УДК 004.056
doi:10.31799/1684-8853-2019-6-32-42

Научные статьи
Articles

Модель и метод диагностирования компьютерных инцидентов в информационно-коммуникационных системах, основанные на глубоком машинном обучении

А. В. Маликов[а], *адъюнкт, orcid.org/0000-0002-4285-5360*
В. С. Авраменко[а], *канд. техн. наук, доцент, профессор, orcid.org/0000-0002-2452-0380*
И. Б. Саенко[а, б], *доктор техн. наук, профессор, orcid.org/0000-0002-9051-5272, ibsaen@comsec.spb.ru*
[а]*Военная академия связи, Тихорецкий пр., 3, Санкт-Петербург, 194064, РФ*
[б]*Санкт-Петербургский институт информатики и автоматизации РАН, 14-я линия В. О., 39, Санкт-Петербург, 199178, РФ*

Введение: *модели и методы диагностирования компьютерных инцидентов, фиксируемых в информационно-коммуникационных системах, являются важнейшими компонентами математического обеспечения систем защиты информации. Основным требованием, предъявляемым к процессу диагностирования, является оперативность выявления характеристик нарушения безопасности. Сложность этой задачи обусловлена объемностью и вариативностью исходных данных о нарушении безопасности информации.* ***Цель:*** *разработка модели диагностирования компьютерного инцидента и метода, позволяющего оперативно определять значения характеристик нарушения безопасности.* ***Результаты:*** *определение значений характеристик нарушения безопасности, важных для принятия решения по реагированию на выявленный компьютерный инцидент, осуществляется с использованием глубоких искусственных нейронных сетей. Особенностью структуры предложенной глубокой искусственной нейронной сети является то, что она объединяет кодирующую часть автоэнкодера и многослойный персептрон. Кроме того, метод реализует параллельный режим обработки информативных событий, произошедших в информационно-коммуникационной системе до обнаружения компьютерного инцидента, путем использования для каждой вторичной характеристики нарушения безопасности отдельной предложенной искусственной нейронной сети. Метод определения значений вторичных характеристик нарушения безопасности позволяет достигнуть достаточно высокого значения показателя оперативности диагностирования при приемлемых значениях показателей точности и полноты для искомых характеристик нарушения безопасности. Исследована зависимость значений показателей полноты и точности классификации от числа нейронов скрытого слоя. Экспериментально определено достаточное число нейронов скрытого слоя для достижения требуемой оперативности обучения.* ***Практическая значимость:*** *разработанные модель и метод могут быть реализованы на типовых программно-аппаратных средствах (серверах) информационно-коммуникационной системы организации. Их совместное использование с существующими моделями и методами мониторинга и диагностирования позволяет значительно повысить эффективность системы защиты информации.*

Ключевые слова *— компьютерный инцидент, диагностический признак, искусственная нейронная сеть, персептрон, автоэнкодер.*

Для цитирования: 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, с. 32–42. doi:10.31799/1684-8853-2019-6-32-42
For citation: 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. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2019, no. 6, pp. 32–42 (In Russian). doi:10.31799/1684-8853-2019-6-32-42

Введение

Увеличение количества, форм и способов вредоносных воздействий на информационно-коммуникационные системы как государственных организаций, так и коммерческого сектора, отражаемое в отчетах различных компаний сферы информационной безопасности [1, 2], стало катализатором совершенствования методов и средств защиты информации. На первый план стали выходить системы управления событиями, регистрируемыми от разнообразных средств защиты информации и элементов информационно-коммуникационных систем.

Помимо основных средств защиты информации, таких как средства антивирусной защиты, межсетевые экраны, системы обнаружения атак, средства разграничения и управления доступом, возможно применение дополнительных средств — сканеров защищенности, анализаторов журналов событий, SIEM-систем [3] и т. д. Возникает достаточно актуальная проблема эффективной обработки и анализа предоставляемой ими информации о нарушении.

Острота этой проблемы обусловлена следующими причинами:

— различием форматов отчетов об одном и том же виде нарушения, формируемых различными средствами (для автоматизации процесса диагностирования необходимо сведения о событиях приводить к единому формату);

— сложностью задачи определения взаимосвязи событий;

— наличием скрытых и распределенных во времени событий безопасности и т. д.

При этом оперативность принятия решения по реагированию на выявленный компьютерный инцидент зависит от эффективности процесса диагностирования. Под *диагностированием компьютерного инцидента* будем понимать процесс определения значений характеристик нарушения безопасности.

Существуют объективные трудности в построении системы диагностирования компьютерных инцидентов, которые вызваны:

— сложностью структуры информационных потоков в системе защиты;

— разнородностью средств защиты и автоматизации;

— необходимостью анализа большого количества событий и диагностических признаков.

В силу этого оперативное диагностирование компьютерных инцидентов является одной из актуальных ключевых задач мониторинга и управления системой защиты информации информационно-коммуникационной системы.

В настоящей статье рассматривается новый подход к диагностированию компьютерных инцидентов в информационно-коммуникационной системе, основанный на применении глубоких искусственных нейронных сетей (ИНС). При этом метод глубокого обучения используется совместно с существующими подходами к диагностированию.

Основной теоретический вклад работы заключается в следующем. Во-первых, обоснована необходимость рассмотрения задачи диагностирования компьютерных инцидентов в качестве отдельной функции системы защиты и возможность ее реализации на основе аппарата глубоких искусственных нейронных сетей. Во-вторых, предложены модель и метод диагностирования компьютерных инцидентов в информационно-коммуникационной системе, в основе которых применено глубокое машинное обучение. Наконец, экспериментально подтверждено, что реализация предложенного метода позволяет получить достаточно высокие значения показателя оперативности диагностирования, точности и полноты определяемых значений характеристик нарушения безопасности.

Состояние исследований в области диагностирования компьютерных инцидентов. Постановка задачи

Основные подходы к поиску, сбору и обработке событий, связанных с компьютерными инцидентами, отражены в ряде работ, например [4–7]. В них указывается, что важной особенностью анализа является необходимость автоматизации процедур сбора и обработки, так как количество событий, генерируемых информационно-коммуникационной системой, столь велико, что изучение журналов событий администратором безопасности вручную, без средств автоматизации, становится крайне неэффективным.

