электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК 004.056; 004.89

Использование технологий нейронных сетей при решении задач информационной безопасности

***Марков Г.А.**, студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»

Научный руководитель: Глинская Е.В., старший преподаватель
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана
кафедра «Информационная безопасность»
glinskaya@bmstu.ru

Введение

Возникающее противоречие между ростом сложности и разнородности современных информационно-коммуникационных систем и традиционными директивными мерами защиты информации обусловливает необходимость исследования новых соответствующих технологий, методов и механизмов информационной безопасности. Одним из перспективных направлений является исследование возможности применения аппарата технологий нейронных сетей для решения практических задач информационной безопасности. Обзору известных исследований и практическим реализациям посвящена данная статья.

1. Проблемные моменты современных средств защиты информации

Развитие современных распределенных и гетерогенных сетей, рост сложности и динамизма разнородного программного обеспечения связано с трудностями разработки и применения традиционных подсистем безопасности информации, ориентированных на заранее заданные классы угроз информационной безопасности [1]. Приведем примеры проблемных вопросов, связанных с некоторыми подсистемами информационной безопасности.

1.Идентификация и аутентификация. Одно из направлений развития указанной подсистемы безопасности связывают с внедрением биометрических средств. Однако, на практике, разработчики систем сталкиваются с проблемой изменения работы биометрических устройств в зависимости от здоровья и настроения человека, эффекта

старения организма и травм, а также с учетом влияния окружающей среды на сами технические устройства (сканеры), что приводит к большому количеству ошибок 1-го и 2-го рода. При разработке подобных устройств, зачастую, трудно заранее определить аналитические закономерности, т.е. использовать заранее детерминированные модели и методы.

Другим примером исследования подсистем идентификации является проблема проверки устойчивости средств противодействия автоматическому подбору паролей, типа CAPTCHA, визуальный вид и алфавит которых может постоянно меняться.

2.Антивирусная защита. Современные средства антивирусной защиты, использующие сигнатурные методы, в настоящее время переживают серьезный кризис. По оценкам некоторых специалистов, современные антивирусные средства не могут защитить от 80% «нежелательных» программ. Особенно это наглядно показали факты заражения троянскими программами промышленного применения, которые современные антивирусные средства не обнаруживали в течение 5-8 лет [2].

3.Обнаружение и предупреждение вторжений. Системы обнаружения компьютерных атак, как и антивирусные средства, главным образом, ориентированы на сигнатурные («по шаблону») методы, которые бессильны перед новыми классами атак. Одной из главных проблем систем обнаружения вторжений также является их склонность к большому числу ложных срабатываний из сложности количественной идентификации недоваренного трафика.

4. Управление рисками информационной безопасности. При проведении анализа риска возникает проблема невозможности описания ряда факторов безопасности количественными мерами. Более того, многие факторы имеют совершенно разную природу и закономерности их возникновения и проявления.

5.Выявление уязвимостей. Современные методы тестирования, ориентированные на выявление ошибок (не имеющих злонамеренную природу), сталкиваются с проблемами «проклятья размерности» и неэффективностью при выявлении ошибок, связанных с редко используемыми входными данными. Это обусловливает сложность их использования при поиске программных закладок и «забытой» отладочной информации.

Этот список можно продолжить. Таким образом, следует сделать вывод, что возникает необходимость в исследовании новых методов и технологий в области информационной безопасности. Одним и перспективных направлений в области развития информационных технологий считается аппарат искусственных нейронных сетей.

2. Искусственные нейронные сети

Под искусственными нейронными сетями (НС) понимают совокупность моделей биологических нейронных сетей. Структурно НС представляют собой сеть элементов - искусственных нейронов, связанных между собой синоптическими соединениями. НС обрабатывает входную информацию и в процессе изменения своего состояния во времени формирует совокупность выходных сигналов.

Каждый нейрон характеризуется своим текущим состоянием по аналогии с нервными клетками головного мозга, которые могут быть возбуждены или заторможены. Он обладает группой синапсов – однонаправленных входных связей, соединенных с выходами других нейронов, а также имеет аксон – выходную связь данного нейрона, с которой сигнал (возбуждения или торможения) поступает на синапсы следующих нейронов. Общий вид нейрона приведен на рис. 1.

Каждый синапс характеризуется величиной синаптической связи X_iи ее весом w_i, который по физическому смыслу эквивалентен электрической проводимости.

