УДК 681.3.067

Е.Н. Пивкин, В.М. Белов, С.А. Белкин

К вопросу об анализе защищенности объектов информатизации с использованием нейронных сетей

Предложена общая схема оценки защищенности объектов информатизации с использованием нейронных сетей. Определены частные и общие показатели оценки защищенности объектов информатизации.

Ключевые слова: защищенность объектов информатизации, нейронные сети.

При эксплуатации объектов информатизации (ОИ) в организациях на всех этапах жизненного цикла ОИ возникают проблемы обеспечения безопасности информации. Одной из задач обеспечения безопасности информации на ОИ является оценка состояния защищенности ОИ, позволяющая выявить недостатки системы защиты ОИ и принять соответствующие меры по противодействию дестабилизирующим факторам [6]. Решение задачи оценки защищенности зависит от степени влияния множества факторов, а поскольку неизвестна взаимосвязь между исходными показателями защищенности, то функцию итогового показателя сложно определить формально.

В нашей работе для решения обозначенной выше задачи предлагается применять искусственные нейронные сети (НС), так как использование традиционных вычислений трудоемко и слабо отражает реальные физические процессы и объекты.

Нужно отметить, что выделяют следующие частные задачи анализа защищенности ОИ [1, 4, 7]:

– оценка уровня защищённости информационных систем (ИС);

– определение наиболее незащищённых мест в ИС;

– разработка моделей нарушителей информационной безопасности (ИБ);

– анализ возможных угроз ИБ;

– оценка рисков ИБ ИС;

– выработка рекомендаций по повышению эффективности систем защиты ИС от внешних и внутренних угроз;

– прогнозирование попыток несанкционированного доступа в компьютерную систему;

– моделирование противоборства злоумышленника и специалиста по защите информации.

По итогам рассмотрения различных нейропакетов для анализа защищенности ОИ был выбран нейропакет Neural Network Toolbox системы Matlab. Он обладает возможностью автоматизации процесса поиска оптимальной НС для решения поставленной задачи. Общий алгоритм оценки защищенности ОИ с применением НС представлен на рис. 1.

Решение задачи анализа защищенности ОИ с применением НС можно рассмотреть поэтапно [2, 3]:

1. Постановка задачи в терминах НС. Проверка гипотезы о разумности применения НС для решения задачи, представление ожидаемого результата работы НС и способ его дальнейшего использования.

2. Выбор топологии сети. Выбирают тип сети, исходя из постановки задачи и имеющихся данных для обучения.

3. Подбор характеристик сети. Экспериментально подбирают параметры сети: число слоев, число блоков в скрытых слоях, наличие или отсутствие обходных соединений, передаточные функции нейронов и т.д.

4. Отбор данных, формирование обучающей выборки. В обучающую выборку включают данные, которые описывают условия, близкие к условиям дальнейшего использования нейросистемы.

5. Подбор параметров обучения. Значения параметров обучения выбирают экспериментально, руководствуясь при этом критерием завершения обучения (например, минимизация ошибки или ограничение по времени обучения).

6. Обучение НС. Обучение НС заключается в процессе представления НС обучающих данных.

7. Проверка адекватности обучения. Тестирование качества обучения НС проводится на примерах, которые не участвовали в ее обучении. Если полученные результаты существенно отличаются от ожидаемых, то необходимо вернуться к постановке задачи [2, 3].

