УДК 004.056 DOI:10.31854/1813-324X-2020-6-4-120-126

Адаптация структуры диагностической искусственной нейронной сети при появлении новых обучающих примеров

А.В. Маликов[1*]

[1]Военная академия связи имени Маршала Советского Союза С.М. Буденного,
Санкт-Петербург, 194064, Российская Федерация
[*]Адрес для переписки: mkv.vas@yandex.ru

Информация о статье
Поступила в редакцию 19.09.2020
Принята к публикации 25.10.2020.

Ссылка для цитирования: Маликов А.В. Адаптация структуры диагностической искусственной нейронной сети при появлении новых обучающих примеров // Труды учебных заведений связи. 2020. Т. 6. № 4. С. 120–126. DOI:10.31854/1813-324X-2020-6-4-120-126

Аннотация: *По отчетам специалистов информационной безопасности, сохраняется тренд увеличения количества компьютерных инцидентов на объектах информационной инфраструктуры различных секторов экономики. Выявленные компьютерные инциденты подлежат диагностированию, в ходе которого выясняются характеристики нарушения безопасности информации (цель, причины, последствия и др.). Для решения задачи диагностирования компьютерных инцидентов наиболее перспективным путем является применение методов автоматизации сбора и обработки событий, происходящих вследствие реализации сценариев нарушений безопасности информации. Ввиду сильной вариативности данных сценариев, а также из-за совершенствования технологий реализации компьютерных атак, составить диагностические наборы событий на каждый компьютерный инцидент проблематично. Для решения классификационной задачи по отнесению диагностического набора данных (информационного образа компьютерного инцидента) к одному из возможных значений характеристики нарушения могут применяться искусственные нейронные сети. При этом успех решаемой задачи классификации зависит от выбора структуры сети, от количества и качества обучающих примеров. Целью работы является адаптация структуры искусственной нейронной сети, позволяющей при появлении новых обучающих примеров осуществлять достоверное диагностирование компьютерных инцидентов.*

Ключевые слова: *диагностирование, компьютерный инцидент, многослойный персептрон, автоэнкодер, характеристика нарушения безопасности.*

Введение

Диагностирование компьютерных инцидентов (КИ) является одной из основных задач системы управления системой защиты информации инфокоммуникационой системы. Задача диагностирования должна решаться по каждому КИ, обнаруживаемому в защищаемой системе. Под диагностированием КИ понимается процесс сбора и анализа данных о нарушении безопасности информации с целью идентификации значений характеристик данного нарушения, таких как тип, цель, причины, последствия и других, для принятия обоснованного решения по реагированию. В настоящее время задача диагностирования КИ решается, как правило, путем визуального поиска и сопоставления предварительно отобранных данных, представляющих собой записи журналов событий операционных систем, средств защиты информации, сведений из других источников (напри-мер, от систем контроля доступа в помещение). Имеющиеся средства защиты информации содержат общие характеристики нарушения безопасности информации (время обнаружения, идентификаторы, наименование нарушения), но не отвечают на вопросы касаемые целей, причин, последствий.

Для проведения диагностирования КИ требуется собрать данные практически из всех основных элементов инфокоммуникационной системы и охарактеризовать произошедшее нарушение. Следует отметить, что, несмотря на необходимость охвата максимального количества источников информации, диагностирование требуется проводить в минимально короткие сроки.

Перспективным путем снижения продолжительности диагностирования КИ при сохранении полноты охвата источников информации является

автоматизация рутинных операций. Процедура сбора данных для диагностирования автоматизирована достаточно давно и представлена различными программными продуктами [1]. Процедура анализа собранных данных вызывает затруднения, связанные с высокой динамикой фиксируемых действий пользователей и событий информационной системы, неопределенностью связей между рядом событий. При этом анализ осуществляется на достаточно сильно выраженном зашумленном фоне, образованном событиями, не имеющими отношения к нарушению безопасности.

