ОСОБЕННОСТИ ПРИМЕНЕНИЯ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ К ЗАДАЧЕ КОНТРОЛЯ ЗАЩИЩЁННОСТИ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

FEATURES OF APPLICATION OF NEURAL NETWORK TECHNOLOGY TO THE TASK OF MONITORING THE SECURITY OF AUTOMATED INFORMATION SYSTEMS

A. Vershinin

Summary. In outlining the scope of the NS, it should be taken into account that the capabilities of the network largely depend on the type of the NSM. The results of research indicate that the development of modern NS is by adapting the basic architecture to the solution of practical problems. At the same time, a number of architectures have already lost their leading positions and are used only as auxiliary ones.

Keywords: signal of the neuron, corrective communication, calculation.

Вершинин Александр Николаевич
Старший преподаватель, МИРЭА — Российский технологический университет
ve.sa.2009@mail.ru

Аннотация. Очерчивая сферу применения НС следует учесть, что возможности сети в значительной степени зависят от вида НСМ. Результаты исследований указывают на то, что развитие современных НС идет путем приспособления базовых архитектур к решению практических задач. При этом ряд архитектур уже потеряли свои передовые позиции и используются только в качестве вспомогательных.

Ключевые слова: сигнал нейрона, корректирующие связи, расчет.

Под термином НС понимают сеть элементов (искусственных нейронов), связанных между собой синаптическими связями [5, с. 12]. Основными конструктивными параметрами НС является количество входящих, скрытых и выходных нейронов, структура связей (топология сети), правила распространения и комбинирования сигналов, правила исчисления выходного сигнала нейрона и правила обучения, корректирующие связи в сети. Совокупность указанных параметров определяют (архитектуру НС) вид НСМ.

Методы разработаны в рамках нейросетевой технологии обнаружения сетевых компьютерных атак с помощью программного комплекса «Snort», описанной в работе [13, с. 60]. Технология предусматривает применение двух нейросетевых методов обнаружения атак — простой классификации (ПСК) и семантической классификации (ССК). В качестве входных параметров используются параметры сетевых пакетов транспортного уровня стека протоколов TCP/IP. В методе ПСК использовано МСП с 10 входными нейронами и 2 нейронами в выходном слое. Для оптимизации количества скрытых нейронов предлагается применение конструктивных алгоритмов. Приведенное выражение для расчета коррекции весовых коэффициентов нейронов выходного слоя:

$$\Delta m_{jk}(i) = -\eta\big(y_n(i) - f(x_i)\big)\varphi`(v_n(i))y_n \qquad (1)$$

где η — коэффициент скорости обучения,

n — номер нейрона в выходном слое,

i — номер учебной итерации,

v_n — информационное поле, полученное на входе функции активации,

y_n — выходной сигнал n-го выходного нейрона,

φ — производная функции активации,

$f(x_i)$ — желаемый отклик n-го нейрона.

Отметим отсутствие детального описания процесса оптимизации структуры МСП. В методе ССК предлагается использование топографической ТК, выбор которой обосновывается ее невысокой ресурсоемкостью. В обоих методах предусмотрена обработка входных параметров с целью уменьшения количества входных параметров НС.

Метод нейросетевой фильтрации спама (НФС), приведен в работе [11, с. 210]. Доказывается оптимальность использования аддитивных НС. Вид НСМ избран с позиций максимизации точности распознавания, возможности автоматизации обучения и возможности представления результатов в графическом виде. То есть использована процедура многокритериальной оптимизации процесса определения архитектуры НС. В качестве входных параметров НСМ использованы частоты встречи в спаме и в целевых электронных письмах информативных слов. Также предложена процедура многокритериальной оптимизации параметров НС, в которой использовано критерии максимизации вычислительной мощности и минимизации срока обучения.

