достижения данного результата является способность модифицированного алгоритма качественно оценивать вклад членов и поддерживать баланс между их точностью и разнообразием. Так с позиций точности им были выбраны 10-я, 1-я, 9-я и 6-я сети (перечислены в порядке уменьшения вкладов), однако со стороны разнообразия данный выбор не случаен, т.к. сети обучались на символах с максимально допустимыми вариациями высоты [16, 24] и ширины [10, 18] для данного эксперимента.

Подчеркнем, что полученная точность распознавания тестового MNIST достаточно уникальна, т.к. она является наивысшей для классификаторов архитектуры LeNet-5 и других не нейросетевых, включая SVM, K-NN и др., при этом международное соперничество по распознаванию образов данной базы, проводимое с 1998 г. по настоящее время десятками ученых, является одним из наиболее престижных в области машинного обучения. В сравнении с полученным, более высоким является лишь результат швейцарской команды исследователей (0.35%, 0.27%, и 0.23%, 2010–2012 гг. [3]), который был получен благодаря применению более громоздких архитектур, например, MLP с числом нейронов по слоям: 1-20-40-60-80-100-120-120-10. Кроме того, ими было использовано мощное оборудование, в частности несколько расчетных GPU, что позволило повысить скорость обучения CNN в десятки раз. Отметим критичность данного фактора в проведении эффективной экспериментальной работы, связанной с созданием нейросетевых классификаторов.

Таким образом, можно сделать следующие выводы: 1) селективные алгоритмы способны уменьшить количество членов комитета, а следовательно, и вычислительную сложность; 2) обеспечивая хороший баланс между точностью и разнообразием членов, они способны сформировать более эффективное объединение, чем исходное; 3) качество работы селективных алгоритмов может быть повышено при учете особенностей модели классификаторов. На основании указанных выводов можно предположить, что данные алгоритмы могут оказаться существенным фактором в преодолении проблемы "хрупкости".

Заключение. Основные результаты исследования: 1) обнаружена перспективная трактовка задачи построения универсального классификатора образов цифр как преодоление проблемы "хрупкости", учет которой может способствовать прогрессу в области построения промышленных систем распознавания; 2) проведена теоретическая и экспериментальная работа, показавшая эффективность применения комитетов CNN, обученных на базах с различным стилем начертания образов в сочетании с регулярным варьированием их ширины и высоты, для разрешения данной проблемы; 3) сформирован комитет CNN обладающий уникальной точностью распознавания тестового MNIST (0.36%); 4) построен классификатор, средняя точность которого (98.39%) соответствует уровню коммерческих OCR.

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. Головко, В.А. Нейронные сети: обучение, организация и применение. – М., 2001.
2. LeCun, Y. Gradient-Based Learning Applied to Document Recognition // Proceedings of the IEEE, 86(11), 1998 / Y. LeCun, L. Bottou, Y. Bengio and P. Haffner – P. 2278–2324.
3. Simard, P. Best practices for convolu-tional neural networks applied to visual document analysis // ICDAR / P. Simard, D. Steinkraus, and J. Platt, 2003. – P. 958–963.
4. Dan Ciresan, Ueli Meier, Jürgen Schmidhuber Multi-column deep neural networks for image classification // CVPR, 2012. – P. 3642–3649.
5. Alexander, K. Seewald On the Brittleness of Handwritten Digit Recognition Models // ISRN Machine Vision, 2012.
6. Palacios, R. A system for processing handwritten bank checks automatically // Image and Vision Computing, 2008 / R. Palacios, A. Gupta – P. 1297–1313.
7. MNIST database. – Режим доступа: http://yann.lecun.com/exdb/mnist/index.html.
8. Hastie, T. The Elements of Statistic-al Learning. Data Mining, Inference and Prediction / T. Hastie, R. Tibshirani, J. Friedman – New York: Springer, 2001.
9. Optdigits database. – Режим доступа: http://mlearn.ics.uci.edu/databases/optdigits/.
10. Weinman, J.J. Scene text recognition using similarity and a lexicon with sparse belief propagation / J.J. Weinman, E. Learned-Miller, A. Hanson // IEEE on PAMI, 2009. – P. 1733–1746.
11. Bishop, C.M. Neural Networks for Pattern Recognition. – Oxford University, 1995.
12. Kuncheva L.I. Combining Pattern Classifiers. Methods and Algorithms. – Wiley, 2004.
13. Zhenyu, Lu Ensemble pruning via individual contribution ordering // KDD, 2010 / Lu Zhenyu, Wu Xindong, Zhu Xingquan, Josh Bongard – P. 871–880.
14. KADMOS recognition software. Режим доступа: http://www.rerecognition.com.

Материал поступил в редакцию 05.10.12

KUZMITSKY N.N. Actual questions of use of convolutional neural networks and their committees in recognition of digit patterns

The task of creation of the universal qualifier of digit patterns on a basis of convolutional neural networks is investigated. The analysis of "brittleness" of models of systems of statistical training as main problem in the solution of the specified task is made. Prospects of use of committees as integration tool of knowledge of neural networks and increase of their accuracy is shown. Efficiency of application of bases with different writing style of patterns in combination to regular variation of their width and heights for overcoming of a problem of "brittleness " is proved. The qualifier with average accuracy of recognition of digit patterns over 98 % is created. The committee of the neural networks, allowing to receive 0.36 % of mistakes on a test part of the MNIST base is created.

УДК 004.8.032.26

Кочурко П.А., Головко В.А.

АНСАМБЛЬ НЕЙРОСЕТЕВЫХ ДЕТЕКТОРОВ В СИСТЕМАХ ОБНАРУЖЕНИЯ АТАК

Введение. Среди задач, которые решают системы обнаружения атак, основной является обнаружение сетевой активности, которая может нанести урон информационной безопасности вычислительной системы. Подобная активность, выражающаяся в сетевом трафике, отличном от нормального, может считаться атакой. СОА производит перехват трафика, обрабатывает его с формированием характеристик, значимых для последующего анализа. Полученные характеристики трафика проходят предварительную обработку, после чего подаются на вход ИНС, производящих обнаружение атак технологиями обнаружения аномалий и злоупотреблений. Подобная схема позволяет СОА обнаруживать новые, неизвестные ранее атаки.

Системы обнаружения атак реализуют технологии обнаружения аномалий и обнаружения некорректного поведения или злоупотреблений. Применяемые большинством современных систем методы – на основе правил, статистические и другие – недостаточно эффективно обнаруживают атаки, особенно модифицированные и неиз-

Кочурко Павел Анатольевич, *к.т.н., доцент кафедры интеллектуальных информационных технологий Брестсуого государственного технического университета.*
Беларусь, БрГТУ, 224017, г. Брест, ул. Московская, 267.

