5.6% и 8.1% на оценочном наборе для лиц и нелиц соответственно.

Все лица-кандидаты, найденные каскадом, приводятся к размеру 25x25 пикселей и обрабатываются СНС. Только кандидаты с большим, чем пороговое (равное 0), выходным значением СНС принимаются как лица (рис. 4).

Для тестирования разработанной системы использован тестовый набор MIT+CMU [3]. Он состоит из 130 изображений с 507 лицами разных размеров и качества. Предварительные результаты тестирования предложенного подхода к ОЛ поданы в табл. 1.



а)



б)

Рис. 4. Обнаружение лиц-кандидатов (а) и результат их верификации (б)

Таблица 1. Результаты тестирования системы на наборе MIT+CMU

Система ОЛ	Уровень ОЛ, %	ЛПО, шт.
КПК + СНС	75.4	8
КПК [4]	76.1	10
Нейронная сеть (быстрая версия) [3]	76.9	8

Предложенный подход демонстрирует результаты, сопоставимые с лучшими системами ОЛ, работающими с видеопотоком. Уровень ОЛ подхода почти равен результату системы с [4] и немножко ниже, чем результат, достигнутый системой с [3] (но он почти в 10 раз быстрее чем последняя).

Разработанная система была протестирована в нашем институте с использованием камеры Logitech QuickCam Messenger на рабочей станции Intel Celeron 2.3GHz. При использовании параметров по умолчанию система обрабатывала входное изображение размером 352x288 пикселей со скоростью 8-10 к./сек. Более высокая скорость обработки может быть достигнута за счет оптимизации параметров детектора, а также привлечения других средств: сегментации за движением и цветом кожи.

Заключение и направления исследований. В статье представлен комбинированный двухуровневый подход к ОЛ на основе КПК и СНС. Также представлен улучшенный алгоритм обучения нейронной сети. Предварительные экспериментальные результаты показывают хороший потенциал подхода. Существует несколько направлений улучшения его производительности:

- научить КПК на своем тренировочном наборе (параметры тренировочного набора обученного каскада с OpenCV могут отличаться от нашего);
- разработать алгоритм автоматической генерации связей между плоскостями соседних уровней СНС согласно с рекомендациями в [6], чтобы комбинировать признаки, извлеченные разными плоскостями;
- улучшить процесс верификации путем проверки соседних к позиции найденного лица-кандидата подокон;
- изучить результаты работы подхода при меньшем количестве уровней КПК.

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. Ming Hsuan Yang, "Recent Advances in Face Detection", IEEE ICPR 2004 Tutorial, Cambridge, United Kingdom, 2004.
2. Example-based learning for view-based human face detection / K. K. Sung and T. Poggio // IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20, no.1, 1998, pp.39-51.
3. Neural network-based face detection / H. Rowley, S. Baluja, and T. Kanade // IEEE Transactions on Pattern Analysis and Machine Intelligence, vol.20, 1998, pp.22-38.
4. Robust Real-Time Face Detection / P. Viola, M. Jones, // International Journal of Computer Vision, 57 (2), 2004, pp. 137-154.

5. A Neural Architecture for Fast and Robust Face Detection / C. Garcia, M. Delakis // IEEE-IAPR International Conference on Pattern Recognition (ICPR2002), Québec City, 2002, pp. 40-43.
6. Gradient-Based Learning Applied to Document Recognition / Y. LeCun, L. Bottou, Y. Bengio and etc. // Intelligent Signal Processing, IEEE Press, 2001, pp. 306-351.
7. An Extended Set of Haar-like Features for Rapid Object Detection / R. Lienhart, J. Maydt // IEEE ICIP 2002, Vol. 1, Sep. 2002, pp. 900-903.
8. Sharing features: efficient boosting procedures for multiclass object detection / A. Torralba, K. P. Murphy and W. T. Freeman, // Proceedings of the 2004 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR), 2004, pp 762-769.
9. Best Practices for Convolutional Neural Networks Applied to Visual Document Analysis / P. Simard, D. Steinkraus, J. Platt // Seventh International Conference on Document Analysis and Recognition (ICDAR'03), Vol. 2, 2003, p. 958.
10. Efficient training algorithms for a class of shunting inhibitory convolutional neural networks / F. Tivive, A. Bouzerdoum // IEEE Transactions on Neural Networks, 16(3), May 2005, pp. 541-556.
11. V. Golovko. Neurointelligence: theory and application, Brest, vol.1, 1999.
12. OpenCV library: <http://sourceforge.net/projects/opencv/>.
13. Robust Face Detection Using the Hausdorff Distance / O. Jesorsky, K. Kirchberg, R. Frischholz // Audio and Video based Person Authentication - AVBPA 2001, Springer, 2001, pp. 90-95.
14. CVL face database: <http://www.lrv.fri.uni-lj.si/facedb.html>
15. Characterizing virtual eigensignatures for general purpose face recognition / D. Graham, N. Allinson // Face Recognition: From Theory to Applications, ser. NATO ASI Series F, Computer and Systems Sciences, vol. 163, 1998, pp. 446-456.
16. From Few to Many: Illumination Cone Models for Face Recognition under Variable Lighting and Pose / A. Georghiades, P. Belhumeur, D. Kriegman // IEEE Trans. Pattern Anal. Mach. Intelligence, vol. 23(6), 2001, pp. 643-660.

