17. Tsypkin Ya. Z. *Adaptatsiya i obuchenie v avtomaticheskikh sistemakh* [Adaptation and training in automatic systems], Moscow, Nauka Publ., 1968 399p.

18. Erlikh A. A. *Tekhnicheskiy analiz tovarnykh i finansovykh rynkov* [Technical analysis of commodity and financial markets], Moscow, Infra Publ., 1996. 106p.

19. Musina I. R., Ten I. G. Investigation of Self–organizing forecasting algorithm for dynamic processes. *Works of IKECCO'2004 – International Conference on Electronics and Computer in Kyrgyzstan (2 April 2004)*, Bishkek, pp. 25–28.

20. Ten I. G. Synthesis of Optimal Control Under Interval Uncertainty in Models. *Proceeding of the International Conference "Interval'92", Journal: "Interval Computations"*, September 22–25,1992, no. 4 (6) Special Issue, pp. 100–106.

РЕДАКЦИОННЫЙ КОММЕНТАРИЙ К СТАТЬЕ

Задачи краткосрочного прогнозирования на основании данных, представленных во временных рядах (ВР) исследуются уже достаточно давно, при этом применяются различные методы. Однако работ, посвященных прогнозированию стока именно горных рек в русскоязычной периодике почти нет. Таким образом, статья имеет определенную новизну с точки зрения объекта исследований. В целом в работе охват материала достаточно полный и включает в себя следующие направления: подробную гидрологическую характеристику объекта исследований (в т.ч. рек Кыргызстана, реки Чу и ее бассейна); характеристику некоторых существующих методов сглаживания ВР и прогнозирования на основе ВР; описание разработанного прототипа кроссплатформенной автоматизированной системы краткосрочного прогнозирования (АСКП); результаты апробации этой системы на примере стока реки Чу.

Однако по публикуемой работе необходимо сделать ряд замечаний.

1. При построении прогнозов авторы основываются исключительно на ВР по стоку реки – исходя из того, что в нем есть вся необходимая информация. Однако с учетом специфики формирования стока горных рек Кыргызстана представляется, что стоило бы дополнительно использовать при построении прогнозов и метеопрогнозы на ближайший месяц – включая оценки предполагаемых температур воздуха, солнечной инсоляции, величин осадков. Причина – эти факторы могут существенно «корректировать» прогнозы, полученные на основе только ВР.

2. Следовало бы более четко указать, к какому именно створу реки Чу относятся приводимые данные и результаты прогнозирования. Также можно было бы сравнить «качество» прогнозов для разных створов.

3. В работе не обосновывается целесообразность использования шага по времени во ВР в 1 месяц, хотя (как это следует из материала статьи) отсчеты на гидропостах снимаются значительно чаще.

4. В ряде фрагментов статьи смешиваются понятия «сглаживания» ВР и «прогнозирования» на основе ВР. Между тем с позиций пользователей АСКП важно только прогнозирование «вперед по времени», а сглаживание ВР может использоваться лишь как вспомогательный прием, позволяющий убрать «высокочастотные шумы» в экспериментальных данных. Можно ли вообще использовать «сглаживание» при шаге по времени в 1 месяц – этот вопрос, вероятно, следует считать дискуссионным.

5. Представляется, что «алгоритм самоорганизации», на который авторы все время ссылаются, стоило бы представить на примерах более детально. В частности показать размеры «опорных участков» (количества точек во ВР), используемых для построения «прогноза вперед».

6. В работе никак не используется информация об усредненных значениях расходов воды по отдельным месяцам за ряд предшествующих лет. Между тем такая «усредненная годовая зависимость» могла бы быть весьма полезной для прогнозирования – особенно при ее «масштабировании» на водность конкретного года. Последнюю можно оценить, например, по уже имеющимся точкам во ВР за тот год, для которого осуществляется прогнозирование.

7. Целесообразность представления «диаграммы переключений» между методами на рис.7 в виде графика (ломаной линии) вызывает серьезные сомнения. Причина – переключения происходят «скачкообразно» и никаких «промежуточных точек» (соответствующих наклонным участкам ломаной линии) просто не может быть.

8. Перечень дополнительных методов прогнозирования, которые авторы предполагают включить в АСКП, выглядит достаточно кратким. Кроме того, целесообразность использования именно этих методов в статье фактически никак не обосновывается.

УДК 004.056.5

ОТСЛЕЖИВАНИЕ СОСТОЯНИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ НА ОСНОВЕ АНАЛИЗА ДАННЫХ О СОБЫТИЯХ

Статья поступила в редакцию 09.02.2018, в окончательном варианте – 18.02.2018.

Умницын Михаил Юрьевич, Волгоградский государственный университет, 400062, Российская Федерация, г. Волгоград, пр-т Университетский, 100,

старший преподаватель, e-mail: umnitsyn@volsu.ru

Михальченко Светлана Владимировна, Волгоградский государственный университет, 400062, Российская Федерация, г. Волгоград, пр-т Университетский, 100,

