УДК 004.8.032.26

Нейросетевой агент для обнаружения сетевых атак

Войцехович Леонид Юрьевич, аспирант 3-го года обучения кафедры интеллектуальных информационных технологий Брестского государственного технического университета.
Беларусь, БрГТУ, 224017, г. Брест, ул. Московская, 267.
Курош Мадани, д.н., профессор университета Paris Est Créteil (UPEC), Франция.

Введение. Безопасность компьютерных систем – одна из наиболее серьезных проблем современной индустрии информационных технологий. Ее актуальность постоянно возрастает с развитием Интернета и вычислительных мощностей ЭВМ.

Люди в повседневной жизни регулярно сталкиваются с возможностями, предоставляемыми информационными технологиями, поэтому важно быть уверенным, что применяемые программные и технические средства безопасны и защищены от действий злоумышленников. Этот вопрос становится все более актуальным по мере возрастания важности тех данных, с которыми нам приходится сталкиваться в информационном пространстве.

Согласно статистическим исследованиям лаборатории Касперского за 2009 год [1] С*истема Обнаружения Вторжений (Intrusion Detection System - IDS),* реализованная в KIS2010, отразила 219 899 678 сетевых атак (см. таблицу 1). Аналогичный показатель 2008 года составлял чуть более 30 млн. инцидентов.

Существует две основных технологии обнаружения вторжений: обнаружение злоупотреблений и обнаружение аномалий. Обнаружение злоупотреблений (например, IDIOT [2] и STAT [3]) основано на использовании данных о заранее известных атаках или уязвимостях компьютерных систем и сравнении их с наблюдаемой активностью в сети. При соответствии сигнатуры подается сигнал тревоги администратору. Однако обнаружение злоупотреблений не позволяет обнаруживать новые и неизвестные системе атаки, для которых предварительно не заданы сигнатуры и правила.

Системы обнаружения аномалий (например, система IDES [4]) срабатывают в случае значительного отклонения наблюдаемой сетевой активности от заданного профиля нормального поведения пользователя в сети. Этот подход может быть эффективен против неизвестных атак, поскольку не требуются никакие предварительные знания об атаке как таковой. Однако такие системы генерируют большое число ложных срабатываний, поскольку за аномалию может быть принято любое нестандартное поведение пользователя.

Некоторые IDS, например IDES и NIDES [5], используют одновременно оба подхода – обнаружения вторжений и обнаружения аномалий.

Целью данной работы является разработка, изучение и анализ модели классификации для построения системы обнаружения сетевых атак. Предлагаемая в статье мультиагентная модель должна сократить число ложных срабатываний и обеспечить минимальную загрузку вычислительных ресурсов. Хотя эта модель и применена в задаче обеспечения безопасности компьютерных систем от сетевых атак, но, тем не менее, может быть использована для решения других задач: в области экономики, медицины, распознавания образов и т.д.

Статья организована следующим образом: нейросетевая постановка задачи выполнена в разделе 2; вопрос, посвященный использованию образов псевдоатак, рассмотрен в разделе 3; понятие мультиагентной системы приводится в разделе 4; в разделе 5 дано концептуальное описание разрабатываемой мультиагентной системы (структура, функционирование); вопросу реализации посвящен раздел 6; проведенные эксперименты отражены в разделе 7; основные результаты оговорены в заключительной части статьи.

Нейросетевой агент для обнаружения. Сетевые вторжения, представленные в базе KDD [6], можно отнести к одному из четырех классов: DoS, Probe, U2R и R2L, где DoS – это атаки отказа в обслуживании, Probe – сканирование сети с целью обнаружения уязвимых хостов или служб, U2R - предполагает, что злоумышленник пытается получить привилегии root-а или администратора и, наконец, R2L – неавторизованный доступ со стороны удаленной машины. Каждая категория включает атаки различного типа.

В данной работе в качестве основного агента (детектора) системы обнаружения атак (см. рис. 1) предлагается применять нейронную сеть, представляющую собой объединение *Рециркуляционной нейронной сети* (RNN) и *Многослойного персептрона* (MLP).