Для анализа данных в подобных условиях широкое применение получили методы машинного обучения [2–6]. Обучение осуществляется путем нахождения закономерностей для имеющихся наборов исходных данных и соответствующих им правильных ответов, полученных в ходе проведенного диагностирования. Но для искусственных нейронных сетей (а именно – многослойных сетей прямого распространения) существует особенность, заключающаяся в том, что качество результата классификации в основном зависит от структуры искусственной нейронной сети и от количества доступных обучающих примеров. При этом размерности входного и выходного слоев задаются условиями решаемой задачи, а выбор размерности скрытого слоя осуществляется с учетом максимизации показателя качества искусственной нейронной сети Q. Следовательно, выбор оптимальной структуры искусственной нейронной сети для диагностирования КИ является актуальной задачей. Настоящая работа посвящена адаптации структуры искусственной нейронной сети, обеспечивающей сохранение достигнутого значения показателя качества при добавлении новых обучающих примеров в условиях ограничений на продолжительность времени обучения, а также описывает экспериментальную проверку полученных результатов.

Постановка задачи

В процессе функционирования системы защиты информации инфокоммуникационной системы, по результатам диагностирования, появляются новые обучающие примеры. С целью их дальнейшего использования необходимо оперативно, т. е. за минимально возможное время, провести дообучение нейронной сети. Возникает задача минимизации времени T_l, отводимого на обучение. Вместе с тем необходимо обеспечить сохранение ранее достигнутого показателя качества искусственной нейронной сети Q_f. Целевая функция задачи адаптации структуры искусственной нейронной сети для диагностирования КИ может быть представлена в виде:

$$\begin{cases} T_l \rightarrow \min \\ Q_n \geq Q_f \end{cases}, \quad (1)$$

где Q_n – значение показателя качества искусственной нейронной сети после каждого последующего обучения; Q_f – значение показателя качества искусственной нейронной сети, полученное при первоначальном обучении.

С целью определения параметров структуры нейронной сети необходимо провести вычислительный эксперимент.

Структура диагностической искусственной нейронной сети

Обнаружив компьютерный инцидент, система защиты информации осуществляет сбор данных от различных источников, к числу которых относятся журналы событий средств защиты информации, серверов и рабочих станций. Из всего объема этих данных интерес представляют только те, которые потенциально могут иметь отношение к нарушению безопасности информации. Остальные считаются информационным шумом. Иными словами, осуществляется преобразование из исходного множества зарегистрированных в инфокоммуникационной системе событий X в множество информативных диагностических признаков X', F: $X \rightarrow X'$, где $X = \{x_{tsob}^{ist}\}$; $ist = \overline{1, N_s}$; $tsob = \overline{1, N_{ts}}$; N_s – количество источников информации; N_{ts} – количество типов событий; $X' = \{x'_{tpr}\}$; $tpr = \overline{1, N_{tp}}$; N_{tp} – количество типов диагностических признаков.

Далее необходимо по имеющемуся набору диагностических признаков определить значения характеристик нарушения безопасности $hn_j^{zn} \in HN, j = \overline{1, N_{ch}}, zn = \overline{1, N_{zn}}$, где N_{ch} – количество характеристик нарушения безопасности, значения которых требуется определить в ходе диагностирования; N_{zn} – количество возможных значений j-ой характеристики нарушения безопасности. Таким образом, решение задачи диагностирования заключается в нахождении отображения множества информативных диагностических признаков X' на множество значений характеристик нарушения безопасности HN, $F: X' \rightarrow HN$. Множество характеристик нарушения безопасности HN фактически представляет собой детальное описание нарушения безопасности информации. Перечень основных характеристик нарушения безопасности приведен в таблице 1.

Характеристики нарушения безопасности (см. таблицу 1) делятся по способу определения значений на два типа: первичные и вторичные. Значения первичных характеристик определяются путем прямого измерения или расчета (например, идентификаторы пользователей, время и другие). В свою очередь, для определения значений вторичных характеристик требуется построить функциональные зависимости от значений диагностических признаков.

