УДК 621.396

# ОСОБЕННОСТИ НЕЙРОСЕТЕВОГО ПРОТИВОДЕЙСТВИЯ КИБЕРАТАКАМ

***© 2022 И. Я. Львович, Ю. П Преображенский, Е. Ружицкий***

*Воронежский институт высоких технологий (Воронеж, Россия)*
*Панъевропейский университет (Братислава, Словакия)*

*В статье обсуждаются некоторые особенности нейросетевого противодействия кибератакам. Представлена диаграмма декомпозиции нейросетевого распознавания кибератак*

*Ключевые слова: нейросетевая технология, информация, компьютерная сеть, кибератака.*

Для распознавания кибератак, как показывает анализ, весьма эффективным является применение нейросетевого моделирования (НСМ). Главная особенность состоит в том, что необходимо обосновать возможности применения нейросетевых моделей и методов, которые могут быть применимы к условиям включения в существующие ИС.

Условия являются следующими:

-допустимое время, необходимое для разработки;

-возможность найма специалистов;

-возможность иметь постоянный доступ к базам данных, содержащих существующие шаблоны атак, а также шаблонов корректного поведения, на основе которых будет построено обучение НСМ;

-описание особенностей системы контроля основных параметров ИС;

-указание максимально допустимого объема вычислительных ресурсов;

При успешном решении подобных вопросов появится возможность распознавать кибератаки в сети на практике, используя идентичность параметров трафика сети, с имеющимися в базе сигнатурами наиболее часто встречающихся сетевых кибератак.

Стоит учесть, что такие задачи как: фиксация основных параметров функционирования ИС, их предварительная фильтрация, организация сигналов о найденных кибератаках – уже решены, и не будут рассматриваться в данной работе.

Необходимо стремиться к использованию разработок в программно-аппаратном комплексе.

Отметим, что при решении задачи создаваемая оригинальная модель, будет необходима, в первую очередь, для формального определения причинно-следственных связей, неизбежно возникающих при распознавании кибератак на сети. Это поможет повысить уровень защиты ИС.

Также, в концепте модели учтены необходимые условия для функционирования НСМ опознавания кибератак на сетевые структуры, которые определяются характером взаимодействия соответствующих компонентов.

Следующий этап разработки концепта модели, учитывающий существующую технологию использования НСМ, характерен тем, что весь процесс распознавания кибернетических атак, обязан включать в себя учебные примеры и их параметры, выборку для обучения, должен быть определен вид и параметры НСМ, а также его использование с целью распознавания. На основе этого утверждения, построена диаграмма декомпозиции, которая представлена на рисунке 1.

Составляющие представленной диаграммы имеют следующее назначение:

− *Формирование параметров учебных примеров* – параметры входного и выходного типа, определяемые на все виды кибератак, а также способы их кодировки.

- *Формирование обучающей выборки* – количество примеров учебного характера, которые отвечают существующим эталонам кибератак. Их число, качественная состав-

Львович Игорь Яковлевич – Воронежский институт высоких технологий, доктор техн. н., профессор, e-mail: office@vivt.ru.
Преображенский Юрий Петрович – ВИВТ-АНОО ВО, профессор, e-mail: petrovich@vivt.ru.
Ружицкий Евгений – Панъевропейский университет, г. Братислава, Словакия, канд. техн. наук, доцент, e-mail: rush_evg_br53@yandex.ru.

ляющая, а также номенклатурная полнота, обязаны обеспечить обучение НСМ.

- *Определение вида и параметров НСМ* – использовать в работе тот вид НСМ, имеющий определенные параметры, позволяющие выполнить поставленные условия задачи во всей полноте при распознавании кибератак на определенную ИС.

- *Использование НСМ* – распознавание кибернетических атак, идущих на сетевые РИС. Здесь стоит отметить, что при использовании НСМ, на ИС возникает дополнительная нагрузка. Это может повлечь за собой выработку вычислительных ресурсов. На другом этапе создания концепта модели, разработаны схемы используемых компонентов НСС, которые представлены на рисунке 2. В ней показаны основные особенности при реализации НСС, которые присутствуют при распознавании кибернетических атак.