Метод определения фрагментов программного кода (ОФПК), описан в работе. Метод применяется для определения перечня и оценки значений входных параметров НС, используемых в системах детектирования вредоносного программного обеспечения. Также в работе приведено описание и результаты экспериментов по распознаванию ВПО, проведенных с помощью МСП. Анализ приведенных результатов подтверждает перспективность предложенного метода. Можно сделать вывод об использовании в методе процедуры предварительной обработки входных параметров НС, которая повышает их информативность.

Нейросетевые системы обнаружения вторжений (НСОВ), описаны в работе. Система ориентирована на использование МСП для распознавания сетевых атак. Приведены результаты экспериментов, подтверждающие эффективность системы при распознавании атак, сигнатуры которых представлены в базе KDD-99. Выбор типа НС обоснован с позиций максимальной вычислительной мощности. Также проведена однокритериальная оптимизация архитектуры МСП.

Нейросетевой подход выявления SQL-инъекций (НПВИ) представлен в работе. Предложено рассматривать проблему определения вредоносных SQL-запросов в виде проблемы прогнозирования временных рядов. Согласно указанного предложения предлагается использовать рекуррентные НС типа Джордана и Элмана. То есть тип НС избран в соответствии с критерием апробированности в задачах прогнозирования временных рядов. Также приведена процедура предварительной обработки входных параметров и процедура однокритериальной оптимизации структуры НС. Использованы критерий максимизации вычислительной мощности. Приведенные результаты экспериментальных исследований на основе данных портала PhpNuke, подтверждают перспективность предложенного подхода.

Бинарный нейросетевой метод (БНС), описан в работе [10, с. 50]. Метод применяется для решения задачи обнаружения сетевых атак. В основе метода лежит специальная бинарная нейронная сеть, которая имеет два важных свойства. Во-первых, модель приспособлена для решения задач, в которых входная информация имеет сложную, многосвязную и даже фрактальную структуру. Во-вторых, метод обучения модели является прямой вычислительной процедурой и не сводится к поиску глобального экстремума сложной нелинейной функции, не накладывает никаких принципиальных ограничений на размерность задачи. Таким образом, в методе предусмотрен выбор вида НСМ по критерию апробированности в задачах определенного типа и по критерию минимизации продолжительности обучения. К сожалению, в работе отсутствуют экспериментальные данные, что затрудняет сравнительный анализ [11, с. 210].

Метод выделения сетевых атак с типичного сетевого трафика описан в работе. Метод применяется для распознавания сетевых атак. Предложено применение МСП с 2 ССН. ВШ такого МСП состоит из 9 нейронов, а СВ — из 1 нейрона. Отмечено, что выбор МСП с такой структурой объясняется требованиями гибкости и функциональности. То есть использована многокритериальная оптимизация структуры НС. Указано на предварительную обработку статистики, используемой для учебной и тестовой выборки.

Способ обнаружения DDoS-атак приведен в работе [8, с. 536]. Предложено использование нечетких НС. Предложение основывается на перспективности НС такого типа. Акцент ставится на распознавании DDoS-атаки типа SYN Flood. Для формализации знаний экспертов о DDoS-атаки было создано 5 лингвистических переменных, каждая из которых характеризует одну из компонент вектора параметров сетевого трафика, которая используется для формирования входных параметров НС. К указанным лингвистическим переменным относятся: X_1 — время получения пакетов, X_2 — процент пакетов из различных внешних ip-адресов, X_3 — процент пакетов с разных портов, X_4 — процент пакетов с поврежденными заголовками, S — степень уверенности. Разработаны предикатные правила вида: Если X_1 = «большой» $\rightarrow Y \rightarrow$ «высокий». Предложено представить нечеткий классификатор в виде НС с прямым распространением сигнала, который учится с помощью модифицированного алгоритма обратного распространения ошибки. Модификация заключается в приспособлении классического алгоритма к нечетким нейронам «И» и «ИЛИ». Таким образом, основным отличием способа обнаружения DDoS-атак является возможность его применения для обучения НС экспертным знаниям.

