Учреждение образования
«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»

УДК 004.056.53:032.26

КОЧУРКО
Павел Анатольевич

ОБНАРУЖЕНИЕ СЕТЕВЫХ АТАК НА КОМПЬЮТЕРНЫЕ СИСТЕМЫ НА ОСНОВЕ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность

Минск 2012

Работа выполнена в Учреждении образования «Брестский государственный технический университет»

Научный руководитель:	**Головко Владимир Адамович**, доктор технических наук, профессор, заведующий кафедрой интеллектуальных информационных технологий УО «Брестский государственный технический университет».
Официальные оппоненты:	**Бобов Михаил Никитич,** доктор технических наук, профессор, начальник отдела управления высоких технологий ОАО «АГАТ-системы управления»; **Образцов Владимир Алексеевич,** кандидат физико-математических наук, доцент, доцент кафедры информационных систем управления Белорусского государственного университета
Оппонирующая организация:	Учреждение образования «Военная академия Республики Беларусь»

Защита состоится «07» июня 2012 года в 16.00 на заседании совета по защите диссертаций Д 02.15.06 при учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, г. Минск, ул. П. Бровки, 6, корп. 1, ауд. 232-1, тел. (8-017) 293-89-89, e-mail: dissovet@bsuir.by.

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

КРАТКОЕ ВВЕДЕНИЕ

Технологии обнаружения атак – важное звено в цепи средств обеспечения информационной безопасности, противостоящих угрозам реализации уязвимостей. Каждая вторая организация в течение 2009–2010 годов зафиксировала различные атаки на свои информационные ресурсы, а 45,6% из них подверглись целенаправленному нападению. В 2011 году глобальный ущерб от атак на компьютерные информационные технологии превысил 250 миллиардов долларов в год.

К основным недостаткам существующих подходов к обнаружению атак (в первую очередь – на основе правил) можно отнести слабую способность обнаружения новых, неизвестных ранее или модифицированных атак; недостаточно высокую степень адаптивности подобных систем; необходимость постоянного обновления баз правил, а значит – зависимость качества функционирования системы от компании-разработчика и качества сигнатур, полученных от поставщика.

Для того чтобы нивелировать данные недостатки, исследователи обращаются к большому количеству технологий (статистический анализ, деревья решений, искусственные иммунные системы, нечёткая логика и др.) Особо стоит выделить подходы на основе искусственных нейронных сетей, поскольку они сочетают высокое качество распознавания и классификации со способностью к адаптации и обобщению данных. Разработка техники обнаружения и распознавания атак, основанной на искусственных нейронных сетях, позволит избежать проблем, характерных для большинства подходов, поскольку нейросетевая система способна с высоким качеством обнаруживать как известные, так и новые атаки. Кроме того, такая система сможет обновляться как стандартным способом – базы обученных детекторов от разработчика – так и обучаться самостоятельно.

Программная модель системы обнаружения сетевых атак, реализующая комплекс нейросетевых методов анализа сетевой активности, обнаружения и распознавания атак в реальном времени, позволит снизить потери от несанкционированного доступа к информации и нарушений политики информационной безопасности.

В диссертационной работе предлагается новое решение задачи обнаружения и распознавания сетевых атак на компьютерные системы детекторами и классификатором на основе рециркуляционных нейронных сетей. Оно объединяет в едином подходе парадигмы обнаружения аномалий и обнаружения некорректного поведения для лучшего распознавания известных атак, а также обнаружения новых и модифицированных сетевых атак.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с крупными научными программами (проектами) и темами

Диссертационные исследования выполнялись в рамках научно-исследовательских работ при поддержке Белорусского республиканского фонда фундаментальных исследований при НАН Беларуси «Нейросетевые методы обнаружения и идентификации сетевых атак на компьютерные системы» (2004–2006 гг., Т04-347, № госрегистрации 20042037) и «Нейросетевой модуль активной защиты компьютерных сетей от сетевых вторжений в реальном времени» (2008–2009 гг., Б08Б-003/792-3, № госрегистрации 20081933), а также гранта Министерства образования Республики Беларусь «Нейросетевые методы анализа и прогнозирования сетевой активности для обнаружения атак на компьютерные сети» (2006 г., ГБ-06/601, № госрегистрации 20063373).

Цель и задачи исследования

Целью работы является разработка нейросетевых методов и методик анализа сетевого трафика для обнаружения сетевых атак на компьютерные системы и создание программной системы обнаружения атак в реальном сетевом окружении.

Для достижения цели необходимо решить следующие задачи:

1. Разработать нейросетевую методику обнаружения сетевых атак в компьютерных системах на основании анализа данных сетевого трафика.
2. Разработать методику интеграции технологий обнаружения аномалий и злоупотреблений для уменьшения уровней ошибок первого и второго рода.
3. Разработать нейросетевой метод распознавания типов и классов атак исходя из полученного трафика.
4. Разработать прототип программной системы, реализующей данные методы в реальном сетевом окружении.
5. Исследовать эффективность разработанных методик и методов на тестовых базах данных сетевого трафика, в реальном сетевом окружении и режиме реального времени.

Объектом исследования являются системы обнаружения сетевых атак на компьютерные системы. *Предметом* исследования являются методы нейронных сетей для обнаружения сетевых атак на компьютерные системы.

Положения, выносимые на защиту

1. Методика обучения и функционирования детектора сетевых атак на основе рециркуляционной нейронной сети, способного в автоматическом режиме выделять отличительные характеристики сетевых соединений и определять принадлежность входного образа к тому классу соединений, на котором он был обучен.

2. Методика совместного функционирования нейросетевых детекторов аномалий и злоупотреблений, не требующая определения пороговых значений для отдельных детекторов, интегрирующая обнаружение аномалий и обнаружение некорректного поведения в единый алгоритм и позволяющая обнаруживать известные сетевые атаки с точностью 98% и новые сетевые атаки с точностью 92%.

3. Метод распознавания сетевых атак классификатором на базе рециркуляционных нейронных сетей, функционирование которого основано на получении совокупной оценки из выходных данных детекторов отдельных классов, позволяющий распознавать сетевые атаки и благодаря наращиваемости архитектуры дающий возможность автоматически адаптировать классификатор к новым классам сетевых атак, переводя их из разряда аномалий в известное поведение.

4. Исследовательский макет программной системы обнаружения сетевых атак, основанный на классификаторе на базе рециркуляционных нейронных сетей, способный обнаруживать и распознавать известные и модифицированные сетевые атаки в режиме реального времени.