Для диагностирования выхода из строя оборудования информационно-коммуникационной системы предлагается [8, 9] применять ИНС. Журналы событий содержат данные об отказах системы, которые предварительно обрабатываются и передаются для поиска неисправности на вход ИНС.

Предложен подход [10–13], использующий ИНС для поиска атак и аномальных действий. Отмечена высокая точность полученных экспериментальных прогнозов и способность системы прогнозирования функционировать в режиме времени, близком к реальному.

Стремление к получению все большего количества информативных признаков из массива обрабатываемых данных послужило развитию глубоких ИНС. При этом до недавнего времени считалось нецелесообразным обучать глубокие ИНС (кроме сверточных нейронных сетей), поскольку процедуры итеративной оптимизации имели тенденцию «застревать» вблизи слабых локальных минимумов. Однако вскоре были предложены эффективные процедуры оптимизации с использованием обучения без учителя, которые продемонстрировали высокую производительность для глубоких нейронных архитектур [14].

Однако рассмотренные подходы не позволяют обеспечивать автоматическое диагностирование компьютерных инцидентов с высокой достоверностью в реальном или в близком к реальному масштабу времени. В настоящей статье мы предлагаем подход, который позволяет устранить эти недостатки.

Рассмотрим информационно-коммуникационную систему S в момент времени обнаружения компьютерного инцидента t_0. Для проведения диагностирования необходимо собрать из журналов средств автоматизации и защиты информации за определенный интервал времени Δt, предшествующий моменту времени обнаружения компьютерного инцидента t_0, зарегистрированные события $x_i \in X$, $i = \overline{1, N_{\text{с}}}$, где $N_{\text{с}}$ — количество событий; X — множество событий информационно-коммуникационной системы. Затем необходимо выбрать из всего множества X информативные события $x'_i \in X'$, $i = \overline{1, N_{\text{и.с}}}$, где $N_{\text{и.с}}$ — количество информативных событий; X' — множество информативных событий. После этого осуществляется анализ информативных событий с целью определить значения характеристик нарушения безопасности $hn_i \in HN$, $i = \overline{1, N_{\text{хар}}}$, где $N_{\text{хар}}$ — ко-

личество характеристик нарушения безопасности, используемых для принятия решения на реагирование; HN — множество характеристик нарушения безопасности.

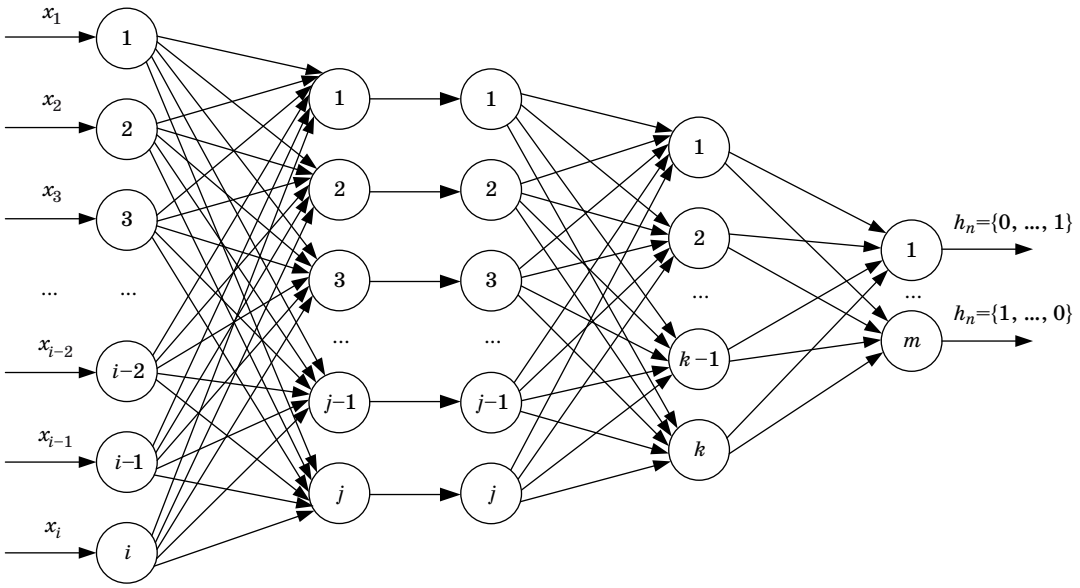
Таким образом, решение задачи диагностирования заключается в отыскании отображения множества информативных событий X' на множество значений характеристик нарушения безопасности HN, $F: X' \to HN$.

Поскольку для современных информационно-коммуникационных систем заданы высокие требования ко времени восстановления после компьютерного инцидента, то это влечет за собой потребность в минимизации времени T_d, отводимого на процесс диагностирования. При этом важно обеспечить соблюдение требований по достоверности результатов диагностирования. Целевая функция для разрабатываемой модели диагностирования может быть представлена в виде $T_d \to \min$, $D_{\text{диаг}} \geq D_{\text{треб}}$, где $D_{\text{диаг}}$ — фактическое значение показателя достоверности диагностирования; $D_{\text{треб}}$ — требуемое значение показателя достоверности диагностирования.

Модель диагностирования компьютерного инцидента

Для разработки метода диагностирования компьютерных инцидентов в информационно-коммуникационных системах необходимо прежде всего разработать модель диагностирования компьютерного инцидента. Такая модель должна позволять оперативно и достоверно определять значения характеристик нарушения безопасности. Для выполнения этих требований необходимо совершенствование способов автоматического сбора и анализа признаков компьютерного инцидента. С задачами подобного типа справляются ИНС, которые нашли весьма широкое применение в диагностировании информационных и технических систем. Это обусловлено тем, что обученная ИНС способна определить степень соответствия возможным значениям характеристики нарушения безопасности для входного множества признаков нарушения безопасности. Данный подход к идентификации значений характеристики нарушения безопасности успешно использовался в работах [15, 16]. Применительно к задаче диагностирования компьютерных инцидентов ИНС способна обобщать диагностические признаки с последующим нахождением значений характеристик нарушения безопасности, а также прогнозировать эти значения. Путем последовательного соединения двух разновидностей ИНС — автоэнкодера и многослойного персептрона — формируется глубокая ИНС (рис. 1).