ТАБЛИЦА 1. Основные характеристики нарушения безопасности информации

TABLE 1. Main Characteristics of an Information Security Breach

Наименование	Значения	Тип
Объект воздействия	Автоматизированное рабочее место Серверное оборудование Сетевое оборудование	Первичная
Тип уязвимости	Уязвимости средств защиты информации Уязвимости операционных систем Уязвимости прикладного программного обеспечения	Первичная
Результаты реализации	Изменение Удаление Создание Блокировка и др.	Первичная
Время обнаружения	Момент времени обнаружения нарушения средствами зашиты информации	Первичная
Идентификатор атаки (компьютерного инцидента)	Наименование атаки, полученное от средств защиты информации	Первичная
Идентификатор пользователя	ID, предъявленный при входе в систему ID, полученный в результате анализа	Первичная
Адрес источника атаки	Сетевой адрес и порт источника атаки	Первичная
Адрес объекта атаки	Сетевой адрес, порт объекта атаки	Первичная
Цель реализации угрозы	Нарушение конфиденциальности информации Нарушение целостности информации Нарушение доступности информации	Вторичная
Источник нарушения	Внешний Внутренний	Вторичная
Стадия реализации	Разведка Проникновение Реализация Скрытие следов	Вторичная
Характер нарушения	Преднамеренное Непреднамеренное	Вторичная
Последствия	Значительный ущерб Незначительный ущерб	Вторичная
Повторяемость	Впервые обнаруженное нарушение Повторно обнаруженное нарушение	Вторичная
Тип атаки	DoS-атака Сканирование Компьютерный вирус Программная закладка и др.	Вторичная
Уровень риска	Критический Высокий Средний Низкий	Вторичная

Рассматривая задачу идентификации значения j-ой характеристики нарушения безопасности hn_j как частный случай задачи классификации, целесообразно использовать многослойный персептрон [7]. Процесс формирования структуры многослойного персептрона для решения задачи классификации подразумевает задание количества нейронов входного N_x, скрытого N_{skr} и выходного N_y слоев.

Количество нейронов входного слоя N_x устанавливается, исходя из количества типов диагностических признаков N_{tp}, используемых для диагностирования КИ, а также от соотношения d общего Δt и единичного $\Delta t'$ временных интервалов сбора признаков ($\Delta t = d \cdot \Delta t'$) $N_x = N_{tp} \cdot d$.

Количество нейронов выходного слоя N_y многослойного персептрона определяется в зависимости от количества возможных значений j-ой характеристики нарушения безопасности. Так, для идентификации бинарной характеристики нарушения безопасности используются два нейрона выходного слоя.

Количество нейронов скрытого слоя N_{skr} оценивается, исходя из количества весов нейронных связей, определяемых зависимостью, полученной Р. Хехт-Нильсеном для персептрона с одним скрытым слоем [8]:

$$N_{skr} = \frac{N_{wsv}}{N_x + N_y}, \tag{2}$$

$$\frac{N_y N_{exm}}{1 + log_2(N_{exm})} \leq N_{wsv} \leq \leq N_y \left(\frac{N_{exm}}{N_x} + 1\right)(N_x + N_y + 1) + N_y, \tag{3}$$

где N_{wsv} – определяемое количество синаптических связей; N_{exm} – количество элементов множества обучающих примеров.

Основываясь на доказательстве В.И. Арнольдом и А.Н. Колмогоровым теоремы о представлении непрерывной функции n-переменных $f(x_1, x_2, \ldots, x_n)$ в виде суммы непрерывных функций одного аргумента $f_1(x_1) + f_2(x_2) + \cdots + f_n(x_n)$, Р. Хехт-Нильсеном была доказана теорема о возможности построения искусственной нейронной сети, позволяющей осуществлять преобразование для каждого входного вектора в соответствующий ему выходной вектор. Преобразование задается любым множеством различающихся между собой обучающих примеров. Установлено, что такой искусственной нейронной сетью является персептрон с одним скрытым слоем, причем активационные функции его нейронов должны быть сигмоидными.

Исходя из теорем Арнольда – Колмогорова – Хехт-Нильсена, для решения задачи классификации достаточно использовать персептрон с одним скрытым слоем сигмоидных нейронов, число которых определяется по формулам (2, 3).