Личный вклад соискателя

Содержание диссертации отражает личный вклад автора. Он заключается в обосновании возможности использования нейросетевого подхода в системе обнаружения атак, разработке методик и методов обучения и функционирования нейросетевых детекторов отдельных классов и совокупного классификатора для обнаружения и распознавания сетевых атак, программной реализации данных подходов и проведении экспериментов по исследованию и подтверждению результатов.

Определение целей и задач исследований, интерпретация и обобщение полученных результатов проводились совместно с научным руководителем – д-м техн. наук, профессором В.А. Головко.

Апробация результатов диссертации

Результаты диссертационных исследований представлены на 19 научных конференциях, в том числе 15 международных: «Исследования и разработ-

ки в области машиностроения, энергетики и управления» (Гомель, 2005, 2006, 2007, 2008); «International Conference on Pattern Recognition and Information Processing» (Минск, 2005); «Intelligent Data Acquisition and Advanced Computing Systems» (София, 2005, Дортмунд, 2007, Прага, 2011); «Современные информационные технологии» (Браслав, 2005, 2006); «International Conference on Neural Networks and Artificial Intelligence» (Брест, 2006); «Нейроинформатика» (Москва, 2007); «International Joint Conference on Neural Networks» (Орландо, 2007); «Современные информационные компьютерные технологии» (Гродно, 2008); «International PhD Workshop OWD» (Висла, 2008).

Кроме того, результаты были представлены на Международной выставке вооружений и военной техники MILEX (Минск, 2007); на Международных специализированных выставках по телекоммуникациям и информационным технологиям TIBO (Минск, 2007, 2009, 2010); выставке «Перспективные технологии и системы» (Брест, 2008).

Опубликованность результатов диссертации

Основные положения диссертации опубликованы в 28 научных публикациях общим объемом 11,19 авторских листа. Из них 9 статей в изданиях, соответствующих п.18 Положения о присуждении ученых степеней и присвоении ученых званий в Республике Беларусь (объемом 5,74 авторских листа); 16 статей – в материалах 12 международных конференций, 4 республиканских конференций, а также в 3 научных и научно-практических журналах, не входящих в Перечень ВАК.

В зарубежных открытых источниках найдено 30 работ, ссылающихся на данные публикации. Среди них 11 статей в научных журналах (в том числе с импакт-факторами до 2,9), 14 статей в сборниках трудов и тезисов международных научных конференций, а также диссертации на соискание ученых степеней магистра (США, Мексика) и кандидата наук (Канада).

Структура и объем диссертации

Диссертационная работа состоит из введения, общей характеристики работы, четырех глав с краткими выводами по каждой главе, заключения, библиографического списка и приложений. В первой главе выполнен обзор современных методов обнаружения атак, рассмотрено состояние данной области науки в работах различных отечественных и зарубежных исследователей, анализируются исходные данные и производится постановка задачи. Во второй главе производится разработка нейросетевых методик обнаружения вредоносной сетевой активности, реализации технологий обнаружения аномалий и злоупотреблений в детекторах на базе рециркуляционных нейронных сетей. Третья глава содержит результаты разработки нейросетевого подхода к распознаванию

типов и классов атак, методику построения и функционирования совокупного нейросетевого классификатора. В четвертой главе разрабатывается макет программной системы, реализующей предварительный анализ сетевого трафика и разработанные методы и методики нейросетевого обнаружения и распознавания атак, производится тестирование в режиме реального времени. В приложениях приведены графические и табличные материалы для основных разделов, а также представлены акты об использовании результатов диссертационной работы в области информационной безопасности и о внедрении результатов работы в учебный процесс учреждения образования «Брестский государственный технический университет».

Общий объем диссертации составляет 168 страниц, в том числе 97 страниц основного текста, 45 иллюстраций на 21 странице, 49 таблиц на 22 страницах и 2 приложения на 28 страницах. Диссертация содержит библиографический список из 129 наименований на 11 страницах и список работ соискателя из 28 наименований на 3 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ

Во **введении** показана актуальность темы диссертационной работы, и определены основные направления исследований.

Первая глава посвящена изучению существующих подходов к обнаружению и распознаванию сетевых атак. Приведены основные понятия, рассмотрены варианты нарушений информационной безопасности, в том числе сетевые атаки. Показаны тенденции увеличения количества и разнообразия сетевых атак на компьютерные системы и наносимого этими атаками ущерба в мировом масштабе. Обоснована необходимость анализа сетевого трафика для обнаружения сетевых атак. Описаны два основных подхода к обнаружению атак: обнаружение аномальной деятельности и обнаружение некорректного поведения или злоупотреблений. В системах обнаружения атак необходимо сочетать оба эти подхода с целью извлечения максимума из достоинств каждого и нивелирования недостатков. Рассмотрены существующие методы обнаружения атак, такие как методы на основе правил, статистические методы, нейросетевые методы и другие. Выявлены недостатки представленных подходов, к которым относятся сложность формирования правил и отсутствие адаптивности к новым атакам, сложность задания профилей поведения и определения пороговых значений, зависимость от баз данных правил и сложность алгоритмов альтернативных подходов. В свою очередь, нейросетевые методы, благодаря способности искусственных нейронных сетей к обобщению, адаптации и самоорганизации

являются перспективным инструментом для качественного обнаружения известных и новых сетевых атак.

Во **второй главе** представлены основные принципы построения детекторов сетевых атак на основе нелинейных рециркуляционных нейронных сетей. Определяется процесс предварительной обработки данных, производится анализ архитектурных особенностей искусственных нейронных сетей и разрабатывается методика обучения и функционирования нейросетевых детекторов атак.

Схема обнаружения сетевых атак основана на анализе собранных характеристик TCP-соединений в режиме реального времени. Процесс функционирования нейросетевой системы обнаружения атак включает в себя перехват трафика и его анализ с целью получения характеристик, формирование обучающих и тестовых выборок, предварительную обработку данных и основной этап – нейросетевой анализ данных с целью обнаружения атаки.

Обнаружение аномалий характеризуется поиском сетевой активности, отличающейся от известного нормального поведения субъектов системы. Вследствие этого необходимо знание характеристик нормального поведения – нормальных сетевых соединений. Основной проблемой реализации обнаружения аномалий является сложность формализации нормального поведения для автоматического получения его характеристик. Для решения данной проблемы предложены нейродетекторы на базе нелинейных рециркуляционных нейронных сетей (РНС), которые при обучении на нормальном трафике в автоматическом режиме смогут получить и сохранить для дальнейшего использования информацию о явных и неявных закономерностях поведения.