Метод использования нейронной сети гибридной структуры типа CounterPropagation (НСГС) описан в работе. Метод предназначен для обнаружения сетевых атак на веб-сервер. Особенностью сети CounterPropagation является комбинация ТК с МСП. Входными данными метода являются параметры сетевого трафика, передаваемого по протоколам IP, TCP, HTTP, HTTPS, CGI, SQLNet. В методе предусмотрена процедура предварительной обработки входных параметров НС за счет представления их в виде графических образов (пифограмм), которые используются в когнитивной графике. Целью предварительной обработки является минимизация размерности входных данных. Графическое представление определило необходимость применения в методе слоя Кохонена. Использование персептронного слоя обосновано с позиций вычислительной эффективно-

сти [12, с. 297]. Таким образом, в методе предусмотрена многокритериальная оптимизация вида и однокритериальная оптимизация параметров НСМ. Также в методе применена процедура оптимизации параметров обучения НС, которая позволяет в 10 раз уменьшить величину ошибки распознавания атак.

Метод построения совокупного классификатора трафика (ПСКТ). Метод предназначен для иерархической классификации компьютерных атак на информационно-телекоммуникационные сети. Особенностью ПСКТ является использование математического метода главных компонент для сжатия статистических данных, используемых в качестве обучающей выборки НС. В методе использовано объединение с 22 нейросетевыми детекторами, каждый из которых обучен распознавать определенный тип атаки, приведенный в базе данных KDD-99. Детектор представляет собой трехслойную НС с 12 входными нейронами и 2 выходными нейронами, один из которых отвечает за наличие, а второй за отсутствие атаки. В качестве СШН использован слой Кохонена. Отметим, что обоснование архитектуры и параметров нейросетевого детектора не приведены. При обнаружении детектором атаки выход первого выходного нейрона равен 1. Для предотвращения ситуации, когда несколько детекторов одновременно сигнализируют о собственном типе атаки, на второй выход каждого из них передается минимальное эвклидовое расстояние между входным образом (входными параметрами — x_i) и весовыми коэффициентами скрытых нейронов ($w_{i,j}$):

$$E_j = min_i\sqrt{(x_i - w_{1,j})^2 + \cdots + (x_{12} - w_{12,j})^2} \qquad (2)$$

В дальнейшем классифицируется и атака, детектор которой имеет минимальное эвклидовое расстояние. В ПСКТ в неявном виде предусмотрена оптимизация обучения и функционирования нейросетевого детектора.

Нейросетевой подход к выявлению сетевых атак (ПВСА) на ИС. Акцент ставится на распознавание атак, сигнатуры которых представлены в БД KDD-99. Согласно данных этой БД, количество входных параметров –41. Предложено использовать критерий выбора оптимального вида НСМ в виде минимума объема обучающей выборки. Путем анализа литературных источников определено, что к допустимым типам относятся ТК, МСП с одним скрытым слоем нейронов и РБФ. Отмечено, что для ТК минимальный объем обучающей выборки (L) должен в 2 раза превышать количество входных нейронов (n). То есть $L \geq 2n$. Для МСП и РБФ объем обучающей выборки рассчитывается так $L \approx W / \varepsilon$,, где W -количество синаптических связей, ε — допустимая ошибка обучения. В дальнейшем в [6, с. 120] сделана попытка определить оптимальную структуру МСП. Заявлено, что определенное экспериментальным путем количество скрытых нейронов равно $m = 10$. При этом количество выходных нейронов равно 2. Соответственно, необходимый объем обучающей выборки ТК составляет $L = 82$ примеры, а для МСП и РБФ при $\varepsilon = 0{,}1$, $L = (m(n + 3) + 2) / \varepsilon = 4420$. Поэтому оптимальным типом нейросетевой модели выбрана ТК. Отметим, что правильность рассчитанных величин вызывает сомнения, ведь, согласно теории НС [8, с. 536], при заданной точности обучения количество скрытых нейронов МСП напрямую зависит от величины стремительной выборки. В дальнейшем в [6, с. 108] проводится оптимизация структуры ТК. Неявно использован критерий максимизации точности обучения. Также использована аналогичная процедура предварительной обработки входных параметров.