вестные [1–3].Исследователи применяют для решения данной задачи множество методов, в том числе искусственные нейронные сети, имеющие большой потенциал в этой области.

Нейросетевые методы обнаружения атак продолжают развиваться, чему подтверждением является большое количество работ за последние годы ([4–9]). Причём основная тенденция, о которой уже говорилось выше, – применение иерархических или гибридных структур, в том числе комбинации нейросетей с другими методами.

Доказано [10, 11], что наилучшего качества обнаружения и распознавания как известных, так и неизвестных атак можно добиться при объединении технологий обнаружения аномалий и злоупотреблений в рамках одной системы.

В данной работе предложено использование рециркуляционных нейронных сетей (РНС) в качестве детекторов аномалий и детекторов злоупотреблений, с их последующим объединением в ансамбль для улучшения качества обнаружения атак. Учитывая способность искусственных нейронных сетей к функционированию на зашумленных данных, обобщению, РНС являются хорошим механизмом для построения СОА, отвечающей требованиям рынка.

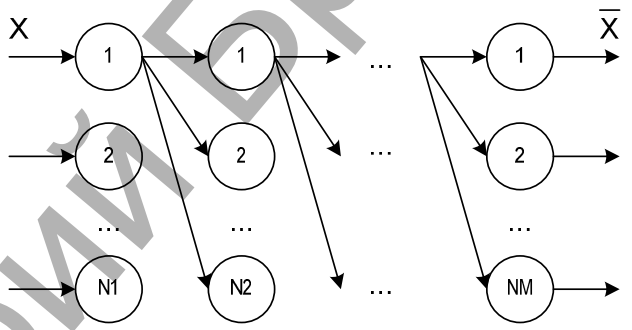
Для тестирования предложенныхи архитектур СОА проведен ряд экспериментов. Предложенные алгоритмы обосновываются результатами экспериментов на базе данных 1999KDDCup [12–13]. Она представляет собой информацию о TCP-соединениях реальной локальной вычислительной сети Air Force's Research Laboratory из Рима, штат Нью-Йорк, на основе которых были смоделированы две недели сетевого трафика, включавшего неизвестные и известные атаки. Каждое соединение описывается 41 параметром – основными параметрами (длительность, протоколы, и т.д.), параметрами данных (количество логинов, системных обращений, и т.д.) и статистическим (количество подключений к данному сервису за последнее временное окно и т.д.). Все соединения в базе данных подразделяются на пять классов: нормальные соединения; DOS-атаки (отказ в обслуживании); probe-атаки (сканирование портов и др.); U2R-атаки (неавторизованное получение привилегий root на данной системе); R2L-атаки (неавторизованный доступ с удалённой системы). Всего – 22 типа атак и нормальные соединения.

Статья организована следующим образом. В разделах 2–3 описываются нейросетевые детекторы и алгоритмы их обучения, настройки и функционирования. В разделах 4–5 представлен ансамбль нейросетевых детекторов и результаты тестирования предложенных подходов. Сделаны выводы и определены дальнейшие направления развития.

Детекторы аномалий на базе РНС. Обнаружение аномальной деятельности характеризуется поиском сетевой активности отличающейся от нормального поведения компонентов системы. Вследствие этого необходимо знание характеристик нормального поведения – нормальных сетевых соединений. Основной проблемой здесь является сложность формализации нормального поведения для автоматического получения его характеристик. Для решения данной задачи предлагаются нейродетекторы на базе нелинейных рециркуляционных нейронных сетей, которые при обучении на нормальном трафике в автоматическом режиме смогут получить и сохранить для дальнейшего использования информацию о явных и неявных закономерностях поведения.

Рециркуляционные нейронные сети (рис. 1) отличаются от других ИНС тем, что информация, подающаяся на вход, в том же виде восстанавливается на выходе. Применяются они для сжатия и восстановления информации (прямое и обратное распространение информации в сетях «с узким горлом») [14–15], для определения резко выделяющихся векторов на фоне общего массива входных данных [16].

В процессе обучения весовые коэффициенты РНС настраиваются таким образом, чтобы минимизировать среднеквадратичную ошибку для всех тренировочных входных векторов. Итогом такого обучения станет то, что в процессе функционирования РНС подаваемые на вход вектора будут восстанавливаться на выходе тем более точно, чем больше они схожи с векторами из тренировочного набора. Сильно выделяющиеся вектора, в свою очередь, будут восстанавливаться недостаточно корректно. Как видим, данная ситуация идеально подходит для применения РНС в качестве детекторов аномалий: если обучение производить на нормальной сетевой активности, то РНС автоматически инкапсулирует в себе информацию о профиле нормального поведения субъекта.



Ni – количество нейронных элементов в i-м слое; NM=N1 – количества нейронных элементов во входном и выходном слоях равны

Рис. 1. Структура РНС из M слоёв

Численная характеристика, которая позволяет судить о том, насколько данный входной вектор «похож» или «не похож» на вектор из тренировочного набора – ошибка реконструкции вектора:

$$E = \frac{1}{n}\sum_{j=1}^{n}(\bar{X}_j - X_j)^2 , \qquad (1)$$

где n – количество параметров во входном векторе X и выходном $\overline{X}$. При этом, чем меньше ошибка реконструкции (2.4), тем больше входной вектор похож на нормальный. Если $E^k > T$, где T – некий заданный для данной РНС порог, то соединение признаётся аномалией, или атакой, в противном случае – нормальным соединением (см. рис. 2 и 3).