Текущее состояние нейрона определяется, как взвешенная сумма его входов:

$S = \sum_{i=1}^{n} X_i w_i$.

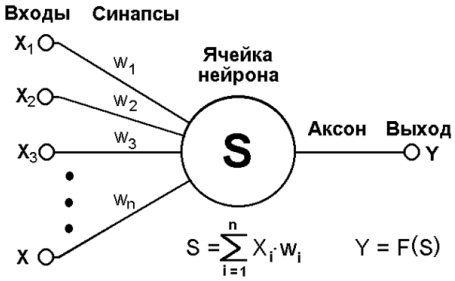

Рис. 1. Общий вид нейрона

Для НС вводится функция, определяющая порог срабатывания $Y = F(S)$.

В настоящее время чаще всего используют многослойные архитектуры нейронных сетей. Обычно такая сеть состоит из входного слоя, одного или нескольких скрытых слоев и выходного слоя (рис.2).

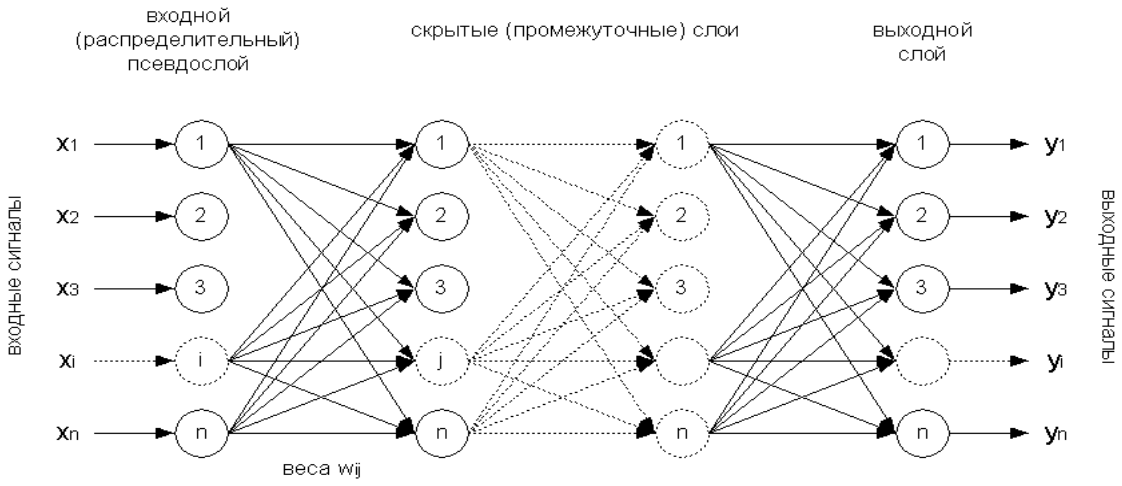

Рис. 1. Многослойная сеть

Можно выделить следующие наиболее распространенные архитектуры НС:

- сети прямого распространения, в которых все связи НС направлены строго от входного слоя к выходному;

- сети обратного распространения, когда сигнал может передаваться обратно к входному слою;

- сеть Кохонена –сеть с определенным слоем (слой Кохонена), таким, что сигналы этого слоя обрабатываются по правилу «победитель забирает всё», причем, наибольшему сигналу присваивается единица, а остальные сигналы обращаются в ноль.

Выбор структуры НС осуществляется в соответствии с особенностями и сложностью задачи.

Обучение НС – это процесс, в котором свободные параметры нейронной сети настраиваются посредством моделирования среды, в которую эта сеть встроена. Тип обучения определяется способом подстройки этих параметров.

Есть два варианта обучения НС: обучение с учителем и без.

В первом случае сети предъявляются значения как входных, так и желательных выходных сигналов, и она по некоторому внутреннему алгоритму подстраивает веса своих синаптических связей. Во втором случае выходы НС формируются самостоятельно, а веса изменяются по алгоритму, учитывающему только входные и производные от них сигналы.

Существует множество различных алгоритмов обучения, которые делятся на два больших класса:

- детерминистские;

- стохастические.

В первом из них подстройка весов представляет собой жесткую последовательность действий, во втором – она производится на основе действий, подчиняющихся некоторому случайному процессу.

3. Преимущества и недостатки нейронных сетей

Достоинством нейронных сетей является то, что, с одной стороны, они могут вести себя как детерминированный автомат, а с другой как нечеткая система, выдавая оценки на новые данные (не принимавших участие в формировании сети). И в том, и в другом случае такой результат достигается обучением сети, а не программированием (составлением правил реакций) как это делается в классических подходах.

