ПОСТРОЕНИЕ НЕЙРОСЕТЕВОЙ И ИММУНОКЛЕТОЧНОЙ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Браницкий Александр Александрович,
лаборатория проблем компьютерной безопасности, СПИИРАН,
Полушин Владимир Юрьевич,
к.т.н., доцент, ЗАО «НПП «Телда»

РусКрипто'2015, 19 марта 2015 г.

Задачи исследования

- Создание гибридной схемы обнаружения и классификации сетевых атак
- Программная реализация нейросетевого и иммуноклеточного модулей для обнаружения атак
- Сравнение предложенных подходов по критерию эффективности распознавания атак

Введение

Большинство коммерческих СОВ работают на основе экспертного или сигнатурного подходов. Их недостатками являются:

- Невозможность обнаружения неизвестных типов угроз
- Необходимость постоянного обновления базы сигнатуры атак или правил

Одним из решений является применение адаптивных методов.

Релевантные работы

Авторы и ссылка на работу	Предложенный метод	Входные данные	Цель применения
Silva L., Santos A., Silva J., Montes [1], Vollmer T., Manic M. [2]	Нейронная сеть	Сигнатуры системы Snort	Обнаружение вторжений
Mukkamala S., Sung A.H., Abraham A., Ramos V. [3]	Нейронные сети, SVM, MAP-сплайны	DARPA 1998	Классификация сетевых соединений
Tan K. [4]	Нейронная сеть	Системный журнал событий	Обнаружение аномального поведения
Ryan J., Lin M.-J., Miikkulainen R. [5]	Нейронная сеть	Наборы команд	Идентификация пользователей
Jiang J., Zhang C., Kame M. [6], Liu Y. [7]	Радиально-базисная сеть	KDD99	Классификация сетевых соединений
Wang W., Guan X., Zhang X., Yang L. [8]	СОК Кохонена, скрытая марковская модель	Параметры системных вызовов	Обнаружение аномальных процессов
Vaitsekhovich L. [9], Komar M., Golovko V., Sachenko A., Bezobrazov S. [10]	Иммунные нейросетевые детекторы, сгенерированные по алгоритму клонального отбора	KDD99	Обнаружение и классификация сетевых атак
Stibor T., Timmis J., Eckert C. [11]	Иммунные детекторы, сгенерированные по алгоритму отрицательного отбора	KDD99	Обнаружение вторжений

Релевантные работы

- [1] Silva L., Santos A., Silva J., Montes A. A neural network application for attack detection in computer networks // Proceedings of International Joint Conference on Neural Network, 2004. Vol. 2. P. 1569–1574.
- [2] Vollmer T., Manic M. Computationally efficient neural network intrusion detection security awareness // 2nd International Symposium on Resilient Control Systems, 2009. P. 25–30.
- [3] Mukkamala S., Sung A.H., Abraham A., Ramos V. Intrusion detection systems using adaptive regression splines // Sixth International Conference on Enterprise Information Systems, 2006. P. 211–218.
- [4] Tan K. The application of neural networks to UNIX computer security // In Proceedings of the IEEE International Conference on Neural Networks, 1995. Vol. 1. P. 476–481.
- [5] Ryan J., Lin M.-J., Miikkulainen R. Intrusion detection with neural networks // Advances in Neural Information Processing Systems, 1998. P. 943–949.
- [6] Jiang J., Zhang C., Kame M. RBF-based real-time hierarchical intrusion detection systems // In Proceedings of the International Joint Conference on Neural Networks, 2003. Vol. 2. P. 1512–1516.
- [7] Liu Y. QPSO-optimized RBF neural network for network anomaly detection // Journal of Information & Computational Science, 2011. Vol. 8, No. 9. P. 1479–1485.
- [8] Wang W., Guan X., Zhang X., Yang L. Profiling program behavior for anomaly intrusion detection based on the transition and frequency property of computer audit data // Computers & Security, 2006. Vol. 25, Iss. 7. P. 539–550.
- [9] Vaitsekhovich L. Intrusion Detection in TCP/IP networks using immune systems paradigm and neural network detectors // XI International PhD Workshop OWD, 2009. P. 219–224.
- [10] Komar M., Golovko V., Sachenko A., Bezobrazov S. Development of neural network immune detectors for computer attacks recognition and classification // IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), 2013. Vol. 2. P. 665–668.
- [11] Stibor T., Timmis J., Eckert C. A comparative study of real-valued negative selection to statistical anomaly detection techniques // Artificial Immune Systems, 2005. P. 262–275.