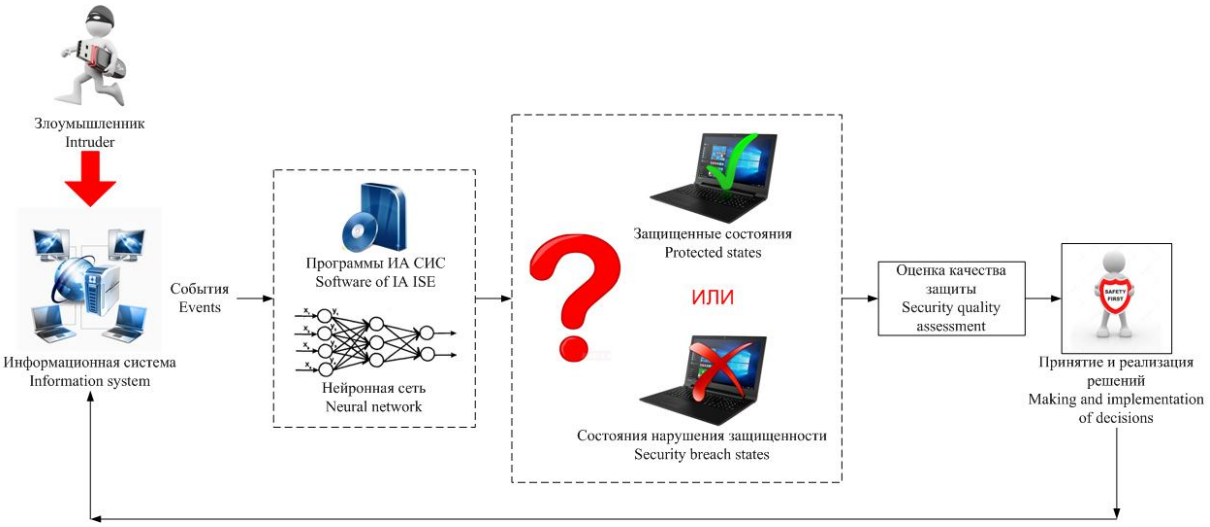
студент, e-mail: infsec@volsu.ru

Для обеспечения полноценной защиты информационной системы (ИС) требуется систематически анализировать события, происходящие в ней. Результаты такого анализа позволяют, в частности, обнаруживать переход ИС из защищенного состояния в состояние нарушения защищенности. Интеллектуальный анализ (ИА) событий ИС (СИС)

с помощью нейронных сетей позволяет обнаруживать подобные переходы. Проанализированы функциональные возможности и вычислительная эффективность программ, позволяющих проводить ИА СИС; сформулированы критерии оценки качества таких программ. Разработано оригинальное программное средство, позволяющее производить автоматизированную оценку программ ИА СИС по совокупности значений критериев оценки. С использованием этого программного средства проведены расчеты для ряда программ ИА СИС, использующих нейросетевые технологии: STATISTICA Automated Neural Networks, Deductor Studio, Neural network toolbox, MemBrain Neural Network, Neuro Solutions. Для выполнения расчетов все программы обучали и выполняли анализ с помощью наиболее широко применяемой нейронной сети – многослойного персептрона. По результатам расчетов определена наиболее подходящая программа для ИА СИС — STATISTICA Automated Neural Networks. Применение этой программы позволит повысить эффективность отслеживания возникновения возможных переходов из защищенных состояний ИС в состояния нарушения защищенности; своевременно принимать меры по повышению уровня защищенности ИС.

Ключевые слова: информационная система, состояние информационной системы, событие информационной системы, информационная безопасность, интеллектуальный анализ, нейронная сеть, программа для интеллектуального анализа, алгоритм оценки

Графическая аннотации (Graphical annotation)



TRACKING STATUS OF INFORMATION SYSTEM BASED ON ANALYSIS OF EVENT DATA

The article was received by editorial board on 09.02.2018, in the final version – 19.02.2018.

Umnitsyn Mikhail Yu., Volgograd State University, 100 Universitetskiy Ave., Volgograd, 400062, Russian Federation,
Senior Lecturer, e-mail: umnitsyn@volsu.ru
Mihalchenko Svetlana V., Volgograd State University, 100 Universitetskiy Ave., Volgograd, 400062, Russian Federation,
student, e-mail: infsec@volsu.ru

In order to ensure full protection of information system (IS), it is necessary to systematically analyze events taking place in it. The results of such an analysis allow, in particular, to detect IS transition from a protected state to a state when protection is breached. Data Mining (DM) of IS events (ISE) using neural networks allows to detect such transitions. Functional capabilities and computational efficiency of programs allowing ISE DM are analyzed; criteria for evaluating effectiveness of use of such programs are formulated. The original software tool allowing automated assessing ISE DM programs for multiple weights of evaluation criteria is developed. With the help of this software there were made calculations for a number of ISE DM programs using neural network technologies: STATISTICA Automated Neural Networks, Deductor Studio, Neural network toolbox, Membrane Neural Network, Neuro Solutions have been carried out. To perform calculations, all the programs trained and made their analysis using the most widely used neural network — multilayer perceptron. According to the results of calculations, the most appropriate ISE DM program is STATISTICA Automated Neural Networks. Applying this program will allow to improve effectiveness of tracking possible transitions from protected IS states to the state when protection is breached as well as to take measures to improve IS protection.

Keywords: information system, information system state, information system event, information security, data mining, neural network, software for data mining, evaluation algorithm

Введение. В настоящее время информационные системы (ИС) широко применяются для решения различных задач в сферах производства, оказания услуг (включая информационные), управления технологическими процессами, банковской деятельности, здравоохранения, образования и т.д. Основными харак-

теристиками ИС считаются следующие: функциональность, вычислительная эффективность, эргономичность. Наряду с ними все большее внимание начинает уделяться вопросам защиты информации в ИС. Решение этих вопросов актуально для всех этапов жизненного цикла ИС: проектирование, ввод в действие, эксплуатация (включающая возможную модернизацию), вывод из эксплуатации [6]. Особое внимание должно быть уделено этапу эксплуатации ИС, как наиболее продолжительному по времени. Хотя вопросы информационной безопасности эксплуатации ИС и рассматриваются в существующих публикациях, но некоторые направления исследований не находят эффективного решения в настоящее время. Одним из таких направлений является динамический контроль состояний ИС с позиций информационной безопасности – для обнаружения случаев вероятного перехода ИС в состояния «нарушения защищенности». Поэтому целью данной статьи было проведение анализа (оценки) программных средств, которые могут быть использованы для выявления перехода в состояния «нарушения защищенности» в процессе эксплуатации ИС. Обнаружение таких переходов позволяет принять меры по повышению защищенности ИС – организационного, административного, программно-аппаратного характера и пр. [2].