Автоэнкодер снижает размерность вектора исходных данных X_i, $i = \overline{1, N_{\text{пр}}}$, где $N_{\text{пр}}$ — число признаков, подаваемых на вход ИНС [17]. Таким образом, осуществляется первый этап по обобщению входных данных (выполняется их сжатие): $X_i \xrightarrow{f_{\text{аэ}}} X_j$. В скрытом слое автоэнкодера формируются групповые диагностические признаки X_j. Далее они поступают на вход многослойного персептрона, который осуществляет процедуру обработки диагностических признаков и на выхо-



■ ***Рис. 1.*** Структура глубокой ИНС для определения значения m-арной характеристики нарушения безопасности

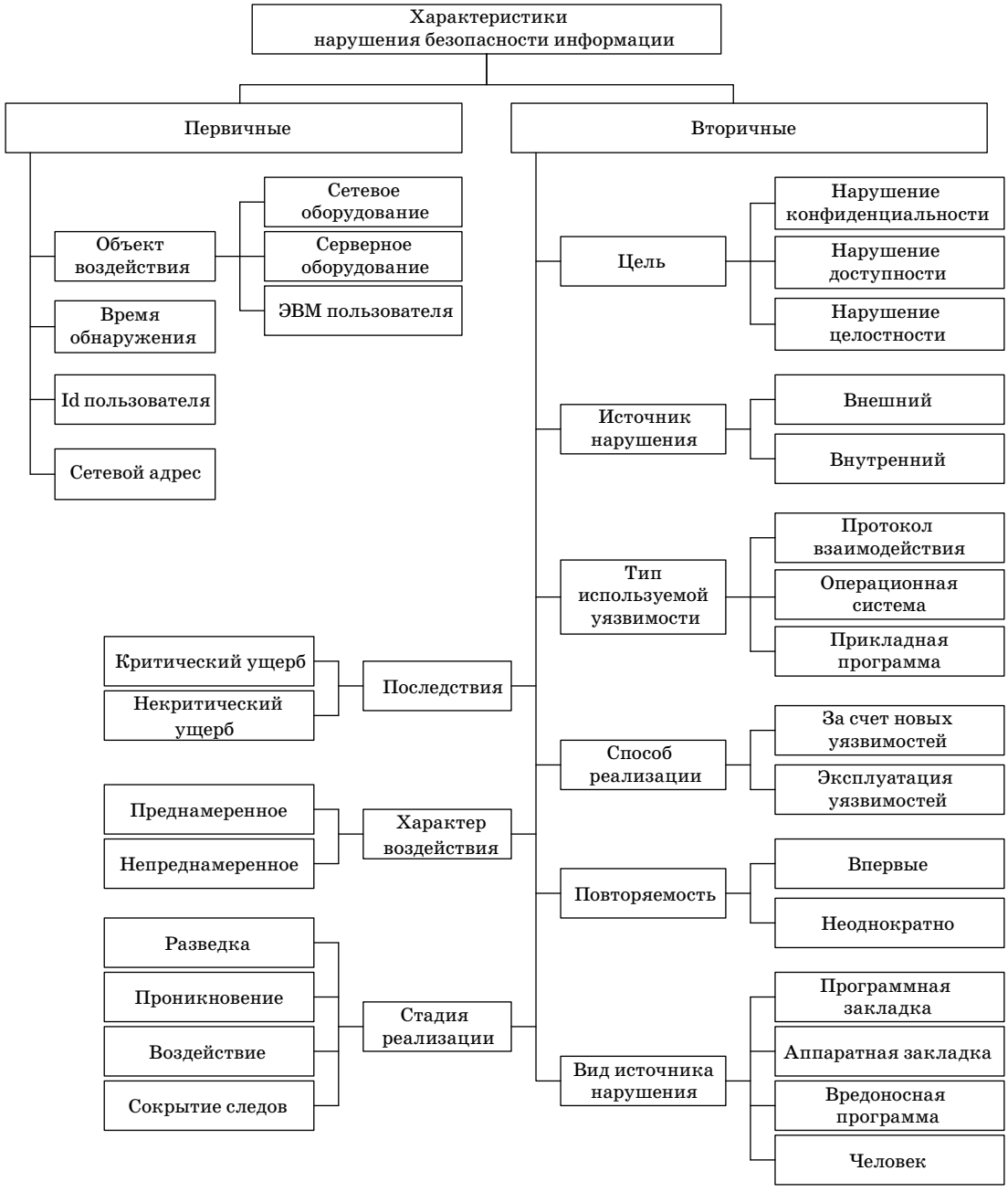
■ ***Fig. 1.*** Structure of a deep artificial neural network to determine the value of the m-ary characteristic of a security violations

де выдает набор значений m-арной характеристики нарушения безопасности, т. е. $X_j \xrightarrow{F} HN$.

