И. В. Машкина, А. Ю. Сенцова

АВТОМАТИЗАЦИЯ ЭКСПЕРТНОГО АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОЙ НЕЙРОННОЙ СЕТИ[1]

Аудит информационной безопасности (ИБ) — один из аспектов управления ИБ. Аудит целесообразно проводить после разработки системы обеспечения информационной безопасности (СОИБ) для оценивания результатов проектирования; аудит проводится в ходе эксплуатации информационной системы (ИС) для оценки эффективности существующих мер защиты, активный аудит проводится при расследовании инцидентов ИБ в режиме реального времени.

Качество аудита безопасности зависит от адекватности информации об объекте оценки: сведений о топологии сети, сведений об инфраструктуре информационной системы, об установленных средствах защиты, об используемой политике информационной безопасности, программном обеспечении, схеме информационных потоков.

Аудит нарушения ИБ обеспечивает получение и *оценку* объективных данных о текущем состоянии защищенности информационной системы. Необходимость осуществления аудита безопасности связана со сложностью инфраструктуры современных ИС, множеством используемых приложений, обрабатываемым объемом данных, сложностью реализации системы информационной безопасности, необходимостью учета всего спектра потенциально возможных угроз.

Аудит безопасности ИС — это экспертиза состояния защищенности, включающая *получение объективных данных* о параметрах и условиях функционирования системы, которые могут влиять на защищенность, *и их анализ*. В результате эксперт выявляет, насколько рационально решены вопросы безопасности информации и контроля доступа, как минимизировать риски при обработке в ИС конфиденциальной информации заказчика, выявляет локализацию слабых мест в системе обеспечения информационной безопасности и выдает рекомендации о путях решения существующих проблем.

Для осуществления процедуры анализа исходных данных аудитор может применить методику, которая позволила бы оценить соответствие используемых в системе обеспечения информационной безопасности механизмов защиты требованиям существующих стандартов информационной безопасности. Однако на сегодняшний день такие методики отсутствуют [1], а стандарты информационной безопасности для облачных сред находятся в процессе разработки [2]. Другой подход к проведению анализа в ходе аудита основан на *оценке рисков*. В этом случае должны быть идентифицированы все возможные угрозы, выявлены и оценены уязвимости. Эксперт в аудиторском отчете указывает используемый им при анализе метод расчета информационных рисков.

В работах [3, 5] предложена модель процесса оценки риска нарушения информационной безопасности, которая базируется на *построении* нечетких когнитивных карт в качестве моделей угроз, на *определении* вероятности реализации каждой возможной угрозы в зависимости от величин уязвимостей компонентов инфраструктуры и средств защиты на физическом пути распространения атаки, а также на *определении* показателя «ценность информации» для защищаемых информационных активов. Для описания модели оценки уровня риска используются графическое и аналитическое представления. Графическое представление — когнитивные карты — позволяет учесть множество угроз, аналитическое представление в виде математических формул позволяет провести расчеты. Полученная в ходе аудита оценка риска нарушения ИБ показывает, насколько эффективно применяемые средства и технологии защиты способны противостоять угрозам на путях их распространения. В зависимости от результатов анализа разрабатываются рекомендации по повышению уровня защищенности объекта оценки.

[1] Работа выполнена при поддержке гранта РФФИ № 14-07-00928-а.

Такой подход к проведению аудита позволит, используя рекомендации эксперта, обоснованно *планировать* деятельность по обеспечению безопасности своей информационной системы и эффективно использовать ее для развития бизнеса. Оценка *прогнозируемого* значения риска связана со *стратегией* безопасности, которая разрабатывается заблаговременно. В ходе мониторинга безопасности обеспечивается получение информации о состоянии сетевых устройств, о событиях, нарушающих безопасность, в *режиме реального времени*. При проявлении атаки или обнаружении таких событий в информационной системе необходимы тактические действия. Тактические действия должны быть результатом организованного взаимодействия систем мониторинга и управления устройствами сетевой безопасности. Такой мониторинг называют *активным* аудитом [1].

В работе [3] предложено для получения оценки прогнозируемого значения риска и оперативного значения риска в ходе активного аудита использовать искусственную нейронную сеть (ИНС).