Адаптивная система обнаружения атак (АСОА), описана в работе. Система предназначена для распознавания сетевых атак и базируется на совместной работе ТК и МСП, выполняющих задачи кластеризации и классификации данных [14, с. 102]. Обнаружение атак, которое проводится в несколько этапов, стало возможным благодаря тому, что в базу данных экспертной системы вносилась информация об изменениях в поведении конкретного объекта в течение некоторого отрезка времени. Доказывается, что оптимизация архитектуры позволит повысить точность и оперативность распознавания. В качестве входных данных использованы параметры сетевого трафика по протоколу TCP. Для обработки входных данных использован метод скользящего временного окна. ТК использована для предварительной обработки данных, поступающих на вход МСП с целью их сжатия и повышения информативности. Приведено математическое выражение для расчета частоты определения нейрона в позиции (i, j) в качестве нейрона-победителя:

$$\beta_{i,j} = f_{i,j} + \sum_{x=1}^{r}\left(\frac{f_{i-x,j}+f_{i,j-x}+f_{i+x,j}+f_{i,j+x}}{1+x}\right) \qquad (3)$$

где $f_{i,j}$ — количество раз когда нейрон в позиции (i, j) был нейроном-победителем.

r — расстояние между центрами кластеров,

x — длина входного вектора.

В дальнейшем эта частота используется для определения центров и границ кластеров. Структура МСП оптимизирована с точки зрения соответствия объема контролируемых ресурсов.

Нейросетевая технология обнаружения и классификации сетевых атак (ОКСА), описана в работе. В технологии предложено использование трехслойной НС, что учится методом обратного распространения ошибки. При этом для распознавания каждого вида сетевой атаки применяется отдельная НС. Как входные параметры используются параметры сетевого трафика по стеку протоколов TCP/IP. Для формирования обучающей вы-

борки предлагается использовать базу данных KDD-99. Приведены словесное описание и фрагменты программного кода для подготовки входных данных из этой базы данных к виду входных параметров НС. Одной из целей подготовки является уменьшение объема обучающей выборки НС. Описания подходов к оптимизации вида и параметров НСМ отсутствуют.

Система обнаружения аномального поведения вычислительных процессов (ОАВП), разработанная в работе [4, с. 280]. Система предназначена для обнаружения атак на компоненты информационной системы, функционирующие на базе микроядерных операционных систем. Подробно разработана методика сбора и подготовки входных параметров для НС. Предлагается использование ТК и МСП. Описания процедуры оптимизации вида и параметров НСМ не приведены.

Модель кибернейрона (МКН), разработанная и описанная в работе [15, с. 28]. Модель предлагается использовать для распознавания компьютерных вирусов. Основным отличием модели кибернейрона является отсутствие функции активации, вместо которой используется таблица подстановки, а основным преимуществом — потенциально высокая вычислительная мощность [9, с. 448]. Разработаны алгоритмы обучения кибернейрона. В качестве входных параметров используются или фрагменты подопытного файла или хэш-коды указанных фрагментов. Определение указанных фрагментов предлагается реализовать методом скользящего окна. Задачей НС является распознавание чистых и зараженных фрагментов. Следует отметить, что модель кибернейрона появилась относительно недавно, является практически не апробированной, а использование табличной активационной функции теоретически малообоснованно. Соответственно, применение кибернейрона в сфере защиты информации требует серьезной доработки.