Определение количества нейронов скрытого слоя определяется путем решения задачи по максимизации значения показателя качества искусственной нейронной сети в заданных ограничениях на количество обучающих примеров N_{exm}:

$$Q(N_{skr}) \rightarrow \max_{N_{skr}}, \quad (4)$$

где $Q(N_{skr})$ – показатель качества созданной искусственной нейронной сети с числом нейронов скрытого слоя N_{skr}.

В качестве показателя качества искусственной нейронной сети может использоваться показатель F-мера, который вычисляется как среднее гармоническое показателей точности (precision, Pr) и полноты (recall, Rc):

$$F = \frac{2Pr * Rc}{Pr + Rc}. \quad (5)$$

Количество событий, произошедших в типовой инфокоммуникационной системе и влияющих на результат диагностирования КИ, может составлять от единиц до десятков тысяч, в зависимости от ширины временного интервала, количества охватываемых типов событий, представляющих собой диагностические признаки. Данное количество событий определяет размерность входного слоя искусственной нейронной сети, используемой для распознавания информационного образа нарушения безопасности информации. Для обучения такой нейронной сети требуется большой объем обучающих примеров. В связи с этим требуется проведение оптимизации структуры нейронной сети для недопущения негативного эффекта переобучения сети на ограниченном числе примеров, т. е. чтобы нейронная сеть смогла обобщать имеющиеся образы, а не просто их запоминать. С этой целью предлагается построение комбинированной искусственной нейронной сети, состоящей из кодирующей части автоэнкодера и многослойного персептрона [9, 10]. Проходя через кодирующую часть автоэнкодера, входные данные преобразуются в групповые диагностические признаки значительно меньшей размерности. Далее осуществляется классификация полученного набора групповых диагностических признаков на множестве значений одной характеристики нарушения безопасности. Структура комбинированной искусственной нейронной сети, применяемой для диагностирования КИ, приведена на рисунке 1. Подчеркивая предназначение рассматриваемой комбинированной нейронной сети, далее будем называть ее диагностической.

В общем виде зависимость значения j-ой характеристики нарушения безопасности от входного набора диагностических признаков X' с применением комбинированной искусственной нейронной сети имеет вид:

$$hn_j = f_3(f_2(f_1(W_1 \cdot X') \cdot W_2) \cdot W_3),$$

где $W_k \in W, k = \overline{1,3}$ - вектор весовых коэффициентов k-го слоя; f_k – функция активации нейронов k-го слоя.

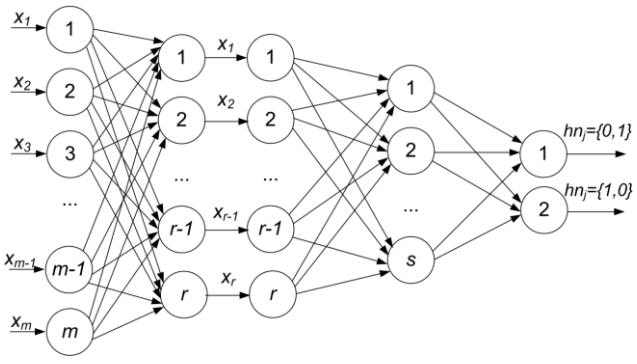

Рис. 1. Структура комбинированной искусственной нейронной сети для определения значения бинарной характеристики нарушения безопасности

Fig. 1. Structure of a Combined Artificial Neural Network for Determining the Value of a Binary Characteristic of a Security Breach

Значение на выходах диагностической искусственной нейронной сети представляет собой оценку степени соответствия значениям характеристики нарушения безопасности для предъявленной на входе совокупности диагностических признаков. Значения весовых коэффициентов W_k определяется путем обучения комбинированной искусственной нейронной сети.