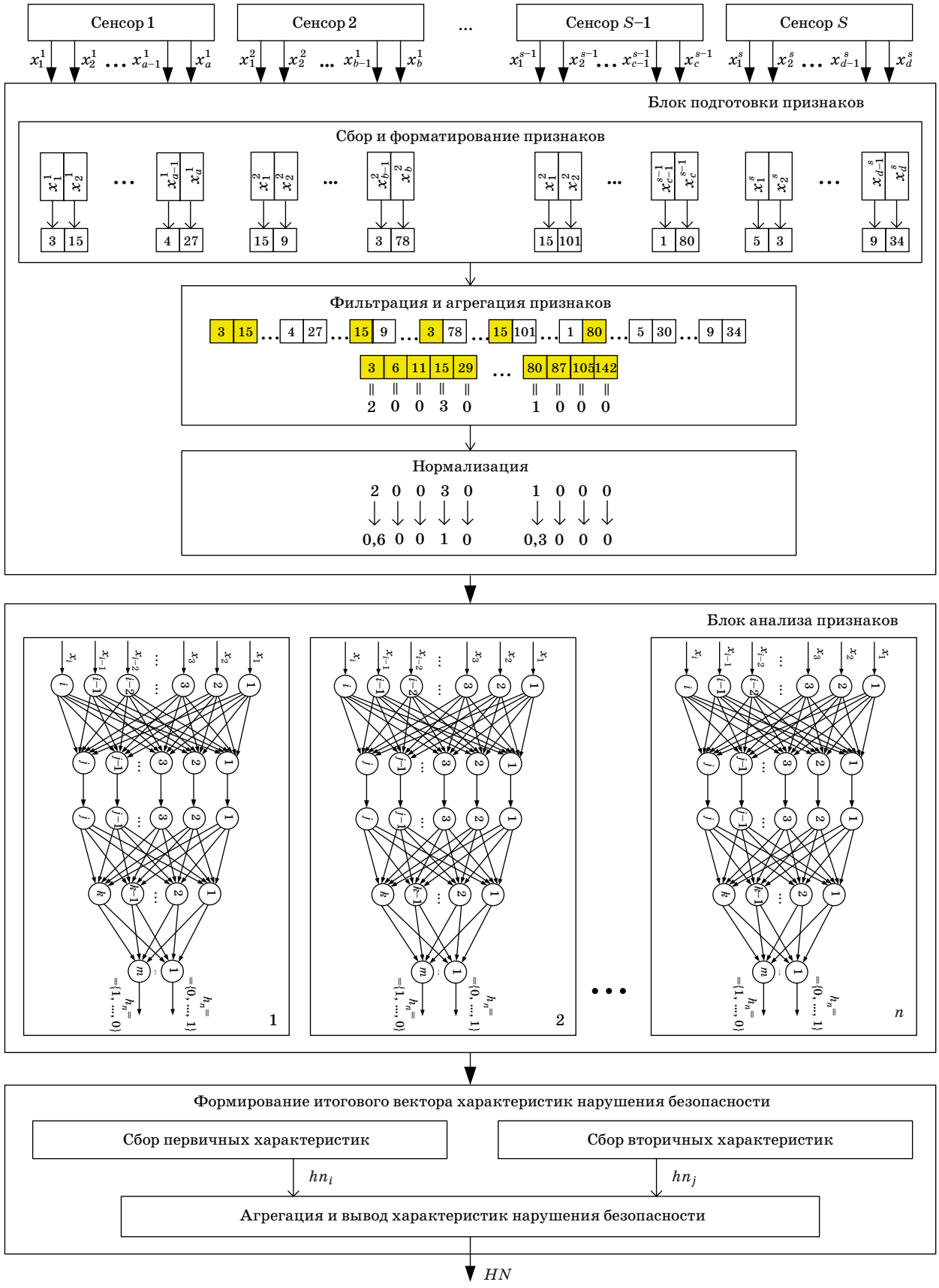
Множество характеристик нарушения безопасности HN представляет собой совокупность значений, по которым можно получить детальное описание выявленного нарушения безопасности. Перечень основных характеристик нарушения безопасности приведен на рис. 2.

Ряд характеристик нарушения безопасности может быть получен путем прямого измерения или расчета (таких как идентификаторы пользователей, время и др.). Назовем их условно первичными характеристиками. Однако для некоторых характеристик нарушения безопасности отсутствует возможность определить их функциональную зависимость от значений диагностических признаков. Определение значений этих характеристик, условно называемых вторичными характеристиками, является нетривиальной задачей.

Модель процесса диагностирования представлена на рис. 3. Установленные сенсоры передают сообщения о событиях из журналов регистрации



■ ***Рис. 2.*** Основные характеристики нарушения безопасности
■ ***Fig. 2.*** The main characteristics of a security violation



■ ***Рис. 3.*** Модель диагностирования компьютерного инцидента в информационно-коммуникационной системе

■ ***Fig. 3.*** Model of computer incident diagnostics in information and communication system

в блок подготовки признаков, где осуществляется их обработка и представление к необходимому виду перед подачей на вход глубоких ИНС. Поступив в блок анализа, нормализованные значения признаков компьютерного инцидента обрабатываются несколькими ИНС. Количество ИНС зависит от количества вторичных характеристик нарушения безопасности, которые необходимо определить. Работа организована в параллельном режиме. Затем формируется итоговый вектор характеристик нарушения безопасности, который объединяет как первичные, так и вторичные характеристики.

На основании имеющегося набора значений характеристик нарушения безопасности информации принимается решение по реагированию на нарушение. В общем случае перечень характеристик нарушений безопасности должен соответствовать возможностям системы защиты по реагированию на угрозы безопасности.

Метод диагностирования компьютерных инцидентов

К разработанному методу диагностирования компьютерных инцидентов предъявляются следующие требования:

— функционирование в реальном или близком к реальному режиме времени;

— поддержание заданных показателей точности и полноты;

— простота реализации.

Процесс диагностирования компьютерных инцидентов в соответствии с разработанным методом состоит из трех этапов:

1) настройки, в ходе которой осуществляется обучение ИНС;

2) сбора и подготовки диагностических признаков, подаваемых на вход ИНС;

3) формирования вектора значений характеристик нарушения безопасности.

Предварительным этапом настройки системы диагностирования (до обучения ИНС) является формирование множества исходных данных, подаваемых на вход ИНС. В работе [9] показано, что число ключевых слов в записях, важных для анализа журналов событий, не превосходит 170. В проведенном эксперименте было выбрано 128 слов и словосочетаний из журналов событий, появление которых является признаком компьютерного инцидента или предпосылкой его появления.

В зависимости от имеющихся сведений об инциденте, поступающих от средств защиты, выбирается размер временного интервала. Для каждого журнала событий информационно-коммуникационной системы строится вектор слов в выбранном временном интервале. На вход диагностической ИНС поступает суммарный вектор по всем журналам событий. Так, для информационно-коммуникационной системы, состоящей из 40 компьютеров с установленной операционной системой семейства Linux, могут быть эффективно использованы 400 журналов событий. Соответственно, входной вектор диагностической ИНС должен содержать 51 200 нейронов.

Альтернативный метод обработки журналов событий предложен в работах [18, 19]. Записи из журналов событий могут быть проанализированы на уровне исходных кодов, после чего к результатам анализа применяется метод машинного обучения. Полученный результат может быть преобразован в дерево решений, отображающее критические сообщения, связанные с обнаруженными проблемами. Однако разработчики данного метода оценивали способность анализа технических неисправностей, не рассматривая компьютерные инциденты.