Метод распознавания аномалий сетевого трафика (РАСТ), разработан в работе [1, с. 199]. Методом предусмотрено использование НС типа МСП. В качестве входных данных НС использованы параметры заголовков IP-дейтаграмм. Выбор архитектуры НС базируется на утверждении о высоких аппроксимационных возможностях МСП. МСП состоит из трех слоев нейронов. Количество нейронов ВС — 18, равно числу параметров заголовке IP-дейтаграммы. Количество нейронов в СВ 2. Выход нейрона № 1 отвечает за наличие аномалии, а выход нейрона № 2 за безопасное состояние сетевого трафика. Приведены выражения для расчета количества нейронов в ССН. Таким образом, методом предусмотрена оптимизация параметров архитектуры НС. Для упрощения создания репрезентативной выборки разработан метод уточняющих сигнатур, суть которого заключается во введении дополнительных искусственно созданных сигнатур, что описывают априорно аномальный трафик [2, с. 10]. Таким образом, в методе в неявном виде возможно использовать экспертные данные о сетевых атаках.

Нейросетевая искусственная иммунная система (НИИС), описана в работе. НИИС предназначена для распознавания в сканированных файлах ВПО. Использованы НС типа ТК. Выбор забора НС обоснован по критерию минимизации допустимого объема обучающей выборки (L), который для ПК зависит только от количества нейронов ССН (m): L ≥ 2m. Процедуры предварительной обработки входных параметров и оптимизации процесса обучения не предусмотрены.

Модель ТК для распознавания компьютерных вирусов (МТК), разработана в работе [3, с. 239]. Модель предназначена для использования в антивирусных сканерах. Предусмотрен блок предварительной обработки входных параметров. Выбор типа модели реализован путем сравнительных численных экспериментов. В качестве критерия сравнения использован срок обучения. Оптимизация параметров и процедуры обучения нейросетевой модели не проводилась.

Метод обнаружения несанкционированного доступа к базе данных (ОНДБД) разработан в работе. Предложено использование ДСП. ВС состоит из 4 нейронов, а СВ из 1. В качестве входных данных использованы: объем загружаемой информации в базу данных, количество транзакций за одну минуту, количество операций модификации за одну минуту, признаки обращений к словарю. Предварительная обработка входных параметров заключается в их ранжировании и нормализации.

Алгоритм преобразования параметров трафика (АППТ) описан в работе [7, с. 36]. Алгоритм предназначен для получения из сетевого трафика входных данных для нейросетевой системы обнаружения сетевых атак. В качестве входной информации указанного алгоритма используются параметры TCP-сессии. Преобразование параметров трафика применяется с целью уменьшения количества входных параметров НС и увеличения их информативности и реализуется с помощью математического аппарата, основанный на методе главных компонент. В алгоритме оптимизация вида и параметров НСМ не предусмотрена.

Нейросетевая технология обнаружения сетевых атак (ТОСА) на информационные ресурсы описана в. В технологии предусмотрен модуль сжатия входных данных, который базируется на применении нейросетевого аналога метода главных компонент — рециркуляционной нейронной сети с двумя слоями нейронов. Путем чис-

Таблица 1. Базовые характеристики нейросетевых методов и моделей

Метод	Распознавание				Тип НС								
	ВПО	АБД	спам	СА	МП	КН	ТКК	ВНС	АНС	САРТ	БНМ	РНС	все типы
ВФПК	+	-	-	-	+								
МКН					-	+	-	-	-	-	-	-	-
МТК					-	-	+	-	-	-	-	-	-
НИИС													
НПВИ	-	+	-	-	-	-	-	+	-	-	-	-	-
ВНДБД					+								
НФС	-	-	+	-	-	-	-	-	+	-	-	-	-
АППТ	-	-	-	+	-	-		-	-	-	-	-	+
ПСКТ					+	-		-	-	-	-	-	-
НСВВ													
ТОКА													
ТОСА													
РАСТ													
СКСА					-	-	+	-	-	-	-	-	-
НГС	-	-	-	+	+	-	+	-	-	-	-	-	-
ПСКТ													
ПВСА													
АСОА)													
ВАПВП)													
СОДА					-	-		-	-	+	-	-	-
БНС					-	-		-	-	-	+	-	-
ТОКСА					-	-		-	-	-	-	+	-