В процессе обучения весовые коэффициенты РНС настраиваются таким образом, чтобы минимизировать среднеквадратичную ошибку для всех тренировочных входных векторов. Итогом такого обучения станет то, что в процессе функционирования РНС подаваемые на вход вектора будут восстанавливаться на выходе тем более точно, чем больше они схожи с векторами из тренировочного набора. Сильно выделяющиеся вектора, в свою очередь, будут восстанавливаться недостаточно корректно. Данная схема идеально подходит для применения РНС в качестве детекторов аномалий: если обучение производить на нормальной сетевой активности, то РНС автоматически инкапсулирует в себе информацию о профиле нормального поведения субъекта.

Для определения степени подобия входного вектора с векторами из обучающей выборки предлагается численная характеристика – ошибка реконструкции вектора:

$$E^k = \sum_{j=1}^{N(X)} (\bar{X}_j^k - X_j^k)^2, \qquad (1)$$

где $N(X)$ - размерность входного вектора X. Чем меньше ошибка реконструкции (1), тем больше входной вектор похож на нормальный. Если $E^t > T$, где T – некий заданный для данной РНС порог, то соединение признаётся атакой, иначе – нормальным соединением.

Представленный подход с небольшими изменениями предложено использовать для *обнаружения злоупотреблений*. Способность РНС к автоматическому формированию профиля сетевой активности на основании тренировочного набора соединений может быть использована для построения шаблонов вредоносной сетевой активности. Нелинейные РНС могут обучаться на наборе из соединений-атак и в дальнейшем использоваться для определения принадлежности проверяемого входного соединения либо к атакам (если ошибка реконструкции (1) меньше порога), либо к нормальным соединениям.

Таким образом, нелинейные РНС могут использоваться для построения единообразных детекторов аномалий и детекторов злоупотреблений. Сочетание обоих подходов в рамках одной системы позволяет избежать некоторых недостатков, присущих каждой из технологий в отдельности, не теряя при этом их достоинств. Это, во-первых, позволяет снизить ошибки первого и второго рода; во-вторых, возможные неточности, связанные с недостаточным качеством обучения одного из детекторов могут быть устранены применением второго детектора.

При совместном использовании детекторов, построенных на различных технологиях, существует сложность принятия окончательного решения. В свою очередь, построение ансамбля из детекторов одинаковой природы позволяет анализировать не только двоичные вектора результатов, но и формировать общее решение из выходной информации самих детекторов.

Совместное использование детекторов аномалий и злоупотреблений на базе РНС одинаковой архитектуры (см. рисунок 1), обученных до одинакового уровня ошибки, позволяет произвести принятие решения исходя из ошибок реконструкции (1) на обоих детекторах:

$$\begin{cases} X \in A_N, \ \textit{если} \ \ E_A \le E_3, \\ X \in A_P, \ \textit{если} \ \ E_A > E_3, \end{cases} \qquad (2)$$

где E_A – ошибка реконструкции детектора аномалий, E_3 – ошибка реконструкции детектора злоупотреблений, A_N – нормальные соединения, A_P – соединения-атаки.

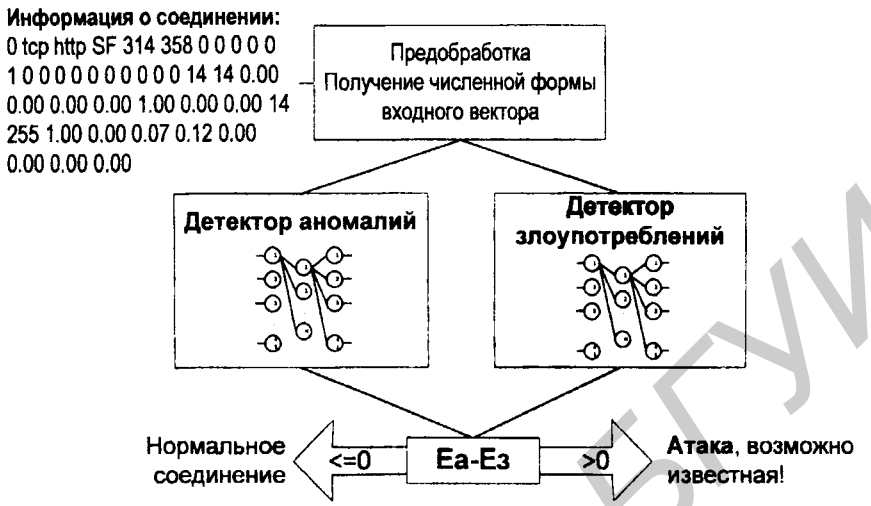

Рисунок 1 – Схема совместного функционирования детекторов аномалий и злоупотреблений на базе РНС

Необходимое условие возможности применения данного подхода – одинаковое количество синаптических связей в детекторах и одинаковая среднеквадратичная ошибка, до которой производилось обучение. В противном случае ошибки реконструкции будут несравнимы, и можно будет применять только принятие решения каждым из детекторов по отдельности, с последующим принятием общего решения на базе двоичных векторов результатов.

Экспериментальные результаты показали, что архитектурные особенности РНС существенно не влияют на качество работы системы. Детектор аномалий и детектор злоупотреблений на базе РНС способны обнаруживать известные и неизвестные атаки с высоким качеством, но совместное функционирование детекторов обладает более высокой точностью обнаружения атак, чем каждый из детекторов по отдельности: точность классификации при совместном функционировании превышает 98% на известных атаках и до 92% на наборе данных из модифицированных и неизвестных атак. Для любого уровня значимости от 0,005 до 0,05 мощность ансамбля трёхслойных РНС-детекторов составляет от 0,9895 до 0,9985 и превышает мощность каждого из детекторов по отдельности.

Третья глава посвящена решению задачи распознавания сетевых атак при помощи классификаторов, основанных на детекторах на базе РНС. Предлагаются варианты построения нейросетевых детекторов для распознавания классов и типов сетевых атак, сравнивается их эффективность. Описывается автор-

ская методика формирования и функционирования совокупного классификатора на базе нейросетевых детекторов.

Детекторы отдельных классов атак являются производным от детекторов злоупотреблений на базе РНС. Нейросетевой детектор определяет сходство входного вектора с векторами из тренировочного набора. При обучении РНС не на всём наборе вредоносного трафика, а только на выборке из атак конкретного класса, детектор сможет определить принадлежность входного образа именно к данному классу атак. Далеко отстоящие вектора (ошибка реконструкции (1) превышает пороговое значение) в этом случае не будут являться нормальными соединениями, а могут быть охарактеризованы как соединения, не принадлежащие данному классу атак.