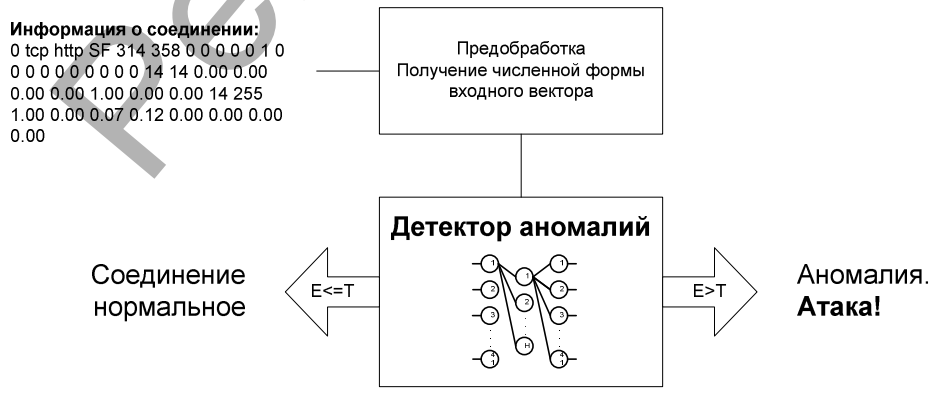


Рис. 2. Схема функционирования нейросетевого детектора аномалий

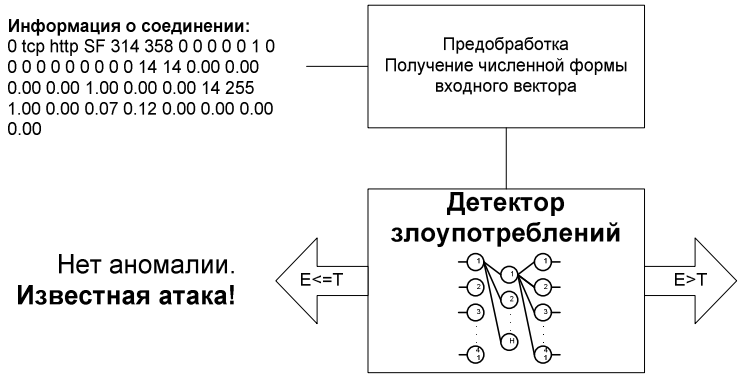


Рис. 4. Схема функционирования нейродетектора злоупотреблений

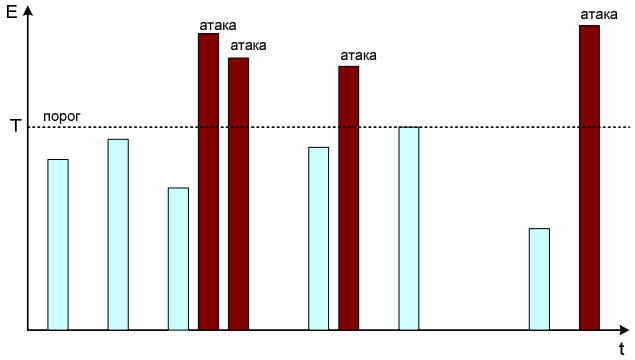


Рис. 3. Соотношение ошибок реконструкции нормальных ианомальных входных векторов-соединений

Таким образом, нулевая гипотеза H_0 будет принята, если ошибка реконструкции (1) не превысит порогового значения T, иначе будет принята альтернативная гипотеза H_1об аномальности соединения. При этом возникает проблема определения порога T, обеспечивающего наиболее качественное обнаружение аномальных соединений. Определить его можно исходя из максимизации значения ACC – точности обнаружения атак. При этом делается предположение, что ошибки первого и второго рода одинаково нежелательны. В противном случае можно использовать некие экспертные стоимостные характеристики ошибок – предполагая, что пропуск атаки (ошибка второго рода) обходится для системы дороже, чем ложное срабатывание (ошибка первого рода), соответственно стоимость у неё должна быть больше.

Детекторы злоупотреблений на базе РНС. Обнаружение аномалий – только один из двух противоположных подходов к обнаружению атак. Разработанную выше технику нейросетевого обнаружения аномалий можно применить и в рамках обнаружения некорректного поведения или обнаружения злоупотреблений. Для этого необходимо поменять местами классы соединений (нормальные и атаки), и соответствующим образом отразить это в процессе обучения нейродетекторов. Нелинейные РНС могут автоматически обучаться на вредоносном трафике и в дальнейшем использоваться для поиска отличных от атак соединений, то есть нормального трафика.

Описанную в разделе 2 методику определения принадлежности входного вектора к одному из двух классов – «нормальные» или «атаки», то есть «не-нормальные» – с помошью рециркуляционных нейронных сетей можно применить и прямо противоположным образом. Если при обучении детектора аномалий использовались нормальные векторы, которые восстанавливались в себя и на основании этого делался вывод об их принадлежности к классу «нормальных», то, обучая детектор на соединениях-атаках, которые должны восстановиться в себя, можно делать вывод об их принадлежности к классу «атаки» (см. рис. 4). Таким образом, если в процессе функционирования данного детектора ошибка реконструкции (1) превышает определённый порог, то данное соединение можно отнести к классу «не-атак», то есть нормальных соединений (см. рис. 5). Так как обучение ведётся на векторах-атаках, то данный подход реализует именно технологию обнаружения злоупотреблений, и оправданно его применение совместно с подходом, реализующим технологию обнаружения аномалий.

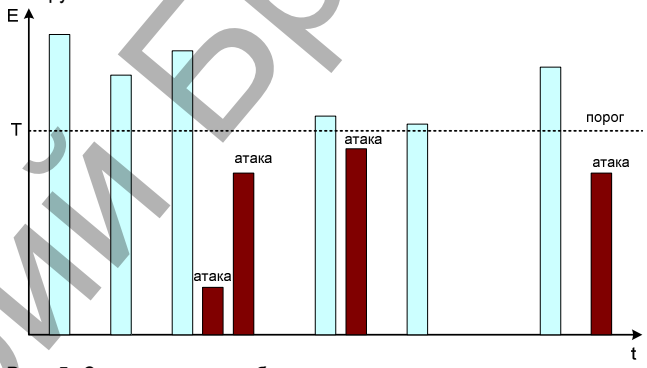


Рис. 5. Соотношение ошибок реконструкции нормальных соединений и атак на детекторе злоупотреблений

Таким образом, одна РНС может применяться для определения принадлежности входного вектора к одному из двух классов – тому, на котором обучалась (класс A), или ко второму (класс $\bar{A}$), которому соответствуют далеко отстоящие вектора:

$$\begin{cases} X \in A, \ \textit{если} \ \ E \le T \\ X \in \bar{A}, \ \textit{если} \ \ E > T \end{cases}, \qquad (2)$$

где E – ошибка реконструкции, T – порог.

Ансамбль детекторов аномалий и злоупотреблений на базе РНС. Как уже отмечалось, недостатком детекторов аномалий является высокое количество ложных срабатываний, а детекторов некорректного поведения – пропуск атак, непохожих на атаки из обучающей выборки. Применение двух подходов – обнаружения злоупотреблений и обнаружения аномалий – в рамках одной системы позволяет избежать недостатков, присущих каждой из технологий в отдельности, не теряя при этом их достоинств. Это, во-первых, позволит снизить ошибки первого и второго рода, увеличив точность предсказания; во-вторых, возможные неточности, связанные с недостаточным качеством обучения одного из детекторов будут устранены применением второго детектора.