В продолжение этих исследований были проведены эксперименты с различными архитектурами искусственных нейронных сетей для получения численных оценок как прогнозируемого, так и оперативного значений уровней риска нарушения ИБ. Анализ полученных результатов показал целесообразность использования архитектуры ИНС на основе многослойного персептрона. Многослойный персептрон состоит из нейронов, расположенных на разных уровнях, причем, помимо входного и выходного слоев, число нейронов в которых формируется на основе размерности обучающей выборки искусственной нейронной сети, имеется еще один внутренний скрытый слой. Целью обучения многослойного персептрона является подбор таких значений весов-коэффициентов для всех слоев сети, чтобы при заданном входном векторе (inputs) получить на выходе значения, которые с требуемой точностью будут совпадать с ожидаемыми значениями (targets). Фрагмент массива данных множества обучающей выборки, использованной для обучения искусственной нейронной сети, приведен в таблице 1.

Таблица 1. Фрагмент массива данных для обучения ИНС

Ра_ЗЛ	Ра_ВНШ_КЛ	Ра_АДМ	Ра_КЛ	C1 Cl	C2 КЭШ	C3 ADM	C4 V	R
0	0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	0	0
0	0	0	1	0	0	0,3	0,7	0,008
0	0	0	1	0	0,1	0,3	0,6	0,0288
0	0	0	1	0,1	0,1	0,3	0,5	0,041
0	0	0	1	0,2	0,1	0,3	0,4	0,054
0	0	0	1	0,3	0,1	0,3	0,3	0,066
0	0	0	1	0,4	0,1	0,3	0,2	0,079
0	0	0	1	0,5	0,1	0,3	0,1	0,091
0	0	0	1	0,6	0,1	0,3	0	0,1
0	0	0	1	0,7	0	0,3	0	0,095
0	0	1	0	0	0	0	0	0
0	0	1	0	0	0	0,3	0,7	0,15
0	0	1	0	0	0,1	0,3	0,6	0,13
0	0	1	0	0,1	0,1	0,3	0,5	0,11
0	0	1	0	0,2	0,1	0,3	0,4	0,088

0	0	1	0	0,3	0,1	0,3	0,3	0,066
0	0	1	0	0,4	0,1	0,3	0,2	0,044
0	0	1	0	0,5	0,1	0,3	0,1	0,22
0	0	1	0	0,6	0,1	0,3	0	0
0	0	1	0	0,7	0	0,3	0	0
…								
1	1	1	1	0	0	0	0	0
1	1	1	1	0	0	0,3	0,7	0,257
1	1	1	1	0	0,1	0,3	0,6	0,2496
1	1	1	1	0,1	0,1	0,3	0,5	0,238
1	1	1	1	0,2	0,1	0,3	0,4	0,227
1	1	1	1	0,3	0,1	0,3	0,3	0,22
1	1	1	1	0,4	0,1	0,3	0,2	0,2
1	1	1	1	0,5	0,1	0,3	0,1	0,193
1	1	1	1	0,6	0,1	0,3	0	0,18
1	1	1	1	0,7	0	0,3	0	0,177

В работе использовалась многослойная сеть с одним скрытым слоем и десятью нейронами в скрытом слое. Как показали эксперименты, проведенные в среде Matlab, увеличение числа слоев приведет к переобучению нейронной сети, когда она хорошо функционирует на примерах обучающей выборки (train), но показывает плохие результаты на тестовых примерах (test), подчиненных тому же статистическому распределению. Выбранная для расчетов архитектура искусственной нейронной сети показана на рис. 1.