Используемые математические модели

- Система из статически обученных многослойных нейронных сетей
- Система из динамически обучающихся карт Кохонена (иммунных клеток)

Обучающие и тестовые множества

- KDD Cup 99 (4898431 записей о сетевых соединениях)
- NSL KDD (125973 записей о сетевых соединениях)
- 41 параметр сетевого трафика
- 4 класса атак и 22 типа
- Для распознавания 9 типов атак использовалось 29 параметров

Классы сетевых атак

- DoS (Denial of Service)
  - Отказ в обслуживании
- U2R (Unauthorized access to local root privileges)
  - Получение привилегий суперпользователя со стороны локального пользователя
- R2L (Unauthorized access from a remote machine)
  - Получение доступа незарегистрированного пользователя к удаленному компьютеру
- Probing (Surveillance and other probing)
  - Сканирование портов

Классы сетевых атак

- DoS (Denial of Service)
  - back, neptune, pod, smurf, teardrop
- U2R (Unauthorized access to local root privileges)
  - Получение привилегий суперпользователя со стороны локального пользователя
- R2L (Unauthorized access from a remote machine)
  - Получение доступа незарегистрированного пользователя к удаленному компьютеру
- Probing (Surveillance and other probing)
  - ipsweep, nmap, portsweep, satan

Процесс обучения

SELECT * FROM kdd_data WHERE attack_type = pod ORDER BY RAND()