Таблица 2. Величины критериев, характеризующих нейросетевые методы и модели

Метод	Параметр f для НС								
	МП	КН	ТКК	ВНС	АНС	САРТ	БНМ	РНС	все типы
ВФПК	1	0	-1	0	-1	0	1	-1	-1
МКН	1	1	-1	-1	-1	-1	-1	-1	-1
МТК	1	1	-1	0	-1	-1	-1	-1	-1
НИИС	–1	1	–1	1	–1	–1	–1	–1	–1
НПВИ	1	1	0	0	-1	0	-1	-1	-1
ВНДБД	1	0	-1	0	-1	-1	-1	-1	-1
НФС	1	1	0	1	0	1	-1	-1	-1
АППТ	1	-1	-1	-1	-1	-1	-1	0	-1
ПСКТ	1	0	-1	0	-1	0	-1	-1	-1
НСВВ	0	0	–1	0	–1	0	–1	–1	–1
ТОКА	1	0	–1	0	–1	–1	–1	–1	–1
ТОСА	–1	1	–1	0	–1	–1	0	–1	–1
РАСТ	0	0	–1	0	–1	–1	1	–1	–1
СКСА	1	0	-1	0	-1	0	-1	-1	-1
НГС	1	1	0	0	-1	-1	-1	-1	-1
ПСКТ	1	0	-1	0	-1	0	-1	-1	-1
ПВСА	1	1	-1	0	-1	0	-1	-1	-1
АСОА	1	1	0	1	1	0	-1	-1	-1
ВАПВП	1	-1	-1	-1	-1	-1	-1	-1	-1
СОДА	0	0	-1	0	-1	0	-1	-1	-1
БНС	-1	0	-1	-1	-1	1	-1	-1	-1
ТОКСА	1	-1	-1	-1	-1	-1	-1	-1	-1

ленных экспериментов доказана возможность использования предложенной технологии для обнаружения сетевых атак, сигнатуры которых представлен в базе данных KDD-99.

Базовые характеристики проанализированных нейросетевых методов и моделей приведены в табл. 1.1. Анализ данных этой таблицы указывает на то, что большинство известных НСС предназначены для распознавания сетевых атак. При этом в качестве базовых видов НСС используются МСП и ТК.

Кроме того, в результате проведенного анализа установлено, что обеспечение эффективности современных нейросетевых методов и моделей идет путем обеспечения в них определенных возможностей, которые характеризуются с помощью следующих критериев: $\phi_{по}$ — предварительная обработка входящих параметров, $\phi_{ота}$ -однокритериальная оптимизация вида архитектуры, $\phi_{бва}$ — многокритериальная оптимизация вида архитектуры, ϕопа — однокритериальная оптимизация параметров архитектуры, $\phi_{бпа}$ — многокритериальная оптимизация параметров архитектуры, $\phi_{омо}$ -оптимизация метода обучения, $\phi_{иэп}$ — возможность использования экспертных правил. Приведенный перечень дополнен критериям $\phi_{мна}$ и $\phi_{одв}$, которые указывают на возможность применения в методе классических и перспективных видов НСМ и возможность принципиальной оценки целесообразности применения НС для решения поставленной задачи. Основой использования параметра $\phi_{мна}$ является приведенное утверждение о том, что в СЗИ, как и в большинстве известных приложений, развитие нейросетевых методов и моделей идет путем приспособления базовых и перспективных нейросетевых архитектур к условиям поставленных практических задач. Основой использования параметра $\phi_{одв}$ является объективная необходимость четкого определения области применений НС в СЗИ.

Величины предложенных критериев в первом приближении можно оценить так: критерий равен 1, когда соответствующая возможность в нейросетевом методе или модели не обеспечивается, 0 — когда обеспечивается опосредованно и 1 — когда обеспечивается непосредственно.

