ТЕХНОЛОГІЇ ЗАХИСТУ КОМП'ЮТЕРНИХ СИСТЕМ І МЕРЕЖ

УДК 004.056.5:004

Бапиев И.
докторант Казахского национального технического университета им. К.И. Сатпаева, Казахстан, г. Алма-Ата

Корченко А. Г.
доктор технических наук, заведующий кафедрой безопасности информационных технологий Национального авиационного университета, Украина, г. Киев

Терейковский И. А.
доктор технических наук, профессор кафедры системного программирования и специализированных компьютерных систем Национального технического университета Украины «КПИ им. И. Сикорского», Украина, г. Киев

Терейковская Л. А.
кандидат технических наук, ассистент кафедры информационных систем Киевского национального университета строительства и архитектуры, г. Киев

КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ И ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ЭФФЕКТИВНОСТИ НЕЙРОСЕТЕВОГО РАСПОЗНАВАНИЯ КИБЕРАТАК

Аннотация *Статья посвящена развитию методологической базы использования нейронных сетей для распознавания кибератак. Предложена концептуальная модель, позволяющая определить перспективные направления дальнейших исследований для создания эффективных нейросетевых систем распознавания кибератак. Также предложен ряд новых принципов использования нейронных сетей для распознавания кибератак, применение которых обеспечивают возможность повышения эффективности нейросетевых моделей.*

Ключевые слова: Нейронная сеть, кибератака, модель, эффективность, концепция

Введение

В современных условиях одним из самих перспективных направлений повышения эффективности распознавания кибератак на сетевые ресурсы информационных систем (РИС) является применение интеллектуальных методов, базирующихся на использовании нейросетевых моделей (НСМ) [1, 5]. Перспективность указанного направления подтверждается как известными удачными случаями использовании НСМ в системах распознавания кибератак (СРК) (продукция компании Cisco), так и большим количеством соответствующих теоретико-практических исследований, анализ которых достаточно глубоко проведен в [1, 5, 9, 15]. Вместе с тем большое количество неправильных срабатываний, значительный срок разработки, нестабильность обучения, требовательность к объему и качеству обучающей выборки, недостаточная адаптация ко многим особенностям современных ИС, связанная в первую очередь с методологическими недостатками, значительно снижают эффективность нейросетевых систем распознавания (НСР), что и предопределяет актуальность исследований в этом направлении

Анализ литературных данных и формулировка проблемы

Отметим, что в общем случае в соответствии с [4, 7, 12] под понятием кибератака понимают реализацию в киберпространстве угроз безопасности его компонент (а именно конфиденциальности, целостности и доступности) с учетом их уязвимостей. В ракурсе проблематики данной статьи рассматриваются те кибератаки, которые реализуются только с использованием параметров сетевого трафика и учитывают уязвимости только сетевых ресурсов информационных систем. Целью таких кибератак является нарушение правильности сетевых функциональных характеристик атакуемых ресурсов. Характерными примерами таких кибератак являются DOS и DDOS-атаки.

Анализ научно-практических работ, посвященных усовершенствованию СРК позволяет утверждать, что в этих системах НСМ используются для распознавания кибератак на основании обобщения статистических данных, которые отображаются в обучающей выборке [2, 3, 8, 13]. Кроме этого, можно сформулировать вывод о том, что большая часть соответствующих исследований направлена на адаптацию архитектуры НСМ к условиям практической задачи. Так в работе [9] разработан метод оптимизации вида архитектуры НМ, в зависимости от особенностей поставленной задачи распознавания. В работах [3, 9, 10] рассмотрены особенности применения НСМ для распознавания попыток подбора парольных данных и распознавания DDOS-атак. Работа [14] посвящена решению задачи усовершенствования структуры та алгоритма обучения многослойного персептрона,

предназначенного для использования в СРК. Еще одним распространенным направлением исследований является разработка способов использования в СРК новых малоапробированных видов НСМ. Например, работа [2] посвящена средствам распознавания на базе кибернейрона, а в роботе [16] предлагается использовать карту Кохонена, функционирующую в соответствии с принципами искусственных иммунных систем. Вместе с тем, итоговый анализ результатов этих работ указывает на то, что одной из основных причин их низкой эффективности является недостаточная развитость методологической базы обеспечения эффективного использования нейронных сетей для распознавания кибератак на сетевые РИС.

Цель и задачи исследования

В соответствии с общей проблематикой исследований в области нейросетевых систем распознавания кибератак и результатом проведенного анализа литературных данных в этом направлении, основной целью исследований является развитие методологической базы обеспечения эффективного использования нейронных сетей для распознавания кибератак на сетевые РИС. На первом этапе исследований для достижения заявленной цели предлагается решить задачи:

- разработки концептуальной модели использования нейронных сетей для распознавания кибератак;
- разработки принципов эффективного использования нейронных сетей для распознавания кибератак

Разработка концептуальная модель и принципов обеспечения эффективности нейросетевого распознавания кибератак

Результаты исследований [1, 12, 17] указывают на то, что важным направлением развития СРК на сетевые РИС является внедрение в них НСР распознавания кибератак. Для этого необходимо решить научное задание нейросетевого распознавания кибератак, на основании анализа подконтрольных на эксплуатации параметров функционирования ИС. Особенностью сформулированного задания является необходимость теоретического обоснования характеристик нейросетевых моделей и методов, адаптированных к условиям внедрения в современные СРК. К указанным условиям относятся допустимый срок разработки, возможность привлечения трудовых ресурсов, наличие доступа к базам данных шаблонов атак и шаблонов нормального поведения, необходимых для обучения НСМ, особенности системы контроля функциональных параметров ИС и допустимый объем вычислительных ресурсов, которые потребляет СРК.