Общая характеристика проблематики работы. Типичная корпоративная ИС представляет собой сложную систему, включающую в себя множество подсистем, взаимодействующих между собой. Как правило, такие ИС строятся на базе локальных вычислительных сетей, а также могут допускать обращения к ним извне, например, посредствам глобальной сети Интернет [18].

Подобные системы могут находиться во множестве различных состояний {S} – обычно это множество является счетным и конечным. С точки зрения информационной безопасности все состояния (т.е. множество {S}) можно разделить на два класса (не пересекающихся подмножества): защищенные состояния $\{S_N\}$ и состояния нарушения защищенности $\{S_I\}$ [5].

Каждое событие переводит ИС из одного состояния в другое. Для определения того, в какое состояние перейдет ИС в заданный момент времени, необходимо проанализировать данные о текущих событиях, происходящих в ней. Обычно такими данными являются следующие:

- сетевой трафик;
- записи в журналах событий отдельных компонентов ИС;
- текущая деятельность субъектов ИС (процессов, пользователей и т.д.) [12].

Чтобы обеспечить полноценную защиту ИС, необходимо определить то множество событий, возникновение которых приводит к переходу ИС из состояния класса $\{S_N\}$ в состояние класса $\{S_I\}$. В общем случае данная задача является достаточно сложной. Поэтому представляется целесообразным использовать системы искусственного интеллекта (ИИ) для анализа данных о событиях, происходящих в ИС. В качестве такой системы ИИ целесообразно использовать искусственную нейронную сеть (НС) [4].

Выходной слой такой НС будет содержать два нейрона, соответствующих двум возможным классам состояний: класс защищенных состояний и класс состояний нарушения защищенности.

Количество нейронов входного слоя НС определяется количеством характеристик событий ИС, на основании которых делаются заключения о нарушении защищенности или об отсутствии таких нарушений, и зависит от компонента ИС, для которого зафиксировано событие [13].

В качестве примера, для событий безопасности операционной системы хоста ИС, которые фиксируются в журнале событий операционной системы, можно указать следующие характеристики: код события; уровень важности; идентификатор учетной записи; дата и время возникновения события [15].

Если обучить НС на событиях, которые происходят в ИС, когда она находится в состоянии класса $\{S_N\}$, то возникновение событий, несвойственных для ее нормального функционирования, можно расценивать, как переход ИС в состояние класса $\{S_I\}$ [3].

Для решения этой задачи актуальным является выбор наиболее подходящей программы интеллектуального анализа (ИА) событий информационной системы (СИС) с помощью НС [8].

Типичные примеры нарушений состояния защищенности ИС приведены в таблице 1 [17].

Таблица 1 – Примеры нарушений состояния защищенности ИС

Нарушения состояния защищенности	**Признаки нарушения состояния защищенности**
Попытка подбора пароля учетной записи операционной системы хоста злоумышленником	Появление нескольких событий неуспешного входа в операционную систему (код события: 4625 – Не удалось осуществить вход в аккаунт; уровень важности: аудит отказа)
Неуспешная попытка пользователя операционной системы хоста обратиться к объекту операционной системы	Появление события неуспешного доступа к объекту операционной системы (код события: 4663 – Произведена попытка доступа к объекту; уровень важности: аудит отказа)
Злоумышленник проводит разведку с помощью сканирования портов	Появление в сети множества пакетов (установленные TCP флаги: FIN, URG и PSH)
Атака «Land»	Появление в сети пакетов (IP-адрес отправителя=IP-адресу получателя; порт отправителя=порту получателя; установленные TCP флаги: SYN)

Обзор программных средств, которые могут быть применены для ИА СИС. Количество таких программ достаточно велико. Наиболее функциональными и популярными являются следующие:

1. STATISTICA Automated Neural Networks (SANN) - программный пакет для создания и обучения НС, который позволяет решать широкий спектр задач [21]. Фирмой разработчиком данного программного средства является StatSoft (http://statsoft.ru/products/STATISTICA_Neural_Networks). Последней версией программного средства является STATICTICA 13.3 EN.

2. Deductor Studio – аналитическая платформа, которая позволяет на базе единой архитектуры пройти все этапы построения аналитической системы: от консолидации данных до построения моделей и визуализации полученных результатов [16]. Фирмой разработчиком данного программного средства является BaseGroup Labs (https://basegroup.ru/deductor/components/studio). Последней версией программного средства является Deductor Studio 5.3.

3. Neural network toolbox (NNTool) – пакет расширения MATLAB, содержащий средства для проектирования, моделирования, разработки и визуализации НС [21]. Фирмой разработчиком данного программного средства является MathWorks (https://www.mathworks.com/products/neural-network.html). Последней версией программного средства является Neural network toolbox R2017b.

4. MemBrain Neural Network – представляет собой мощный графический редактор и симулятор НС. Это программное средство поддерживает НС различных архитектур, любого размера. Разработчиком данного программного средства является Thomas Jetter (http://www.membrain-nn.de/main_en.htm). Последней версией программного средства является MemBrain 08.00.00.00.