Материал поступил в редакцию 24.01.08

PALIJ I.O., SACHENKO A.A., TURCHENKO V.A., KURILIAK U.O., KAPURA V.A. Detection of the persons with the help of the combined cascade of qualifiers for video supervision

The method of detection of the persons with the help of the combined cascade is submitted which unites the cascade of qualifiers on a basis Хаар of similar attributes for search of the persons - candidates and curtailing neuron a network for their verification. The method works with the large speed and very low level of detection of false positive examples.

УДК 681.325

Яцкив Н.Г., Яцкив В.В., Крепыч Р.В.

МЕТОД КОДИРОВАНИЯ ДАННЫХ В БЕСПРОВОДНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ НА ОСНОВЕ ПРЕОБРАЗОВАНИЯ СИСТЕМЫ ОСТАТОЧНЫХ КЛАССОВ

В современных беспроводных компьютерных сетях широко используются методы передачи, основанные на расширении спектра сигнала. Основная идея указанных методов заключается в том, чтобы распределить информационный сигнал по полосе частот, намного большей, чем минимально необходимая для передачи данных. Это значительно усложняет перехват сигналов и создание преднамеренных помех.

Системы передачи на основе расширенного спектра сигнала обладают следующими преимуществами:

- обеспечивают более высокую помехоустойчивость в условиях интенсивных помех;
- позволяют организовать одновременную работу многих абонентов в общей полосе частот, данное свойство используется в технологии мобильной связи, известной как многочисленный доступ с кодовым разделением (code division multiple access – CDMA);
- позволяют реализовать асинхронно-адресные принципы системы связи и кодовое разделение абонентов;
- обеспечивают эффективное использование спектра частот на ограниченной территории относительно узкополосным системам связи;
- позволяют скрывать и шифровать сигналы. Восстановить зашифрованные данные может только пользователь, которому известен код расширения.

В стандарте IEEE 802.11 определены два метода передачи данных на основе расширения спектра. Это метод прямой последовательности (direct sequence spread spectrum – DSSS) и метод скачкообразного изменения частоты (frequency-hopping spread spectrum FHSS) [1, 2, 3].

При расширении спектра методом прямой последовательности, каждому исходному биту соответствует псевдослучайная последовательность. В качестве псевдослучайной последовательности используют последовательности максимальной длины, генерируемые регистром сдвига с обратной связью.

При использовании расширения спектра со скачкообразным изменением частоты передача сигнала происходит с помощью определенного набора несущих частот, которые изменяются через определенные интервалы времени по псевдослучайному закону. Для передачи данных используется 2^k несущих частот. Расстояние между несущими частотами выбирается равным ширине полосы входного сигнала. Каждый канал использует фиксированный интервал времени, на протяжении которого происходит передача определенного количества битов. В зависимости от времени переключения несущих частот, различают метод расширения спектра с медленной скачкообразной перестройкой частоты и метод с быстрой перестройкой частоты.

Менее распространенным является метод переключения временных интервалов (time hopping – TH), используется при наличии преднамеренных помех, поскольку он скрывает координаты сигнала.

В связи с широким внедрением беспроводных компьютерных сетей актуальной является проблема повышение надежности передачи данных и защита от несанкционированного доступа к информации в процессе передачи.

Предложенный метод кодирования и передачи данных базируется на расширении спектра сигнала методом скачкообразной перестройки частоты и преобразования системы остаточных классов (СОК).

Пусть задан набор из k взаимнопростых натуральных чисел, тогда под СОК будем понимать такую систему, в которой целое число представляется в виде неотрицательных остатков по выбранным модулям P_i [4, 5].

$$b_i = \text{res } N \pmod{P_i}, \quad (1)$$

где res – символ операции получения остатка, N – входное значение или

Яцкив Наталия Георгиевна, доцент кафедры информационно-вычислительных систем и управления Тернопольского национального экономического университета, г. Тернополь, Украина.

Яцкив Василий Васильевич, доцент кафедры специализированных компьютерных систем Тернопольского национального экономического университета, г. Тернополь, Украина.

Крепыч Роман Владимирович, инженер Тернопольского национального экономического университета, г. Тернополь, Украина.