Решение данного научного задания позволит развязать такие практические задачи, как определение кибератак на сетевые РИС на

основании схожести подконтрольных функциональных параметров от шаблонов нормального поведения, так и на схожести с шаблонами атак. При этом задачи фиксации параметров функционирования ИС, предварительной фильтрации таких параметров, а также сигнализации о выявленных кибертаках считаются решенными и в данной работе не рассматриваются.

В соответствии с рекомендациями [12, 15], отправным пунктом решения сформулированного задания должна быть разработка концептуальной модели обеспечения эффективности нейросетевого распознавания кибератак на сетевые РИС.

В общем случае концептуальная модель представляет собой модель предметной области, которая состоит из перечня взаимосвязанных понятий, которые используются для описания этой области вместе с свойствами и характеристиками, классификацией этих понятий за типами, ситуациями, признаками в этой области. а также законов реализации в них процессов [15]. Другими словами концептуальная модель является отображением концепции, под понятием которой понимают определенный способ суждения, трактовки некоторых событий, основную точку зрения, управляющую идею для их систематического освещения. Следует отметить, что на сегодня разработка концептуальной модели является общепринятым отправным пунктом формализации поставленной научно-практической задачи, а также отправным пунктом развития методологической базы, которая в свою очередь представляет собой систему принципов (способов) организации построения теоретической и практической деятельности, а также знаний о этой системе.

В связи с тем, что ожидаемый практический результат данного научного исследования предусматривает создание программно-аппаратного комплекса, то для определения эффективности процесса нейросетевого распознавания кибератак на сетевые РИС, предусмотрено использовать терминологию в области защиты информации, компьютерной и программной инженерии.

В соответствии с международными стандартами в этой области, эффективность это множество атрибутов, которые определяют взаимосвязь уровней исполнения программной системы, использование ресурсов (средства, аппаратура, материалы и др.) и услуг, которые выполняются штатным обслуживающим персоналом и др. К характеристикам эффективности программной системы относятся:

– Оперативность – атрибут, который указывает на время отклика, обработки и выполнении функций.

– Ресурсоемкость – атрибут, который определяет количество использованных ресурсов и продолжительность такого использования при выполнении функций программной системы.

– Согласованность – атрибут, который указывает на соответствие данного атрибута заданным стандартам, правилам и предписаниям.

В соответствии указанным определениям, на первом этапе создания концептуальной модели было проведено гармонизацию терминологии, которая используется в области использования НМ для распознавания кибератак на сетевые РИС. Гармонизация проведена с позиций отображения современного состояния науки и практики, а также с точки зрения поддержки процесса решения поставленных задач.

В результате определены следующие термины:

– Кибератака – реализация в кибернетическом пространстве угроз безопасности его компонентов (а именно конфиденциальности, целостности и доступности) с учетом их уязвимостей [4, 7].

– Кибернетическое пространство – виртуальное пространство, полученное в результате взаимодействия пользователей, программного и аппаратного обеспечения, сетевых технологий для поддержки и управления процессами преобразования информации с целью обеспечения информационных потребностей общества [4, 7].

– РИС – отдельный программный или аппаратный компонент, обеспечивающий функционирование ИС [6, 12].

– Сетевой РИС – РИС, который используется для обеспечения сетевых функций ИС [15].

– Совокупность функциональных параметров – зарегистрированное в определенный интервал времени множество функциональных параметров РИС.

– Портрет (сигнатура) кибератаки – сигнатура функциональных параметров при реализации определенного вида кибератаки [6].

– НС – сеть, состоящая из искусственных нейронов, объединенных между собою синаптическими (взвешенными) связями [13].

– Искусственный нейрон – простейший вычислительный процессор, преобразовывающий множество входных сигналов в выходной сигнал. При этом сигналы имеют дискретный числовой характер.

– НСМ – модель НС, которая характеризуется методом обучения, способом распространения сигнала, структурой связей и типом искусственного нейрона. Указанные параметры и их комбинации определяют вид НСМ [13, 15]. Синонимом понятия вида НСМ есть архитектура НС. Производными от термина НСМ являются нейросетевые методы, НСС и НСР, т. е. это методы, системы и средства, которые базуются на НС. Поскольку в общем случае под понятием средство понимают снаряжение (предмет, приспособление, совокупность приспособлений) необходимое для

выполнения определенной функции, то в данной статье понятие НСР является обобщающим для НСМ и НСС, которые используются для распознавания кибератак на сетевые РИС. Аппаратно-программную реализацию таких приспособлений будем называть инструментальным НСР.

Также определено, что в контексте задачи данного исследования концептуальная модель, прежде всего, предназначена для формализации причинно-следственных связей, которые свойственны процессу распознавания кибератак на сетевые РИС, определенных необходимостью повышения уровня защищенности современных ИС. Кроме этого, в концептуальной модели учтено:

– Условия функционирования НСР распознавания кибератак на сетевые РИС, определяемые характером взаимодействия отдельных частей СРК и компонентами ИС.

– Необходимость реализации эффективного использования НСМ для распознавания кибератак и основные направления улучшения его функционирования.

– Возможность управления НСР и определение его настраиваемых переменных.