Реализация диагностической искусственной нейронной сети

Для каждой определяемой вторичной характеристики нарушения безопасности информации предполагается своя диагностическая искусственная нейронная сеть. Обучение диагностических искусственных нейронных сетей осуществлялось на основе имеющейся базы данных о нарушениях безопасности информации, составленной экспертным путем. Экспериментальная база данных содержит описание двух характеристик нарушения безопасности «характер нарушения» и «последствия». Она состоит из 276 записей, которые включают наборы диагностических признаков из журналов событий для 20 рабочих станций. Для характеристики нарушения безопасности «характер нарушения» из 276 записей 113 соответствуют преднамеренному нарушению, а 163 – непреднамеренному нарушению. Для характеристики нарушения безопасности «последствия» реализации нарушения из 276 записей 164 соответствуют значительному ущербу, а 112 – незначительному.

Эксперименты проводились по следующей схеме. Первоначально осуществлялось формирование базы данных обучающих примеров, включающей в себя множество пар наборов диагностических признаков и соответствующих им значений характеристик нарушения безопасности. Данные пары предназначены для обучения комбинированных искусственных нейронных сетей и проверки их

готовности к функционированию. Затем в эту же базу данных сохраняются новые обучающие примеры, что требует изменение структуры нейронных сетей. Обучение осуществляется методом обратного распространения ошибки, в ходе которого происходит корректировка весовых коэффициентов каждой связи искусственных нейронов между собой [7].

Далее осуществлялось формирование структуры диагностических нейронных сетей. Размер входного слоя для всех диагностических нейронных сетей соответствует размеру вектора диагностических признаков. Для охвата исследуемых диагностических признаков на длительном интервале времени в ходе эксперимента размер входного слоя составил 32400. Выходной слой каждой комбинированной нейронной сети определяется по числу значений вторичной характеристики нарушения безопасности.

Размеры скрытых слоев автоэнкодера и персептрона первоначально выбирались, исходя из минимально достаточного согласно условию (2 и 3) Р. Хехт-Нильсена, и составляли 12 и 1, соответственно.

Для обучения и проверки качества искусственной нейронной сети база данных была разделена на две части. Первоначально 180 записей были взяты для обучения и 76 записей – для тестирования. Оценка качества комбинированной нейронной сети проводилась по показателю *F*-мера, значение которого рассчитывается согласно выражению (5). В свою очередь показатели точности *Pr* и полноты *Rc* вычисляются следующим образом:

$$Pr = \frac{TP}{TP + FP},$$

$$Rc = \frac{TP}{TP + FN},$$

где *TP* – количество записей, классифицируемых как истинное значение характеристики, в то время как оно истинное; *FP* – количество записей, классифицируемых как истинное значение характеристики, в то время как оно фактически ложное; *FN* – количество записей, классифицируемых как ложное значение, в то время как оно истинное.

В ходе вычислительного эксперимента со 180 обучающими примерами получены зависимости значений показателя *F*-меры от количества нейронов скрытых слоев автоэнкодера N_{ae} и персептрона N_{perc} для характеристики нарушения безопасности «характер воздействия», которые приведены на рисунке 2, а для характеристики нарушения безопасности «последствия» – на рисунке 3.

Как видно из рисунков 2 и 3, диагностические нейронные сети достигают максимума значения показателя *F*-меры при числе нейронов скрытого слоя автоэнкодера порядка 180 и 4 нейронов скрытого слоя персептрона. При увеличении числа нейронов скрытых слоев повышение показателя *F*-меры не наблюдается и впоследствии даже снижается из-за возникновения негативного эффекта переобучения.

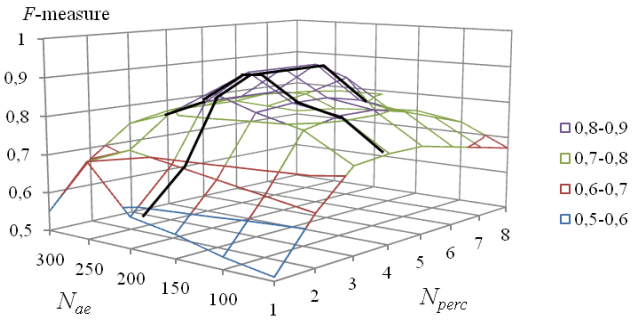

Рис. 2. Значения показателя *F*-мера для характеристики нарушения безопасности «характер воздействия»

Fig. 2. Values of the Indicator F-Measure for the Characteristic of a Security Breach «Nature of Impact»