Для проанализированных случаев величины указанных критериев приведены в табл. 1. При этом для всех проанализированных методов $\phi_{мна} = \phi_{одв}$ = –1. Только для АППТ $\phi_{мна} = 1$, а $\phi_{одв} = 0$.

То есть в большинстве из проанализированных методов нельзя использовать весь перечень классических и перспективных видов НСМ и ни в одном из методов (моделей) не предусмотрена оценка принципиальной целесообразности его применения. Также отметим, что базовый перечень параметров может быть в дальнейшем расширен.

Практическая ценность данных табл. 1.2 заключается в обрисовке недостатков и перспектив совершенствования современных нейросетевых методов и моделей. Например, величины $\phi_{по}$= 0, $\phi_{бва} = -1$ свидетельствуют о том, что к недостаткам метода НСОВ можно отнести недостаточную оптимизацию вида НСМ. Это свидетельствует о возможности соответствующего совершенствования указанного метода. При этом ни один из рассмотренных методов не предполагает полноценной оптимизации НСМ, согласно условий поставленной задачи и полноценного использования в такой модели экспертных правил.

Также в результате проведенного анализа показано, что в современных СВА в основном используются классические виды НСМ, которые в той или иной степени адаптированы к условиям поставленной задачи.

В результате проведенного анализа можно сделать вывод о том, что важным и актуальным направлением повышения эффективности контроля защищённости автоматизированных информационных систем является применение нейросетевых моделей, методов и средств оценки параметров безопасности. Несмотря на определенные достижения в этой области, эффективному применению таких средств оценивания мешают ряд недостатков. Основными из них являются:

- недостаточная оперативность реагирования на новые виды кибератак;
- недостаточная адаптация к вариативности условий применения и действия при ограниченных вычислительных ресурсах;
- недостаточная точность распознавания кибератак;
- недостаточная взаимосвязь известных нейросетевых подходов, моделей и методов оценки параметров безопасности для обнаружения кибератак;
- отсутствие нейросетевых систем, которые на основе комплексной нейросетевой методологии позволят решать наиболее актуальные задачи контроля защищённости ИАИС.

Для исправления этих недостатков определены два направления научных исследований:

1. Развитие теоретического базиса нейросетевого оценивания параметров безопасности.
2. Применение разработанных теоретических положений для последовательного создания нейросетевых моделей, методов и систем оценки параметров безопасности.

Определение направлений развития теоретического базиса основывается на следующих предпосылках:

- эффективное использование нейросетевых средств требует разработки типовых подходов к применению нейросетевых моделей для распознавания различных видов кибератак;
- отсутствие оперативности распознавания новых типов кибератак в основном связано с длительным накоплением статистических данных, необходимых для обучения нейронной сети. Для обеспечения оперативности возможно для обучения нейронной сети использовать экспертные данные;
- обеспечить приспособленность нейросетевых средств к вариативности условий применения возможно за счет оптимизации вида и параметров контроля защищённости автоматизированных информационных систем, что лежит в основе таких средств;
- для адаптации нейросетевых средств к функционированию при ограниченных вычислительных ресурсах необходимо как оптимизировать вид и параметры нейросетевой модели, так и априорно оценивать объем вычислительных ресурсов для ее реализации;
- использование нейросетевых средств связано с определенным набором условий и ограничений, определяемых условиями задачи оценки и характеристиками нейросетевой модели. Поэтому необходимо провести как определение принципиальной целесообразности применения нейросетевых средств, так и оценку эффективности их разработки;
- повысить точность распознавания кибератак возможно за счет адаптации математического обеспечения нейросетевых моделей до функциональных зависимостей, соответствующих процессам распознавания. Кроме того, для повышения точности распознавания длительных кибератак целесообразно использовать марковский шаблон поведения параметров безопасности, который позволяет частично нивелировать временную составляющую процесса распознавания;
- использование нейронных сетей в высокоответственных средствах распознавания кибератак требует теоретической верификации нейросетевых моделей оценивания параметров безопасности.