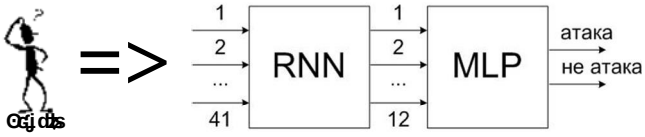

Рис. 1. Отдельный агент (детектор) для мультиагентной системы

Таблица 1. Сетевые атаки в интернете TOP-10

№	Название	Количество атак	%
1	**DoS.Generic.SYNFlood**	156550484	71,192
2	**Intrusion.Win.NETAPI.buffer-overflow.exploit**	32605798	14,828
3	**Intrusion.Win.MSSQL.worm.Helkern**	23263431	10,579
4	**Intrusion.Win.DCOM.exploit**	3245943	1,476
5	**Scan.Generic.UDP**	1799685	0,818
6	**Intrusion.Win.LSASS.exploit**	812775	0,37
7	**Intrusion.Generic.TCP.Flags.Bad.Combine.attack**	604621	0,275
8	**Intrusion.Win.LSASS.ASN1-kill-bill.exploit**	555107	0,252
9	**DoS.Generic.ICMPFlood**	131925	0,06
10	**Scan.Generic.TCP**	101737	0,046

Для тестирования будет использована база данных KDD. На вход подается 41 параметр, определенный в базе. RNN, применение которой с линейной функцией активации аналогично использованию метода главных компонент, выполняет сжатие 41 параметра входного вектора в 12-размерный выходной вектор [7]. MLP обрабатывает полученные в результате сжатия данные и дает заключение относительно входного вектора, является ли он атакой определенного типа или же это нормальное соединение. На выходе детектора возможны два состояния: “да” – если входной образ является атакой, “нет” – входной образ не является атакой.

В мультиагентной системе можно применить детекторы другого вида [8, 9].

После выполнения процедуры обучения нейронные сети могут использоваться в задаче обнаружения вторжений.

Эмуляция образов псевдоатак. Содержимое базы KDD не совсем подходит для построения обучающих выборок для нейросетевых моделей, поскольку отдельные типы атак представлены единичными записями, в то время как другие – десятками, а то и сотнями тысяч, что негативно сказывается на результатах обучения нейронных сетей.

Поэтому в данной работе предлагается расширить те записи, которые представлены в недостаточном количестве, записями о псевдоатаках. *Псевдоатаки* представляют собой не реальные данные, полученные из компьютерной сети, а лишь в некоторой степени схожие с ними, отражающие отдельные признаки, характерные для того или иного типа сетевой активности. Используя записи о псевдоатаках, процесс обучения нейронной сети можно сделать более эффективным, и, возможно, добиться лучших показателей работы модели.

Подготовка записей о псевдоатаках проводится в несколько этапов (см. рис. 2):

1. На первом этапе немногочисленные записи об атаках определенного типа используются для подготовки классификатора (в данном случае нейросетевого классификатора);
2. На втором этапе на базе имеющихся в распоряжении записей генерируются случайным образом новые записи;
3. При помощи подготовленной на первом этапе нейронной сети выполняется классификация всего множества полученных на втором этапе образов. Далее отбираются те образы о псевдоатаках, на которые обученная нейронная сеть отреагировала как атака;
4. Каждая запись о псевдоатаке маркируется как принадлежащая к тому или иному типу сетевой активности, в соответствии с выполненной классификацией.

В результате можно пополнить обучающую выборку образами о псевдоатаках.

Рис. 2. Процесс подготовки записей о псевдоатаках из базы KDD

Понятие мультиагентной системы. В общем случае под *мультиагентной системой* понимается такая система, которая состоит из некоторого числа “интеллектуальных” агентов, которые взаимодействуют между собой. Мультиагентная система может применяться для решения задач, которые слишком сложны для отдельных агентов или для монолитной системы.

Мультиагентная система способна повысить производительность системы в целом, особенно в разрезе эффективности компьютерных вычислений, надежности, расширяемости, устойчивости, скорости реакции, гибкости и т.п.

Однако очевидно, что мультиагентная система может оказаться слишком сложной для разработки и понимания ее функционирования. Все это привносит дополнительные трудности на этапах проектирования и реализации мультиагентных систем.

Тем не менее, интерес к использованию мультиагентных систем в области сложных распределенных систем в последнее время возрастает. Предполагается, что отдельные компоненты в такой системе в некоторой степени автономны и способны контролировать свое поведение для достижения своих собственных целей. В последнее время все больше внимания уделяется исследованиям в области мультиагентных систем (искусственные иммунные системы, коллективное поведение и т.п.), как перспективному направлению современного научного познания.

Каким образом можно применить мультиагентную систему в области обнаружения вторжений?