На этапе настройки необходимо осуществить обучение глубокой ИНС и проверить ее готовность к функционированию. Обучение ведется по полученным экспертным путем парам значений (X, Y), где X — множество признаков, поступающих на вход искусственной нейронной сети; Y — значение характеристики нарушения безопасности, соответствующее данному набору признаков. Они хранятся в базе данных, которая предназначена, в том числе, для сохранения новых пар (X, Y) и последующей корректировки ИНС. Процесс обучения осуществляется методом обратного распространения ошибки, в ходе которого происходит корректировка весовых коэффициентов каждой связи искусственных нейронов между собой [20]. На вход ИНС подаются признаки, полученные из журналов событий и сохраненные в базе данных. На выходе ожидается отклик ИНС на этот набор признаков. Полученный отклик Y' сравнивается с правильным ответом Y, и в случае совпадения осуществляется переход к следующему набору признаков. При расхождении значений отклика Y' и правильного ответа Y сначала изменяются весовые коэффициенты связей нейронов от входного до выходного слоя. После этого производится переход к новому набору признаков, который также подается на вход ИНС. Обучение продолжается до тех пор, пока ошибка обучения на множестве всех наборов признаков достигнет допустимого значения либо число итераций не превысит определенного значения [21, 22].

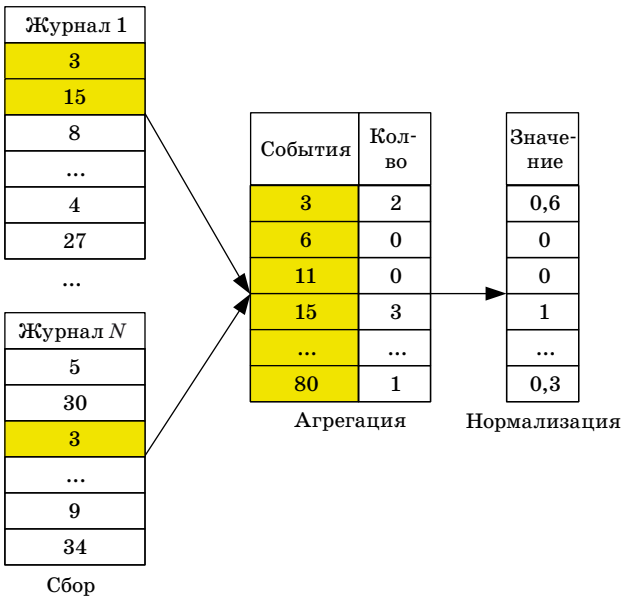
Также важным этапом настройки является задание временного окна — интервала времени, в течение которого будет осуществляться сбор признаков нарушения безопасности. Ввиду большого количества анализируемой информации возникает необходимость уменьшения ее объема.

Из всех событий, фиксируемых в ходе функционирования информационно-коммуникационной системы, отбираются информативные события, которые могут содержать признаки нарушения безопасности. Остальные события не рассматриваются. Порядок формирования входного вектора признаков представлен на рис. 4. Временной интервал может быть выбран исходя из ресурсов информационно-коммуникационной системы по хранению журналов событий с учетом выявленного компьютерного инцидента.

На этапе функционирования системы диагностирования после получения сигнала о компьютерном инциденте и первичной информации от средств защиты осуществляется уточнение временного окна, а затем — сбор и обработка событий. В выбранном временном окне происходит подсчет числа информативных событий по каждому источнику, фиксирующему события в информационно-коммуникационной системе. Полученные значения нормализуются для последующей подачи на вход ИНС. В итоге формируется вектор информативных признаков.

Сформированный вектор поступает на вход комбинированной ИНС для определения значения характеристик нарушения безопасности. Для каждой характеристики нарушения безопасности, значение которой невозможно получить напрямую от средств детектирования компьютерных инцидентов, предполагается отдельная глубокая ИНС, обученная на определение одного конкретного значения характеристики. В связи с этим количество нейронов выходного слоя персептрона будет определяться количеством возможных значений характеристики нарушения безопасности. Индивидуальные комбинированные ИНС работают параллельно. Вектор информативных признаков поступает на все ИНС одновременно, а также сохраняется в базе данных для учета и запоминания варианта реагирования на компьютерный инцидент. Выбор числа определяемых характеристик нарушения безопасности зависит от ситуации, в которой обнаружен компьютерный инцидент, и определяется различными параметрами, такими как важность защищаемых ресурсов, имеющийся ресурс на проведение анализа и потенциальные возможности по реагированию.

По результатам работы совокупности комбинированных ИНС формируется набор значений характеристик нарушения безопасности. Он используется для выбора варианта реагирования на компьютерный инцидент исходя из ограничений и имеющихся возможностей.



■ ***Рис. 4.*** Подготовка вектора признаков для подачи на вход ИНС

■ ***Fig. 4.*** Preparation of a vector features for input of an artificial neural network

Анализ экспериментальных данных

Обучение диагностической ИНС осуществлялось на основе имеющейся базы данных о нарушениях безопасности информации, составленной экспертным путем. База данных состоит из 276 записей, которые включают наборы диагностических признаков из журналов событий для 20 компьютеров. Для характеристики нарушения безопасности по характеру воздействия из 276 записей 113 соответствуют преднамеренному нарушению, а 163 — непреднамеренному нарушению. Для характеристики нарушения безопасности по последствиям реализации из 276 записей 164 соответствуют критическому ущербу, а 112 — некритическому ущербу.

Система диагностирования была реализована на языке программирования Python. Для настройки ИНС база данных была разделена на две части. Для обучения было взято 194 записи. Оставшиеся 82 записи использовались для тестирования. Оценка диагностической ИНС проводилась по общепринятым показателям точности Pr и полноты Rc:

$$Pr = \frac{TP}{TP + FP}; \quad Rc = \frac{TP}{TP + FN},$$

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, классифици-

руемых как ложное значение, в то время как оно истинное. Значения показателей, полученные в ходе эксперимента, для характеристики нарушения безопасности по характеру воздействия в зависимости от количества нейронов скрытого слоя приведены на рис. 5, *а*, а для характеристики нарушения безопасности по последствиям реализации — на рис. 5, *б*.