При совместном использовании детекторов, построенных на различных подходах, существует сложность принятия окончательного решения. Так, результатом анализа входного образа на двух детекторах может быть один из следующих двоичных векторов – (0;0), (0;1), (1;0) или (1;1), где 1 означает, что данный детектор обнаружил атаку, а 0 – не обнаружил.

Очевидно, что наибольшую проблему составляют результаты, когда один из детекторов атаку обнаружил, а второй – нет. В таких

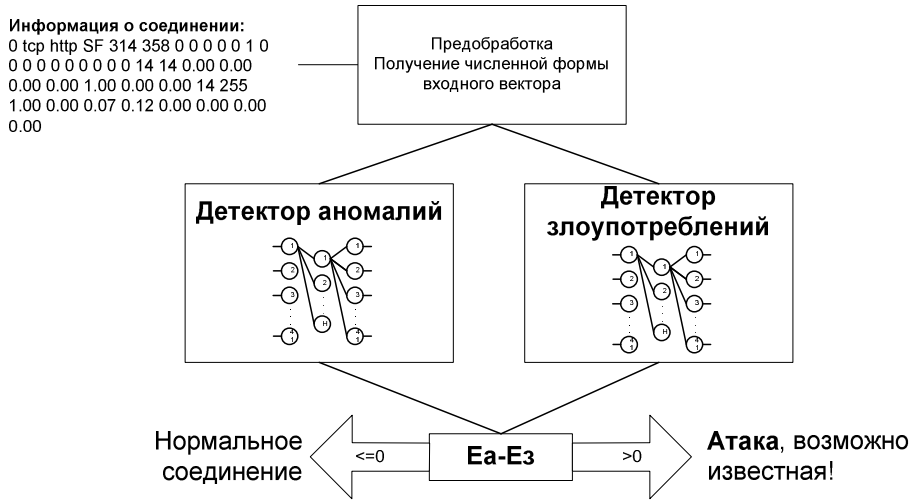


Рис. 6. Схема совместного функционирования нейродетекторов аномалий и злоупотреблений

случаях необходим дополнительный показатель, согласно которому можно сделать вывод о том, какой из детекторов прав. Для детекторов разной природы и архитектуры таким показателем может быть только экспертная оценка вида «больше доверяем детектору аномалий», что может привести к большому количеству ошибок.

В свою очередь, построение ансамбля из детекторов одинаковой природы позволяет анализировать не только двоичные векторы результатов, но и формировать общее решение из выходной информации самих детекторов. То есть решение принимается не на базе решений двух детекторов, а непосредственно по их работе.

Использование нейродетекторов аномалий и злоупотреблений на базе РНС одинаковой архитектуры, обученных до одинакового уровня ошибки, позволяет произвести принятие решения (см. рис. 6 и 7) исходя из ошибок реконструкции (1) на обоих детекторах:

$$\begin{cases} X \in A_N, \ \textit{если} \ \ E_A \le E_З, \\ X \in A_P, \ \textit{если} \ \ E_A > E_З, \end{cases} \quad (3)$$

где E_A – ошибка реконструкции детектора аномалий,

$E_З$ – ошибка реконструкции детектора злоупотреблений,

A_N – нормальные *(negative)* соединения,

A_P – соединения-атаки *(positive)*.

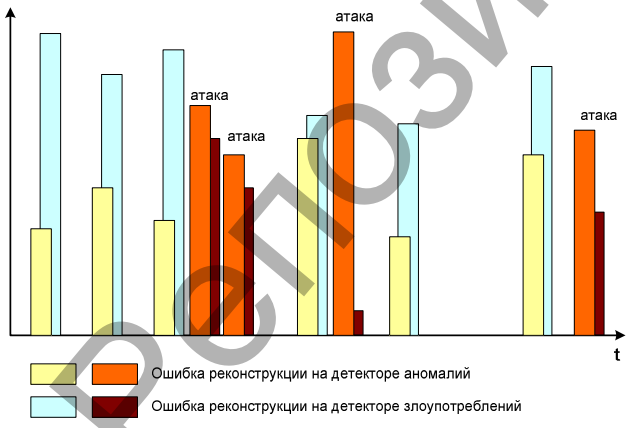


Рис. 7. Соотношение ошибок реконструкции нормальных соединений и атак при совместном функционировании детекторов аномалий и злоупотреблений

Необходимое условие возможности применения данного подхода – одинаковое количество синаптических связей в детекторах и одинаковая среднеквадратичная ошибка, до которой производилось обучение. В противном случае ошибки реконструкции (1) будут несравнимы, и можно будет применять только принятие решения каждым из детекторов по отдельности согласно (3), с последующим принятием общего решения на базе двоичных векторов результатов.

Тестирование нейросетевых детекторов и ансамбля. Вследствие необходимости сравнения и оценки качества работы разрабатываемых методов нужно сформировать выборки данных, которые будут использоваться всеми методами как для обучения, так и тестирования.

База данных KDD'99 состоит из почти пяти миллионов записей о соединениях, из которых только 20% представляют нормальный трафик. В качестве основного тестового набора данных (далее – «ALL») будем использовать базу данных, представляющую собой 10% всей базы KDD. В базе содержатся записи о 494020 соединениях 41 службы, в том числе об атаках 22 типов.

Для проверки способности обнаруживать неизвестные ранее атаки к данным наборам добавим тестовую выборку «ALL-NEW», представляющую собой тестовый набор из базы KDD, включающий нормальные соединения и атаки 32 типов, в том числе отсутствовавшие в 10%-й базе.

Обучающие выборки сформируем следующим образом (см. таблицу 1). Для обучения детекторов нормальному сетевому трафику выберем случайным образом 500 нормальных соединений, а для обучения некорректному поведению – по 200 атак каждого типа из базы KDD'99.