Поэтому на следующем этапе построения концептуальной модели была разработана контекстная диаграмма процесса нейросетевого распознавания кибератак на сетевые РИС, которая отображает его основную функцию и взаимодействие с внешней средой (см. рис. 1).

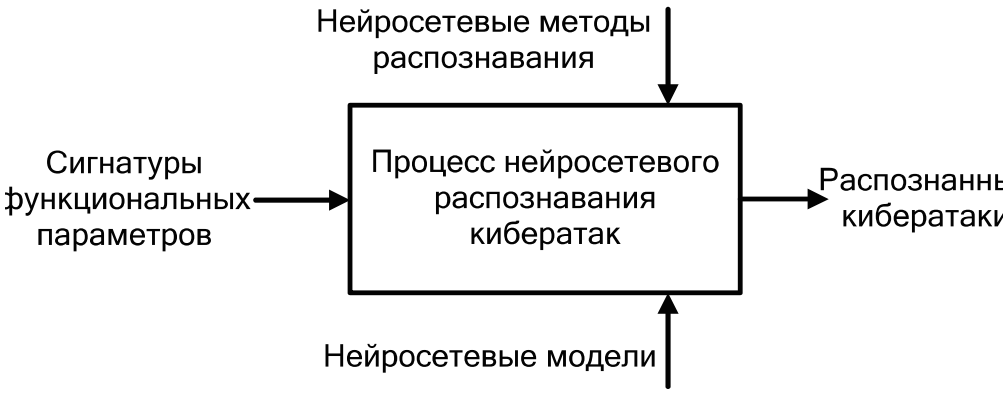

Рис. 1. Контекстная диаграмма процесса нейросетевого распознавания кибератак

Следует отметить, что в построенной диаграмме процесс распознавания реализуется с помощью НСМ, кторые применяются соответственно решений, определенных в нейросетевых решениях. Учитывая общепринятую технологию использования НСМ для решения практических задач, можно утверждать, что процесс нейросетевого распознавания кибератак на сетевые

РИС должен состоять из следующих этапов:

– Формирование параметров учебных примеров.
– Формирование обучающей выборки.
– Определение вида и параметров НСМ.
– Использование НСМ для распознавания.

Использование данного утверждения позволило построить, показанную на рис. 2, диаграмму декомпозиции нейросетевого распознавания кибератак на сетевые РИС.

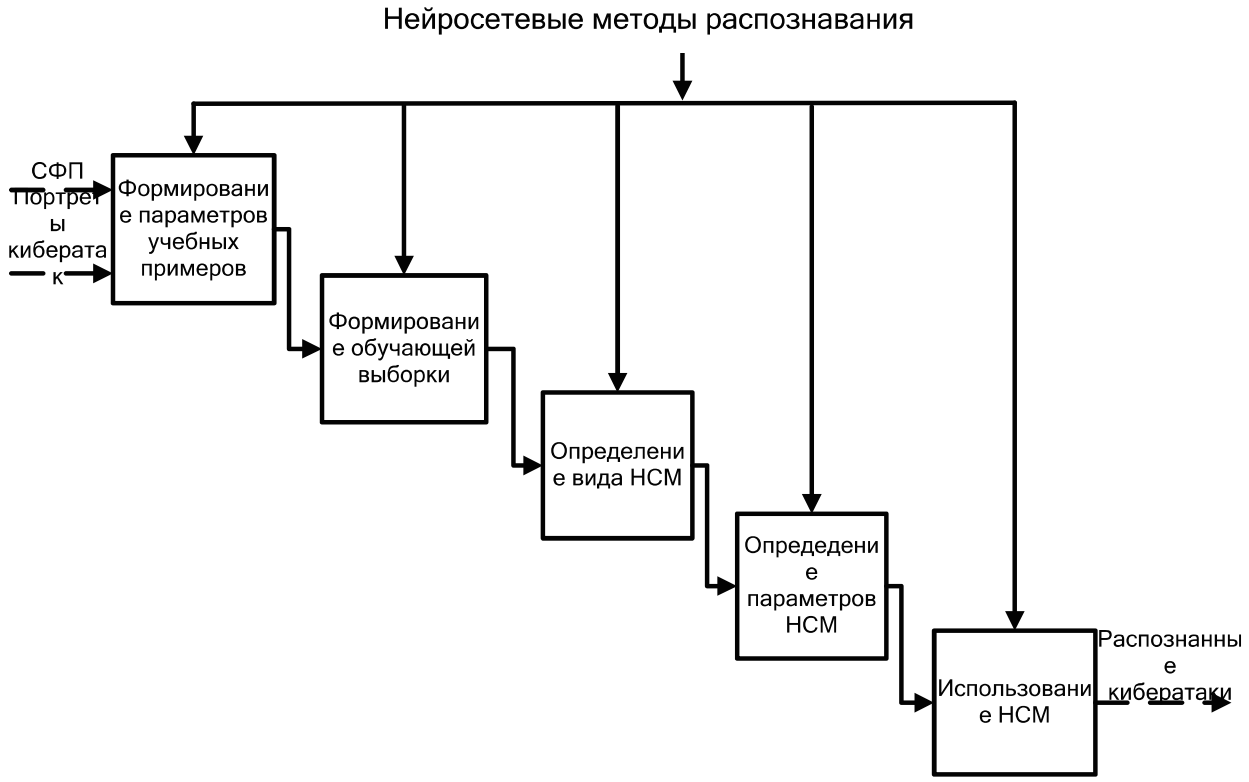

Рис. 2. Диаграмма декомпозиции нейросетевого распознавания кибератак

Назначение составляющих данной диаграммы состоит в следующем:

– Формирование параметров учебных примеров – определение для каждого типа кибератак множества входных и выходных параметров и способа их кодирования к виду, приспособленному для использования в НСМ.