Данные детекторы способны оценивать принадлежность входного вектора к классам по отдельности. Для распознавания сетевой атаки и получения ответа на вопрос, к какому классу она относится, детекторы отдельных классов объединяются в общий *классификатор*. Он отличается от широко распространённых методов тем, что совокупная оценка строится исходя из оценок детекторов одинаковой природы, отвечающих за один класс.

Предложенный классификатор (рисунок 2) состоит из N детекторов отдельных классов на базе рециркуляционных нейронных сетей, каждый из которых имеет порог T_i, и при реконструкции входного образа выдаёт ошибку реконструкции E_i. Данные значения можно сравнивать, если все индивидуальные детекторы имеют одинаковые архитектурные особенности (например, количество нейронов скрытого слоя) и условия обучения (минимальная среднеквадратичная ошибка). Подобный подход был применен при совместном функционировании детекторов аномалий и злоупотреблений. При выполнении данных условий решение о принадлежности входного образа к одному из классов может приниматься *по минимальной абсолютной ошибке реконструкции*:

$$\begin{cases} X \in A_m, \\ E_m = \min\limits_i E_i . \end{cases} \qquad (3)$$

Существенным достоинством данного подхода является полная независимость от порогов детекторов, а значит – отсутствие необходимости их вычисления. В свою очередь, недостатком является недостаточная гибкость и жесткие требования по архитектуре и обучению детекторов. Учитывая, что нейродетекторы описывают совершенно различные классы, обучение на которых может производиться также с разным успехом и, более того, в разное время, данный недостаток становится очень серьёзным.

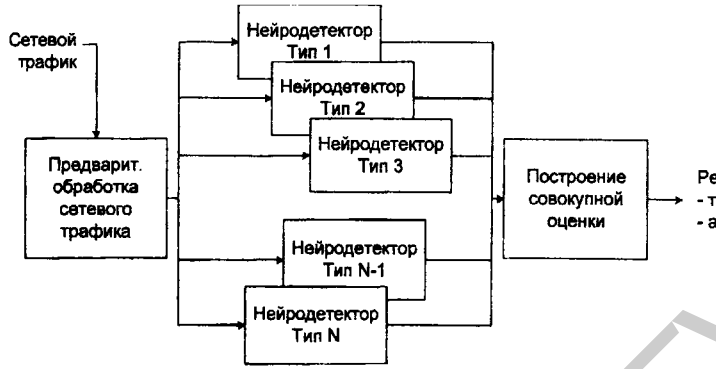

Рисунок 2 – Схема общего классификатора из нескольких нейродетекторов отдельных классов

Для приведения оценок детекторов, обученных в разных условиях, к сравнимым значениям, ошибка реконструкции может быть масштабирована по порогу: $\delta_i = E_i / T_i$ – относительная ошибка реконструкции. Чем меньше δ_i, тем более вероятна принадлежность входного образа X к классу A_i. Поэтому совокупная оценка может определяться по *минимальной относительной ошибке реконструкции*:

$$\begin{cases} X \in A_m, \\ \delta_m = \min\limits_i \delta_i . \end{cases} \qquad (4)$$

При обучении отдельных РНС-детекторов пороги T_i находятся для каждого детектора независимо от других детекторов. Однако значения порогов имеют существенное влияние на общее поведение системы. Следовательно, необходимо решить задачу настройки порогов детекторов T_i таким образом, чтобы уменьшить ошибки неверной классификации. Для этого предложен алгоритм настройки, изменяющий пороги отдельных детекторов в зависимости от взаимных значений ошибок классификации

Одним из аргументов против технологии обнаружения злоупотреблений является тот факт, что невозможно знать заранее, как будет выглядеть атака, и поэтому обучать систему на известных шаблонах априори неверно.

Система, использующая метод совокупного классификатора, может гибко изменяться и подстраиваться под новые входные данные. Если при анализе очередного входного образа ни один из детекторов не определяет принад-

лежность данного вектора к своему классу, может быть зарезервирован дополнительный класс. Входной вектор помещается в хранилище, в котором будут накапливаться столь же неизвестные вектора до тех пор, пока не будет набрано их количество, достаточное для обучения дополнительного частного детектора. После обучения данный детектор будет функционировать наряду с остальными.

Таким образом, изначально в системе может быть только детектор аномалий, обученный на нормальном трафике. В дальнейшем, при обнаружении им аномальных соединений – атак – для их последующего распознавания могут быть обучены соответствующие детекторы (см. рисунок 3). За счёт этого может быть достигнута большая гибкость СОА.

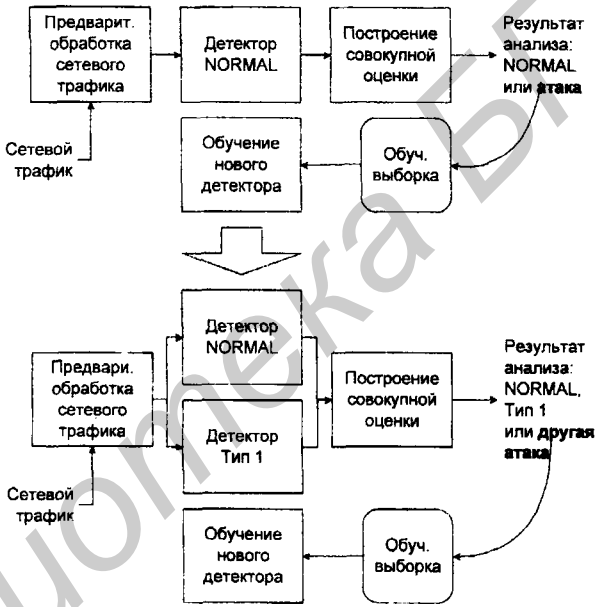

Рисунок 3 – Режим работы совокупного классификатора с генерацией нового детектора

Тестирование разработанных методик показало, что точность обнаружения и распознавания известных атак совокупным классификатором на базе РНС-детекторов отдельных классов находится на уровне 99%, а качество обнаружения неизвестных атак – на уровне 98%. В зависимости от количества входящих в классификатор детекторов от 80% до 98% обнаруженных неизвестных атак распознаются как атаки класса «неизвестная атака».