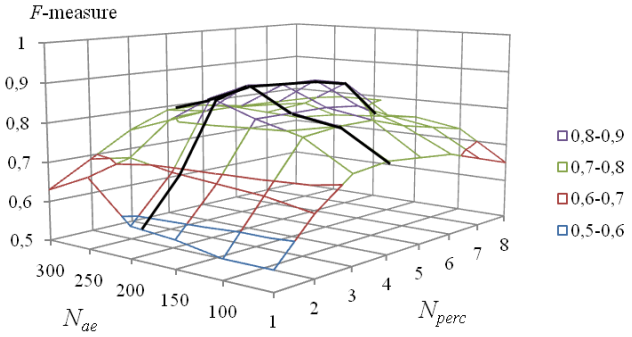

Рис. 3. Значения показателя *F*-мера для характеристики нарушения безопасности «последствия»

Fig. 3. Values of the F-Measure Indicator for the «Consequences» Characteristic of a Security Breach»

Затем количество обучающих примеров было увеличено до 194, а количество тестовых – до 82. В результате комбинированная нейронная сеть имеет высокие значения показателя точности определения значения бинарной характеристики нарушения безопасности при числе нейронов 186 для скрытого слоя автоэнкодера и 4 для скрытого слоя персептрона. Задача оптимизации времени обучения нейронной сети решается путем выбора минимально достаточного количества нейронов скрытого слоя без потери качества первоначально созданной сети. На рисунке 4 приведена зависимость значений показателей *F*-меры и продолжительности обучения T_l от структуры комбинированной искусственной нейронной сети на примере характеристики нарушения безопасности «характер воздействия». При увеличении количества нейронов время обучения возрастает, а значения показателей точности и полноты сначала остаются прежними, но затем снижаются. При уменьшении числа нейронов скрытых слоев вместе с незначительным снижением времени обучения снижаются значения показателей точности и полноты, что недопустимо по условиям задачи.

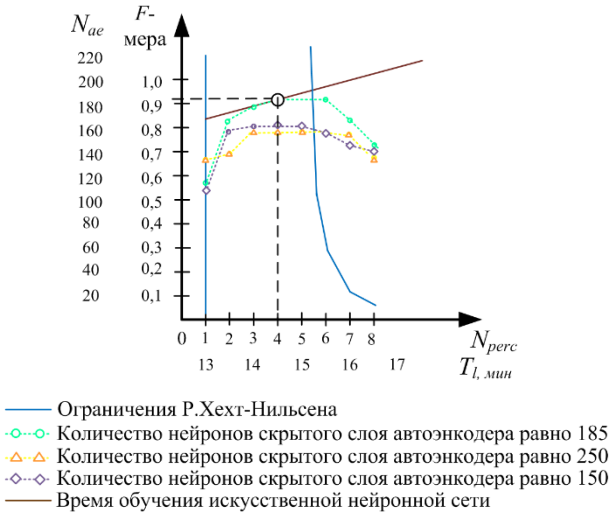

Рис. 4. Зависимости значений показателя *F*-мера и продолжительности обучения от структуры комбинированной искусственной нейронной сети

Fig. 4. Values of the Indicator F-Measure for the Characteristic of a Security Breach «Nature of Impact»

Данные результаты указывают на необходимость адаптации структуры диагностической нейронной сети при пополнении базы обучающих примеров, при этом для обучающих примеров числом до 200 нейронов скрытого слоя автоэнкодера целесообразно выбирать порядка 185, количество нейронов скрытого слоя персептрона – 4. С увеличением числа обучающих примеров на 14 значения показателя *F*-мера осталось прежним при увеличении числа нейронов скрытого слоя автоэнкодера на 6 (186–180) и сохранении 4 нейронов скрытого слоя персептрона.

Заключение

Таким образом, результаты вычислительного эксперимента подтвердили необходимость адаптации структуры диагностической нейронной сети с целью минимизации времени обучения при добавлении новых обучающих примеров. Учитывая реализуемость предложенной структуры комбинированной искусственной нейронной сети в виде программного средства, представляется возможным ее практическое применение в составе системы защиты информации типовой инфокоммуникационной системы. Своевременное и достоверное диагностирование позволит обеспечить высокую безопасность и тем самым устойчивость инфокоммуникационных систем.