– Формирование обучающей выборки – определение такого множества учебных примеров, которое отвечает эталонам кибератак. Количество, качество и номенклатура примеров должны быть достаточными для обучения НСМ.

– Определение вида и параметров НСМ – определение для использования такого вида НСМ, с такими параметрами, которые наиболее полно отвечают условиям задачи распознавания кибератак на сетевые ресурсы конкретной ИС.

– Использование НСМ – распознавание кибератак на сетевые РИС. Следует учесть, что использование НСМ влечет за собой дополнительную нагрузку на ИС, что может вызвать исчерпание вычислительных ресурсов.

Следующим этапом создания концептуальной модели стала разработка показанной на рис. 3, схемы компонентов НСС распознавания кибератак. В схеме учтены особенности реализации НСС, предназначенных для распознавания кибератак на сетевые РИС и результаты анализа литературных данных, которые касаются недостатков известных НСР для распознавания кибератак на сетевые РИС. Таким образом, в процессе разработки учтено:

– Несовершенство методов формирования параметров обучающих примеров для НСМ предназначенных для распознавания кибератак на сетевые РИС.

– Длительный период формирования обучающей выборки для НСМ в случае ограниченного доступа к базам данных портретов кибератак.

– Сложность доступа к существующим базам данных портеров кибератак.

– Дополнительную нагрузку на аппаратно-программное обеспечение ИС за счет функционирования НСР.

Поэтому в схеме предусмотрена возможность формирования параметров обучающих примеров и учебной выборки с помощью экспертных данных.

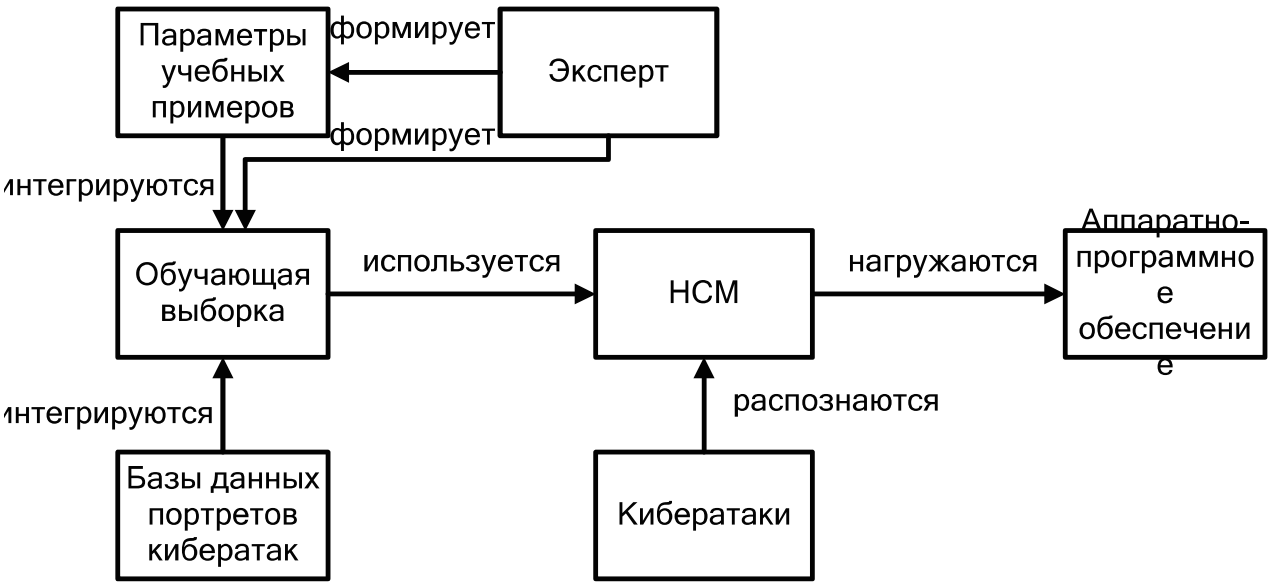

Рис. 3. Схема взаимодействия компонентов НСС распознавания кибератак на сетевые РИС

Анализ данных, показанных на рис. 2 и рис. 3 позволяет утверждать, что на эффективность нейросетевого распознавания фонем кибератак на сетевые РИС влияют ряд факторов, показанных на рис. 4. Кроме этого, возможно

утверждать, что эффективность нейросетевого распознавания целесообразно оценивать как с точки зрения эффективности процесса использования НСР, так и с точки зрения эффективности процесса обучения НСМ. При этом показатели эффективности должны отображать длительность, ресурсоемкость и точность названных процессов.