С уверенностью можно констатировать, что разработать универсальный нейросетевой детектор, способный справляться с обнаружением и классификацией всех видов сетевой активности, достаточно проблематично, ввиду многочисленности и разнообразия сетевых атак.

Очевидный выход из этой ситуации – не ограничивать классификатор одним детектором, а использовать сразу несколько детекторов для решения поставленной задачи (см. рис. 3). Таким образом, исходная сложная задача разбивается на некоторое количество небольших и относительно простых задач. Эти простые задачи распределяются среди множества имеющихся в распоряжении детекторов. Каждый из этих детекторов своего рода эксперт в собственной области знаний. На завершающей стадии сформированные каждым отдельным детектором решения объединяются в общее заключение классификатора. Для формирования общего заключения можно воспользоваться мнением лишь части детекторов, которые отбираются по некоторому определенному алгоритму. Однако в общем случае, если в расчет не берутся вычислительные ресурсы системы, можно принимать во внимание мнение всего набора детекторов, образующих мультиагентную среду (как это было сделано в предыдущей работе [10]).

Проектирование. Одна из возможностей сокращения вычислительных ресурсов, необходимых мультиагентной системе IDS для работы, – уменьшение числа детекторов, задействованных в процессе формирования окончательного решения.

Это может быть реализовано посредством использования некоторого множества предопределенных правил, устанавливающих набор детекторов и задающих очередность их применения в ходе продвижения поступившего образа через классификатор, структура которого задана набором дуг и ребер. Относительно используемых правил решение принимает разработчик в ходе проектирования и построения системы IDS. Эти правила могут быть представлены направленным графом, в узлах которого располагаются отдельные детекторы, а ребра определяют направление передачи данных от одного детектора к другому (см. пример на рис. 4).

Таким образом, каждый узел состоит из отдельного детектора (или ансамбля детекторов) и алгоритма, в соответствии с которым выбирается очередной детектор (в случае если узлу инцидентны несколько исходящих ребер). В узле располагается любой из детекторов, предложенных в предыдущих работах [8, 9], и не обязательно только нейросетевые детекторы. Можно применить искусственную иммунную систему в качестве классификатора в рамках отдельного узла [10].

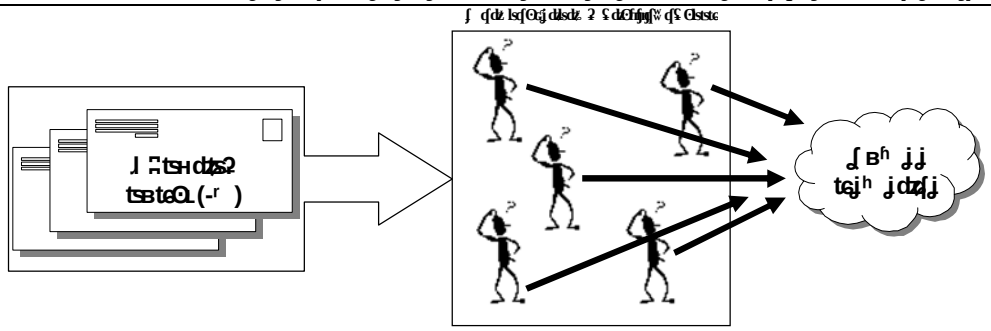

Рис. 3. Мультиагентная система

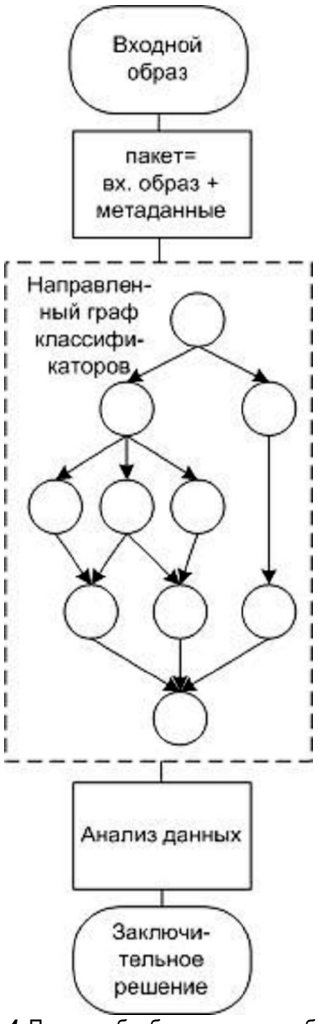

Рис. 4. Пример обработки входного образа

Алгоритм выбора очередного узла может быть как детерминированный, так и случайный. В первом случае очередной узел для передачи образа выбирается в соответствии с результатом, подготовленным детектором в текущем узле или в предыдущих узлах. Во втором случае следующий узел выбирается случайным образом, что привносит в такую модель классификации некоторый элемент случайности.