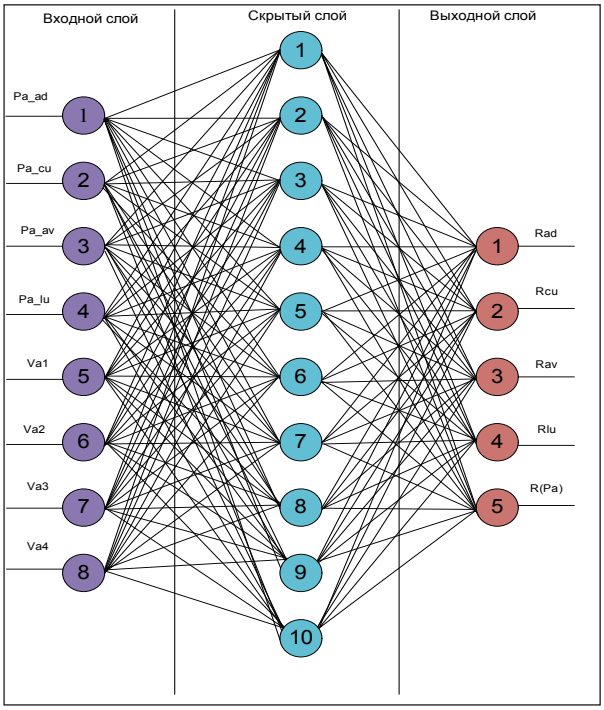

Рис. 1. Архитектура искусственной нейронной сети

Для обучения многослойного персептрона был выбран алгоритм обратного распространения ошибки, который впервые был описан А. И. Галушкиным, а также независимо и одновременно с ним Полом Дж. Вербосом и считается в настоящее время одним из наиболее эффективных алгоритмов обучения искусственной нейронной сети [4]. Данный алгоритм определяет стратегию подбора весов многослойной сети с применением градиентных методов оптимизации. В процессе обучения рассчитывается целевая функция в виде квадратичной суммы разностей между фактическим и ожидаемым значениями выходных сигналов. Для обучения ИНС с помощью сформированного массива данных был использован программный модуль Matlab. Нейронная сеть прошла 9 эпох, постепенно обучаясь и сокращая ошибку обучения. При *обучении* ошибка составила около 10^{-7} мсэ, при *тестировании* сети — от 10^{-5} до 10^{-2} мсэ. График, иллюстрирующий процесс обучения нейронной сети, представлен на рис. 2.

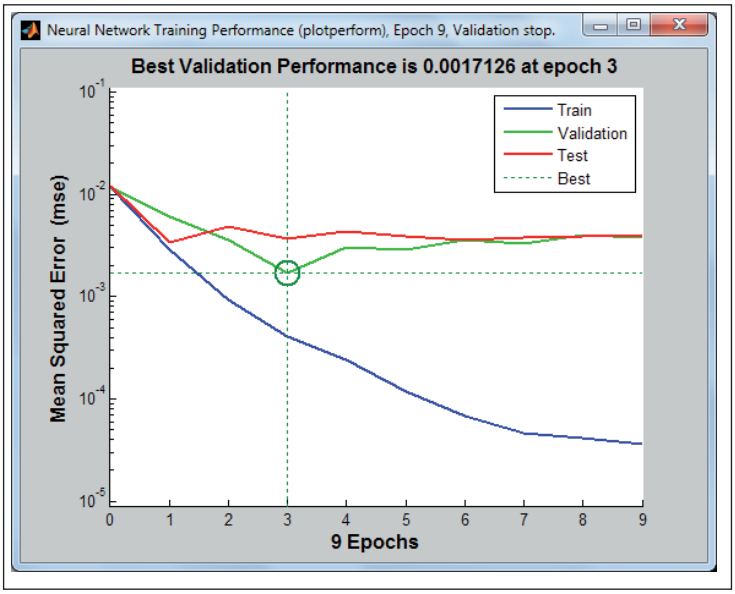

Рис. 2. График обучения ИНС

После обучения была проведена проверка результатов обучения в среде Simulink на контрольном примере. Все пять выходов искусственной нейронной сети с требуемой точностью совпадают с ожидаемыми значениями. Работа в среде Simulink проиллюстрирована на рис. 3 и 4.