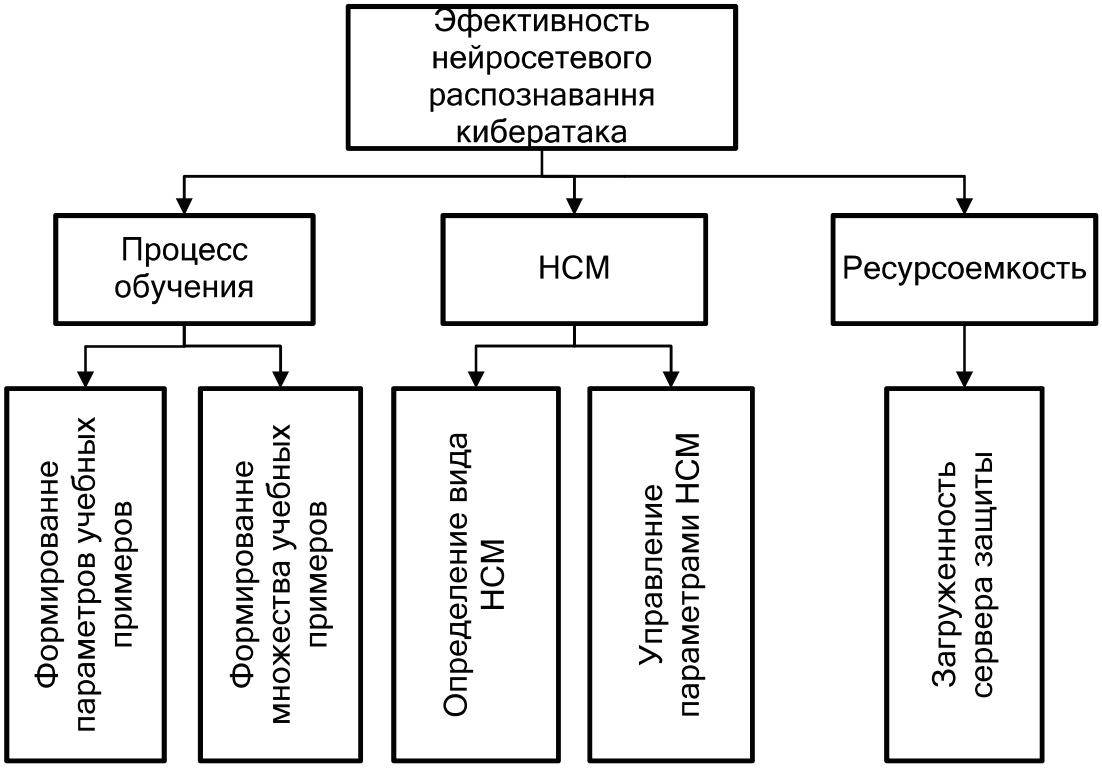

Рис. 4. Факторы влияющие на эффективность распознавания

Таким образом, обоснованы показанные на рис. 5, показатели оценки эффективности нейросетевого распознавания кибератак на сетевые РИС.

В результате определено, что в аналитическом виде концептуальную модель обеспечения эффективности процесса нейросетевого распознавания кибератак на сетевые РИС возможно отобразить с помощью выражений:

$$E_{\Sigma} = f(E_{HCP}, E_{OB}), \quad (1)$$

$$E_{HCP} = f(e_1, e_2, e_3), \quad (2)$$

$$E_{OB} = f(e_4, e_5), \quad (3)$$

где E_{Σ} – интегральная эффективность процесса, E_{HCP} – эффективность создания и использования НСР, E_{OB} – эффективность создания обучающей выборки, e_1 – определение эффективных видов НСМ, e_2 – определение параметров НСМ, e_3 – ресурсоемкость использования НСР, e_4 – определение параметров обучающих примеров, e_5 – формирование обучающей выборки.

Анализ разработанной концептуальной модели позволяет утверждать,

что для эффективного использования НСМ для распознавания кибератак на сетевые РИС необходимо дополнить существующую методологическую базу рядом принципов: допустимости использования вида НСМ, определения множества эффективных видов НСМ, оценивания эффективности вида НСМ, определения ожидаемого выходного сигнала для портретов кибератак, прогнозированного использования НСС распознавания кибератак вычислительных ресурсов сервера, обеспечивающего систему защиты, оценки эффективности НСР и использования экспертных знаний для формирования обучающей выборки.