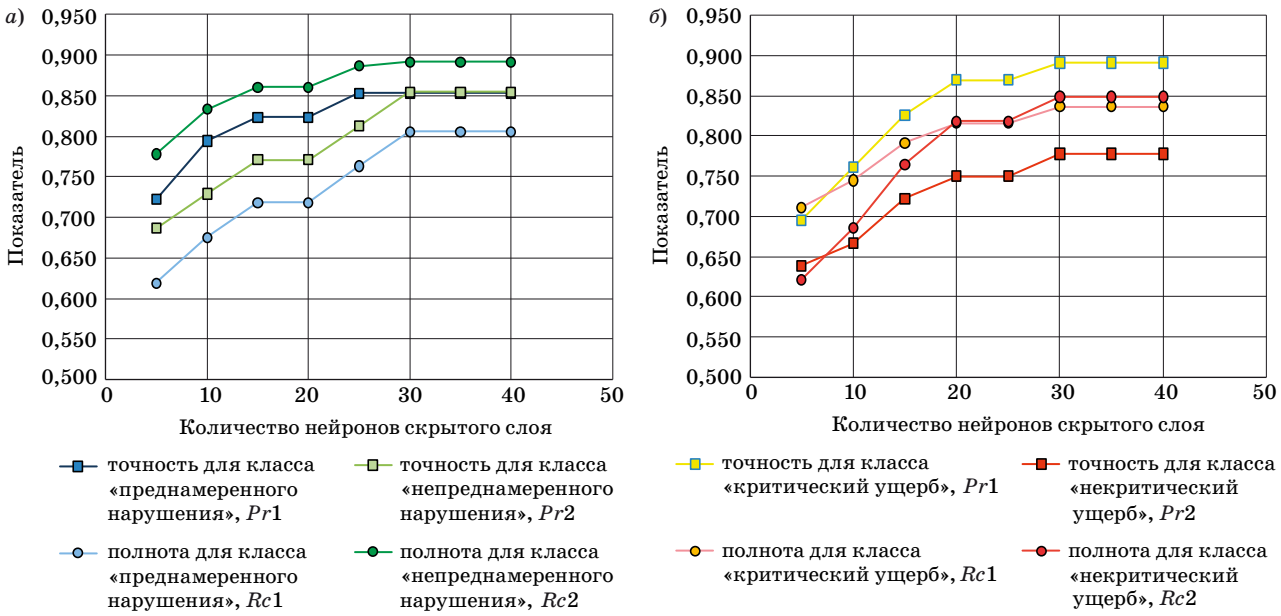
Для решения задачи оптимизации общего времени диагностирования возникает необходимость преобразования структуры ИНС путем уменьшения числа нейронов для сокращения времени обучения без существенной потери точности результата. Полученные зависимости показателей точности и полноты от числа нейронов предпоследнего слоя комбинированной ИНС, представленные на рис. 5, позволяют судить о том, что диагностическая ИНС показывает весьма высокие значения показателя точности определения значения бинарной характеристики нарушения безопасности. В случае если предпоследний слой содержит свыше 30 нейронов, показатель точности составляет более 75 %, что говорит о большой доле правильно классифицированных преднамеренных нарушений среди всего объема нарушений, классифицированных как преднамеренные из тестовой выборки. Показатель полноты при этом составляет 85 % и указывает на долю правильно найденных значений преднамеренных нарушений из всего объема реально преднамеренных нарушений, имеющихся в тестовой выборке. При этом 30 нейронов предпоследнего слоя являются оптимальным количеством для комбинированной ИНС для диагностирования системы из 20 компьютеров, поскольку увеличение числа нейронов не приводит к значительному приросту точности и полноты результатов. При этом время обучения ИНС возрастает с 330 до 446 секунд.

Заключение

В настоящей работе предложены модель и метод диагностирования компьютерных инцидентов в информационно-коммуникационной системе, основанные на использовании алгоритмов глубокого обучения искусственных нейронных сетей.

Ключевой особенностью компьютерных инцидентов как объекта анализа для определения значений характеристик нарушения безопасности является наличие важных диагностических признаков, сохраняемых в журналах регистрации событий элементов информационно-коммуникационных систем. Для экспериментальной оценки предложенного метода были выбраны показатели полноты и точности определения значений характеристик нарушения безопасности.

Экспериментальная оценка предложенного метода показала, что он позволяет определять значения характеристик нарушения безопасности с достаточно высокой точностью и в реальном или в близком к реальному масштабе времени.



■ ***Рис. 5.*** Значения показателей *Pr* и *Rc* для характеристики нарушения безопасности по характеру воздействия (*а*) и по последствиям реализации (*б*)

■ ***Fig. 5.*** Values of *Pr* and *Rc* indicators for characteristic the security violation by character of influence (*а*) and by implementation consequences (*б*)

Дальнейшие направления исследований связываются с разработкой методов применения частично предобученных глубоких ИНС и дообучением их с использованием технологии переноса знаний (transfer learning).

Финансовая поддержка

Работа выполнена при частичной поддержке РФФИ (проект 18-07-01369) и бюджетной темы № АААА-А16-116033110102-5.