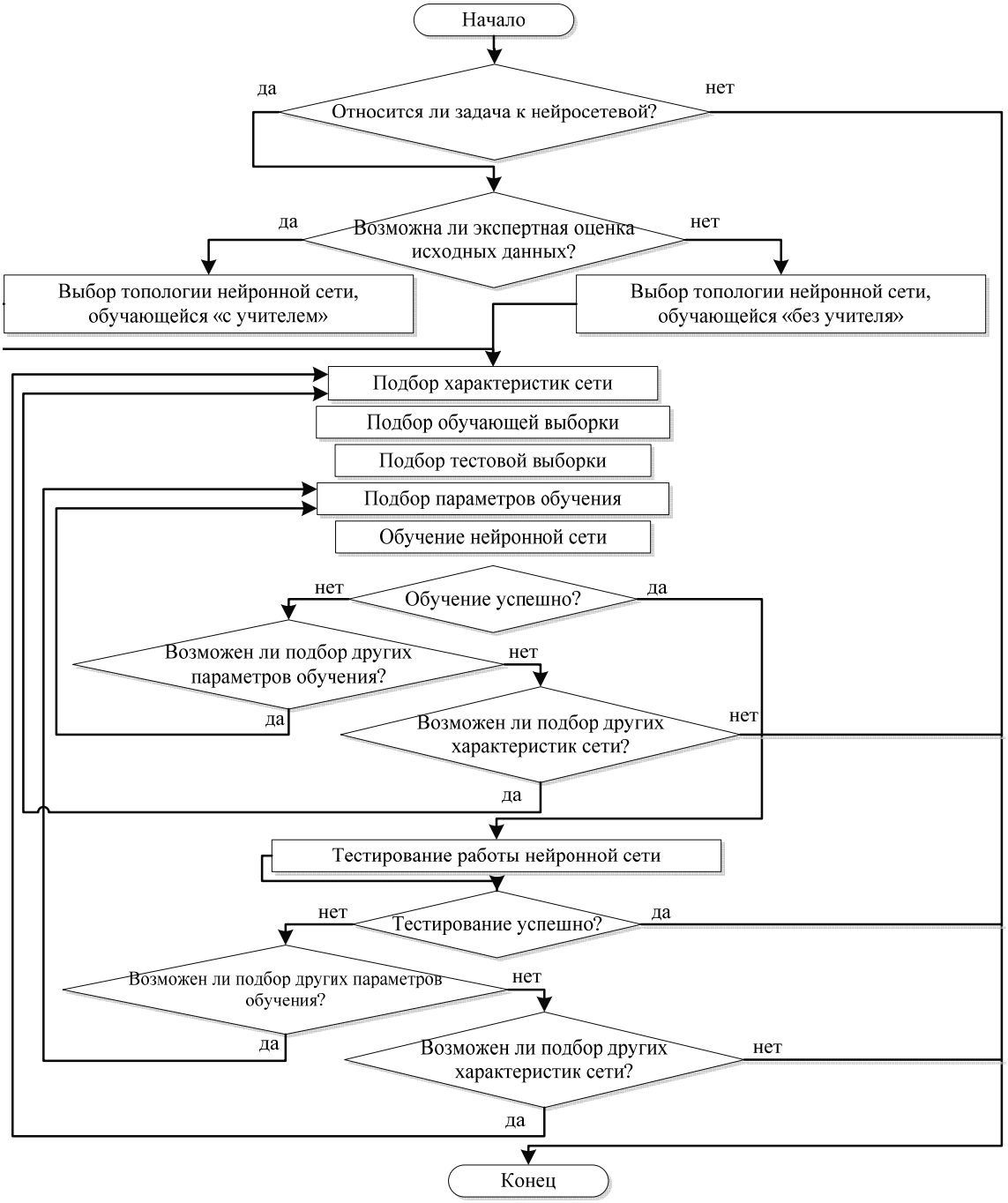

Рис. 1. Общий алгоритм оценки защищенности с использованием НС

Оценку защищенности ОИ выполняют с использованием отечественных и зарубежных методик, различных стандартов, в соответствии с которыми решение задачи сводят к анализу определенного количества показателей.

Предлагается осуществлять оценку уровня защищенности по следующим 8 групповым показателям: управление доступом; регистрация и учет; управление сетью; антивирусная защита; организация защиты персональных данных; контроль целостности и резервное копирование; физическая безопасность; криптографическая защита (при необходимости).

Для каждого направления оценки сформирован набор частных показателей. Всего выделено 79 частных показателей. Рассмотрим следующие частные показатели защищенности для направления «Контроль целостности и резервное копирование»:

1. Определены ли в документах организации, выполняются ли и контролируются ли процедуры контроля целостности?

2. Реализованы ли в системах, используемых в организации, защитные меры, обеспечивающие невозможность отказа от авторства проводимых сотрудниками операций и транзакций (например, электронная подпись (ЭП))?

3. Выполняется ли проверка целостности программного обеспечения, занимающегося обработкой критических данных (и самих данных)?

4. Определены ли в документации и осуществляются ли в организации процедуры регулярного резервного копирования информации?

5. Располагаются ли резервные копии вместе с инструкциями по восстановлению в месте, территориально отдаленном от основной копии информации?

6. Осуществляется ли регулярная проверка носителей, на которые осуществляется резервное копирование, на отсутствие сбоев?

7. Проводятся ли регулярные проверки процедур восстановления с целью поддержания возможности восстановления данных в установленном порядке и за гарантированный промежуток времени?

При оценке защищенности ОИ необходимо использовать экспертные оценки. Оценка должна основываться на свидетельствах, в качестве основных источников которых рекомендуется использовать:

– внутренние нормативные документы проверяемой организации и при необходимости документы третьих лиц, относящиеся к обеспечению ИБ организации;

– устные высказывания сотрудников проверяемой организации в процессе проводимых опросов;

– результаты наблюдений членов экспертной группы за деятельностью сотрудников проверяемой организации в области ИБ;

– результаты обследования экспертами ИС проверяемой организации;

– результаты использования экспертами инструментальных средств анализа защищенности.