Рисунок 1. Диаграмма декомпозиции нейросетевого распознавания кибератак

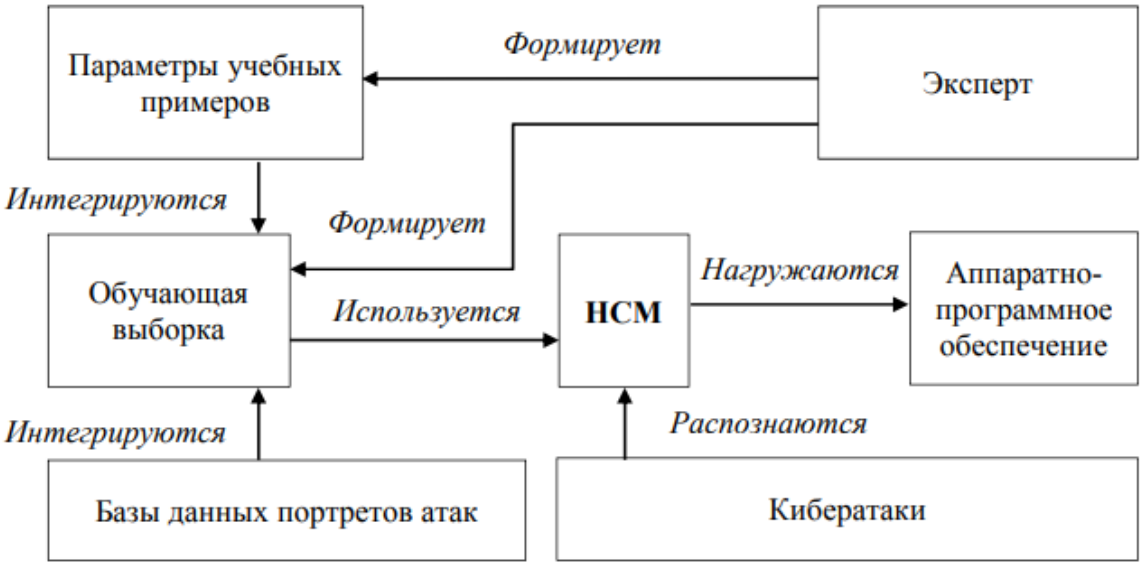

Рисунок 2. Схема взаимодействия компонентов НСС распознавания кибератак

В итоге отметим, что при разработке учтено:

1. недостаточная проработка методов, формирующих параметры примеров для обучения НСМ;
2. большой период, в течение которого формируется обучающая выборка для НСМ, если ограничен доступ к базам данных, которые содержат портреты кибернетических атак;
3. сложный доступ к действующим базам данных портеров кибернетических атак;
4. возникновение дополнительной нагрузки на аппаратно-программном обеспечении ИС, при работе НСМ.

Учитывая все это, в данной схеме возможно создание параметров, определяющих примеры обучения, и учебной выборки, используя экспертные данные.

Анализируя данные, которые представлены на рисунке 1 и рисунке 2, можно сделать вывод о том, что эффективность распознавания кибернетических атак зависит от нескольких факторов, представленных на рисунке 3.

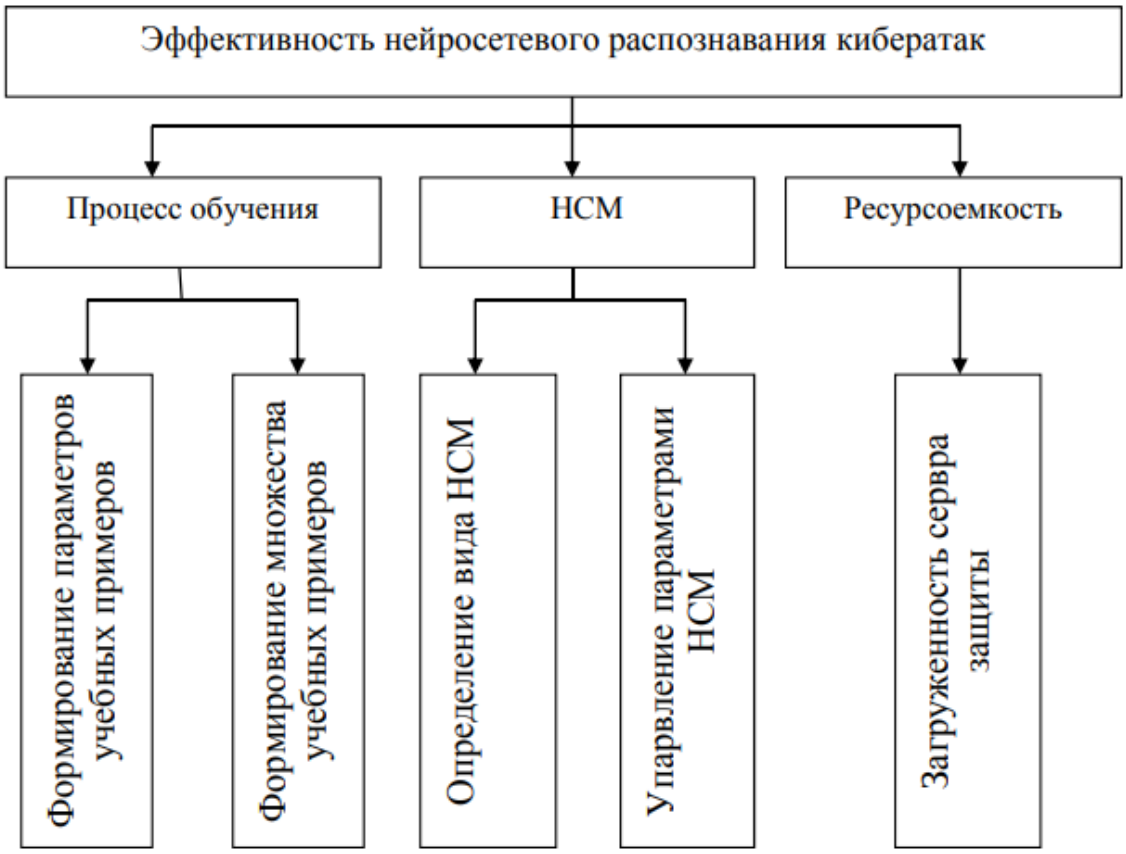


Рисунок 3. Факторы, которые влияют на эффективность распознавания

Также, можно сделать вывод, что оценку эффективности распознавания необходимо проводить как с позиции эффективного протекания процесса при использовании НСМ, так и с позиции его эффективного обучения.