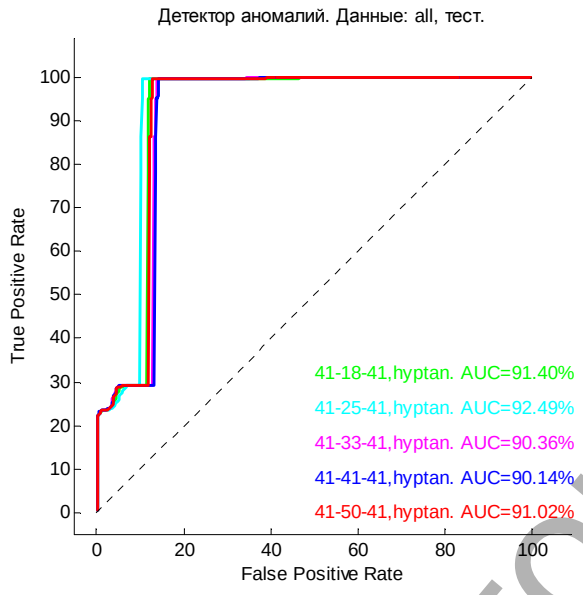
Таблица 1. Объёмы основных тестовых и обучающих выборок

НАБОР ДАННЫХ	*P* КОЛ-ВО АТАК	*N* КОЛ-ВО НОРМАЛЬНЫХ	КОЛ-ВО ТИПОВ СОЕДИНЕНИЙ	
			K ВСЕГО	В Т.Ч. ТИПОВ АТАК
ТЕСТОВЫЕ НАБОРЫ ДАННЫХ				
ALL	396743	97277	23	22
ALL-NEW	250436	60592	33	32
ОБУЧАЮЩИЕ НАБОРЫ ДАННЫХ				
НОРМАЛЬНЫЕ СОЕДИНЕНИЯ	*0*	500	1	0
СОЕДИНЕНИЯ-АТАКИ	4400	0	22	22

Тестирование детекторов аномалий. Основные результаты тестирования на выборках ALL и ALL-NEW представлены в таблице 2 и на рисунке 8, который представляет собой кривые операционных характеристик (ROC-кривые). Такая кривая отображает зависимость значений *TPR* и *FPR* для всего спектра возможных пороговых значений детектора. Идеальная ROC-кривая включает в себя и точку (0;1), то есть 100% обнаружение атак при 0% ложных срабатываний. При визуальном сравнении результатов нескольких детекторов можно говорить, что один детектор функционирует лучше, если его ROC-кривая ближе к идеальной. Среднее время обучения трёхслойной сети до среднеквадратичной ошибки 0,0005 составило 20 секунд.

Таблица 2. Результаты тестирования детекторов аномалий на базе трёхслойных РНС

Кол-во нейронов в скр. слое	Функция активации – tanh			Функция активации – logsig		
	FPR, %	FNR, %	ACC, %	FPR, %	FNR, %	ACC, %
Тестовый набор ALL						
18	12,73	0,09	**97,43**	14,62	0,10	**97,04**
25	10,88	0,10	**97,78**	10,72	0,11	**97,80**
33	14,35	0,09	**97,10**	16,87	0,10	**96,60**
41	14,40	0,09	**97,09**	13,84	0,10	**97,20**
50	12,93	0,36	**97,16**	10,22	0,10	**97,91**
Тестовый набор ALL-NEW						
18	8,41	17,98	**83,88**	9,37	17,09	**84,41**
25	7,43	19,56	**82,80**	7,42	18,22	**83,88**
33	8,97	18,05	**83,72**	10,35	17,93	**83,55**
41	9,04	18,02	**83,73**	9,39	18,23	**83,49**
50	9,03	17,93	**83,80**	7,20	18,86	**83,41**



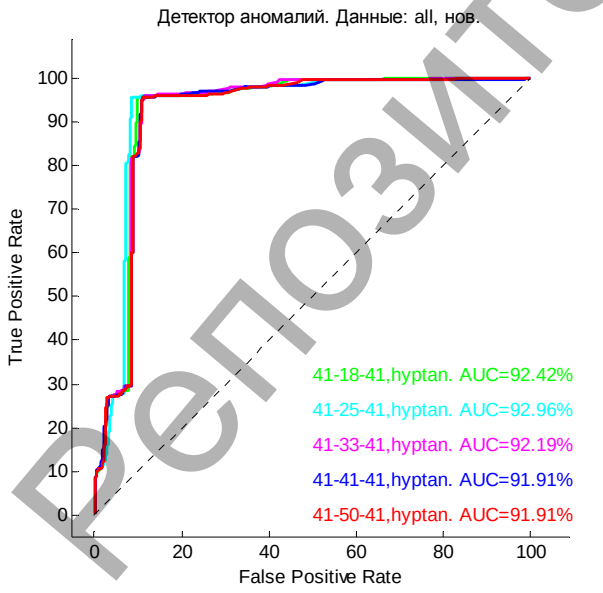


Рис. 8. ROC-кривые для некоторых детекторов аномалий с различным количеством нейронов в скрытом слое при обнаружении атак на наборах ALL и ALL-NEW

По результатам тестирования можно сделать следующие выводы:

- данный метод подходит для обнаружения аномалий в сетевом трафике, поскольку уровень ошибок первого и второго рода сравнительно низок (см. раздел 1.5);
- наилучшими архитектурами являются сети с узким горлом – 25 нейронов в скрытом слое – за счёт выделения наиболее значимой информации из входных данных. Это подтверждают и значения AUC для ROC-кривых детекторов (см. рис. 2.8);
- влияние выбора функции активации в общем случае невелико – схожие результаты показывают как на выборках ALL и ALL-NEW обе функции активации скрытого слоя;
- качество обнаружения на тестовом наборе данных с неизвестными соединениями ALL-NEW ниже, чем на тестовом наборе ALL, из которого формировалась обучающая выборка. Необходимо улучшение подхода путём комбинированного применения с детектором злоупотреблений;
- таким образом, нейродетекторы могут быть построены на любой из представленных трёхслойных архитектур с качеством обнаружения 97%.

Тестирование детекторов злоупотреблений. Для определения, насколько данный подход способен реализовывать обнаружение злоупотреблений, проведём тестирование (см. таблицу 3 и рис. 9), аналогичное описанному в предыдущем пункте. Среди РНС тех же архитектур определим наиболее подходящее количество слоёв, нейронов в скрытом слое, функции активации. Для обучения детекторов используем выборку из всех типов атак, содержащую 4400 образов. Поскольку размер обучающей выборки для детектора злоупотреблений больше, чем для детектора аномалий, то и процесс обучения длится дольше: обучения трёхслойного детектора злоупотреблений до среднеквадратичной ошибки 0,0005 в среднем занимает 130 секунд.