Общая схема оценки защищенности ОИ представлена на рис. 2.

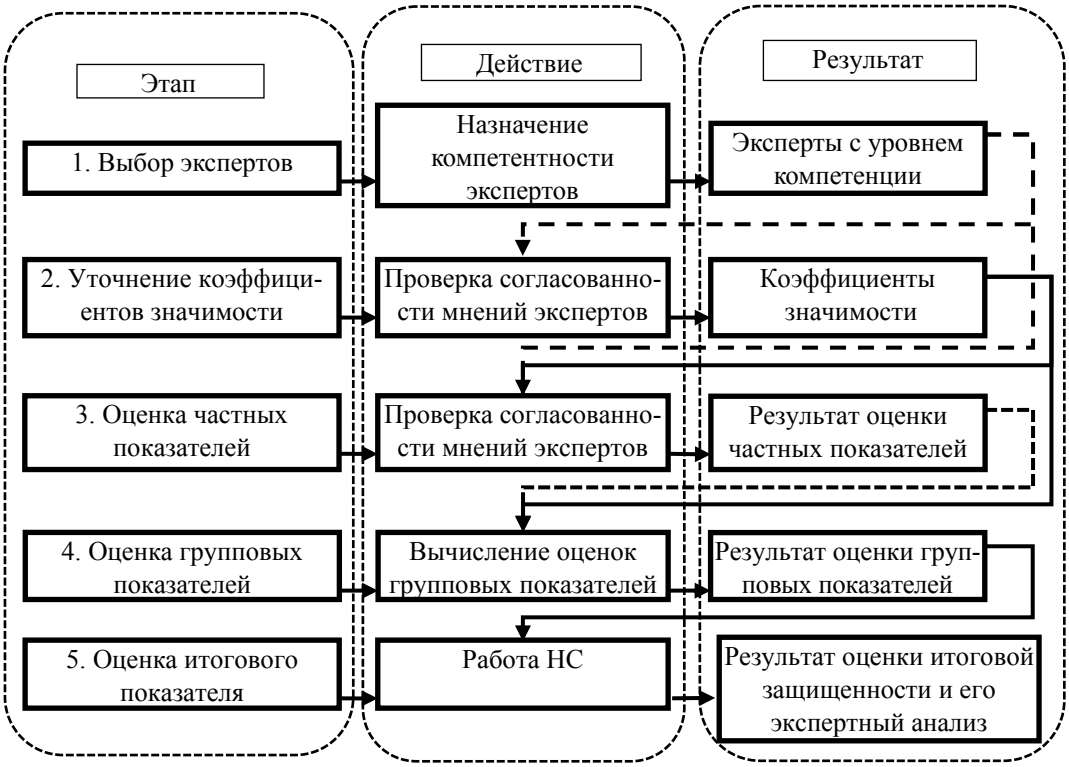

Рис. 2. Общая схема оценки защищенности ОИ с использованием НС

Сначала производят выбор экспертной группы. Формирование группы экспертов осуществляют из специалистов по обеспечению безопасности информации организации, обладающих достаточными знаниями. Эксперты имеют разную степень компетентности, которую учитывают при определении общей оценки частного показателя защищенности или коэффициента значимости частного показателя. Каждый эксперт независимо выставляет оценку каждому частному показателю (воз-

можные значения [0, 1]). После оценки согласованности мнений экспертов определяют итоговые оценки частных показателей с учетом степеней компетентности экспертов и оценки групповых показателей с учетом степеней коэффициентов значимости частных показателей. Групповые показатели оценивают как с использованием экспертных оценок, так и путем применения НС. Групповые показатели подают на вход НС и получают итоговый показатель оценки защищенности.

Предложена следующая архитектура НС [5]: полносвязная сеть прямого распространения «Многослойный персептрон», обучающаяся алгоритмом обратного распространения ошибки. Функция активации нейронов – логистическая. Количество слоев сети и число нейронов в каждом скрытом слое определялось экспериментально. Были смоделированы следующие НС:

– однослойная сеть с 8–16 скрытыми нейронами;

– двухслойная сеть с 8–24 нейронами в 1-м скрытом слое и с 8–20 нейронами во 2-м скрытом слое;

– трехслойная сеть с 12–24 нейронами в 1-м скрытом слое и с 12–20 нейронами во 2-м скрытом слое, с 8–16 нейронами в 3 скрытом слое.

Из рассмотренных НС была выбрана – двухслойная НС с 12 нейронами в 1-м скрытом слое, 8 нейронами во 2-м скрытом слое (ошибка обучения составляет 0,0862).