Показатели, отвечающие за эффективность, обязаны показывать длину по времени, объем ресурсов и точность указанных названных процессов.

**ЛИТЕРАТУРА**

1. Диденко С. С. Применение мультиагентных технологий в контекстно-ориентированной среде компонента умного дома / С. С. Диденко // Моделирование, оптимизация и информационные технологии. – 2021. – Т. 9. – № 2 (33). – С. 18-19.

2. Lvovich I. Ya. Modeling of information processing in the internet of things at agricultural enterprises / I. Ya. Lvovich, Ya. E. Lvo-

vich, A. P. Preobrazhenskiy, Yu. P. Preobrazhenskiy, O. N. Choporov // IOP Conference Series: Earth and Environmental Science. Krasnoyarsk Science and Technology City Hall of the Russian Union of Scientific and Engineering Associations. – 2019. – С. 32029.

3. Машков В. Г. Предварительная оценка вероятности принятия правильного решения в автоматизированных системах управления / В. Г. Машков, В. А. Малышев, Ю. В. Никитенко // Моделирование, оптимизация и информационные технологии. – 2021. – Т. 9. – № 3 (34). – С. 12-13.

4. Lvovich I. Optimization of the subsystem for the movement of electronic documents in educational organization / I. Lvovich, A. Preobrazhenskiy, Y. Preobrazhenskiy, Y. Lvovich, O. Choporov // Proceedings – 2021 1st International Conference on Technology Enhanced Learning in Higher Education, TELE 2021. – 1. – 2021. – С. 328-332.

5. Борзова А. С. Особенности построения системы принятия решений при многовариантной оптимизации структуры цифрового управления логистическим процессом в организационной системе на основе имитационного моделирования / А. С. Борзова, В. В. Муха // Моделирование, оптимизация и информационные технологии. – 2021. – Т. 9. – № 3 (34). – С. 15-16.

6.Львович Я. Е. Исследование характеристик защищенности мобильных сенсорных сетей / Я. Е. Львович, И. Я. Львович, А. П. Преображенский, Ю. П. Преображенский, О. Н. Чопоров // Радиолокация, навигация, связь. Сборник трудов XXV Международной научно-технической конференции, посвященной 160-летию со дня рождения А. С. Попова. В 6-ти томах. – 2019. – С. 239-244.

7. Печенкин В. В. Моделирование динамики серверной нагрузки стохастическими сетями петри с приоритетами (на примере системы видеоконференцсвязи) / В. В Печенкин, А. Т. Х. Аль-Хазраджи, С. С. Гельбух // Моделирование, оптимизация и информационные технологии. – 2021. – Т. 9. – № 1 (32). – С. 10-11.

8. Lvovich I. Managing developing internet of things systems based on models and algorithms of multi-alternative aggregation / I. Lvovich, A. Preobrazhenskiy, Y. Preobrazhenskiy, Y. Lvovich, O. Choporov // 2019 International Seminar on Electron Devices Design and Production, SED 2019 – Proceedings. – 2019. – С. 8798413.

9. Новосадов К. С. Анализ спектрально эффективных схем модуляции, применяемых в высокоскоростных системах радиосвязи / К. С. Новосадов // Моделирование, оптимизация и информационные технологии. – 2021. – Т. 9. – № 1 (32). – С. 20-21.

10. Lvovich I. Ya. Modelling of information systems with increased efficiency with application of optimization-expert evaluation / I. Ya. Lvovich, Ya. E. Lvovich, A. P. Preobrazhenskiy, Yu. P. Preobrazhenskiy, O. N. Choporov // Journal of Physics: Conference Series. International Scientific Conference "Conference on Applied Physics, Information Technologies and Engineering - APITECH-2019". Krasnoyarsk Science and Technology City Hall of the Russian Union of Scientific and Engineering Associations; Polytechnical Institute of Siberian Federal University. – 2019. – С. 33079.

## THE FEATURES OF THE NEURAL NETWORK COUNTERACTION TO CYBER ATTACKS

***© 2022 I. Ya. Lvovich, Yu. P. Preobrazhensky, E. Ruzhitsky***

*Voronezh Institute of High Technologies (Voronezh, Russia)*
*Pan-European University (Bratislava, Slovakia)*

*The paper discusses some features of neural network counteraction to cyberattacks. A decomposition diagram of neural network recognition of cyberattacks is presented.*

*Keywords: neural network technology, information, computer network, cyberattack.*