5. Neuro Solutions – «сверхсовременный» программный пакет. Он совмещает модульный (с иконным представлением) интерфейс разработки НС с реализацией усовершенствованных процедур обучения. Фирмой разработчиком данного программного средства является NeuroDimension (http://www.neurosolutions.com/neurosolutions). Последней версией программного средства является NeuroSolution 7.

Помимо указанных программ на многих интернет-ресурсах (включая специализированные) имеются различные средства конструирования НС, проведения с их помощью вычислений в режимах дистанционного использования [19].

Таким образом, приведенный перечень не следует рассматривать как исчерпывающий – были выбраны лишь наиболее популярные «представители» программных средств для решения рассматриваемых задач.

Оценка «качества» программных средств. Чтобы оценить качество указанных выше программных средств были сформулированы критерии для их оценки [1, 7].

С точки зрения авторов, приводимые ниже критерии удовлетворяют требованиям «необходимости и достаточности».

- Скорость обучения ($К_1$) – определяет время, затрачиваемое на расчет величин весов связей между нейронами, отвечающих заданным требованиям по точности.
- Понятность графического интерфейса ($К_2$) – оценивается по наличию удобного и интуитивно понятного пользователю интерфейса;
- Наглядность представления информации ($К_3$) – наличие возможности графического представления информации по окончанию обучения и проведения моделирования с использованием НС.
- Возможность реализации основных видов НС и алгоритмов обучения ($К_4$) – способность программного средства реализовать как можно большее количество стандартных видов НС и алгоритмов их обучения.
- Функциональность в отношении создания собственных структур НС ($К_5$) – возможность создания (разработки) пользователем собственных структур НС – в т.ч. задания таких параметров как тип сети, количества скрытых слоев; количества нейронов в слоях и т.д.
- Функциональность в отношении использования собственных алгоритмов ($К_6$) – возможность для пользователя подключения собственных алгоритмов обучения НС в виде программных модулей;
- Функциональность в отношении автоматизированного формирования НС ($К_7$) – возможность автоматического подбора наилучших параметров, что облегчает использование такой программы;
- Функциональность в отношении интеграции с системами программирования ($К_8$) – возможность сохранять результаты в различные файлы и подключать их к приложениям (прикладным программам).
- Наличие и функциональность генератора исходного кода ($К_9$) – возможность сгенерировать исходный программный код нейросетевых моделей на различных языках программирования;
- Определение взаимосвязей (корреляции) событий ($К_{10}$) – возможность программного средства учитывать то, как события связаны между собой. Если в пакете предусмотрена такая функция, то это позволяет обнаруживать атаки на ИС, которые состоят из нескольких шагов.

В таблице 2 приведены качественные значения критериев для рассматриваемых программных средств.

Таблица 2 – Качественные значения критериев для рассматриваемых программных средств

Нейросетевые программы	Критерии оценки									
	$К_1$	$К_2$	$К_3$	$К_4$	$К_5$	$К_6$	$К_7$	$К_8$	$К_9$	$К_{10}$
STATISTICA Automated Neural Networks	высокая	да	средняя	высокая	да	да	да	средняя	да	да
Deductor Studio	высокая	да	высокая	средняя	нет	нет	нет	высокая	нет	да
Neural network toolbox	низкая	нет	низкая	средняя	нет	нет	нет	низкая	нет	да
MemBrain Neural Network	высокая	нет	низкая	низкая	да	да	да	средняя	да	нет
Neuro Solutions	средняя	нет	средняя	средняя	да	да	нет	средняя	да	нет

Значения критериев были получены экспертно. Экспертная группа состояла из 7 человек. Каждый из экспертов выбирал одно из значений критериев: «низкий», «средний» или «высокий» для критериев $К_1$, $К_3$, $К_4$, $К_8$; «да» или «нет» для критериев $К_2$, $К_5$, $К_6$, $К_7$, $К_9$, $К_{10}$.

При этом была определена следующая система предпочтений:

«низкий» $\prec$ «средний» $\prec$ «высокий»; «да» $\prec$ «нет».

Общая (итоговая) оценка группы экспертов для каждого программного средства по каждому критерию находилась с помощью «метода совещаний» [10].

Так как ни одно из рассмотренных программных средств не обладает наилучшим набором критериев (соответствующих значениям «высокая» и «да»), то целесообразно разработать методику и программное средство для автоматизации выбора (по совокупности критериев) наиболее подходящей программы ИА СИС.

Представим сначала математическую модель, реализующую эту методику.

Сформируем вектор критериев $K = (K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_8, K_9, K_{10})$ для каждого оцениваемого объекта. Для перехода от качественных оценок к количественным, согласно системе предпочтений, используем следующие значения.

$$K_{1,3,4,8}=\begin{cases} 0, низкая \\ 0.5, средняя \\ 1, высокая \end{cases} \quad (1)$$

$$K_{2,5,6,7,9,10}=\begin{cases} 0, нет \\ 1, да \end{cases}$$

Существует наилучший вектор «K^*», в котором все значения критериев максимальны, т.е. равны «1» [14].

$$K^*= (1,1,1,1,1,1,1,1,1,1)$$

Для оценки качества нейросетевых пакетов (в отношении удовлетворения приведенным выше критериям) целесообразно использовать скалярную величину, равную Эвклидовому расстоянию между «наилучшим вектором» K* и вектором критериев, полученным для *i*-го оцениваемого программного средства:

$$K^{(i)} = (K_1^{(i)}, K_2^{(i)}, K_3^{(i)}, K_4^{(i)}, K_5^{(i)}, K_6^{(i)}, K_7^{(i)}, K_8^{(i)}, K_9^{(i)}, K_{10}^{(i)}).$$

Эвклидово расстояние между каждой парой векторов K^* и $K^{(i)}$ рассчитывается по формуле.

$$P^{(i)} = \sqrt{\sum_{j=1}^{10} (K_j^* - K_j^{(i)})^2}, \quad (2)$$

где индекс *j* соответствует номеру компоненты векторов [9].

