Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Чикалина В.А. Применение искусственных нейронных сетей в обеспечении информационной безопасности // Академия педагогических идей «Новация». Серия: Студенческий научный вестник. – 2018. – №8 (август). – АРТ 451-эл. – 0,2 п.л. - URL: http: //akademnova.ru/page/875550

РУБРИКА: ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 004.056

Чикалина Виктория Андреевна
студентка 2 курса, факультет прикладной математики и информатики
Научный руководитель: Харитонова И.В., к.п.н., доцент
ФГАОУ ВО «Северный (Арктический) федеральный университет имени М.В. Ломоносова»
г. Коряжма, Российская Федерация
e-mail: public@narfu.ru

ПРИМЕНЕНИЕ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: В данной статье рассматриваются возможности применения искусственных нейронных сетей для решения практических задач информационной безопасности. Анализируются особенности и преимущества применения таких сетей.

Ключевые слова: искусственные нейронные сети, защита информации, информационная безопасность.

Chikalina Victoria
2nd year student, faculty of applied mathematics and informatics
Supervisor: I.Kharitonova, PhD, Associate Professor
FGAOU VO «Northern (Arctic) Federal University named after M.V. Lomonosov»
Koryazhma, Russian Federation

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

APPLICATION OF ARTIFICIAL NEURAL NETWORKS TO ENSURE INFORMATION SECURITY

Abstract: This article explores the possibilities of using artificial neural networks to solve practical problems of information security. The features and advantages of using such networks are analyzed.

Keywords: artificial neural networks, data protection, information security.

В современном мире необходимость защиты большого объема данных приводит к непрерывному поиску способов и методов обеспечения информационной безопасности. Ученые и исследователи разрабатывают различные подходы к проблеме обнаружения атак, в частности, одним из таких подходов является использование искусственных нейронных сетей.

Искусственные нейронные сети (ИНС) строятся по принципу организации и функционирования их биологических аналогов, то есть их основная идея заключается в совместной работе группы взаимодействующих друг с другом элементов. В отличие от необучаемых экспертных систем, нейронные сети проводят анализ информации и предоставляют возможность оценки согласования данных с характеристиками, которые они обучены распознавать. Точность такой оценки будет полностью зависеть от эффективности этапа обучения [1].

Существует два варианта обучения ИНС: обучение с учителем (предъявляются значения входных и желательных выходных сигналов); обучение без учителя (предъявляются входные данные, а выходные формируются самостоятельно) [2].

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

На основании всего вышесказанного можно выделить ряд особенностей и преимуществ систем обнаружения атак на основе ИНС:

– возможность работы системы в режиме реального времени;

– гибкость и адаптивность алгоритмов;

– способность анализировать неполные и/или искаженные данные из сети;

– «изучение» ранее не встречаемых характеристик атак и выделение их особенностей.

Помимо преимуществ, так же существуют и недостатки систем обнаружения атак на основе ИНС, которые являются продолжением достоинств. К ним можно отнести:

– невозможность описать поведение системы в целом или отдельных её элементов из-за стохастического характера функционирования системы;

– проблемы с обучением системы, которые связаны с формированием большого количества атак.

В настоящее время многие компании эффективно используют ИНС при решении задач обеспечения безопасности: отслеживание подозрительных финансовых сделок, обнаружение мошеннических операций, обеспечение информационной безопасности и т.п. К таким примерам можно отнести:

– ПО Falcon, разработанное компанией HNC Software Inc., позволяет выявлять и предотвращать большое количество мошеннических операций с банковскими картами;

– компанией Nestor разработано основанное на использовании ИНС, экспертных систем и статических методов семейство систем PRISM, которое помогает обнаружению мошенничества с кредитными и дебетовыми картами;

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

– ПО KnowledgeSeeker было разработано фирмой Angoss для управления рисками, а так же для идентификации злоумышленников, прогнозирующее с высокой долей вероятности задержки выплат по кредитам [3].

ИНС в системах обеспечения информационной безопасности достаточно эффективны при решении задач анализа трафика, аудита без данных, эвристического детектирования вредоносных атак и новых типов вирусов.

На сегодняшний день роль искусственных нейронных сетей при обеспечении информационной безопасности трудно переоценить, если учитывать, как быстро растет объем накопленной информации. Данное направление является весьма перспективным и в будущем будет продолжать развиваться и совершенствоваться.

Список использованной литературы:

1. Крыжановский, А. В. Применение искусственных нейронных сетей в системах обнаружения атак / А. В. Крыжановский. // Технические науки. – 2008. – №2 (18), часть 1. – С. 104-105.
2. Круглов, В. В. Искусственные нейронные сети. теория и практика / В. В. Круглов, В. В. Борисов. – М. : Горячая линия - Телеком, 2002. – 382 с.
3. Нейросетевые технологии в безопасности [Электронный ресурс]. – Режим доступа : http://www.itsec.ru/articles2/Oborandteh/neyrosetevye-tehnologii-v-biznese, свободный. – [Дата обращения: 01.08.2018]

Дата поступления в редакцию: 07.08.2018 г.
Опубликовано: 11.08.2018 г.