Нейронная сеть представляет собой параллельное вычислительное устройство, так как в её основе лежит множество простых вычислительных элементов – нейронов, функционирующих параллельно. Другой стороной такой распределенной архитектуры является устойчивость к повреждениям, то есть сеть будет работать даже в том случае, когда часть нейронов выйдет из строя.

Следует отметить и ряд проблемных моментов внедрения нейронных сетей.

В первую очередь - это существование большого количества моделей нейронных сетей, что затрудняет их изучение, и выбор (особенно для начинающего) наилучшей модели для решения конкретной задачи.

Существуют модели, способные решать огромное количество задач, но такие модели не всегда являются наилучшими по качеству результата, в сравнении с другими узкоспециализированными моделями нейронных сетей. Но даже в том случае, когда модель выбрана, для лучшего функционирования сети необходимо подбирать ряд характеризующих сеть параметров, что является далеко нетривиальной задачей.

Другим недостатком является необходимость, в большинстве случаев, проводить предварительную обработку данных, в частности масштабировать в определенный диапазон и проводить стандартизацию. Однако эти операции легко автоматизируются.

Еще одним недостатком, в случае большой обучающей выборки с немалой размерностью входных векторов, могут быть ощутимые затраты по времени на процесс обучения сети. Хотя, если учесть, что другие методы в таких случаях не работают вообще (например, из-за «проклятья размерности») или их временные затраты еще больше, то значительное время обучения сети уже не является недостатком.

Есть несколько советов по подбору данных. Самое важное правило, о котором следует помнить, это необходимость снабдить сеть достаточным количеством данных, чтобы покрыть всю область определения задачи. Хорошее практическое правило заключается в том, чтобы использовать количество тренировочных примеров в 10 раз превышающее количество входов.

Для решения задач автоматизации расчетов НС можно использовать ряд специализированных прикладных пакетов программ. Рассмотрим наиболее популярные из них.

1. Пакет НейроПрактикум - пакет обучающих программ. Пакет включает в себя пять программ, объединённых типовым интерфейсом и основными приёмами работы:

- сети с обратным распространением ошибки - решение задач классификации;
- сети Кохонена - решение задач кластеризации;
- сеть с общей регрессией - решение задач классификации;
- рекуррентные сети с обратным распространением ошибки;
- линейный и нелинейный анализ главных компонент.

2. NeuroShell 2 - это универсальный пакет, предназначенный для нейросетевого анализа данных. С его помощью можно решать широкий спектр задач, начиная с широко распространенных задач, таких как прогнозирование курсов акций (облигаций, фьючерсов, валют, цен на нефть и т.д.), и заканчивая менее распространенными задачами, такими как, например, обратные задачи в геофизике и другие сложные задачи.

3. GeneHunter представляет собой комплекс мощных программных средств для решения оптимизационных задач с помощью генетических алгоритмов.

4. NeuroShell Predictor быстро создает мощные модели для предсказаний и не требует предварительной установки параметров. Этот пакет был разработан для тех, кто не имел опыта работы с нейронными сетями. NeuroShell Predictor позволяет строить прогнозы, не заботясь о тонкостях настройки нейронной сети.

5. NeuroShell Classifier (Классификатор) был разработан, подобно NeuroShell Predictor, для тех, кто не имел предварительного опыта работы с нейронными сетями. В отличие от программы NeuroShell Predictor, которая на выходе нейронной сети дает непрерывное значение предсказываемой величины, нейронная сеть NeuroShell Classifier имеет несколько выходов, которые определяют вероятность принадлежности предъявленного образа к каждой из нескольких категорий.

4. Обзор исследований в области нейронных сетей

В литературе можно встретить множество публикаций, посвященных научным исследованиям возможности использования НС при решении задач информационной безопасности. К сожалению, подавляющее большинство таких исследований носит теоретический характер и не доведены до широкого практического внедрения. Приведем примеры.

1. Обнаружение вторжений. Исследованию указанной проблемы посвящено самое большое число публикаций [3-11].Например, в [3, 4] рассматриваются методики построения обучающей модели для нейросети на базе СОВ с открытым кодом «Snort».

В указанных работах, как правило, в качестве архитектуры НС рассмотрены различные виды сетей адаптивного резонанса (классификаторы Карпентера-Гроссберга) и обобщенно-регрессионная сеть.