Тот нейросетевой пакет (программное средство), для которого расстояние, вычисленное по формуле (2) окажется наименьшим, можно считать наиболее рациональным выбором.

Формулу (2) следует рассматривать как упрощенную. В общем случае для каждой из компонентов могут дополнительно вводиться весовые коэффициенты [20].

Методика и результаты проведения экспериментов. Для проведения экспериментальных исследований с помощью каждого нейросетевого пакета были построены НС (персептроны с двумя скрытыми слоями) для анализа событий, используемых для оценки состояния защищенности ИС. Входной слой НС состоял из четырех нейронов, соответствующих характеристикам событий безопасности ИС: код вида события; уровень важности события; идентификатор учетной записи; дата и время возникновения события. Эти поля являются наиболее информативными в основном источнике информации о событиях ИС – журнале событий безопасности.

Выходной слой НС содержал два нейрона, соответствующих двум возможным классам СИС: класс событий, которые не переводят ИС в состояние нарушения защищенности; класс событий, которые переводят ИС в состояние нарушения защищенности.

Обучение каждой НС проводилось на 10000 наборах характеристик событий безопасности ИС с помощью алгоритма обучения в виде обратного распространения ошибки. Наборы были сгенерированы случайным образом в границах допустимых значений характеристик событий безопасности ИС, т.к. конкретные значения не являются существенными для данного исследования.

После обучения на входы НС поочередно подавались наборы характеристик событий безопасности ИС (всего по 100 наборов для каждой из НС).

Для каждого нейросетевого пакета было проведено по пть экспериментов. В результате них были получены значения обобщенных оценок по формуле (2). Для каждого нейросетевого пакета они представлены на рисунке 1.

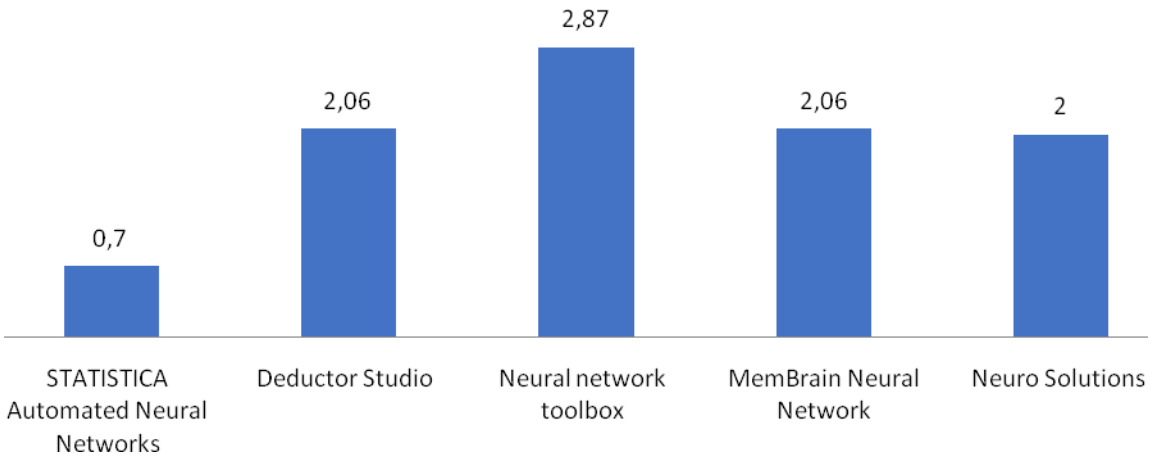


Рисунок 1 – Обобщенные оценки нейросетевых пакетов по критерию, представленному формулой (2)

Сравнив полученные результаты, можно прийти к выводу, что наиболее рациональным выбором является программа STATISTICA Automated Neural Networks. Отметим, что у нее значения критерия «4» («Реализация основных видов НС и алгоритмов обучения») и критерия «7» («Наличие автоматизированной НС») имеют наивысшие показатели среди всех сравниваемых программ.

Применение выбранного программного средства для ИА данных о СИС в отношении уровня ее информационной безопасности, позволит более эффективно отслеживать возникновение возможных переходов ИС из защищенных состояний в состояния нарушения защищенности. Как следствие могут быть своевременно приняты меры по повышению защищенности ИС. Отметим также, что эти меры могут приниматься и в упреждающем порядке (в порядке про-активного управления безопасностью ИС).

Список литературы

1. Ажмухамедов И. М. Введение метрических характеристик для решения задачи оценки и управления рисками / И. М. Ажмухамедов, О. Н. Выборнова // Прикаспийский журнал: управление и высокие технологии. – 2016. – № 1. – С. 10.

2. Ажмухамедов И. М. Management of information security risks in a context of uncertainty / И. М. Ажмухамедов, О. Н. Выборнова, Ю. М. Брумштейн // Automatic Control and Computer Sciences. – 2016. – Т. 50, № 8. – С. 657–663.

3. Аникин И. В. Методы оценки и управления рисками информационной безопасности в корпоративных информационных сетях / И. В. Аникин, Л. Ю. Емалетдинова, А. П. Кирпичников // Вестник технологического университета. – 2015. – Т. 18, № 6. – С. 195–197.