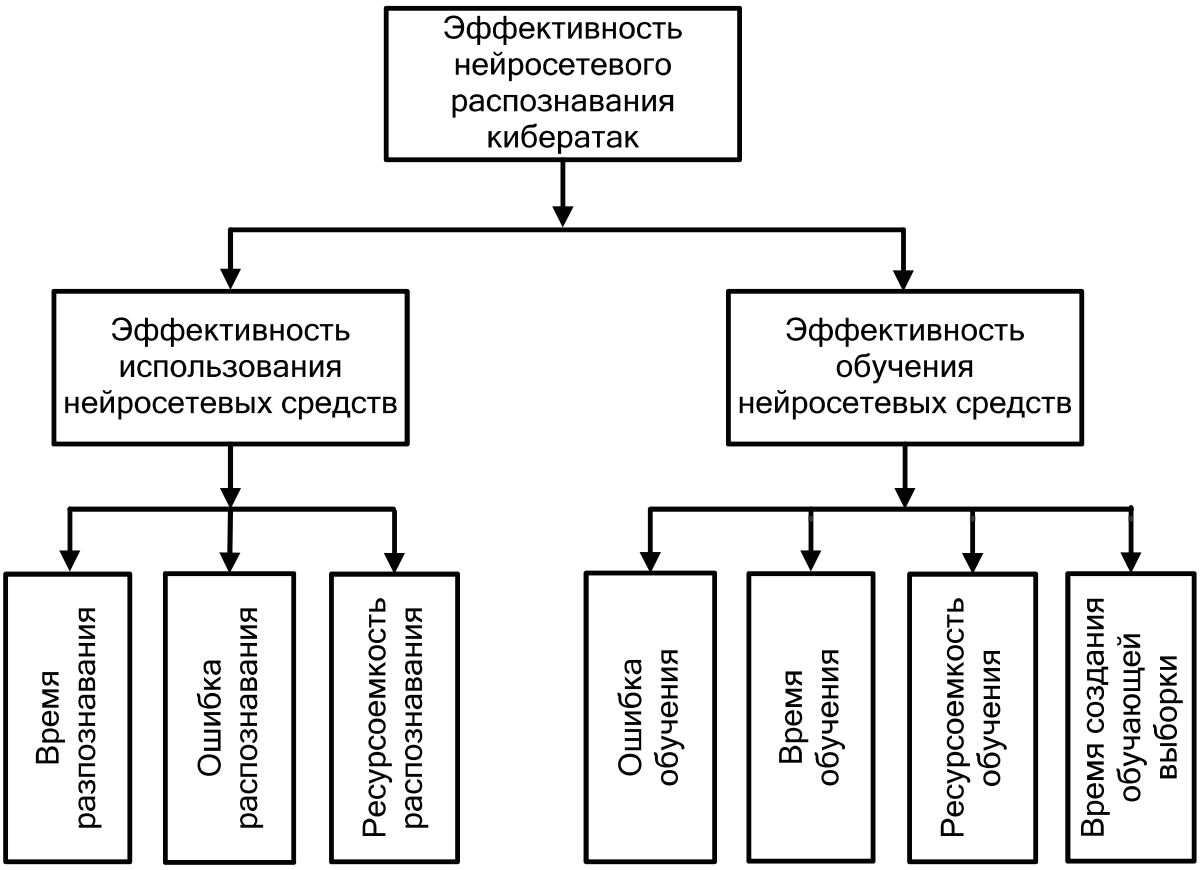

Рис. 5. Показатели оценки эффективности нейросетевого распознавания

Принцип допустимости использования вида НСМ для распознавания кибератак на сетевые РИС. Как показывают результаты 13, 15], основным фактором, который влияет на формирование множества допустимых видов НСМ, которые используются для распознавания кибератак та сетевые РИС является обеспечение эффективного обучения НСМ. Для этого необходимо за допустимое время выполнить набор следующих процедур: определить множество входных и выходных параметров НСМ, провести кодирование указанных входных и выходных параметров, создать обучающую выборку, реализовать процесс обучения. Выполнение первой

процедуры реализуется на подготовительном этапе разработки НСР. Поэтому основное внимание акцентировано на выполнении второй и третьей процедуры. При этом приемлемый срок создания обучающей выборки и обучения НСМ определяется на основании требований к созданию ИС. Следовательно:

$$t_{\Sigma} \le t_d, \tag{4}$$

где t_{Σ} – общий срок обучения НСМ распознавания кибератак на сетевые РИС, t_d – приемлемый срок создания НСР распознавания кибератак.

Таким образом, принцип допустимости использования *i*-го вида НСМ для распознавания кибератак на сетевые РИС можно задать с помощью такого правила:

$$If \;\; t_{\Sigma}(net_i) \le t_d \rightarrow net_i \in \boldsymbol{Net_d}, \tag{5}$$

где net_i – *i*-ый вид НСМ; $\boldsymbol{Net_d}$ – множество допустимых видов НСМ.

Принцип определения множества эффективных видов НСМ для распознавания кибератак на сетевые РИС. В соответствии с выводами [13, 15] для определения множества видов НСМ, которые обеспечат эффективное распознавание кибератак на сетевые РИС, предлагается использовать процедуру вида:

$$\boldsymbol{Net_a} \rightarrow \boldsymbol{Net_d} \rightarrow \boldsymbol{Net_e}, \tag{6}$$

где $\boldsymbol{Net_a}$ – множество доступных видов НСМ, $\boldsymbol{Net_d}$ – множество допустимых видов НСМ, $\boldsymbol{Net_e}$ – множество эффективных видов НСМ.

Принцип оценивания эффективности вида НСМ, предназначенной для распознавания кибератак на сетевые РИС. По аналогии с [15] будем считать, что среди множества допустимых, *i*-ый вид НСМ является наиболее эффективным, если для него функция эффективности примет максимальное значение:

$$\max_{V_i} = \{ V_1, V_2, .. V_I \}, \tag{7}$$

где I – количество видов НСМ, V_i – функция эффективности *i*-го вида НСМ.

Расчет функции эффективности выполняется так:

$$V_i = \sum_{k=1}^{K} \alpha_k R_k(net_i), \quad net_i \in \boldsymbol{Net_d}, \; i = 1,...I. \tag{8}$$

где $\alpha_k = [0..1]$ – весовой коэффициент *k*–го критерия эффективности; net_i – *i*-ий вид НСМ, $\boldsymbol{Net_d}$ – множество допустимых видов НСМ, K – количество критериев эффективности, $R_k(net_i)$ – значение *k*-го критерия для НСМ *i*-го вида.

В соответствии с результатами [13, 15], критерии выбора наиболее

эффективного вида НСМ должен отображать меру его приспособленности к условиям поставленной прикладной задачи. Таким образом, под *k*-ым критерием определения наиблее эффективного вида НСМ буд понимать меру обеспечения в НСМ *k*-ого требования задачи распознавания кибератак на сетевые РИС. В качестве одного из примеров такого критерия можно назвать меру обеспечения в НСМ требования к интерпретации результатов распознавания за пределами обучающей выборки..