В качестве критериев для сравнения эффективности предложенного подхода с существующими методами использовались следующие показатели: *FPR*

– уровень ложных срабатываний, *FNR* – уровень пропуска цели, *ACC* – точность классификации, *CR* и CR_i – уровень распознавания в рамках всего набора данных или *i*-го класса атак. Для обучения и тестирования детекторов использовалась база данных DARPA/KDD, содержащая атаки 22 типов, принадлежащие четырём классам – DOS, U2R, R2L, Probe.

Методы, не использующие нейронные сети, имеют ошибки *FPR* и *FNR* до 10%, а при высоком качестве распознавания атак класса DOS (CR_{dos}=97–99%), качество распознавания атак классов R2L и U2R значительно ниже – CR_{r2l}=1–46%, CR_{u2r}=2–50%. В свою очередь, нейросетевые подходы показывают значительно более высокие результаты. Наименьший показатель вероятности ошибок первого и второго рода – 0,3–1,2%, и распознавание всех классов атак на уровне 98–99%. Однако, при таких высоких показателях качества обнаружения и распознавания известных атак не обеспечивается обнаружение новых, неизвестных атак.

В таблице 1 показано, что ансамбль из детекторов аномалий и злоупотреблений, а также совокупный классификатор имеют ошибки первого и второго рода на уровне лучших нейросетевых методов. Результаты распознавания типов и классов атак, представленные в таблице 2, показывают, что 99% известных атак и нормальных соединений распознаются правильно.

Таблица 1 – Результаты тестирования методик обнаружения атак

Технология	FPR, %	FNR, %	ACC, %
Детектор аномалий	12,93	0,36	97,18
Детектор злоупотреблений	0,04	2,73	97,96
Совместное функционирование	0,02	1,79	98,36
Совокупный классификатор 4-х классов атак	3,74	0,01	99,23
Совокупный классификатор 22-х типов атак	1,94	0,14	99,51

Таблица 2 – Результаты тестирования методики распознавания атак

	CR_{dos}, %	CR_{probe}, %	CR_{r2l}, %	CR_{u2r}, %	CR, %
Совокупный классификатор 4-х классов атак	99,31	99,12	97,86	100,0	98,78
Совокупный классификатор 22-х типов атак	99,78	95,18	97,60	100,00	99,40

Таким образом, результаты, полученные при использовании предложенных методов и методик обнаружения и распознавания атак на основе РНС, значительно превосходят результаты других исследователей.

В **четвёртой главе** рассматриваются структура, основные модули и тестирование нейросетевой системы обнаружения атак. Структура системы представлена на рисунке 4.

Рисунок 4 – Схема работы нейросетевой системы обнаружения атак

Макет системы реализован для операционной системы GNU/Linux с использованием программного обеспечения с открытым исходным кодом BroIDS, mawk, bash, tee, gcc, распространяемого по лицензии GNU Public License.

Для *тестирования* нейросетевой системы обнаружения атак (НСОА) был выбран узловой вариант реализации: в локальной сети две рабочие станции играли роли жертвы (установлена НСОА) и злоумышленника.

Нейросетевой детектор аномалий обучался на нормальной сетевой активности «жертвы». Сетевые атаки сканирования и на отказ в обслуживании, производились с компьютера-«злоумышленника» с помощью специализированных программ, распространяемых в сети Интернет. НСОА в режиме реаль-

ного времени производила анализ трафика, генерацию детекторов для новых классов атак, обнаружение новых и распознавание известных атак.

Тестирование показало, что классификатор обнаруживает известные и новые атаки с точностью до 99%, причем от 91% до 98% известных атак корректно распознаются. Благодаря наращиваемости архитектуры, с переводом новых обнаруженных атак в разряд известных при обучении новых детекторов увеличивается точность обнаружения и качество распознавания. Сравнение с известными системами показало, что одни и те же известные и новые атаки НСОА обнаруживает с точностью 99,92%, а Snort, Prelude, Tamandua, Firestorm с точностью до 55%.

В **приложениях** представлены табличные данные, дополняющие основное содержание диссертации, включающие описание всех параметров сетевых соединений и развёрнутые результаты экспериментов. Также представлены акты и справки о внедрениях результатов диссертации в технологический процесс предприятий и учебный процесс УО «БрГТУ».

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

Диссертационная работа посвящена разработке нейросетевого подхода к обнаружению и распознаванию сетевых атак, объединяющего парадигмы обнаружения аномалий и обнаружения злоупотреблений. Получены следующие результаты:

1. Разработаны методика обучения и функционирования нейросетевого детектора атак на базе рециркуляционной нейронной сети. Детектор обнаруживает аномалии по отношению к тому классу образов, на котором обучен, тем самым определяя принадлежность входного образа к данному классу. Обучение детектора может производиться на нормальных сетевых соединениях, после чего данный детектор способен оценивать наличие аномалии в сетевом трафике. Аналогично при обучении на соединениях-атаках данный детектор способен оценивать принадлежность входного образа к такой атаке. Отличительными особенностями данного подхода являются возможность автоматического накопления информации о нормальном или аномальном трафике без формирования правил или статистических расчетов, единообразие реализации обнаружения аномалий и обнаружения злоупотреблений, способность функционировать на зашумленных и модифицированных образах [2–А, 3–А, 8–А, 13–А, 15–А, 19–А].

2. Разработан обобщённый алгоритм работы нейросетевой системы обнаружения атак, который базируется на перехвате и предварительной обра-

ботке сетевого трафика узла или сегмента сети, с последующим анализом нейросетевыми детекторами. Показана возможность формирования общей оценки ансамбля из нейросетевых детекторов аномалий и злоупотреблений без определения пороговых значений отдельных детекторов. Такой ансамбль детекторов функционирует с более высокой точностью, чем каждый из детекторов по отдельности и способен функционировать с точностью классификации свыше 98% на известных атаках и до 92% на наборе данных из модифицированных и неизвестных атак [1–А, 2–А, 5–А, 16–А, 21–А].

3. Предложена структура классификатора на основе нейросетевых детекторов отдельных классов, который отличается высоким качеством распознавания известных атак и способностью обнаруживать новые атаки благодаря интеграции в одном подходе технологий обнаружения аномалий и злоупотреблений. В отличие от известных подходов, в данном совокупном классификаторе каждый детектор способен оценивать принадлежность входного образа только к одному классу. Независимо от того, класс это нормальных соединений или атак, оценка строится единообразно [3–А, 17–А, 19–А, 21–А].