В целом процесс распознавания может пониматься как продвижение входного *пакета* от первого (входного) узла по направлению к последнему (выходному) узлу направленного графа. Входной пакет состоит из самого входного образа, который представляет активность в компьютерной сети в виде некоторого набора рассчитанных параметров (см. раздел 2) и структуры, содержащей дополнительную информацию (структуры метаданных). Эти метаданные сохраняют в первую очередь результаты выполненной классификации в каждом из узлов, в который попал пакет в ходе продвижения по графу, т.е. в нем сохраняется история продвижения входного образа через внутренние структуры классификатора. На завершающем этапе метаданные собраны и могут быть проанализированы для построения заключительного решения.

Такой подход обладает несколькими полезными особенностями:

- Во-первых, нет необходимости подготавливать детектор, который будет сохранять всю имеющуюся в базе данных информацию. Это упрощает процедуру обучения и сокращает время на подготовку каждого отдельно детектора;
- Во-вторых, такой детектор – это своего рода эксперт в некоторой области знаний. Он хорошо справляется со своей задачей, поэтому реже допускает ошибки;
- Мультиагентную систему можно легко сделать динамической, замещая неэффективные детекторы новыми или добавляя в классификатор детектор, представляющий новые знания, которые отсутствовали в системе до этого.

Реализация. Рассмотрим одну из реализаций мультиагентной системы в том виде, как она предложена в разделе 5.

Было выполнено моделирование архитектуры, показанной на рис. 5, а также проведены эксперименты. Этот пример является демонстрацией того, как с помощью набора правил можно организовать и описать совместную работу некоторого конечного числа агентов. Каждый агент в этой системе решает определенную задачу, но в то же время результаты его работы используются для построения обобщенного решения.

Представленная на рисунке модель классификации включает три уровня, причем каждый последующий уровень подтверждает или опровергает результаты, полученные на предшествующем уровне. Такая модель способна определить, является ли входной образ нормальным соединением или это атака определенного класса (DoS, U2R, R2L или Probe). Кроме того, можно также установить тип атаки (SynFlood, Neptune, …). Детекторы на каждом уровне отличаются друг от друга по структуре (в первую очередь, числом выходов, которому соответствует набор возможных решений).

На первом уровне устанавливается класс атаки или нормальное соединение (см. рис. 5, 6). На втором – выбирается детектор, ответственный за этот класс, и выполняется попытка определить тип атаки. Если тип атаки определить не удается, и детектор второго уровня указывает на нормальное состояние, то решение детектора первого уровня о наличии атаки отменяется и принимается решение о нормальном состоянии контролируемого сегмента сети. Иначе пакет передается на обработку на третий уровень, на котором каждый из детекторов работает с отдельными типами атак и подтверждает или опровергает решение детекторов второго уровня об атаке определенного типа. Если тип атаки на третьем уровне установить не удалось, то однозначно можно констатировать только класс атаки, за который проголосовали два предыдущих детектора. В этом алгоритме в процессе обработки входного пакета задействовано максимум три детектора.

Результаты экспериментов. В этом разделе рассмотрены результаты экспериментов. Для обучения и тестирования использовались данные, представленные в таблице 2. В таблице 3 показаны результаты классификации по классам сетевой активности. Детекторы второго уровня (см. рис. 5, 6) позволяют определить тип атаки.