Принцип определения ожидаемого выходного сигнала НСМ для портретов кибератак. Значение выходного сигнала должно отображать схожесть обучающих примеров. В противоположном случае обучение НСМ может существенно ухудшиться. Поэтому выходной сигнал для портретов кибератак предлагается описать выражением:

$$\boldsymbol{Y_Ф} = f(\boldsymbol{d}_Ф), \tag{9}$$

где $\boldsymbol{Y_Ф}$ – ожидаемые выходные сигналы НСМ для портретов кибератак вида $\boldsymbol{Ф}$, $\boldsymbol{d}_Ф$ – множество мер схожести между компонентами $\boldsymbol{Ф}$.

Поскольку предусмотрено распознавать кибератаки на основании анализа соответствующих характеристик РИС, то предлагается, что бы близость этих характеристик отображалась в мере схожести кибератак между собой.

Принцип прогнозирования использования НСР для распознавания кибератак вычислительных ресурсов сервера системы защиты. В соответствии с результатами п. 1.4 нагрузка на сервер защиты из-за использования НСР распознавания кибератак непосредственно зависит от объема сетевого трафика к защищаемому сетевому РИС. В соответствии с [11], в первом приближении можно принять, что указанный объем можно определить на основании является экспертных оценок. В дальнейшем можно исследовать возможность прогнозирования с помощью вейвлет-модели изменения количества обращений к РИС во времени:

$$Q_{сз} = f(W), \tag{2.10}$$

где $Q_{сз}$ – нагрузка сервера защиты, W – вейвлет-модель изменения количества обращений к серверу.

Принцип оценки эффективности НСР распознавания кибератак. По аналогии с [15], предлагается оценивать эффективность НСР на основании множества параметров, которые определяют степень обеспеченности выполнения в них процедур, которые считаются необходимыми для эффективного распознавания кибератак на сетевые РИС:

$$E_{НСР} = f(\boldsymbol{П}), \tag{11}$$

где $E_{НСР}$ – эффективность НСР, $\boldsymbol{П}$ – множество предложенных параметров.

Принцип использования экспертных знаний для формирования обучающей выборки. По аналогии с [6, 11] данный принцип предусматривает, что обучающие примеры возможно формировать на основании экспертных знаний касательно кибератак в виде продукционных правил вида:

$$If\ x_1 \in \left[X_1^{\min}, X_1^{\max}\right]_l \wedge \ldots x_k \notin \left[X_k^{\min}, X_k^{\max}\right]_l \ldots \wedge x_K \in \left[X_K^{\min}, X_K^{\max}\right]_l \rightarrow Y, \quad (12)$$

где $x_1,\ldots x_K$ – параметры идентифицирующие кибератаку, $\left[X_1^{min}, X_1^{max}\right],\ldots,\left[X_K^{min}, X_K^{max}\right]$ – заданные диапазоны $x_1,\ldots x_K$, K – количество идентифицирующих параметров, Y – результат продукционного правила (ожидаемая кибератака).

Перспективы дальнейших исследований

Разработанная концептуальная модель и сформулированные принципы обеспечения эффективности нейросетевого распознавания кибератак могут послужить основой для создания моделей процессов использования НСМ для распознавания кибератак, которые в последствии должны стать базой для создания метода создания обучающей выборки НСМ и метода использования НСР для распознавания кибератак на сетевые РИС.

Выводы

– Получила дальнейшее развитие концептуальная модель, которая за счет конкретизации параметров оценивания и факторов, влияющих на эффективность процесса нейросетевого распознавания кибератак, позволила детализировать направления дальнейших исследований.

– Получили дальнейшее развитие принципы использования нейронных сетей для распознавания кибератак, которые за счет учета степени обеспечения нейросетевой моделью характеристик поставленной задачи, соотнесения ожидаемых выходных сигналов нейросетевой модели с схожестью кибератак между собой, применения теории вейвлет-преобразований для прогнозирования количетсва запросов к серверу и использования продукционных правил при формировании учебных примеров, обеспечивают возможность повышения эффективности нейросетевых моделей.

Список литературы

1. *Абрамов Е. С. Разработка и исследование методов построения систем обнаружения атак: дис. ... канд. техн. наук: 05.13.19 / Абрамов Е. С. – Таганрог, 2005. – 199 с.*

2. *Артеменко А.В., Головко В. А. Анализ нейросетевых методов распознавания компьютерных вирусов /Материалы секционных заседаний. Молодежный инновационный форум «ИНТРИ» – 2010. — Минск: ГУ «БелИСА», 2010. – 239 с.*

3. *Большев А. К. Алгоритмы преобразования и классификации трафика для обнаружения вторжений в компьютерные сети: авторефер. дисс. на соискание научн. степени канд. техн. наук : спец. 05.13.19 – Методы и системы защиты информации, информационная безопасность / А. К. Большев – Санкт-Петербург, 2011. – 36 с.*

4. *Бурячок В.П. Завдання, форми та способи ведення воєн у кібернетичному простор / В. Л. Бурячок, Г. М. Гулак, В. О. Хорошко // Наука і оборона . – 2011. – №3. – С. 35-43.*

5. *Гамаюнов Д. Ю. Обнаружение компьютерных атак на основе анализа поведения сетевых объектов: авторефер. дисс. на соискание научн. степени канд. техн. наук : спец 05.13.11 – математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей / Д.Ю. Гамаюнов – Москва, 2007. – 11 с.*