Направления дальнейших исследований связываются с исследованием вопросов применения диагностических нейронных сетей для определения значений вторичных характеристик нарушений безопасности информации, зависящих от других, ранее определенных значений характеристик, в том числе и первичных, за счет добавления в структуру рекуррентных связей.

Список используемых источников

1. Kotenko I.V., Saenko I.B. Creating New-Generation Cybersecurity Monitoring and Management Systems // Herald of the Russian Academy of Sciences. 2014. Vol. 84. No. 6. PP. 424–431. DOI:10.1134/S1019331614060033

2. Feiya Lv., Wen C., Bao Z., Liu M. Fault diagnosis based on deep learning // Proceedings of the American Control Conference (ACC, Boston, USA, 6–8 July 2016). IEEE, 2016. PP. 6851–6856. DOI:10.1109/ACC.2016.7526751

3. Zou D.Q., Qin H., Jin H. UiLog: Improving Log-Based Fault Diagnosis by Log Analysis // Journal of Computer Science and Technology. 2016. No. 31(5). PP. 1038–1052. DOI:10.1007/s11390-016-1678-7

4. Fu Q., Lou J.G., Wang Y., Li J. Execution Anomaly Detection in Distributed Systems Through Unstructured Log Analysis // Proceedings of the 9th IEEE International Conference on Data Mining (Miami, USA, 6–9 December 2009). IEEE, 2009. PP. 149–158. DOI:10.1109/ICDM.2009.60

5. Nolle T., Seeliger A., Muhlhauser M. Unsupervised Anomaly Detection in Noisy Business Process Event Logs Using Denoising Autoencoders // Proceedings of the 19th International Conference on Discovery Science (DS, Bari, Italy, 19–21 October 2016). Lecture Notes in Computer Science. Cham: Springer, 2016. Vol. 9956. PP. 442–456. DOI:10.1007/978-3-319-46307-0_28

6. Sakurada M., Yairi T. Anomaly Detection Using Autoencoders with Nonlinear Dimensionality Reduction // Proceedings of the 2nd Workshop on Machine Learning for Sensory Data Analysis (MLSDA'14, Gold Coast, Australia, 2 December 2014). New York: Association for Computing Machinery, 2014. PP. 4–11. DOI:10.1145/2689746.2689747

7. Хайкин С. Нейронные сети: полный курс / пер. с англ. М.: Издательский дом «Вильямс», 2006. 1104 с.

8. Hecht-Nielsen R. Kolmogorov's Mapping Neural Network Existence Theorem // Proceedings of the 1st Annual International Conference on Neural Networks (San Diego, USA, 21–24 June 1987). IEEE, 1987. Vol. 3. PP. 11–15.

9. Маликов А.В., Авраменко В.С., Саенко И.Б. Модель и метод диагностирования компьютерных инцидентов в информационно-коммуникационных системах, основанные на глубоком машинном обучении // Информационно-управляющие системы. 2019. № 6(103). С. 32–42. DOI:10.31799/1684-8853-2019-6-32-42

10. Авраменко В. С., Маликов А.В. Диагностирование нарушений безопасности в инфокоммуникационных системах на основе комбинированной нейронной сети // VIII Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (Санкт-Петербург, Россия, 27–28 февраля 2019). СПб.: СПбГУТ, 2019. Т. 2. С. 14–19.