2. Моделирование испытаний по требованиям безопасности. В работе [12] приведено авторское исследование по оценке и планированию испытаний программных средств защиты. Исследование показала эффективность применения технологий нейронных сетей при испытаниях интегрированных программных изделий, включающих компоненты с открытым кодом, когда рост степени технологической безопасности имеет немонотонный характер (см. рис.3). В частности, в работе показано, что лучше всего с поставленной задачей справились простая 4-слойная нейронная сеть, а также нейронные сети с обходными соединениями.

3. Использование технологии нейронных сетей в биометрии. Одно из популярных направлений развития нейросетевых технологий связано с биометрией. Причем, речь не только об аутентификации отпечатков пальцев или сетчатки глаза, но и о поведенческих характеристиках, например почерк [13,14]

4.Нейронные сети в криптографии и стеганографии. Хоть использование нейросетевых технологий в криптографии не сильно обсуждаемая тема, но есть несколько интересных публикаций в данной тематике.

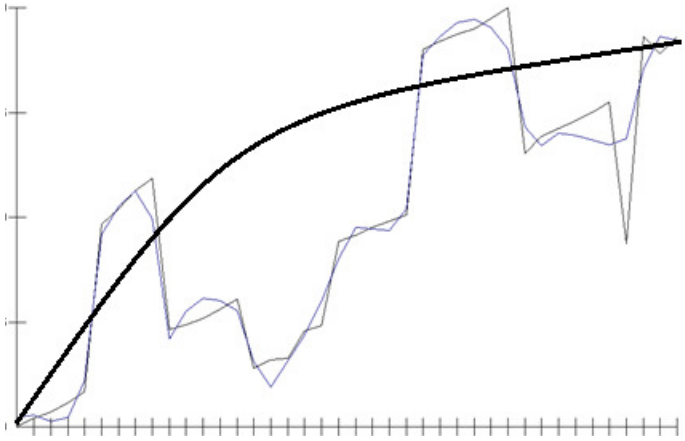

Рис. 3. Модели оценки уровня технологической безопасности программ(НС-модель показана тонкой линией, экспоненциальная – толстой)

В основном применение НС связано с криптосистемами, когда в качестве открытого ключа криптосистемы используется ключ Меркла-Хэллмана[15].

5. Другие применения аппарата нейронных сетей в области информационной безопасности. Например, в [16] предложен нейросетевой подход к иерархическому представлению коммуникационной сети, что может быть актуальным при исследовании безопасности, например, социальных сетей. Другим примером является использование нейронной сети для тестирования CAPTCHA [19].

Кроме указанных примеров теоретических изысканий, в открытых источниках можно встретить упоминание практических реализаций, например:

- системы распознавания, которые разрабатывает лаборатория GoogleX [18, 19];

- работы ряда фирм, ориентированных на борьбу с мошенничеством в банковской сфере [20].

Что касается первого примера, то следует отметить технологический стартап Vicarious, в рамках которого, как заявлено, решена задача прохождения CAPTCHA-тесты, в том числе наиболее популярной в современном интернете - reCAPTCHA. Исследователям удалось достичь 90% точности распознавания CAPTCHA от Google, Yahoo, PayPal, Captcha.com и других проектов. Это исследование показывает, что современные CAPTCHA уже не эффективны в качестве теста Тьюринга. В рамках другого проекта ученые лаборатории Google X, работающие над созданием экспериментальной

компьютерной нейронной сети, научили ее самостоятельно распознавать в видеопотоке морфологические объекты, например, кошек[20].

Выводы

Как показал анализ литературы, в мире проводится ряд исследований по применению технологий нейронных сетей для решения различных задач информационной безопасности, ряд из которых доведен до практической реализации.

Наиболее проработанным в плане моделирования является направление обнаружения новых классов компьютерных атак и инцидентов информационной безопасности. В тоже время наметился ряд направлений исследований, касающийся самого широкого класса задач информационной безопасности, в том числе организационных мер.

С другой стороны, надо понимать, то широкое внедрение технологий нейронных сетей частично сопряжено с решением задач получения представительной статистики и ее нормализации, объединения вычислительных ресурсов, развития супервычислений.