4. Разработана методика формирования и функционирования классификатора наращиваемой архитектуры, которая позволяет адаптировать систему к новым классам атак и переводить их обнаружение из разряда аномалий в обнаружение злоупотреблений. Отличительной особенностью данной методики является сочетание возможностей автоматической генерации детекторов для новых классов атак и дополнения классификатора специально обученными детекторами. Результаты распознавания сетевых атак с помощью данного метода выше, чем показанные другими применявшимися ранее методами, качество распознавания достигает 99,4% [3–А, 4–А, 19–А, 28–А].

5. Реализован исследовательский макет системы обнаружения сетевых атак на базе предложенного классификатора, который способен анализировать сетевой трафик в режиме реального времени, обнаруживать и распознавать известные и новые атаки в процессе их совершения. Данная система производит перехват сетевого трафика и его предварительную обработку с приведением к виду, аналогичному формату базы данных Darpa/KDD, обеспечивает формирование обучающих выборок и обучение нейросетевых детекторов, генерацию, настройку и функционирование нейросетевого классификатора. [6–А, 7–А, 9–А].

6. Проведены эксперименты по тестированию нейросетевой системы обнаружения атак. Система, построенная на классификаторе из нейродетекторов отдельных классов, может функционировать в режиме реального времени, обнаруживая как известные, так и новые атаки с точностью до 99%, причём от 91% до 98% известных атак корректно распознаются. Наращивание системы

путём генерации детекторов новых классов улучшает качество обнаружения и позволяет распознавать новые атаки [6–А, 8–А, 28–А].

Рекомендации по практическому использованию результатов

Разработанные в рамках диссертационной работы методики обнаружения и распознавания сетевых атак на компьютерные системы используют в качестве детекторов атак рециркуляционные нейронные сети. Ключевыми свойствами данного подхода являются наращиваемость архитектуры и адаптивность к изменяющемуся поведению субъекта сети, благодаря чему система обнаружения атак обнаруживает не только известные, но и модифицированные и неизвестные сетевые атаки.

Методика построения и функционирования нейросетевого классификатора предназначена для использования в качестве подсистемы обнаружения атак в составе систем защиты сетевого периметра. Для обеспечения активной реакции на обнаруженное вторжение необходима интеграция системы обнаружения атак с межсетевым экраном и программными средствами проактивной защиты.

Система на базе нейросетевого классификатора способна улучшить степень защищенности системы, функционируя в качестве дополнительного эвристического анализатора сетевого трафика наряду со стандартными сигнатурными системами обнаружения атак и антивирусными комплексами либо в их составе.

Разработанный подход обеспечивает единообразие анализа сетевого трафика как отдельного узла сети, так и сегмента ЛВС. В данной ситуации достаточно установить систему обнаружения атак на входе в данный сегмент сети – это позволит защититься от внешних угроз.

Метод распознавания образов классификатором на базе нейродетекторов может с успехом применяться в различных задачах распознавания образов.

Результаты диссертационных исследований внедрены в технологический процесс ЧТДУП «АкваБел-Брест», ООО «Папилио» и ЧТЭУП «МегаТрансТрейд», а также применены в УО «БрГТУ» в учебном курсе «Методы защиты компьютерных сетей» для студентов специальности 40 03 01 – Искусственный интеллект.

Перспективным направлением дальнейших исследований является организация взаимодействия нейросетевых детекторов сетевых атак в распределённой многоагентной системе обнаружения атак.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

Статьи в научных журналах

1–А. Golovko, V. Intrusion recognition using neural networks / V. Golovko, P. Kochurko // Computing. – 2005. – Vol. 4, Issue 3. – P. 37–42.

2–А. Golovko, V. Some Aspects of Neural Network: Approach for Intrusion Detection / V. Golovko, P. Kochurko // NATO Science. Mathematics, Physics and Chemistry. – Springer, 2005. – Vol. 196: Cyberspace Security and Defense: Research Issues. – P. 349–382.

3–А. Кочурко, П.А. Совокупность детекторов на основе рециркуляционных нейронных сетей для распознавания класса сетевых атак / П.А. Кочурко // Вестн. Брестск. гос. техн. ун-та. Сер. Физика, математика, информатика. – 2005. – №5.– С. 61–66.

4–А. Кочурко, П.А. Нейросетевой детектор аномалий / П.А. Кочурко // Известия Белорусской инженерной академии. – 2005. – №1(19)/2. – С. 78–81.

5–А. Кочурко, П.А. Совокупный детектор атак на основе нейронных сетей / П.А. Кочурко // Инженерный вестник. – 2006. – №1(21)/1. – С. 90–96.

6–А. Кочурко, П.А. Распознавание классов сетевых атак: применение нейронных сетей различных архитектур / П.А. Кочурко // Вестн. Брестск. гос. техн. ун-та. Сер. Физика, математика, информатика. – 2006. – №5. – С. 32–35.

7–А. Войцехович, Л.Ю. Система обнаружения атак как основной элемент защиты компьютерной сети / Л.Ю. Войцехович, В.А. Головко, П.А. Кочурко // Вестн. Брестск. гос. техн. ун-та. Сер. Физика, математика, информатика. – 2008. – №5. – С. 12–19.

8–А. Кочурко, П.А. Построение нейросетевой системы обнаружения и распознавания атак / П.А. Кочурко, В.А. Головко // Вестн. Брестск. гос. техн. ун-та. Сер. Физика, математика, информатика. – 2010. – №5, – С. 7–13.

9–А. Neural Network and Artificial Immune Systems for Malware and Network Intrusion Detection / V. Golovko [et al.] // Studies in Computational Intelligence. – Springer, 2010. – Vol. 263: Advances in Machine Learning II. – P. 458–513.

Статьи в прочих научных и научно-практических изданиях

10–А. Головко, В.А. Некоторые аспекты применения нейронных сетей для обнаружения атак / В.А.Головко, Д.В. Каменда, П.А. Кочурко // Вестн. Брестск. гос. техн. ун-та. Сер. Физика, математика, информатика. – 2004. – №5. – С. 35–39.

11–А. Головко, В.А. Нейросетевая система для обнаружения и распознавания сетевых атак / В.А. Головко, П.А. Кочурко, В.Г. Брич // Управление защитой информации. – 2006. – №1 (36). – С. 45–46.

12–А. Кочурко, П.А. Нейросетевое распознавание классов сетевых атак / П.А. Кочурко // Управление защитой информации. – 2006. – №4 (39). – С. 420–421.