* * *

Adaptation of the Diagnostic Artificial Neural Network Structure When New Training Examples Appear

A. Malikov[1]

[1]Telecommunications Military Academy,
St. Petersburg, 194064, Russian Federation

Article info
DOI:10.31854/1813-324X-2020-6-4-120-126
Received 19st September 2020
Accepted 25th October 2020

For citation: Malikov A. Adaptation of the Diagnostic Artificial Neural Network Structure When New Training Examples Appear. *Proc. of Telecom. Universities.* 2020;6(4): 120–126. (in Russ.) DOI:10.31854/1813-324X-2020-6-4-120-126

Abstract: *In this paper we can see that identified computer incidents are subject for diagnostics, during which the characteristics of information security violations are clarified (purpose, causes, consequences, etc.). To diagnose computer incidents, we can use methods of automation while collection and processing the events that occur as a result of the implementation of scenarios for information security violations. Artificial neural networks can be used to solve the classification problem of assigning diagnostic data set (information image of a computer incident) to one of the possible values of the violation characteristic. The purpose of this work is to adapt the structure of an artificial neural network that allows the accuracy diagnostics of computer incidents when new training examples appear.*

Keywords: *diagnostics, computer incident, multi-layer perceptron, autoencoder, security violation characteristic.*

References

1. Kotenko I.V., Saenko I.B. Creating New-Generation Cybersecurity Monitoring and Management Systems. *Herald of the Russian Academy of Sciences*. 2014;84(6):424–431. DOI:10.1134/S1019331614060033
2. Feiya Lv., Wen C., Bao Z., Liu M. Fault diagnosis based on deep learning. *Proceedings of the American Control Conference, ACC, 6–8 July 2016, Boston, USA*. IEEE; 2016. p.6851–6856. DOI:10.1109/ACC.2016.7526751
3. Zou D.Q., Qin H., Jin H. UiLog: Improving Log-Based Fault Diagnosis by Log Analysis. *Journal of Computer Science and Technology*. 201631(5):1038–1052. DOI:10.1007/s11390-016-1678-7
4. Fu Q., Lou J.G., Wang Y., Li J. Execution Anomaly Detection in Distributed Systems through Unstructured Log Analysis. *Proceedings of the 9th IEEE International Conference on Data Mining, 6–9 December 2009, Miami, USA*. IEEE; 2009. p.149–158. DOI:10.1109/ICDM.2009.60
5. Nolle T., Seeliger A., Muhlhauser M. Unsupervised Anomaly Detection in Noisy Business Process Event Logs Using Denoising Autoencoders. *Proceedings of the 19th International Conference on Discovery Science, DS, 19–21 October 2016, Bari, Italy. Lecture Notes in Computer Science*. Cham: Springer; 2016. vol.9956. p.442–456. DOI:10.1007/978-3-319-46307-0_28
6. Sakurada M., Yairi T. Anomaly Detection Using Autoencoders with Nonlinear Dimensionality Reduction. *Proceedings of the 2nd Workshop on Machine Learning for Sensory Data Analysis, MLSDA'14, 2nd December 2014, Gold Coast, Australia*. New York: Association for Computing Machinery; 2014. p.4–11. DOI:10.1145/2689746.2689747
7. Khaikin, S.: Neural networks: A Comprehensive Foundation. Moscow: Williams Publ.; 2006. (In Russ.)
8. Hecht-Nielsen R. Kolmogorov's Mapping Neural Network Existence Theorem. *Proceedings of the 1st Annual International Conference on Neural Networks, 21–24 June 1987, San Diego, USA*. IEEE; 1987. vol.3. p.11–15.
9. Malikov A.V., Avramenko V.S., Saenko I.B. Model and Method for Diagnosing Computer Incidents in Information and Communication Systems Based on Deep Machine Learning. *Information and Control Systems*. 2019;6(103):32–42 (In Russ.) DOI:10.31799/1684-8853-2019-6-32-42
10. Avramenko V.S., Malikov A.V. Diagnosis of Security Breaches in Information and Communication Systems Based on Combination of a Neural Network. *Proceedings of the VIIIth International Conference on Infotelecommunications in Science and Education, 27–28 February 2019, St. Petersburg, Russia*. St. Petersburg: The Bonch-Bruevich Saint-Petersburg State University of Telecommunications Publ.; 2019. vol.2. p.14–19. (In Russ.)

Сведения об авторе:

МАЛИКОВ Альберт Валерьянович — адъюнкт кафедры автоматизированных систем специального назначения Военной академии связи имени Маршала Советского Союза С.М. Буденного, mkv.vas@yandex.ru
https://orcid.org/0000-0002-4285-5360