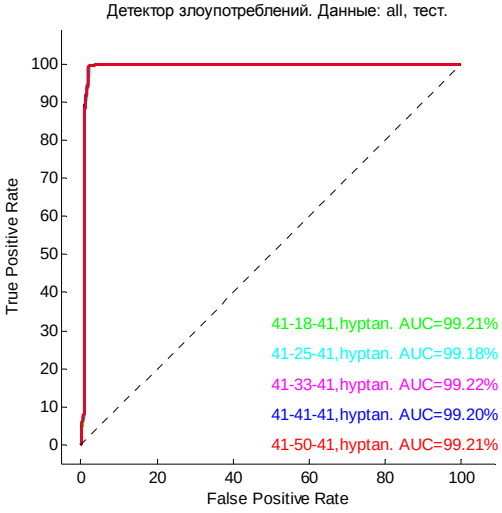
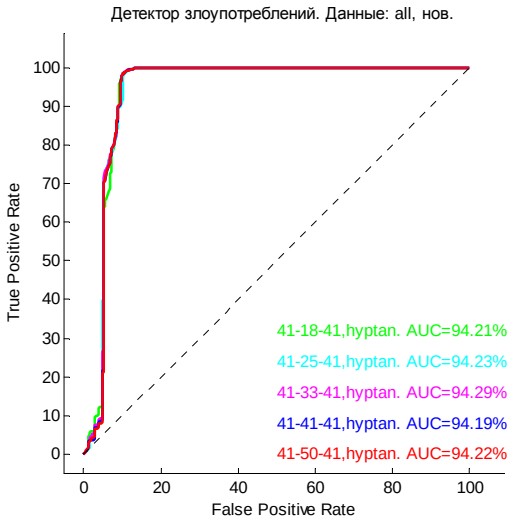


Таблица 3. Результаты тестирования детекторов злоупотреблений на базе трёхслойных РНС

Кол-во нейронов в скр. слое	Функция активации – tanh			Функция активации – logsig		
	FPR, %	FNR, %	ACC, %	FPR, %	FNR, %	ACC, %
Тестовый набор ALL						
18	0,25	2,71	**97,77**	0,23	2,19	**98,20**
25	0,10	2,73	**97,79**	0,28	2,24	**98,15**
33	0,15	2,91	**97,63**	0,22	2,18	**98,20**
41	0,04	2,97	**97,61**	0,24	2,19	**98,19**
50	0,04	2,73	**97,80**	0,24	2,29	**98,12**
Тестовый набор ALL-NEW						
18	0,30	11,57	**90,63**	0,30	11,57	**90,63**
25	0,17	19,56	**84,22**	0,17	19,56	**84,22**
33	0,28	11,97	**90,31**	0,28	11,97	**90,31**
41	0,28	11,84	**90,41**	0,28	11,84	**90,41**
50	0,26	12,10	**90,21**	0,26	12,10	**90,21**



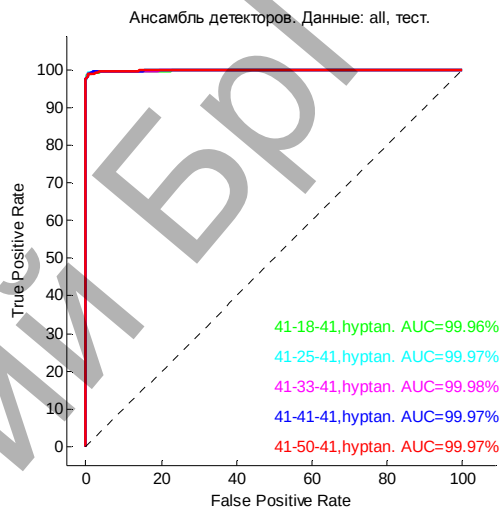


Рис. 9. ROC-кривые обнаружения атак трёхслойными детекторами злоупотреблений с различным количеством нейронов в скрытом слое на наборах ALL и ALL-NEW

По результатам тестирования детекторов злоупотреблений можно сделать следующие выводы:

- в качестве функции активации скрытого слоя может использоваться и гипертангенс, и сигмоидная функция, их результаты отличаются незначительно;
- если детектор аномалий имел низкое количество пропущенных атак при высоком проценте ложных срабатываний, то детектор злоупотреблений, наоборот, малое количество ложных срабатываний, но пропускает атаки, непохожие на атаки из обучающей выборки;
- тем не менее качество работы даже этих детекторов превышает 95%, что является хорошим показателем для систем обнаружения атак.

Таким образом, нейродетекторы на базе РНС могут использоваться в качестве детекторов злоупотреблений, причем предпочтительной является трёхслойная архитектура с узким горлом.

Тестирование ансамбля детекторов аномалий и злоупотреблений. Для определения возможности применения данного подхода для обнаружения атак протестируем (см. таблицу 4 и рис. 10) нейродетекторы, обученные в предыдущих разделах, в совместном использовании.

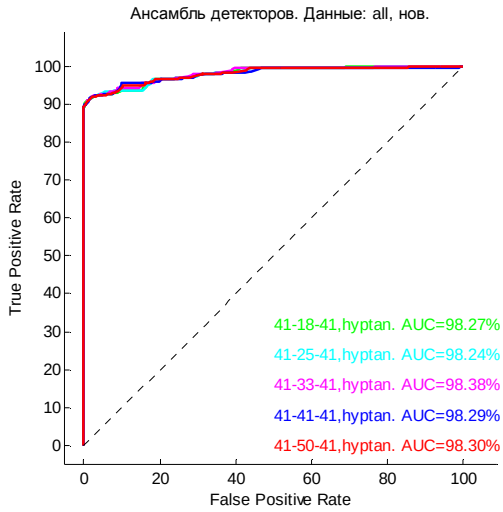


Рис. 10. ROC-кривые обнаружения атак ансамблем из трёхслойных нейродетекторов на наборах ALL и ALL-NEW

По результатам тестирования ансамблей из трёхслойных детекторов аномалий и злоупотреблений можно сделать следующие выводы:

- наилучшее качество обнаружения атак показывают ансамбли, составленные из детекторов с архитектурой, показавшей наилучшие результаты и ранее – с узким горлом 25 или 33 нейрона;
- ансамбли детекторов показывают лучшие результаты, чем каждый детектор по отдельности. ROC-анализ подтверждает общее преимущество ансамбля перед отдельными детекторами: на тестовом наборе ALL значение интегральной характеристики *AUC*, показывающей способность обнаружения атак независимо

Таблица 4. Результаты тестирования ансамбля детекторов злоупотреблений и аномалий на базе трёхслойных РНС