6. *Гірницька Д. А. Визначення коефіцієнтів важливості для експертного оцінювання у галузі інформаційної безпеки / Д.А. Горніцька, В.В. Волянська, А.О. Корченко // Захист інформації. – 2012. – Том 14, №1 (54). – С. 108-121.*

7. *Гнатюк С. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи . / С. Гнатюк // Безпека інформації. – 2013. – Том 9, №2. – С. 118 – 129.*

8. *Ежов А. А. Нейрокомпьютинг и его применения в экономике и бизнесе / А. А. Ежов, С. А. Шумский. – М. : МИФИ, 1998. – 224 с.*

9. *Емельянова Ю. Г. Нейросетевая технология обнаружения сетевых атак на информационные ресурсы / Ю. Г. Емельянова, А. А. Талалаев, И. П. Тищенко, В. П. Фраленко // Программные системы: теория и приложения. – 2011. – №3(7). – С. 3–15.*

10. *Комар М.П. Нейросетевой подход к обнаружению сетевых атак на компьютерные системы / М.П. Комар, И.О. Палий, Р.П. Шевчук, Т.Б. Федысив // Інформатика та математичні методи в моделюванні – 2011. – Том 1, №2. – С. 156-160.*

11. *Корченко А. А. Модель эвристических правил на логико-лингвистических связках для обнаружения аномалий в компьютерных системах / А. А. Корченко // Захист інформації – 2012. – № 4. – С. 109-115.*

12. *Корченко А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / А. Г. Корченко. – К. : НАУ, 2005. – 339 с.*

13. *Руденко О.Г. Штучні нейронні мережі. Навч. посіб. / О.Г. Руденко, Є.В. Бодянський. – Харків: ТОВ "Компанія СМІТ", 2006. – 404 с.*

14. *Терейковський І.А. Вдосконалення алгоритму навчання багатошарового персептрону призначеного для розпізнавання мережевих атак / І. А. Терейковський // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні – 2012. – Випуск 2(24). – С. 65–70.*

15. *Терейковський І. Нейронні мережі в засобах захисту комп'ютерної інформації / І. Терейковський. – К. : ПоліграфКонсалтинг. – 2007. – 209 с.*

16. *Bezobrazov S., Golovko V. Neural Networks for Artificial Immune Systems: LVQ for Detectors Construction // IDAACS'2007: proceedings of the 4 IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications. – Dortmund, 2010. – P. 180-184.*

17. *Overview of current cyber attacks (logged by 180 Sensors) [Електронний ресурс]. – Режим доступу: http://www.sicherheitstacho.eu/?lang=en. Thursday, 5 December 2013.*

Бапієв І.
докторант Казахського національного технічного університету ім.К.І.Сатпаєва, Казахстан, м. Алма-Ата,

Корченко О. Г.
доктор технічних наук, завідуючий кафедрою безпеки інформаційних технологій
Національного авіаційного університету, м. Київ,

Терейковський І. А.
доктор технічних наук, професор кафедри системного програмування і спеціалізованих комп'ютерних систем Національного технічного університету України «КПІ ім. І.Сікорського», м. Київ

Терейковська Л. О.
кандидат технічних наук, асистент кафедри інформаційних технологій Київського національного університету будівництва і архітектури, м. Київ,

КОНЦЕПТУАЛЬНА МОДЕЛЬ І ПРИНЦИПИ ЗАБЕЗПЕЧЕННЯ ЕФЕКТИВНОСТІ НЕЙРОМЕРЕЖЕВОГО РОЗРІЗНАВАННЯ КІБЕРАТАК

Анотація. *Стаття присвячена розвитку методологічної бази використання нейронних мереж для розпізнавання кібератак. Запропонована концептуальна модель, що дозволяє визначити перспективні напрямки подальших досліджень для створення ефективних нейромережевих систем розпізнавання кібератак. Також запропоновано ряд нових принципів використання нейронних мереж для розпізнавання кібератак, використання яких забезпечить можливість підвищення ефективності нейромережевих моделей.*

Ключові слова*: Нейронна мережа, кібератака, модель, ефективність, концепція*

Bapiev Ideyat
Doctoral Kazakh National Technical University name K. I. Satpayev.,

Korchenko Oleksandr Gryhorovych,
Doctor of Engineering Sciences, Head of IT-Security Academic Department, National Aviation University

Terejkowski Igor Anatolevych,
Doctor of Engineering Sciences, Professor of the Department of system software and specialized computer systems, National Technical University of Ukraine

Terejkowska Lyudmila Alekseevna,
candidate of technical sciences, Assistant of the Department of information systems of Kyiv National University of Construction and Architecture

Annotation*. The article is devoted to the development of a methodological framework use neural networks for recognition of cyber attacks, allowing to identify promising areas for further research to establish effective neural network recognition systems cyberattacks. To this end, developed a conceptual model, which is due to the specification of assessment parameters and factors affecting the efficiency of neural network recognition process cyberattacks, allows detailing areas for further research in this area. There is also provided a number of new guidelines for the use of neural networks for cyber recognition that by taking into account the degree of maintenance of neural network model of the task characteristics correlating the expected outputs of the neural network model with similarity cyberattacks with each other, the application of wavelet transform theory to predict the number of requests to the server and use the productive rules for the formation of case studies provide an opportunity to improve the efficiency of neural network pattern recognition.*