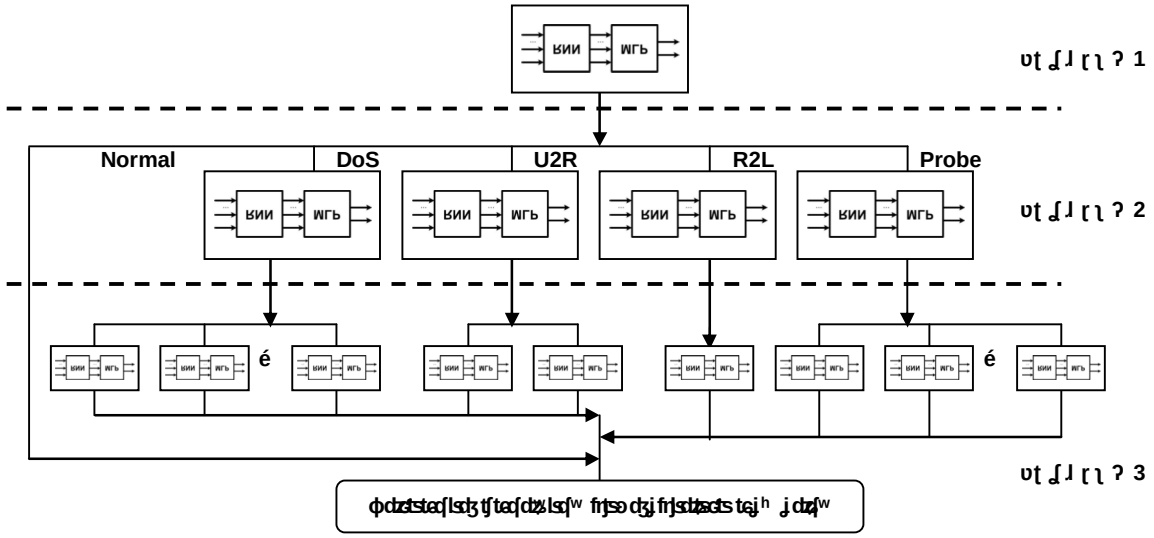

Рис. 5. Структура мультиагентной IDS, представленная в виде направленного графа

Рис. 6. Алгоритм работы классификатора

Таблица 2. Обучающая и тестовая выборки

	DoS	U2R	R2L	Probe	Normal	итого
обучающая выборка	3571	37	278	800	1500	6186
тестовая выборка	391458	52	1126	4107	97277	494020

Таблица 3. Результаты работы мультиагентной системы (класс атаки)

класс	кол-во	обнаружено	распознано
DoS	391458	391125 (99,91%)	370658 (94,68%)
U2R	52	38 (73,08%)	29 (55,77%)
R2L	1126	1068 (94,85%)	1066 (94,67%)
Probe	4107	4056 (98,75)	4056 (98,75)
Normal	97277	---	87245 (89,68%)

Полученные результаты свидетельствуют о том, что одну из поставленных задач удалось решить – снизить количество ложных срабатываний системы. Так, нейросетевая модель RNN+MLP, использованная в узле первого уровня, распознала на тестовой выборке лишь 70% нормальных соединений, но в случае построения совместного решения с учетом мнения классификаторов второго уровня этот показатель составил 90%.

В сравнении с архитектурами систем обнаружения атак, предложенными в более ранних работах, удалось снизить количество ложных срабатываний системы (см. рис. 7).

Рис. 7. Доля ложны срабатываний на данных базы KDD для разных моделей IDS

Как уже было сказано выше, структура исходных данных базы KDD не совсем подходит для обучения нейронных сетей, поскольку отдельные типы и классы атак представлены малочисленными выборками. Это затрудняет процесс обучения и отрицательным образом сказывается на функционировании обученной нейронной сети.

В этой работе для повышения качества распознавания малочисленных атак в ходе обучения классификатора первого уровня использовались псевдоатаки, алгоритм генерирования которых рассмотрен в разделе 3. В результате использования записей о псевдоатаках удалось добиться незначительного повышения качества распознавания записей, относящихся к классам атак, с которыми традиционно возникают проблемы – U2R и R2L. На одной и той же тестовой выборке были опробованы два идентичных нейросетевых классификатора А и В, но при подготовке классификатора В в обучающую выборку были добавлены записи о псевдоатаках (см. таблицу 4).

Таблица 4. Результат обучения с использованием записей о псевдоатаках (А – без псевдоатак; В – с псевдоатаками)

	Классификатор А	Классификатор В
Записи класса U2R	73,08%	78,85%
Записи класса R2L	75,13%	98,67%

Заключение. В данной работе была предложена мультиагентная система обнаружения атак, позволившая в той или иной мере решить следующие задачи:

1. Выполнить двухуровневую классификацию сетевой активности: как по классам, так и по типам атак. Причем каждый последующий уровень иерархии нейросетевых детекторов используется для подтверждения или опровержения решения сгенерированного на вышестоящем уровне;
2. Сократить в мультиагентной системе количество задействованных в принятии окончательного решения детекторов, тем самым снизить нагрузку на требуемые для работы системы вычислительные ресурсы. Эта задача была решена посредством использования набора правил взаимодействия агентов, заданного направленным графом, в узлах которого представлены отдельные классификаторы;
3. Снизить количество ложных срабатываний, благодаря использованию мнений нескольких детекторов и продуманной стратегии обработки пакета в системе;
4. Расширить обучающую выборку образами о псевдоатаках, т.е. пополнить обучающую выборку образами, представленными в недостаточном количестве.