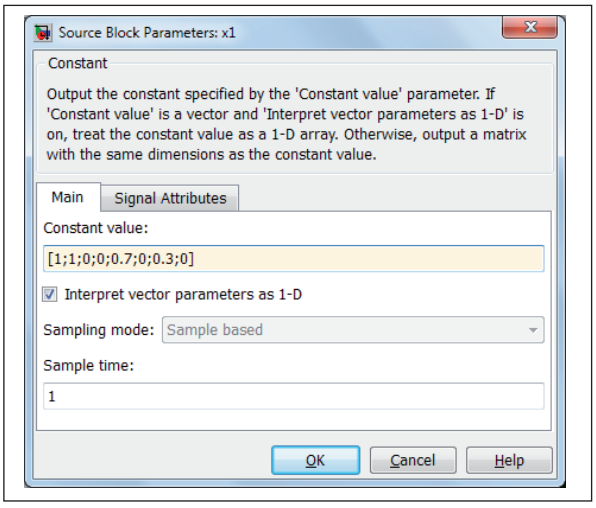

Рис. 3. Окно ввода исходных данных для моделирования

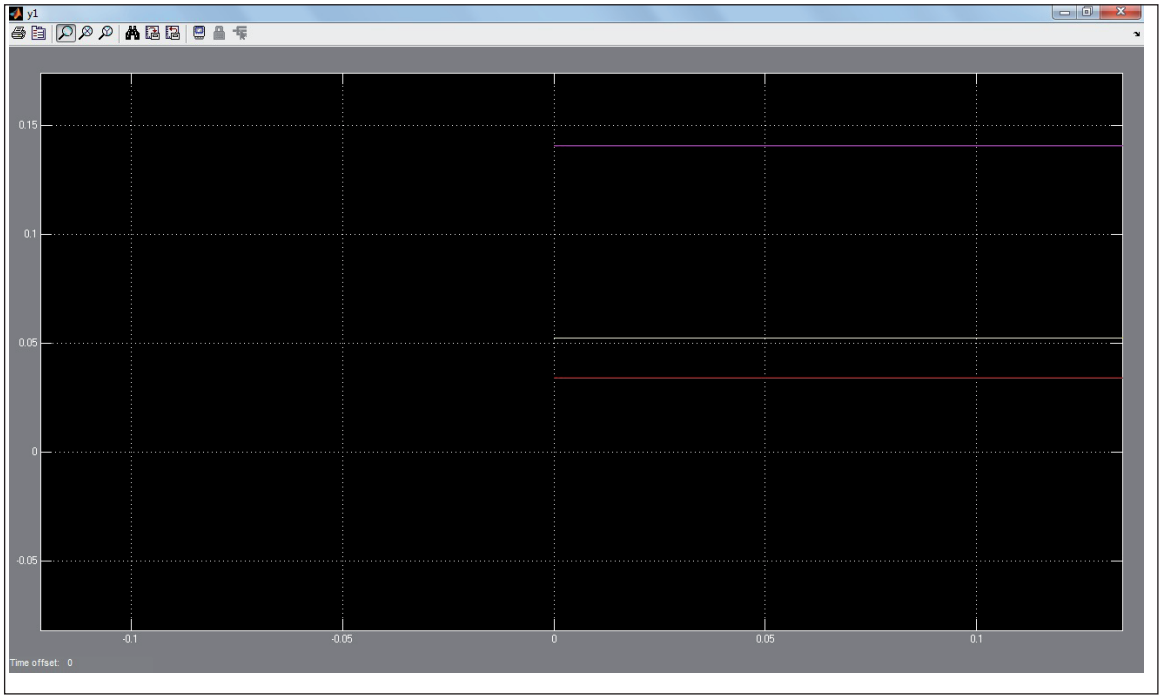

Рис. 4. Экранная форма с результатами контрольного примера

На рис. 3 заданы значения ценностей информационных ресурсов и каналы актуальных угроз, на рис. 4 отображены значения уровней риска нарушения ИБ в случае сложного сценария атаки от двух источников угроз.

Результаты обучения и тестирования нейронной сети показали возможность использования выбранной архитектуры и алгоритма ИНС для разработки модуля численной оценки риска нарушения ИБ в программном комплексе, предназначенном для автоматизации аудита нарушения ИБ информационной системы.

Состав модулей и структура автоматизированной системы проведения экспертного аудита представлены на рис. 5.