Решение второго направления исследований связано с комплексной разработкой моделей, методов и систем, основанных на предложенных теоретических решениях, которые учитывают особенности контроля защищённости АИС.

Таким образом, сформулированная в исследовании проблема создания комплексной методологии разработки широкодоступных эффективных нейросетевых средств контроля защищённости автоматизированных информационных систем на основе применения нейросетевых технологий декомпозируется на ряд следующих задач:

- анализ современных нейросетевых средств оценки параметров безопасности информационных систем;
- развитие теоретических положений построения нейросетевых средств оценивания параметров безопасности информационных систем, позволяющих учиться с помощью экспертных данных, уменьшать погрешности классификации, учитывать особенности современных видов кибератак, условия использования и верифицировать полученные решения;
- построение моделей, учитывающих предложенные теоретические решения и использующиеся в нейросетевых средствах оценки параметров безопасности;
- разработка методов создания нейросетевых средств оценивания параметров безопасности, учитывающих предложенные теоретические решения и построенные модели;
- разработка нейросетевых систем оценки параметров безопасности информационных систем, которые позволяют распознавать вредоносные программы, классифицировать электронную почту и распознавать сетевые кибератаки.

ЛИТЕРАТУРА

1. Абрамов Е. С. Разработка и исследование методов построения систем обнаружения атак. Таганрог. 2005.
2. Айтчанов Б.Х., Бапиев И. М. Разработка процедуры определения ожидаемого выходного сигнала нейросетевой модели распознавания кибератак // Международный журнал прикладных и фундаментальных исследований. 2017. № 5–1.
3. Артеменко А.В., Головко В. А. Анализ нейросетевых методов распознавания компьютерных вирусов. — Минск: ГУ «БелИСА». 2010.
4. Безобразов С. В. Алгоритмы исскуственных имунных систем и нейронних сетей для обнаружения вредоносных программ /Нейроинформатика. 2010. № 7.
5. Беляев А. Системы обнаружения аномалий: новые идеи в защите информации / Экспресс-Электроника. 2004. № 2.
6. Блюменау Д. И. Экстрагирование как один из подходов к автоматизации реферирования /НТИ. Сер.2. 1982. № 2.
7. Большев А. К. Алгоритмы преобразования и классификации трафика для обнаружения вторжений в компьютерные сети. СПб. 2011.

8. Бриллинджер Д. Р. Временные ряды. Обработка данных и теория. М.: Мир. 1980.
9. Вапник В. Н. Восстановление зависимостей по эмпирическим данням. М.: Наука. 1979.
10. Ващук И.Н., Кин Е. А., Очередько О. О. Оценка рисков при проектировании и разработке автоматизированной информационной системы поддержки разработки проекта комплексной системы защиты // В сборнике: Информационные технологии в моделировании и управлении: подходы, методы, решения Материалы I Всероссийской научной конференции: в 2 частях. Министерство образования и науки Российской Федерации; Тольяттинский государственный университет. 2017.
11. Вилков А. С. Информационная безопасность персональных ЭВМ и мониторинг компьютерных сетей.— М.: МИНИТ ФСБ России,. 2005.
12. Гавриленко С.Ю., Бабенко О. С., Игнатова Е. Н. Разработка системы распознавания уровня программном обеспечении на основе нейронных сетей // В сборнике: Метрология, стандартизация, качество: теория и практика материалы Международной научно-технической конференции. 2017.
13. Гришин А. В. Нейросетевые технологии в задачах обнаружения компьютерных атак /Информационные технологии и вычислительные системы. 2011. № 1.
14. Давидюк Н. В. Методика оценки требуемого уровня защищенности информационных ресурсов автоматизированных систем обработки информации и управления // Научный вестник Новосибирского государственного технического университета. 2016. № 4 (65).
15. Дьяконов М. Ю. Нейросетевая система обнаружения аномального поведения вычислительных процессов микроядерных операционных систем. Уфа. 2010.

Журнал «Современная наука: актуальные проблемы теории и практики»