4. Аникин И. В. Технология интеллектуального анализа данных для выявления внутренних нарушителей в компьютерных системах / И. В. Аникин // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. – 2010. – Т. 6, № 113. – С. 112–117.

5. Аникин И. В. Information security risk management in computer networks based on fuzzy logic and cost/benefit ratio estimation / И. В. Аникин, Л. Ю. Емалетдинова // ACM International Conference Proceeding Series 8. Сер. «Proceedings of the 8th International Conference on Security of Information and Networks, SIN 2015». – 2015.

6. Брумштейн Ю. М. Анализ некоторых моделей группового управления рисками / Ю. М. Брумштейн, О. Н. Выборнова // Прикаспийский журнал: управление и высокие технологии. – 2015. – № 4. – С. 64–72.

7. Брумштейн Ю. М. Информация о программных средствах: структура, источники, содержание / Ю. М. Брумштейн // Научно-техническая информация. – 2017. – Сер. 1, № 4. – С. 1–13.

8. Варлатая С. К. Анализ угроз нарушения информационной безопасности информационных систем, существующие модели и методы противодействия компьютерным атакам / С. К. Варлатая, А. В. Кирьяненко // Актуальные проблемы технических наук в России и за рубежом : сборник научных трудов по итогам Международной научно-практической конференции. – Новосибирск, 2015. – № 2. – С. 162.

9. Витенбург Е. А. Системы поддержки принятия решений в информационной безопасности / Е. А. Витенбург, А. В. Никишова, А. Е. Чурилина // Вестник компьютерных и информационных технологий. – 2015. – № 4. – С. 50–56.

10. Князева О.М. Методика оценки качества информационных систем на основе экспертных данных / О. М. Князева, И. М. Ажмухамедов // Математические методы в технике и технологиях – ММТТ. – 2017. – Т. 1. – С. 129–133.

11. Князева О. М. Управление качеством информационных систем на основе процессного подхода / О. М. Князева // Прикаспийский журнал: управление и высокие технологии. – 2016. – № 2. – С. 36–47.

12. Максимова Е. А. Исследование вопросов аудита информационной безопасности автоматизированного рабочего места пользователя по данным системного реестра / Е. А. Максимова, Т. А. Омельченко, Ю. П. Умницын, К .П. Гужаковская // Вестник Волгоградского государственного университета. Серия 10: Инновационная деятельность. – 2016. – № 4 (23). – С. 14–21.

13. Назаров А. О. Распознавание поведения объектов методом нечеткой кластеризации данных / А. О. Назаров, И. В. Аникин // Вестник Казанского государственного технического университета им. А. Н. Туполева. – 2012. – № 4–1. – С. 222–228.

14. Никишова А. В. Модель оценки качества стеганографических систем / А. В. Никишова, С. А. Македонский // Промышленные АСУ и контроллеры. – 2017. – № 7. – С. 37–43.

15. Никишова А. В. Нейросетевой анализ событий безопасности в информационной системе / А. В. Никишова, Р. Ф. Рудиков, Е. А. Калинина // Известия ЮФУ. Технические науки. Тематический выпуск. «Информационная безопасность». – 2014. – № 2 (151). – С. 80–86.

16. Никулин А. Н. Аналитическая платформа «Дедуктор» – применение в информационных системах экономики : методические указания / А. Н. Никулин, И. В. Чернышев. – Ульяновск : УлГТУ, 2012. – С. 37.

17. Силантьев И. О. Выявление внутренних нарушителей в корпоративных сетях с помощью методов нечеткой логики / И. О. Силантьев, И. В. Аникин // Информация и безопасность. – 2017. – Т. 20, № 3 (4). – С. 448-451.

18. Скляров А. В. Управление информационными рисками защищенных экономических систем на основе анализа нечетких временных рядов / А. В. Скляров, Е. Н. Тищенко, М. Б. Стрюков, Т. Н. Шарыпова // Вопросы экономики и права. – 2016. – № 98. – С. 58–60.

19. Тищенко Е. Н. Использование механизмов искусственного интеллекта при проектировании защищенных информационных систем / Е. Н. Тищенко, А. В. Рипка // Россия и ЕС: пути развития и перспективы : материалы Международной научно-практической конференции. – 2016. – С. 848–852.

20. Тищенко Е. Н. Формализация выбора различных вариантов системы защиты информации от несанкционированного доступа в среде электронного документооборота / Е. Н. Тищенко, Т. Н. Шарыпова // Вестник Ростовского государственного экономического университета (РИНХ). – 2010. – № 32. – С. 226–233.

21. Туровский Я. А. Сравнительный анализ программных пакетов для работы с искусственными нейронными сетями / Я. А. Туровский, С. Д. Кургалин, А. А. Адаменко // Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. – 2016. – № 1. – С. 161–168.

References

1. Azhmukhamedov I. M., Vybornova O. N. Vvedenie metricheskikh kharakteristik dlya resheniya zadachi otsenki i upravleniya riskami [Introduction of metric characteristics for the problem of risk assessment and management]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Control and High Tecnologies], 2016, no. 1, pp.10.

2. Azhmukhamedov I. M., Vybornova O. N., Brumshteyn Yu. M. Upravlenie riskami informatsionnoy bezopasnosti v usloviyakh neopredelennosti [Management of information security risks in a context of uncertainty]. Avtomatika i vychislitelnaya tekhnika [Automatic Control and Computer Sciences], 2016, vol. 50, no. 8, pp. 657–663.