Статьи в материалах научных конференций

13–А. Кочурко, П.А. Применение нейронных сетей для обнаружения сетевых атак / П.А. Кочурко // Новые математические методы и компьютерные технологии в проектировании, производстве и научных исследованиях: сборник материалов VIII Респ. науч. конф. студентов и аспирантов, Гомель, 14-16 марта 2005 г. / Гом. гос. ун-т им. Ф. Скорины; редкол.: Д.Г. Лин [и др.]. – Гомель, 2005. – С. 238.

14–А. Кочурко, П.А. Комбинированный нейросетевой подход для обнаружения аномалий / П.А. Кочурко // Исследования и разработки в области машиностроения, энергетики и управления: сб. материалов V Междунар. межвуз. науч.-тех. конф. студентов, магистрантов и аспирантов (посвящ. 60-летию Победы в Великой Отечественной войне), Гомель, 12-13 мая 2005 г. / Гом. гос. техн. ун-т им. П.О. Сухого. – Гомель, 2005. – С. 324–327.

15–А. Golovko, V. Intrusion Recognition Using Neural Networks / V. Golovko, P. Kochurko // Intelligent Data Acquisition and Advanced Computing Systems (IDAACS'2005): proceedings of the Third IEEE Workshop, Sofia, 5-7 September 2005. – Sofia, 2005. – P. 108–111.

16–А. Kochurko, P. Neural Network Approach to Anomaly Detection Improvement / P. Kochurko, V. Golovko // Pattern Recognition and Information Processing (PRIP'05): proceedings of the 8th International Conference, Minsk, 18-20 May 2005 / Belarusian State University of Informatics and Radioelectronics; Eds.: R. Sadykhov [et al.]. – Minsk, 2005. – P. 416–419.

17–А. Кочурко, П.А. Анализ входных данных для нейросетевой системы обнаружения атак в различных сетевых окружениях / П.А. Кочурко // Современные проблемы математки и вычислительной техники: материалы IV Республиканской научной конференции молодых учёных и студентов, Брест, 28-30 ноября 2005 г. / Брест. гос. техн. ун-т; редкол.: В.В. Тур [и др.]. – Брест, 2005. – С. 11–13.

18–А. Kochurko, P. Fusion of Detectors on the Basis of Recirculation Neural Networks for Intrusion Detection / P. Kochurko // International Conference on Neural Networks and Artificial Intelligence (ICNNAI'2006): proceedings, Brest, 31 May - 2

June, 2006 / Brest State Technical University; eds.: V.A. Golovko [et al.]. – Brest, 2006. – P. 44–48.

19–А. Кочурко, П.А. Нейросетевой анализ и принятие решения об обнаружении сетевой атаки / П.А. Кочурко // Новые математические методы и компьютерные технологии в проектировании, производстве и научных исследованиях: материалы IX Респ. конф. студентов и аспирантов, Гомель, 13-15 марта 2006 г. / Гом. гос. ун-т им. Ф. Скорины; редкол.: Д.Г. Лин [и др.] . – Гомель, 2006. – С. 275.

20–А. Dimensionality Reduction and Attack Recognition using Neural Network Approaches / V. Golovko [et al.] // The 2007 International Joint Conference on Neural Networks (IJCNN): proceedings, Orlando, 12-17 August 2007. – Orlando, 2007. – P. 2734–2739.

21–А. Neural Network Ensembles For Intrusion Detection / V. Golovko [et al.] // Intelligent Data Acquisition and Advanced Computing Systems (IDAACS'2007): proceedings of the Fourth IEEE Workshop, Dortmund, 5-7 September 2007. – Dortmund, 2007. – P. 578 –583.

22–А. Кочурко, П.А. Распознавание классов сетевых атак: подходы на основе нейронных сетей / П.А. Кочурко // Нейроинформатика-2007: материалы IX Всероссийской научной конференции, Москва, январь 2007 / МИФИ (ГУ). – Москва, 2007. – С. 27–30.

23–А. Кочурко, П.А. Рециркуляционные нейронные сети в задачах обнаружения сетевых атак / П.А. Кочурко // Исследования и разработки в области машиностроения: материалы VII Международной межвузовской научно-технической конференции студентов, магистрантов и аспирантов, Гомель, 12-14 мая 2007 г. / Гом. гос. техн. ун-т. – Гомель, 2007. – С. 420–423.

24–А. Кочурко, П.А. Нейросетевой подход к распознаванию сетевых атак / П.А. Кочурко // Современные информационные компьютерные технологии (mcIT-2008): материалы международной научно-практической конференции, Гродно, 21-24 апреля 2008 г. / Гродн. гос. Ун-т им. Я. Купалы. – Гродно, 2008. – С. 90–93.

25–А. Кочурко, П.А. Некоторые аспекты обнаружения аномальной сетевой активности / П.А. Кочурко // Исследования и разработки в области машиностроения: материалы VIII Международной межвузовской научно-технической конференции студентов, магистрантов и аспирантов, Гомель, 28-29 апреля 2008 г. / Гом. гос. техн. ун-т. – Гомель, 2008. – С. 390–393.

26–А. Kachurka, P. Neural Network Approach To Real-Time Intrusion Detection / P. Kachurka // X International PhD Workshop (OWD'2008): proceedings, Wisla, 18-21 October 2008. – Wisla, 2008. – P. 470–474.

27–А. Кочурко, П.А. Настройка порогов нейросетевых детекторов для распознавания классов сетевых атак / П.А. Кочурко // Современные проблемы математики и вычислительной техники: материалы VI Республиканской научной конференции молодых учёных и студентов, Брест, 26-28 ноября 2009 г. / Брест. гос. техн. ун-т; редкол.: В.С. Рубанов [и др.]. – Брест, 2009. – С. 18–20.

28–А. Kachurka, P. Neural Network Approach to Real-Time Network Intrusion Detection and Recognition / P.Kachurka, V.Golovko // The 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications: proceedings, 15–17 September 2011. – Prague, 2011. – P. 393–397.

РЭЗЮМЭ

Качурка Павел Анатольевіч

Выяўленне сеткавых атак на камп'ютарныя сістэмы на аснове нейрасеткавых тэхналогій

Ключавыя словы: выяўленне атак, штучныя нейронныя сеткі, распазнаванне вобразаў, інфармацыйная бяспека, дэтэктар анамалій, дэтэктар злоўжыванняў.

Мэта працы: распрацоўка нейрасеткавых метадаў і методык аналізу сеткавага трафіку для выяўлення сеткавых атак на камп'ютарныя сістэмы і стварэнне праграмнай сістэмы выяўлення нападаў у рэальным сеткавым асяроддзі.