Результаты обучения нейронной сети: нейронная сеть обучена за 7 эпох, ошибка достигла 0,00862 при допустимой ошибке 0,01 на обучающей выборке.

Оценку защищенности ОИ организации проводили до и после применения мер по защите информации. Значения групповых показателей приведены в таблице.

Значения групповых показателей

Групповой показатель	Значения до применения защитных мер	Значения после применения защитных мер
Управление доступом	0,7786	0,909
Регистрация и учет	0,5403	0,777
Управление сетью	0,69	0,953
Антивирусная защита	0,9937	1
Организация защиты персональных данных	0,8897	0,9412
Контроль целостности и резервное копирование	0,4421	0,9671
Физическая безопасность	0,47525	0,667625
Криптографическая защита	0,8164	1

Значения групповых показателей были поданы на вход НС. В результате, значение итоговой защищенности, определенное с использованием НС без учета предложенных мер защиты, составляет 0,7344 и не является рекомендуемым. Защищенность с учетом предложенных мер защиты составляет 0,8765 и является рекомендуемой. Разность итоговых показателей определяет эффективность применения предложений защиты и составляет 0,1421, т.е. 14%.

На основе общей схемы оценки защищенности ОИ была разработана методика анализа защищенности ОИ, применение которой позволяет количественно оценить уровень защищенности ОИ, а также эффективность внедренных мер защиты. Методика позволяет выявить не поддающуюся формальному определению взаимосвязь между оцениваемыми показателями и степенью влияния каждого показателя на итоговую защищенность.

Методика может применяться для анализа защищенности ОИ уровня местного самоуправления города. Таким образом, методика анализа защищенности ОИ организации с использованием НС позволяет решить задачу количественной оценки защищенности и обосновать необходимость и (или) эффективность внедрения средств и мер защиты информации в организации.

Литература

1. Галушкин А.И. Нейрокомпьютеры в решении задач обеспечения информационной безопасности // Информационные технологии. – 2011. – № 1. – С. 34–38.

2. Крыжановский А.В. Применение искусственных нейронных сетей в системах обнаружения атак // Доклады ТУСУРа. – 2008. – Т. 2. – С. 104–105.

3. Нестерук Ф.Г. Основы организации адаптивных систем защиты информации: учеб. пособие. – СПб.: СПбГУ ИТМО, 2008. – 112 с.

4. Бахтин А.М. Возможные области применения нейронных сетей при оценке защищенности объектов информатизации / А.М. Бахтин, Е.Н. Пивкин // Измерение, контроль, информатизация: матер. XIV Междунар. науч.-техн. конф. / Под ред. Л.И. Сучковой. – Барнаул: Изд-во АлтГТУ, 2013. – Т. 2. – С. 172–174.

5. Бахтин А.М. Применение нейросетевого подхода для оценки защищенности объекта информатизации / А.М. Бахтин, Е.Н. Пивкин // Матер. X Всерос. науч.-техн. конф. студентов, аспирантов и молодых ученых «Наука и молодежь – 2013» [Электронный ресурс]. – Режим доступа: http://edu.secna.ru/media/f/vsib_tez_2013.pdf, свободный (дата обращения: 25.06.2013).

6. Мещеряков Р.В. Комплексное обеспечение информационной безопасности автоматизированных систем / Р.В. Мещеряков, А.А. Шелупанов. – Томск: В-Спектр, 2007. – 349 с.

7. Ерохин С.С. Модели и методы оценки защищенности информации и информационной безопасности объекта / С.С. Ерохин, Р.В Мещеряков, С.С. Бондарчук // Безопасность информационных технологий. – 2007. – № 4. – С. 39–46.

Пивкин Евгений Николаевич
Канд. техн. наук, главный специалист-эксперт отдела безопасности УФНС России по Московской обл.
Тел.: 8-906-942-02-17
Эл. почта: evpiv@yandex.ru

Белов Виктор Матвеевич
Д-р техн. наук, профессор каф. безопасности и управления в телекоммуникациях
Сибирского государственного университета телекоммуникаций и информатики
Тел.: 8 (383) 269-82-45
Эл. почта: vmbelov@mail.ru

Белкин Сергей Алексеевич
Аспирант каф. информационной безопасности
Новосибирского государственного университета экономики и управления «НИНХ»
Тел.: 8-913-772-86-23
Эл. почта: serega-box2011@yandex.ru

Pivkin E.N., Belov V.M., Belkin S.A.

On the issue of the analysis of the security of objects of informatization using neural networks

A general scheme of assessment of objects of informatization using neural networks is proposed. Private and global indicators for assessing the security object informatization are defined.

Keywords: protection of objects of informatization, neural networks.