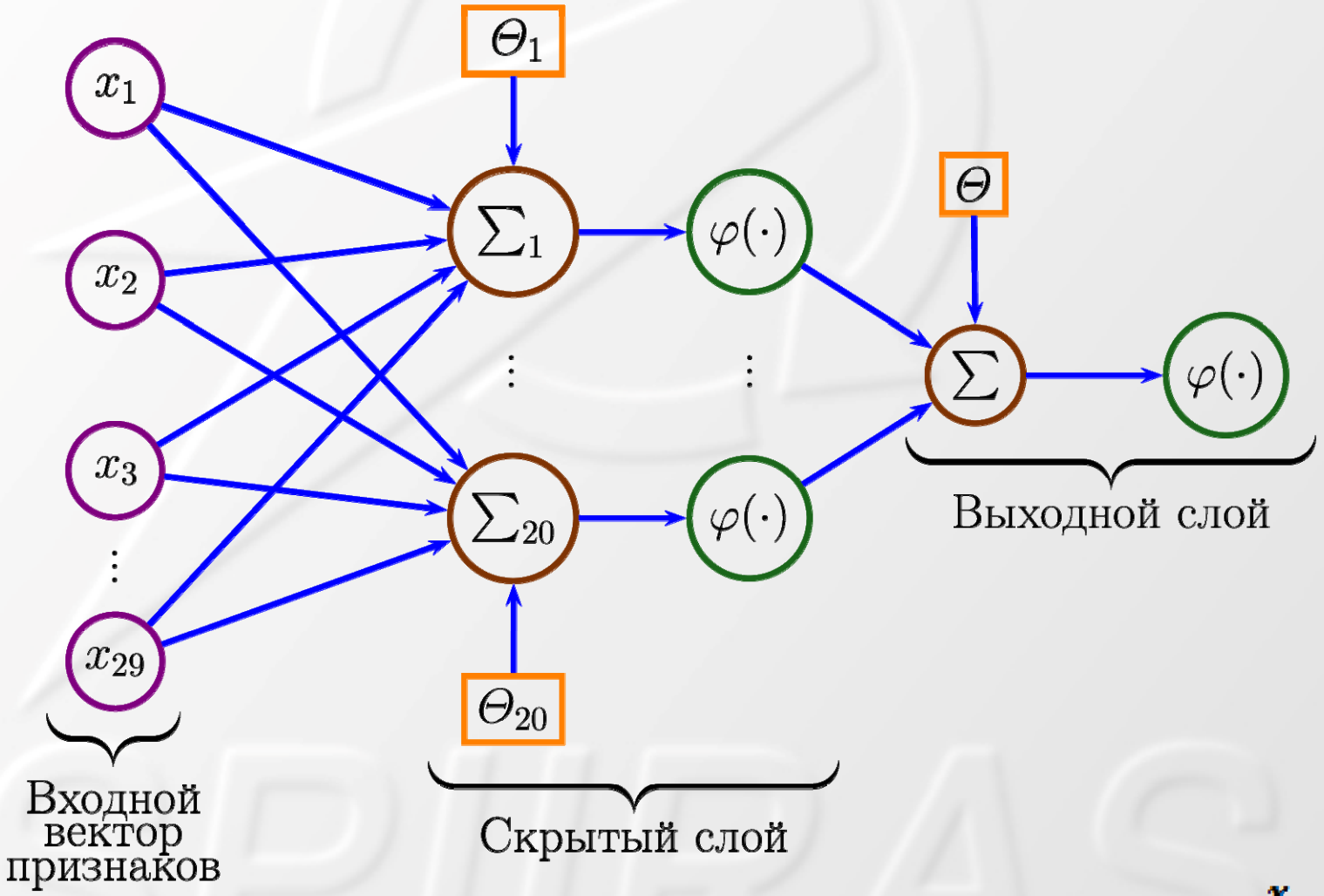
$$y_i = \psi(x_i),\ y_i \in [0;1]$$

1) Построение матрицы ковариации
2) Нахождение собственных векторов и чисел
3) Вычисление новых обучающих векторов