Метады даследавання: ўжываліся эксперыментальныя і тэарэтычныя метады – апарат штучных нейронных сетак, статыстычныя метады класіфікацыі і зніжэння памернасці, метады праграмнага мадэлявання.

Атрыманыя вынікі і іх навізна: распрацавана методыка навучання і функцыянавання дэтэктара сеткавых атак на аснове рецыркуляцыйнай нейронай сеткі, здольнага вызначаць прыналежнасць уваходнага вектара да таго класа злучэнняў, на якім ён быў навучаны, а таксама методыка сумеснага функцыянавання нейрасеткавых дэтэктараў анамалій і злоўжыванняў, якая не патрабуе вызначэння парогавых значэнняў для асобных дэтэктараў. Прапанаваны метад распазнавання сеткавых атак класіфікатарам на базе рецыркуляцыйных нейронных сетак з атрыманнем сукупнай ацэнкі з выходных дадзеных дэтэктараў асобных класаў. Распрацаваны даследчы макет праграмнай сістэмы выяўлення сеткавых атак, заснаваны на прапанаваным класіфікатары. Інтэграцыя ў рамках адзінага нейрасеткаваго падыходу выяўлення анамалій і злоўжыванняў дазволіла забяспечыць выяўленне і распазнаванне вядомых і новых атак ў рэжыме рэальнага часу.

Ступень выкарыстання: прапанаваныя метады і методыкі могуць прымяняцца ў сістэмах выяўлення атак ўзроўня вузла ў сукупнасці з міжсеткавым экранам і дазваляюць павысіць узровень абароненасці сістэм. Вынікі дысертацыйных даследаванняў укаранёныя ў тэхналагічны працэс ЧТДУП «Аквабел-Брэст», ТАА «Папіліа» і ЧТЭУП «МегаТрансТрэйд», а таксама прымяняюцца ў УА «БрДТУ» ў навучальным курсе «Метады абароны кампутарных сетак» для студэнтаў спецыяльнасці 40 30 01 – Штучны інтэлект.

Вобласць ужывання: абарона інфармацыйных сістэм ад несанкцыянаванага доступу.

РЕЗЮМЕ

Кочурко Павел Анатольевич

Обнаружение сетевых атак на компьютерные системы на основе нейросетевых технологий

Ключевые слова: обнаружение атак, искусственные нейронные сети, распознавание образов, информационная безопасность, детектор аномалий, детектор злоупотреблений.

Цель работы: разработка нейросетевых методов и методик анализа сетевого трафика для обнаружения сетевых атак на компьютерные системы и создание программной системы обнаружения атак в реальном сетевом окружении.

Методы исследования: применялись экспериментальные и теоретические методы – аппарат искусственных нейронных сетей, статистические методы классификации и снижения размерности, методы программного моделирования.

Полученные результаты и их новизна: разработана методика обучения и функционирования детектора сетевых атак на основе рециркуляционной нейронной сети, способного определять принадлежность входного образа к тому классу соединений, на котором он был обучен, а также методика совместного функционирования нейросетевых детекторов аномалий и злоупотреблений, не требующая определения пороговых значений для отдельных детекторов. Предложен метод распознавания сетевых атак классификатором на базе рециркуляционных нейронных сетей с получением совокупной оценки из выходных данных детекторов отдельных классов. Разработан исследовательский макет программной системы обнаружения сетевых атак, основанный на предложенном классификаторе. Интеграция в рамках единого нейросетевого подхода обнаружения аномалий и злоупотреблений позволила обеспечить обнаружение и распознавание известных и новых атак в режиме реального времени.

Степень использования: предложенные методы и методики могут применяться в системах обнаружения атак уровня узла в совокупности с межсетевыми экранами и позволяют улучшить уровень защищенности систем. Результаты диссертационных исследований внедрены в технологический процесс ЧТДУП «АкваБел-Брест», ООО «Папилио» и ЧТЭУП «МегаТрансТрейд», а также применяются в УО «БрГТУ» в учебном курсе «Методы защиты компьютерных сетей» для студентов специальности 40 03 01 – Искусственный интеллект.

Область применения: защита информационных систем от несанкционированного доступа.

SUMMARY

Kachurka Pavel Anatolievich

Detection of network intrusions on computer systems basing on neural network technologies

Keywords: intrusion detection, artificial neural networks, image recognition, information security, anomaly detector, misuse detector.

The aim of work: to develop a neural network methods and techniques for analyzing network traffic to detect network attacks on computer systems and the creation of software intrusion detection systems in a real network environment.

Investigation methods: the experimental and theoretical methods were used – the apparatus of artificial neural networks, statistical methods for classification and dimensionality reduction, methods of software modeling.

Obtained results and its novelty: a method for training and operation of the network intrusion detector based on a recirculation neural network is developed, which is able to determine the belonging of the input image to the training class, as well as the method of co-operation of neural anomaly and misuse detectors, which does not require determination of threshold values for individual detectors. A method for detection of network attacks with classifier based on the recirculation neural networks is proposed, which obtains estimates of the total output of the detectors of individual classes. Research model of a software intrusion detection system based on the proposed classifier is developed. Integration into a single neural network approach of the anomaly detection and misuse detection enabled the detection and recognition of known and new attacks in real time mode.

Extent of usage: the proposed methods and techniques can be applied in intrusion detection systems on the host level in conjunction with a firewall and can improve the systems information protection. The results of dissertation research have been implemented into the process of CHTDUP "AquaBel-Brest", LLC "Papilio" and CHTEUP "MegaTransTrade" and used in Brest state technical university in the course "Methods of protection of computer networks" for students majoring in 40 03 01 - Artificial Intelligence.

Field of application: protection of information systems against unauthorized access.

Научное издание

КОЧУРКО
Павел Анатольевич

ОБНАРУЖЕНИЕ СЕТЕВЫХ АТАК НА КОМПЬЮТЕРНЫЕ СИСТЕМЫ НА ОСНОВЕ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ

специальность
05.13.19 – Методы и системы защиты информации, информационная безопасность

Автореферат диссертации на соискание ученой степени кандидата технических наук

Подписано в печать 10.04.2012. Формат 60x84 1/16. Бумага офсетная.
Гарнитура «Таймс». Отпечатано на ризографе. Усл. печ. л. 1,63.
Уч.-изд. л. 1,5. Тираж 60 экз. Заказ 204.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
ЛИ №02330/0494371 от 16.03.2009. ЛП №02330/0494175 от 03.04.2009.
220013, Минск, П. Бровки, 6