Кол-во нейронов в скр. слое	Функция активации – tanh			Функция активации – logsig		
	FPR, %	FNR, %	ACC, %	FPR, %	FNR, %	ACC, %
Тестовый набор ALL						
18	0,03	1,73	**98,60**	0,03	1,78	**98,56**
25	0,03	1,83	**98,52**	0,02	1,83	**98,52**
33	0,02	1,79	**98,56**	0,02	1,76	**98,58**
41	0,02	1,84	**98,52**	0,02	1,78	**98,56**
50	0,03	1,79	**98,55**	0,02	1,77	**98,57**
Тестовый набор ALL-NEW						
18	0,04	10,59	**91,47**	0,01	10,37	**91,65**
25	0,00	12,33	**90,07**	0,00	10,46	**91,58**
33	0,01	10,46	**91,58**	0,03	10,43	**91,60**
41	0,00	10,48	**91,56**	0,01	10,48	**91,56**
50	0,01	10,47	**91,57**	0,02	10,43	**91,60**

от выбранных порогов, для ансамбля равно 99,97%, что выше, чем значение *AUC* для любого из детекторов по отдельности (разница составляет от 0,5% до 7,3%);

- качество обнаружения атак на дополнительной тестовой выборке с новыми атаками ALL-NEW, хотя и уступает качеству обнаружения на выборке ALL, но, тем не менее, превышает 91%, что является достаточно высоким результатом. При этом необходимо отметить, что применение ансамбля и в этом случае более выгодно, чем каждого из детекторов по отдельности – значение *AUC*, равное 98,38%, также выше, чем для каждого из отдельных детекторов (от 4% до 6%).

Заключение. В таблице 5 представлены средние и экстремальные значения качества обнаружения атак, визуальное представление результатов показано на рисунке 11.

Таблица 5. Сравнение средних и экстремальных значений качества обнаружения атак РНС на разных наборах данных

	ALL		ALL-NEW	
	$ACC_{среднее}$, %	ACC_{max}, % ACC_{min}, %	$ACC_{среднее}$, %	ACC_{max}, % ACC_{min}, %
Детектор аномалий	97,18	97,91 96,60	83,73	84,41 82,80
Детектор злоупотреблений	97,96	98,20 97,61	90,51	90,85 84,22
Ансамбль детекторов	98,36	98,60 98,12	90,85	91,58 90,07

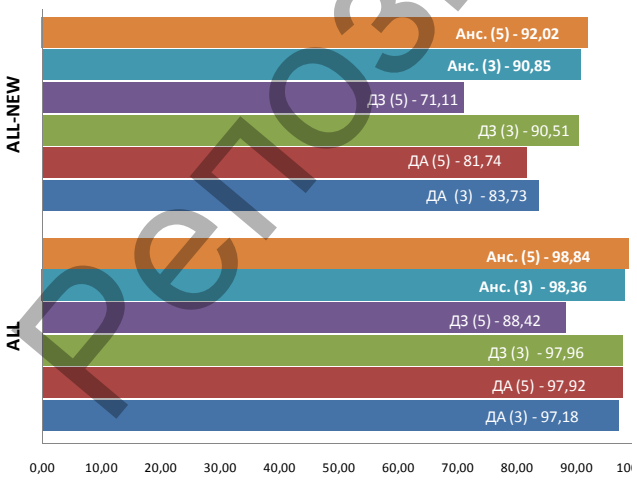


Рис. 11. Сравнение средних результатов тестирования трёхслойных и пятислойных детекторов аномалий, детекторов злоупотреблений и их ансамблей

Таким образом, нейродетекторы на базе РНС могут использоваться как в качестве детекторов аномалий и детекторов злоупотреблений, так и в составе ансамблей, комбинирующих технологии обнаружения и злоупотребления в рамках одной системы. Подобные ансамбли позволяют получить гарантированно высокий результат обнаружения атак, независимо от качества обнаружения каждым из детекторов по отдельности.

Проведенное экспериментальное тестирование предложенных алгоритмов показало, что архитектурные особенности РНС существенно не влияют на качество работы системы. Представленные результаты показывают, что ансамбль детекторов функционирует с более высокой точностью, чем каждый из детекторов по отдельности и способен функционировать с точностью классификации свыше 98% на известных атаках и до 92% на наборе данных из модифицированных и неизвестных атак.Показана возможность формирования общей оценки без необходимости определения пороговых значений отдельных детекторов, что является существенным преимуществом по сравнению с использованием детекторов аномалий и детекторов злоупотреблений по отдельности.

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. Лукацкий, А.В. Обнаружение атак / А.В. Лукацкий. – СПб.: БХВ-Петербург, 2003. – 596 с.
2. Олдер, Р. Snort 2.1. Обнаружение вторжений / Р. Олдер [и др.] – 2-е изд. – М.: Бином, 2006. – 656 с.
3. Норткатт, С. Обнаружение вторжений в сеть. Настольная книга специалиста по системному анализу / С. Норткатт, Дж. Новак. – М.: Лори, 2001 – 384 с.
4. Iftikhar, A. et al. Towards the selection of best neural network system for intrusion detection / A. Iftikhar, A. Azween and A. Alghamdi // International Journal of the Physical Sciences. – 2010. – Vol. 5 (12). – P. 1830–1839.
5. Saravanakumar, S. Development and Implementation of Artificial Neural Networks for Intrusion Detection in Computer Network / S. Saravanakumar, Umamahchwari, D. Jayalakshmi, R. Sugumar // International Journal of Computer Science and Network Security. – 2010. – Vol. 10, №7. – P. 271–275.
6. Ali, A. Intelligent Adaptive Intrusion Detection Systems Using Neural Networks (Comparative study) / A. Ali, A. Saleh, T. Badawy // International Journal of Video & Image Processing and Network Security. – 2010. – Vol. 10, №1. – P. 1–12.
7. Wang, G. A new approach to intrusion detection using Artificial Neural Networks and fuzzy clastering / G. Wang, J. Hao, J. Ma, L. Huang // Expert Systems with Applications. – 2010. – № 2. – P. 6225–6232.
8. Anyanwu, L.O. Scalable Intrusion Detection with Recurrent Neural Networks / L.O. Anyanwu, L. Keengwe, G.A. Arome // International Journal of Multimedia and Ubiquitos Engineering. – 2011. – Vol. 6. – №1. – P. 21–28.
9. Novosad, T. Fast Intrusion Detection System based on Flexible Neural Tree / T. Novosad, J. Platos, V. Snasel, A. Ajith // Sixth International Conference on Information Assurance and Security (IAS): proceedings, USA. – 2010. – P. 142–147.