Литература

1. Актуальные киберугрозы. I квартал 2019 года. Сайт Positive Technologies 2019. https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-q1-2019 (дата обращения: 24.06.2019).
2. Итоги информационной безопасности в 2018 году. https://rvision.pro/blog-posts/itogi-informatsionnoj-bezopasnosti-v-2018-godu/ (дата обращения: 24.06.2019).
3. **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.
4. **Vaarandi R.** A data clustering algorithm for mining patterns from event logs. *Proc. the 3rd IEEE Workshop on IP Operations and Management*, October 2003, pp. 119–126.
5. **Kurd Z.** *Artificial Neural Networks in Safety-critical Applications*. University of York, Department of Computer Science, 2005. 334 p.
6. **Cheng H.-J., Kumar A.** Process mining on noisy logs — Can log sanitization help to improve performance? *Decision Support Systems*, 2015, no. 79, pp. 138–149.
7. **Bose R. P. J. C., Mans R. S., van der Aalst W. M. P.** Wanna improve process mining results? *IEEE Symposium on Computational Intelligence and Data Mining (CIDM)*, 2013, pp. 127–134.
8. **Lv F., Wen C., Bao Z., and Liu M.** Fault diagnosis based on deep learning. *American Control Conference*, 2016, IEEE, 2016, pp. 6851–6856.
9. **Zou D. Q., Qin H., Jin H.** UiLog: Improving log-based fault diagnosis by log analysis. *Journal of Computer Science and Technology*, Sept. 2016, no. 31(5), pp. 1038–1052.
10. **Fu Q., Lou J. G., Wang Y.,** et al. Execution anomaly detection in distributed systems through unstructured log analysis. *Proc. the 9th IEEE International Conference on Data Mining*, Dec. 2009, pp. 149–158.
11. **Nolle T., Seeliger A., Mühlhäuser M.** Unsupervised anomaly detection in noisy business process event logs using denoising autoencoders. *Lecture Notes in Computer Science*, 2016, pp. 442–456.
12. **Sakurada M., Yairi T.** Anomaly detection using autoencoders with nonlinear dimensionality reduction. *Proceedings of the MLSDA 2014 2nd Workshop on Machine Learning for Sensory Data Analysis — MLSDA'14*, 2014, pp. 4–11. doi:10.1145/2689746.2689747
13. **Alkasassbeh M.** An empirical evaluation for the intrusion detection features based on machine learning and feature selection methods. *Journal of Theoretical and Applied Information Technology*, 2017, vol. 95, no. 22, pp. 5962–5976.
14. **Larochelle H., Erhan D., Courville A., Bergstra J., Bengio Y.** An empirical evaluation of deep architectures on problems with many factors of variation. *Proceedings of the 24th International Conference on Machine Learning — ICML '07*, 2007, pp. 473–480.
15. **Авраменко В. С., Бобрешов-Шишов Д. И., Маликов А. В.** *Идентификация характеристик нарушений безопасности информации на основе искусственных нейронных сетей.* Региональная информатика и информационная безопасность: сб. тр. СПб., СПОИСУ, 2018. Вып. 5. С. 68–70.
16. **Авраменко В. С., Маликов А. В.** Нейросетевая модель диагностирования компьютерных инцидентов в инфотелекоммуникационных системах специального назначения. *Проблемы технического обеспечения войск в современных условиях: тр. IV межвузовской науч.-практ. конф.,* Санкт-Петербург, 6 февраля 2019 г. СПб., ВАС, 2019. Т. 1. С. 41–45.
17. **Baldi P.** Autoencoders, unsupervised learning and deep architectures. *Proceedings of the 2011 International Conference on Unsupervised and Transfer Learning workshop — UTLW'11*, Isabelle Guyon, Gideon Dror, Vincent Lemaire, Graham Taylor, and Daniel Silver (Eds.), 2011, vol. 27, JMLR.org 37-50.
18. **Xu W., Huang L., Fox A.,** et al. Detecting large-scale system problems by mining console logs. *Proceedings the 22nd ACM Symposium on Operating Systems Principles*, October 2009, pp. 117–132.
19. **Mineda Carneiro E., Vieira Dias L. A., Marques da Cunha A., Stege Mialaret L. F.** Cluster analysis and artificial neural networks. A case study in credit card fraud detection. *Proceedings the 12th International Conference on Information Technology — New Generations*, 2015, pp. 122–126.
20. **Осовский С.** Нейронные сети для обработки информации / пер. с польского И. Д. Рудинского. М., Финансы и статистика, 2002. 344 с.
21. **Николенко С., Кадурин А., Архангельская Е.** Глубокое обучение. СПб., Питер, 2018. 480 с.
22. **Хайкин С.** Нейронные сети: полный курс. 2-е изд. М., Вильямс, 2006. 1104 с.

UDC 004.056
doi:10.31799/1684-8853-2019-6-32-42

Model and method for diagnosing computer incidents in information and communication systems based on deep machine learning

Malikov A. V.[a], Post-Graduate Student, orcid.org/0000-0002-4285-5360
Avramenko V. S.[a], PhD, Tech., Professor, orcid.org/0000-0002-2452-0380
Saenko I. B.[a,b], Dr. Sc., Tech., Professor, orcid.org/0000-0002-9051-5272, ibsaen@comsec.spb.ru
[a]Military Telecommunications Academy, 3, Tikhoretsky Av., 194064, Saint-Petersburg, Russian Federation
[b]Saint-Petersburg Institute for Informatics and Automation of the RAS, 39, 14 Line V. O., 199178, Saint-Petersburg, Russian Federation

Introduction: Models and methods for diagnosing computer incidents recorded in information and communication systems are the most important components in mathematical support of information security systems. The main requirement for the diagnostics is prompt identification of security violation characteristics. This problem is complicated due to the amount and variability of the initial data on information security violation. **Purpose:** Development of a model for diagnosing a computer incident, along with a method which would allow you to quickly determine the characteristics of a security violation. **Results:** Security breach characteristics important for making a decision about responding to an identified computer incident can be determined via deep artificial neural networks. A structural feature of the proposed deep artificial neural network is combining the coding part of the autoencoder and a multilayer perceptron. In addition, the method implements a parallel mode of processing information events which have occurred in the information and communication system before the incident was detected, by using a separate proposed artificial neural network for each secondary characteristic of the security breach. The method of determining the values of these secondary characteristics allows you to greatly improve the diagnostics efficiency, having acceptable values of precision and recall for the security violation characteristics to determine. The dependence has been studied of the completeness and classification accuracy on the number of neurons in the hidden layer. A sufficient number of neurons in the hidden layer for achieving the required training efficiency is experimentally determined. **Practical relevance:** The developed model and method can be implemented using standard software and hardware (servers) of an information and communication system. Their combined use with the existing models and methods of monitoring and diagnostics can significantly improve the efficiency of an information security system.

Keywords — computer incident, diagnosis sign, artificial neuro network, perceptron, autoencoder.