3. Anikin I. V., Emaletdinova L. Yu., Kirpichnikov A. P. Metody otsenki i upravleniya riskami informatsionnoy bezopasnosti v korporativnykh informatsionnykh setyakh [Methods of information security risk assessment and management in corporate information networks]. *Vestnik tekhnologicheskogo universiteta* [Bulletin of the Technological University], 2015, vol. 18, no. 6, pp. 195–197.

4. Anikin I. V. Tekhnologiya intellektualnogo analiza dannykh dlya vyyavleniya vnutrennikh narushiteley v kompyuternykh sistemakh [Data mining technology to identify insiders in computer systems]. Nauchno-tekhnicheskie vedomosti Sankt-Peterburgskogo gosudarstvennogo politekhnicheskogo universiteta. Informatika. Telekommunikatsii. Upravlenie [St. Petersburg State Polytechnical University Journal. Computer Science. Telecommunication and Control Systems], 2010, vol. 6, no. 113, pp. 112–117.

5. Anikin I. V., Emaletdinova L. Yu. Upravlenie riskami informatsionnoy bezopasnosti v kompyuternykh setyakh na osnove nechetkoy logiki i otsenki sootnosheniya zatrat i vygod [Information security risk management in computer networks based on fuzzy logic and cost/benefit ratio estimation]. *Materialy mezhdunarodnoy konferentsiya ACM. Seriya "Materialy 8-oy Mezhdunarodnoy konferentsii po zashchite informatsii i setey, SIN 2015"* [ACM International Conference Proceeding Series 8. Ser. "Proceedings of the 8th International Conference on Security of Information and Networks, SIN 2015"], 2015.

6. Brumshteyn Yu. M., Vybornova O. N. Analiz nekotorykh modeley gruppovogo upravleniya riskami [Analysis of some models of group risk management]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Control and High Tecnologies], 2015, no. 4, pp. 64–72.

7. Brumshteyn Yu. M. Informatsiya o programmnykh sredstvakh: struktura, istochniki, soderzhanie [Information about the software: structure, sources, content]. *Nauchno-tekhnicheskaya informatsiya* [Scientific and Technical Information], 2017, ser. 1, no. 4, pp. 1–13.

8. Varlataya S. K., Kirzhanenko A. V. Analiz ugroz narusheniya informatsionnoy bezopasnosti informatsionnykh sistem, sushchestvuyushchie modeli i metody protivodeystviya kompyuternym atakam [Analysis of threats to information security of information systems, existing models and methods of countering computer attacks]. *Aktualnye problemy tekhnicheskikh nauk v Rossii i za rubezhom : sbornik nauchnykh trudov po itogam Mezhdunarodnoy nauchno-prakticheskoy konferentsii* [Actual Problems of Technical Sciences in Russia and Abroad. Proceedings of the International Scientific and Practical Conference], Novosibirsk, 2015, no. 2, pp. 162.

9. Vitenburg E. A., Nikishova A. V., Churilina A. E. Sistemy podderzhki prinyatiya resheniy v informatsionnoy bezopasnosti [Decision support systems in information security]. *Vestnik kompyuternykh i infortsionnykh tekhnologiy [*Bulletin of the Computer and Information Technologies], 2015, no. 4, pp. 50–56.

10. Knyazeva O. M., Azhmukhamedov I. M. Metodika otsenki kachestva informatskionnyh sistem na osnove ekspertnykh dannykh [Methods of assessing the quality of information systems based on expert data]. *Matematicheskie metody v tekhnike i tekhnologyakh* [Mathematical Methods in Engineering and Technology], 2017, vol. 1, pp.129–133.

11. Knyazeva O. M. Upravlenie kachestvom informatsionnykh sistem na osnove prostessnogo podkhoda [Quality management of information systems based on process approach]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Control and High Tecnologies], 2016, no. 2, pp. 36–47.

12. Maksimova E. A., Omelchenko T. A., Umnitsyn Yu. P., Guzhakovskaya K. P. Issledovanie voprosov audita informatsionnoy bezopasnosti avtomatizirovannogo rabochego mesta polzovatelya po dannym sistemnogo reestra [Study of information security audit of user's workstation based on registry data]. *Vestnik Volgogradskogo gosudarstvennogo universiteta. Seriya 10: Innovatsionnaya deatelnost* [Bulletin of Volgograd State University. Series 10: Innovation Activity], 2016, no. 4 (23), pp.14–21.

13. Nazarov A. O., Anikin I. V. Raspoznavanie povedeniya obektov metodom nechetkoy klasterizatsii dannykh [Recognition of object behavior by fuzzy clustering]. *Vestnik Kazanskogo gosudarstvennogo tekhnicheskogo universiteta im. A. N. Tupoleva* [Bulletin of the Kazan State Technical University of A. N. Tupolev], 2012, no. 4–1, pp. 222–228.

14. Nikishova A. V., Makedonskiy S. A. Model otsenki kachestva steganograficheskikh system [Model of quality assessment of steganographic systems]. *Promyshlennye ASU i kontrollery* [Industrial ACS and Controllers], 2017, no. 7, pp. 37–43.

15. Nikishova A. V., Rudikov R. F., Kalinina E. A. Neyrosetevoy analiz sobytiy bezopasnosti v informatscionnoy sisteme [Neural network analysis of security events in information system]. *Izvestija JuFU. Tekhnicheskie nauki. Tematicheskiy vypusk. «Informatsionnaya bezopasnost»* [Proceedings of the SFU. Technical Science. Thematic Issue. «Information security»], 2014, no. 2 (151), pp. 80–86.

16. Nikulin A. N., Chernyshev I. V. *Analiticheskaya platforma «Deduktor» – primenenie v informatsionnykh sistemakh ekonomiki* [The analytical platform "Deductor" – application in information systems of the economy: methodical instructions], Ulyanovsk, UlGTU Publ. House, 2012, pp. 37.