1) Алгоритм обратного распространения ошибки
2) Конкурентное обучение

Сериализация объектов в поток байтов или в human-readable формат

Нейронные сети



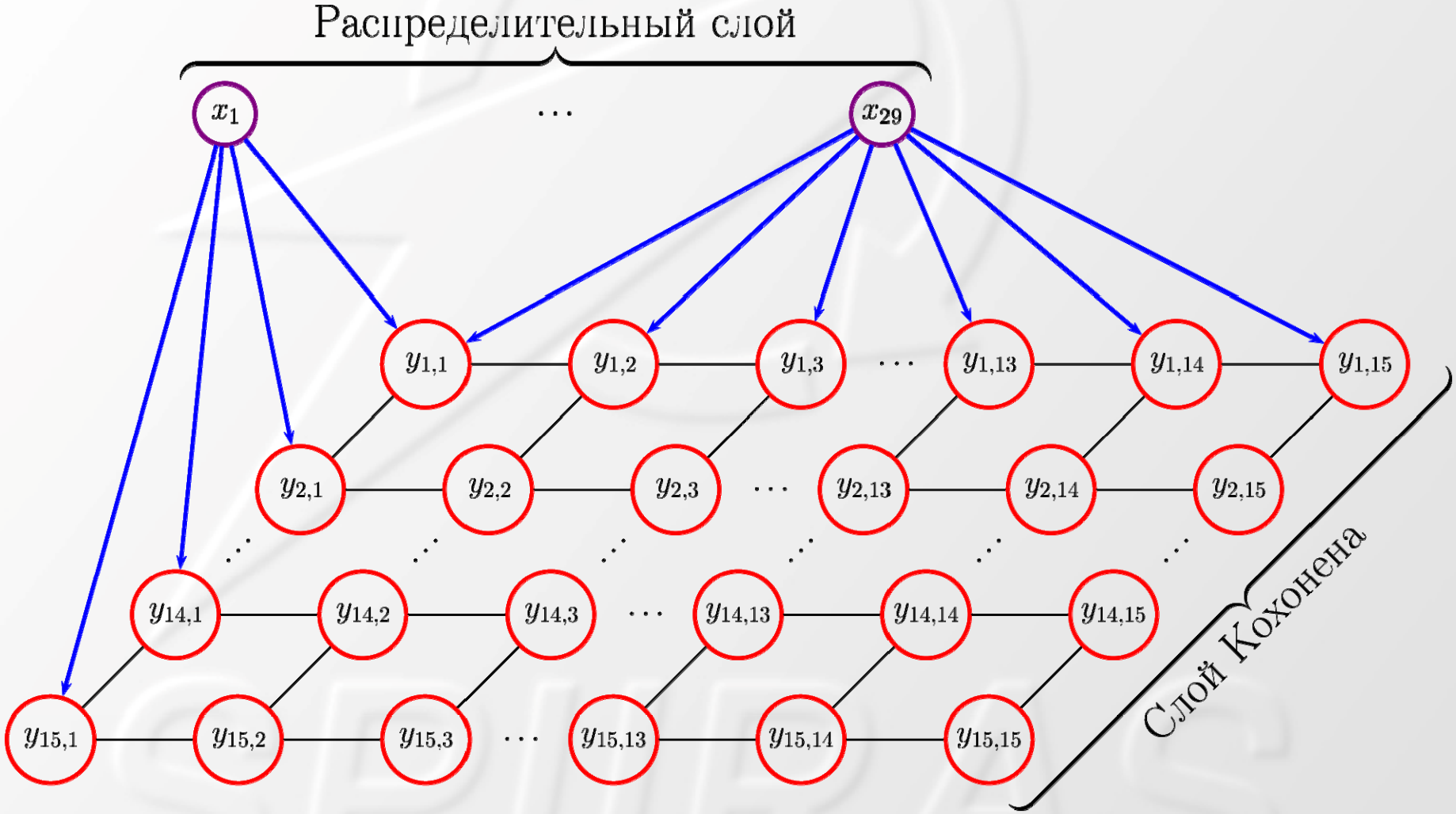
$$\forall i \in [1;29]\ x_i \in [0;1]$$

$$\varphi(x) = th(x) = \frac{e^x - e^{-x}}{e^x + e^{-x}}$$

Нейронные сети

- Трехслойные нейронные сети
- Симметричная функция активации
- Статическое обучение
  - Упругий алгоритм обратного распространения ошибки (RPROP)
  - Равнообъемные выборки положительного и отрицательного трафиков
- Параллельное исполнение

Иммунные клетки



Правило Кохонена: $w_{pq}(t+1) = w_{pq}(t) + \gamma \cdot \left(X - w_{pq}(t)\right)$

Иммунные клетки

- Самоорганизующиеся карты Кохонена
- Динамическое обучение
  - Конкурентное обучение
  - Модификация весовых параметров во время выполнения
  - Обновляемый набор обучающих данных
- Взаимодействие иммунных детекторов
- Отбор корректно обученных иммунных детекторов
- Параллельное исполнение