10. Muna, M.J. Design Network Intrusion Detection System usin hybrid Fuzzy-Neural Network / M.J. Muna, M. Mehrotra // International Journal of Computer Science and Security. – 2010. – Vol. 4 (3). – P. 258–294.
11. Giacinto, G. Fusion of multiple classifiers for intrusion detection in computer networks / G. Giacinto, F. Roli, L. Didaci // Pattern Recognition Letters. – 2003. – № 24. – P. 1795–1803.
12. Lee, W. Mining in a data-flow environment: Experience in network intrusion detection / W. Lee, S.J. Stolfo, K.W. Mok // The Fifth International Conference on Knowledge Discovery and Data Mining (KDD-99): proceedings, San Diego, CA, 15–18 August ,1999 / Eds.: S. Chaudhuri, D. Madigan. – ACM, 1999. – P. 114–124.
13. Lee, W. Adaptive intrusion detection: A data mining approach / W. Lee, S. J. Stolfo, K. W. Mok // Artificial Intelligence Review. – 2000. – Vol. 14. – №6. – P. 533–567.
14. Головко, В.А. Нейронные сети: обучение, организация и применение / В. А. Головко. – М.: ИПРЖР, 2001. – 256 с.
15. Ежов, А.А. Нейрокомпьютинг и его приложение в экономике и бизнесе / А. А. Ежов, С.А. Шумский. – М.: МИФИ, 1998. – 222 с.
16. Kramer, M.A. Nonlinear principal component analysis using autoassociative neural networks / M.A. Kramer // J. Am. Institute Chem. Eng. (AIChE). – 1991. – Vol. 37. – №2. – P.233–243.

Материал поступил в редакцию 22.12.12

KACHURKA P.A., GOLOVKO V.A. Ensemble of neuronetwork detectors in systems of detection of attacks

Approach to detection of network attacks with use of recirculation neural networks as detectors of anomalies and detectors of abuses is presented. Sharing of these detectors within system of detection of attacks is proved. The experimental results confirming prospects of approach are given.

УДК 004.896

Дёмин В.В., Кабыш А.С., Дунец И.П., Дунец А.П., Головко В.А.

ИСПОЛЬЗОВАНИЕ RAM-BASED СЕТЕЙ ДЛЯ ДЕТЕКТИРОВАНИЯ ГРАФИЧЕСКОЙ МЕТКИ

Введение. В данной работе рассмотрена задача распознавания графической метки ведущего робота в системе «ведущий-ведомый роботы». Для решения задачи был разработан метод детектирования на основе RAM-based сетей, позволяющий по расположению метки узнать положение и дальность ведущего робота по графическому паттерну. Обученная RAM-based сеть хранит характеристические особенности паттерна в разных секторах относительно ведомого робота. Сработавший дискриминатор сети будет указывать на сектор, в котором находится ведущий робот. В подробностях описана процедура обучения и настройки RAM-based сети. Преимуществом данного подхода является снижение вычислительных ресурсов, что позволяет применять данное решение на платформах с низкой производительностью.

Использование камер в коммуникации стайных роботов. В задаче следования за лидерами от роботов требуется сформировать паттерн формации, при котором каждый предыдущий робот следует за последующим, а ведущий – лидер, либо управляется оператором, либо следует по заранее заданному пути.

Существуют различные подходы к распознаванию роботами друг друга: инфракрасные датчики, световые паттерны, RFID-метки, компьютерное зрение и т.д. В данной работе распознавание ведущего основано на детектировании визуальной графической метки, закрепленной на корпусе робота при помощи RAM-based нейронных сетей.

Роботы, оснащенные видеосистемой, могут получить необходимый минимум информации о находящихся поблизости роботах группы, если роботов достаточно легко детектировать по их особенностям, паттернам или световым меткам. Цель работы состоит в разработке методики распознавания ведущего робота, не требующей достаточных вычислительных мощностей и устойчивой к помехам во внешней среде.

Отсутствие камеры в целом ограничивает область применения swarm роботов. Большинство камер на роботах swarm-масштаба не являются пригодными для глобального восприятия окружающей среды, а используются только для локальных областей, с максимальным радиусом до 1 метра.

В работе [1] описано стайное поведение группы роботов, окрашенных в красный цвет. Эта их характеристика (красный окрас) была использована при детектировании роботов друг другом с помощью камеры. Если область не менее чем 25 на 25 пикселей по границам имела красный цвет, то область помечалась как вероятный сосед. После фазы распознавания принимались решения о факте наличия робота и дистанции до него.

В работе [2] роботы «s-bot» имели светодиодное кольцо, по периметру робота формирующее триангулярный паттерн из разных цветов, где красный цвет указывает направление движения робота (рис. 1). На роботе установлена всенаправленная камера с эффективной областью обзора в 60 см. Алгоритм обработки изображения на роботе определяет по «цвету» направление движения соседей в области видимости камеры. Для этого используется вероятностный алгоритм определения направления движения соседей по изображению, при заранее заданных оценках распределения. Роботы в данном исследовании решали задачу кооперативного транспорта путем создания формации и определяли направление движения путем переговоров.

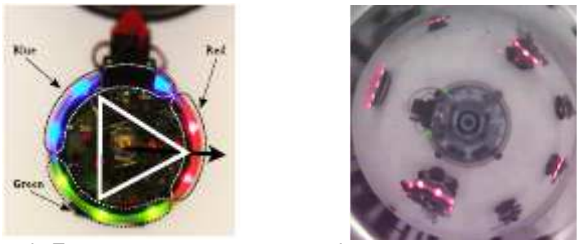


Рис. 1. Триангуляционный паттерн, формируемый светодиодами робота

Описание используемых роботов

Ведущий или **лидер** (*leader*) – автономный робот, основной задачей которого является движение к цели по некоторому маршруту и, возможно, без столкновений с препятствиями. За ведущим роботом следуют **ведомые** (*followers*) роботы, оборудованные видеокамерой для распознавания ведущего робота. В задаче следования за лидером от ведомых роботов требуется не потерять ведущего –

Демин В.В., *магистрант кафедры интеллектуальных информационных технологий Брестского государственного технического университета.*

Кабыш А.С., *ст. преподаватель кафедры интеллектуальных информационных технологий Брестского государственного технического университета.*

Дунец И.П., *аспирант кафедры интеллектуальных информационных технологий Брестского государственного технического университета.*

Дунец А.П., *доцент кафедры интеллектуальных информационных технологий Брестского государственного технического университета.*
Беларусь, БрГТУ, 224017, г. Брест, ул. Московская, 267.