17. Silantev I. O., Anikin I. V. Vyyavlenie vnutrennikh narushiteley v korporativnykh setyakh s pomoshchyu metodov nechetkoy logiki [Identification of insiders in corporate networks by using fuzzy logic methods]. *Informatsiya i bezopasnost* [Information and Security], 2017, vol. 20, no. 3 (4), pp. 448–451.

18. Sklyarov A. V., Tishchenko E. N., Stryukov M. B., Sharypova T. N. Upravlenie informatsionnymi riskami zashchishchennykh ekonomicheskikh sistem na osnove analiza nechetkikh vremennykh ryadov [Information risk management of protected economic systems based on fuzzy time series analysis]. *Voprosy ekonomiki i prava* [Issues of economy and Law], 2016, no. 98, pp. 58–60.

19. Tishchenko E. N., Ripka A. V. Ispolzovanie mekhanizmov iskusstvennogo intellekta pri proektirovanii zashchishchennykh informatsionnykh system [Application of artificial intelligence mechanisms in the design of protected information systems]. *Rossiya i ES: puti razvitiya i perspektivy : materialy Mezhdunarodnoy nauchno-prakticheskoy konferentsii* [Russia and the EU: Ways of Development and Prospects. Proceedings of the International Scientific and Practical Conference], 2016, pp. 848–852.

20. Tishchenko E. N., Sharypova T. N. Formalizatsiya vybora razlichnykh variantov sistemy zashchity informatsii ot nesanktsionirovannogo dostupa v srede elektronnogo dokumentooborota [Formalization of choice of different variants of information protection system against unauthorized access in the electronic document flow environment]. *Vestnik Rostovskogo gosudarstvennogo ekonomicheskogo universiteta (RINH)* [Bulletin of the Rostov State Economic University], 2010, no. 32, pp. 226–233.

21. Turovskiy Ya. A., Kurgalin S. D., Adamenko A. A. Sravnitelnyy analiz programmnykh paketov dlya raboty s iskusstvennymi neyronnymi setyami [Comparative analysis of software packages for work with artificial neural networks]. *Vestnik Voronezhskogo gosudarstvennogo universiteta. Seriya: Sistemnyy analiz i informatsionnye tekhnologii* [Bulletin of the Voronezh State University. Series: Systems Analysis and Information Technology], 2016, no. 1, pp. 161–168.

РЕДАКЦИОННЫЙ КОММЕНТАРИЙ К СТАТЬЕ

Данная статья посвящена актуальной теме – обеспечению информационной поддержки принятия решений, связанных с обеспечением информационной безопасности эксплуатируемых на ЭВМ информационных систем (ИС).

Конкретной целью данной статьи является разработка подходов, обеспечивающих отслеживание изменений состояния защищенности информационной системы на основе анализа данных о событиях. На основе анализа событий, происходящих в ИС делаются выводы о ее переходе из защищенного состояния в состояние нарушения защищенности.

Для этой цели авторами предлагается использование интеллектуального анализа (ИА) событий ИС с помощью нейронных сетей. В связи с этим авторами проанализированы характеристики существующих программных средств (ПС), которые могут быть использованы для ИА; разработана собственная программа, позволяющая давать интегральные оценки этих ПС; эта программа апробирована на ряде распространенных ПС для ИА.

По работе можно сделать некоторые замечания. 1) Название статьи не очень хорошо соответствует ее содержанию. Все же основной акцент в работе сделан не на «отслеживании состояния информационных систем», а на

методах выбора оптимального программного средства для анализа событий информационной системы. 2) Из самой статьи не совсем понятно, что отслеживается – нарушения состояния защищенности операционной системы (и если да, то какой) или собственно ИС. 3) Особенности ИС, о которой идет речь в статье, никак не отражены. Между тем сами по себе ИС могут иметь различную степень уязвимости. 4) В таблице 1 приведены некоторые «примеры» нарушений состояния защищенности ИС. Однако название левой колонки выглядит не совсем правильным – в ней перечисляются скорее некоторые варианты попыток нарушения работы ИС. 5) Указанные в правой колонке таблицы 1 события (ситуации) относятся к операционной системе (неясно, какой именно, хотя приводятся конкретные коды), а упоминаемая «сеть» в работе никак не охарактеризована. Можно предположить, что речь идет об ИС, работающей в локальной сети по технологии «клиент-сервер». 6) Не совсем понятно, откуда взялись эти примеры: являются ли они «умозрительными» или получены по результатам эксплуатации конкретной ИС. 7) Также не совсем понятно, как именно эти события нарушают «состояние защищенности». Это можно было бы отдельно прокомментировать после таблицы. 8) При рассмотрении пяти программных средств для ИА данных приведены только 5 из них. При этом сказано, что они являются «наиболее функциональными и популярными». По крайней мере, в отношении популярности можно было бы сослаться на какие-то источники. 9) При описании «методики и результатов проведения экспериментов» сказано, что используются персептроны с двумя скрытыми слоями. Однако если в отношении входного и выходного слоев дана детальная информация, то о назначении скрытых слоев ничего не сказано. 10) В отношении входной информации вероятно стоило бы пояснить следующее: как используются сведения о «дате и времени возникновения события»; как были назначены «уровни важности событий»; о каких «учетных записях» идет речь; как были взяты «границы допустимых значений характеристик событий безопасности ИС». Таким образом, в целом раздел, посвященный тестированию нейросетевых пакетов, имеет некоторые недоговоренности.