Схема гибридизации

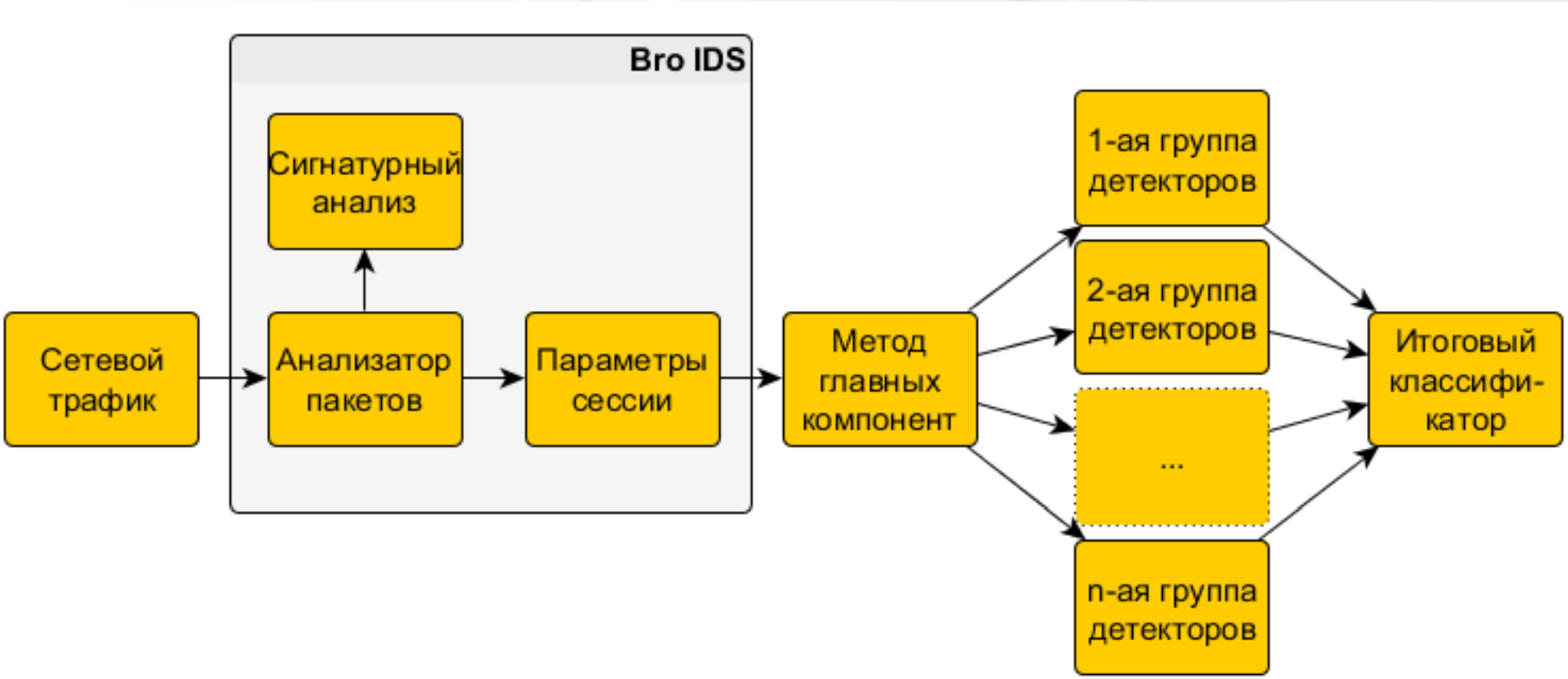


Схема гибридизации

- Анализатор пакетов перехватывает и обрабатывает пакеты, поступающие на сетевую карту
- С помощью дополнительных скриптов вычисляются параметры, необходимые для классификации сетевых соединений
- Параметры сессии сжимаются по методу главных компонент
- Детекторы параллельно обрабатывают набор параметров
- Каждая группа детекторов обучена для распознавания одного типа атак
- Конечный результат классификации выдается на основе процедуры голосования по большинству

Результаты вычислительных экспериментов

- Показатель ложных срабатываний

$$FP = \frac{n_{FP}}{n_{FP} + n_{TN}} \cdot 100\%$$

- Показатель обнаружения атак

$$TP = \frac{n_{TP}}{n_{TP} + n_{FN}} \cdot 100\%$$

- Показатель корректной классификации

$$CC = \frac{n_{CC}}{n} \cdot 100\%$$

Метод	KDD-99			NSL-KDD		
	FP	TP	CC	FP	TP	CC
Нейронные сети	3.56	99.95	73.56	7.08	99.24	56.86
Иммунные детекторы	2.26	91.16	94.82	12.51	93.06	65.65

Результаты вычислительных экспериментов (нейронные сети)

	back	neptune	pod	smurf	teardrop	ipsweep	nmap	portsweep	satan
back	99.17%	0%	0%	0%	1.2%	0.1%	0%	0%	7.24%
neptune	0.78%	99.99%	0%	0%	16.58%	0%	0.14%	99.98%	99.82%
pod	0%	0.49%	99.51%	0%	42.23%	1.46%	1.46%	0.49%	1.94%
smurf	0%	0%	1.33%	18.79%	14%	0.03%	4.22%	0%	98.54%
teardrop	0%	9.8%	61.22%	0%	99.89%	0%	0%	98.37%	0.11%
ipsweep	0%	0%	0.91%	0%	0.35%	98.74%	26.97%	3.3%	4.08%
nmap	0%	19.11%	0.9%	0%	0.13%	65.12%	98.65%	19.11%	21.62%
portsweep	0.08%	35.27%	0.08%	0%	8.14%	0.06%	0.08%	99.02%	74.49%
satan	0.02%	64.14%	0.1%	0%	0.34%	0.18%	3.96%	64.43%	98.33%
normal	0.5%	0.05%	0.02%	0%	0.17%	0.6%	1.72%	0.17%	1.07%

Результаты вычислительных экспериментов (иммунные клетки)

	back	neptune	pod	smurf	teardrop	ipsweep	nmap	portsweep	satan
back	58.67%	0%	0%	0%	0%	0%	0%	0%	0%
neptune	0%	94.51%	0%	0%	0%	0%	0%	0.01%	0%
pod	0%	0.48%	19.32%	0%	0%	0%	0%	0%	0%
smurf	0%	0%	0%	80%	0%	0%	0%	0%	0%
teardrop	0%	0%	0%	0.11%	88.78%	0%	0%	0%	0%
ipsweep	0%	0%	0%	0%	0.15%	71.12%	60.06%	0%	0%
nmap	0%	0%	0%	0%	0%	60.76%	62.03%	0%	0%
portsweep	0%	0%	0%	0%	0%	0%	0.24%	61.06%	0%
satan	0%	0%	0%	0.11%	0%	0%	0%	0%	77.59%
normal	6.77%	0%	0%	0.04%	0%	0%	0%	0.01%	0%

Заключение

Дальнейшая работа:

- Применение гибридных подходов на основе методов Data Mining
- Создание собственных наборов смоделированных данных для проведения экспериментов

Контактная информация

Браницкий Александр Александрович
(СПИИРАН)

branitskiy@comsec.spb.ru

Благодарности

Работа выполнена при финансовой поддержке РФФИ (13-01-00843, 14-07-00697, 14-07-00417, 15-07-07451), программы фундаментальных исследований ОНИТ РАН, проекта ENGENSEC программы Европейского Сообщества TEMPUS и Министерства образования и науки Российской Федерации (соглашение № 14.604.21.0033, уникальный идентификатор соглашения RFMEFI60414X0033; соглашение № 14.604.21.0137, уникальный идентификатор соглашения RFMEFI60414X0137; соглашение № 14.604.21.0147, уникальный идентификатор соглашения RFMEFI60414X0147).