For citation: 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. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2019, no. 6, pp. 32–42 (In Russian). doi:10.31799/1684-8853-2019-6-32-42

References

1. *Aktual'nye kiberugrozy. I kvartal 2019 goda* [Actual cyber threats. The first quarter of 2019. Site of Positive Technologies 2019]. Available at: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-q1-2019 (accessed 24 Jule 2019).
2. *Itogi informacionnoj bezopasnosti v 2018 godu* [Results of information security in 2018]. Available at: https://rvision.pro/blog-posts/itogi-informatsionnoj-bezopasnosti-v-2018-godu/ (accessed 26 Jule 2019).
3. 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.
4. Vaarandi R. A data clustering algorithm for mining patterns from event logs. *Proc. the 3rd IEEE Workshop on IP Operations and Management*, October 2003, pp. 119–126.
5. Kurd Z. *Artificial Neural Networks in Safety-critical Applications*. University of York, Department of Computer Science, 2005. 334 p.
6. Cheng H.-J., & Kumar A. Process mining on noisy logs — Can log sanitization help to improve performance? *Decision Support Systems*, 2015, no. 79, pp. 138–149.
7. Bose R. P. J. C., Mans R. S., van der Aalst W. M. P. Wanna improve process mining results? *IEEE Symposium on Computational Intelligence and Data Mining (CIDM)*, 2013, pp. 127–134.
8. Lv F., Wen C., Bao Z., and Liu M. Fault diagnosis based on deep learning. *American Control Conference*, 2016, IEEE, 2016, pp. 6851–6856.
9. Zou D. Q., Qin H., Jin H. UiLog: Improving log-based fault diagnosis by log analysis. *Journal of Computer Science and Technology*, Sept. 2016, no. 31(5), pp. 1038–1052.
10. Fu Q., Lou J. G., Wang Y., et al. Execution anomaly detection in distributed systems through unstructured log analysis. *Proc. the 9th IEEE International Conference on Data Mining*, Dec. 2009, pp. 149–158.
11. Nolle T., Seeliger A., Mühlhäuser M. Unsupervised anomaly detection in noisy business process event logs using denoising autoencoders. *Lecture Notes in Computer Science*, 2016, pp. 442–456.
12. Sakurada M., Yairi T. Anomaly detection using autoencoders with nonlinear dimensionality reduction. *Proceedings of the MLSDA 2014 2nd Workshop on Machine Learning for Sensory Data Analysis — MLSDA'14*, pp. 4–11. doi:10.1145/2689746.2689747
13. Alkasassbeh M. An empirical evaluation for the intrusion detection features based on machine learning and feature selection methods. *Journal of Theoretical and Applied Information Technology*, 2017, vol. 95, no. 22, pp. 5962–5976.
14. Larochelle H., Erhan D., Courville A., Bergstra J., Bengio Y. An empirical evaluation of deep architectures on problems with many factors of variation. *Proceedings of the 24th International Conference on Machine Learning — ICML '07*, 2007, pp. 473–480.
15. Avramenko V. S., Bobreshov-Shishov D. I., Malikov A. V. *Identifikaciya harakteristik narushenij bezopasnosti informacii na osnove iskusstvennyh nejronnyh setej* [Identification of information security violations characteristics on the basis of artificial neural networks. In: Scientific collection "Regional informatics and information security"]. Saint-Petersburg, Sankt-Peterburgskoe obshchestvo informatiki, vychislitel'noj tekhniki, sistem svyazi i upravleniya Publ., 2018, pp. 68–70.
16. Avramenko V. S., Malikov A. V. Neural network model of diagnosing computer incidents in infotelecommunication systems of special purpose. *Trudy IV mezhvuzovskoj nauchno-prakticheskoj konferencii "Problemy tekhnicheskogo obespecheniya vojsk v sovremennyh usloviyah"* [Proceedings of the IV Interuniversity Scientific and Practical Conference "Problems of technical support of troops in modern conditions"], Saint-Petersburg, 2019, vol. 1, pp. 41–45 (In Russian).

17. Baldi P. Autoencoders, unsupervised learning and deep architectures. *Proceedings of the 2011 International Conference on Unsupervised and Transfer Learning workshop — UTLW'11*, Isabelle Guyon, Gideon Dror, Vincent Lemaire, Graham Taylor, and Daniel Silver (Eds.), 2011, vol. 27, JMLR.org 37-50.
18. Xu W., Huang L., Fox A., et al. Detecting large-scale system problems by mining console logs. *Proceedings the 22nd ACM Symposium on Operating Systems Principles*, October 2009, pp. 117–132.
19. Mineda Carneiro E., Vieira Dias L. A., Marques da Cunha A., Stege Mialaret L. F. Cluster analysis and artificial neural networks. A case study in credit card fraud detection. *Proceedings the 12th International Conference on Information Technology — New Generations*, 2015, pp. 122–126.
20. Osovsky S. *Nejronnye seti dlya obrabotki informacii* [Neural networks for information processing]. Moscow, Finansy i statistika Publ., 2002. 344 p. (In Russian).
21. Nikolenko S., Kadurin A., Arkhangelskaya E. *Glubokoe obuchenie* [Deep learning]. Saint-Petersburg, Piter Publ., 2018. 480 p. (In Russian).
22. Khaikin S. *Nejronnye seti: polnyj kurs* [Neural networks: full course]. 2nd ed. Moscow, Vil'yams Publ., 2006. 1104 p. (In Russian).

УВАЖАЕМЫЕ АВТОРЫ!

Научные базы данных, включая SCOPUS и Web of Science, обрабатывают данные автоматически. С одной стороны, это ускоряет процесс обработки данных, с другой — различия в транслитерации ФИО, неточные данные о месте работы, области научного знания и т. д. приводят к тому, что в базах оказывается несколько авторских страниц для одного и того же человека. В результате для всех по отдельности считаются индексы цитирования, снижая рейтинг ученого.

Для идентификации авторов в сетях Thomson Reuters проводит регистрацию с присвоением уникального индекса (ID) для каждого из авторов научных публикаций.

Процедура получения ID бесплатна и очень проста, есть возможность провести регистрацию на 12-ти языках, включая русский (чтобы выбрать язык, кликните на зеленое поле вверху справа на стартовой странице): https://orcid.org