Список литературы

1. Матвеев В.А., Цирлов В.Л. Состояние и перспективы развития индустрии информационной безопасности Российской Федерации в 2014 г. // Вопросы кибербезопасности. 2013. № 1(1). С. 61-64.
2. Марков А.С., Фадин А.А.Организационно-технические проблемы защиты от целевых вредоносных программ типа Stuxnet // Вопросы кибербезопасности. 2013.№ 1(1). С. 28-36.
3. Гришин А.В. Нейросетевые технологии в задачах обнаружения компьютерных атак // Информационные технологии и вычислительные системы. 2011. №1.С. 53-64.
4. Емельянова Ю.Г., Талалаев А.А., Тищенко И.П., Фраленко В.П.. Нейросетевая технология обнаружения сетевых атак на информационные ресурсы // Программные системы: теория и приложения: электронный научный журнал. 2011. № 3(7).С. 3–15.
5. Израилов К.Е. Модель прогнозирования угроз телекоммуникационной системы на базе искусственной нейронной сети // Вестник ИНЖЭКОНа. Серия: Технические науки. 2012. № 8 (59). С. 150-153.
6. Nesteruk F.G., Nesteruk L.G., Nesteruk G.F. Application of the formal model for describing processes of adaptive information security in computer-aided systems // Automation and Remote Control. 2009. Т. 70. № 3. С. 491-501.

7. Кочеткова А.С. Применение нейронных сетей для мониторинга безопасности // Вестник Волгоградского государственного университета. Серия 9: Исследования молодых ученых. 2007. №6. С. 163-166.
8. Магницкий Н.А. Использование бинарной нейронной сети для обнаружения атак на ресурсы распределенных информационных систем // Динамика неоднородных систем. 2008. С. 200-205.
9. Марченко А.А., Матвиенко С.В., Нестерук Ф.Г. К обнаружению атак в компьютерных системах нейросетевыми средствами // Научно-технический вестник информационных технологий, механики и оптики. 2007. № 39. С. 83-93.
10. Скорик Ф.А., Саенко И.Б. Нейросетевая модель оценки состояния распределенной информационной системы // Сборник «Инновации в науке»: материалы XVI международной заочной научно-практической конференции. 2013. С. 151-156.
11. Тумоян Е.П. Разработка метода моделирования сетевых атак на основе нейронных сетей и вероятностных графов // Известия Южного федерального университета. Технические науки. 2009. Т. 90. № 1. С. 148-153.
12. Марков Г.А. Оценка и планирование испытаний программ с открытым исходным текстом с помощью нейросетевых технологий // Сборник Трудов Четвертой всероссийской конференции / под. ред. В.А.Матвеева. М.: НИИ РиЛТ МГТУ им. Н.Э.Баумана, 2013. С. 90-93.
13. Волчихин В.И., Иванов А.И. Естественное использование искусственных нейронных сетей в биометрии // Системы безопасности. 2002. № 3(45). С. 46-47.
14. Галкин В.А., Чернуха С.Н. Исследование быстродействия нейросетевого распознавателя почерка // Наука и образование: электронное научно-техническое издание. 2011. №12. Режим доступа: http://sntbul.bmstu.ru/doc/458173.html (дата обращения 01.05.2014)
15. Червяков Н., Евдокимов А., Галушкин А., Лавриненко И., Лавриненко А. Применение искусственных нейронных сетей и системы остаточных классов. М.:Физматлит, 2012. 280 с.
16. Басараб М.А., Вельц С.В. Нейросетевой подход к иерархическому представлению компьютерной сети в задачах информационной безопасности// Инженерный журнал: наука и инновации. 2013. № 2 (14). Режим доступа: http://engjournal.ru/catalog/it/security/534.html (дата обращения 29.04.2014)
17. Булдакова Т.И., Миков Д.А. Оценка информационных рисков в автоматизированных системах с помощью нейро-нечёткой модели // Наука и образование: электронное научно-техническое издание. 2013. № 11. Режим доступа:

http://technomag.bmstu.ru/doc/645489.html (дата обращения 01.05.2014)

18. Нейронная сеть, созданная в секретной лаборатории Google X. Режим доступа: http://hitech.newsru.com/article/7Jun2012/gglxbrains (дата обращения 01.05.2014).
19. Vicarious Solves CAPTCHA. Режим доступа: http://news.vicarious.com (дата обращения: 28.01.2014).
20. Писаренко И. Нейросетевые технологии в безопасности // Information Security. 2009. № 4. Режим доступа: http://itsec.ru/articles2/Oborandteh/neyrosetevye-tehnologii-v-biznese (дата обращения 01.05.2014).