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. Kaspersky Security Bulletin 2009. Основная статистика за 2009 год. [Электрон. ресурс]. – Режим доступа: http://www.securelist.com/ru/downloads/vlpdfs/ksb_09_malware2_ru.pdf.
2. Kumar, S. A software architecture to support misuse intrusion detection / S. Kumar and E. H. Spafford. // In Proceedings of the 18th National Conference on Information Security – 1995. – P. 194–204.
3. Ilgun, K.USTAT: A real-time intrusion detection system for Unix. Master's Thesis.University of California at Santa Barbara. – Santa Barbara, CA, 1992.
4. Lunt, T. Detecting intruders in computer systems // In Proceedings of the 1993 Conference on Auditing and Computer Technology, 1993.
5. Anderson, D. Next-generation intrusion detection expert system (NIDES): A summary / D. Anderson, T. Frivolt and A. Vakdes. – SRI-CSL-95-07 (May), 1995.
6. 1999 KDD Cup Competition. Information on: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.
7. Головко, В.А. Нейронные сети: обучение, организация и применение. Кн. 4: учеб. пособие для вузов / Общая ред. А.И. Галушкина. – М.: ИПРЖР, 2001. – 256 с.
8. Головко, В.А. Нейронная сеть как элемент системы обнаружения вторжений // X Всероссийская научно-техническая конференция "Нейроинформатика-2008": сборник научных трудов. В 2-х частях / В.А. Головко, Л.Ю. Войцехович – Москва: Московский инженерно-физический институт, 2008. – Ч. 2. – С. 86–93.
9. Golovko, V. Boosting Algorithms for Ensembles of Neural Network Classifiers in Intrusion Detection Domain / V. Golovko and L. Vaitsekhovich // In Proceedings of the International Conference on Neural Networks and Artificial Intelligence (ICNNAI-2008) – Minsk, 2008. – P. 70–74.
10. Vaitsekhovich, L. Multiagent Intrusion Detection Based on Neural Network Detectors and Artificial Immune System / L. Vaitsekhovich, V. Golovko, U. Rubanau // In Proceedings of the 10th International Conference on Pattern Recognition and Information Processing (PRIP-2009) – May 19-21, 2009. – Minsk, Belarus. – P. 285–289.

[illegible] 10.11.10

VAITSEKHOVICH L.U., GOLOVKO V.A., KUROSH MADANI Construction of system of detection of attacks with use the column of interaction of the agents

In this article a multiagent model of intrusion detection system have been addressed. Its structure and operation algorithm were described. In this model the multilayer architecture of agent hierarchy was applied. The algorithm of agent interaction can be described with a directed graph. The model is able to perform a classification of network intrusions by classes as well as by types. The experiments indicate that such model can decrease the level of false positives. The neural network agents were adapted with the application of pseudoattack samples.

[illegible] 004.75

[illegible]

[illegible]

Введение. Беспроводные сенсорные сети (БСС) являются одним из современных перспективных направлений развития отказоустойчивых распределенных, самоконфигурируемых систем мониторинга и управления ресурсами и процессами [1, 2]. Вместе с тем использование БСС в ряде областей, в частности, в системах управления технологическими процессами, пожарно-охранных системах, системах безопасности, системах мониторинга реального времени выставляет повышенные требования к надежности их функционирования на всех уровнях модели OSI.

В общем, для повышения надежности передачи данных используют следующие подходы: передача данных на основе методов расширения спектра сигналов (DSSS, FHSS), корректирующие коды (циклическая проверка четности, Рида – Соломона, Боуза – Чеудхури – Хоквингхема и другие) [1]. Кроме того, в [3] разработан модифицированный метод, который базируется на расширении спектра сигнала скачкообразной перестройкой частоты и преобразования системы остаточных классов, которая дает возможность осуществлять помехоустойчивое кодирование и распараллеливание обработки информации

Су Цзюнь, *аспирант Тернопольского национального экономического университета.*

Яцкив Василий Васильевич*, доцент кафедры специализированных компьютерных систем Тернопольского национального экономического университета.*

Саченко Анатолий Алексеевич*, заведующий кафедрой информационно-вычислительных систем и управления Тернопольского национального экономического университета.*