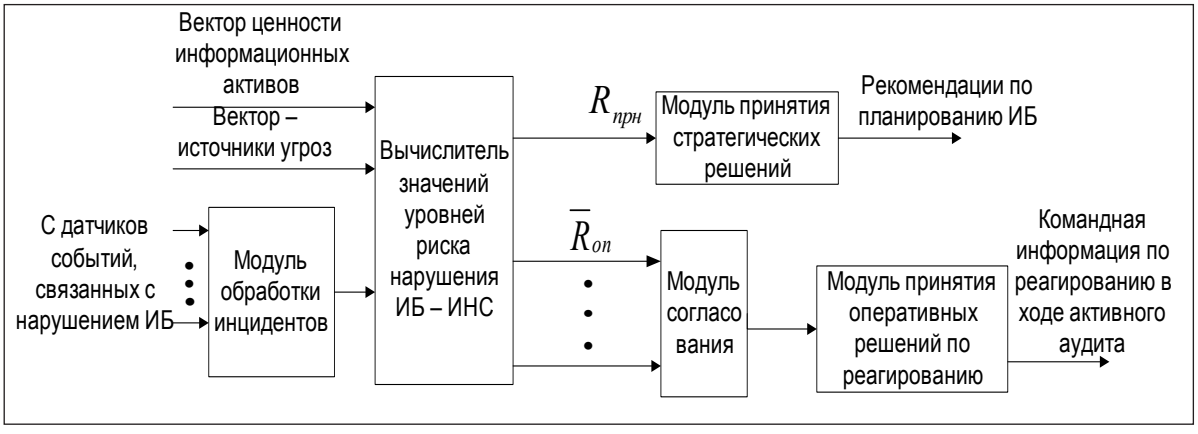

Рис. 5. Структура автоматизированной системы проведения экспертного аудита: $R_{прн}$ — прогнозируемое значение риска; $R_{оп}$ — оперативное значение риска

Настройка вычислителя осуществляется по схеме, приведенной в [3]. Работоспособность метода и автоматизированной системы экспертного аудита проверена на основе тестирования. Прогнозируемые риски связаны с планируемыми к внедрению технологиями для реализации бизнес-процессов, планируемыми средствами и механизмами защиты. Оценивание прогнозируемого

риска позволяет осуществить выбор наилучших наборов контрмер, выбрать наиболее эффективные средства защиты, провести анализ влияния архитектуры безопасности на величину риска.

С другой стороны, очевидно, что администратор безопасности быстрее и более рационально обработает опасное событие, если процедуры обработки, соответствующие технологии определены заранее, а методы реагирования зависят от того оперативного значения риска, который связан с данным инцидентом.

В зависимости от величины риска модуль принятия решений о реагировании формирует командную информацию, например, для информационной системы облачных вычислений: остановить и перезапустить сервер, снять моментальный снимок, остановить сервер и осуществить его замену, почистить сервер и снова запустить его; выполнить определенные процедуры для всех серверов в кластере, устранить уязвимости в образе машины.

В работе предлагается в ходе активного аудита осуществить отображение результатов на консоли, исследуется возможность формирования управляющих команд для реализации их вручную администратором или автоматически с помощью встроенных в средства защиты управляющих модулей.

Преимуществом разработанной автоматизированной системы является то, что в ней используется модель, позволяющая осуществить анализ реально выявленных угроз и выполнить оценку рисков нарушения информационной безопасности с учетом сложных сценариев атак, когда активизируется более одного источника угроз.

СПИСОК ЛИТЕРАТУРЫ:

1. *Шаньгин В. Ф.* Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2010. — 544 с.
2. ГОСТ Р XXXXX—20XX (проект, первая редакция) «Защита информации. Требования по защите информации, обрабатываемой с использованием технологии виртуализации. Общие положения». URL: https://drive.google.com/file/d/0B5PXq-icGjzLbTd4LVlnT21yZ0k/preview (дата обращения: 01.02.2014).
3. *Машкина И. В., Сенцова А. Ю.* Методология экспертного аудита в системе облачных вычислений // Безопасность информационных технологий. 2013. № 4. С. 63—70.
4. *Осовский С.* Нейронные сети для обработки информации / Пер. с польского И. Д. Рудинского. М.: Финансы и статистика, 2002. — 344 с.
5. *Гузаиров М. Б., Машкина И. В., Степанова Е. С.* Построение модели угроз с помощью нечетких когнитивных карт на основе сетевой политики безопасности // Безопасность информационных технологий. 2011. № 2. С. 37—49.

REFERENCE:

1. *Shangin V. F.* Zaschita computernoy informacii. Effektivnye metody i sredstva. M.: DMK Press, 2010. — 544 s.
2. GOST R XXXXX—20XX (proekt, pervaya redakciya) «Zaschita informacii. Trebovaniya po zaschite informacii, obrabativaemoy c ispolzovaniem tekhnologii virtualizacii. Obschie polozheniya» URL: https://drive.google.com/file/d/0B5PXq-icGjzLbTd4LVlnT21yZ0k/preview (data obrascheniya: 01.02.2014).
3. *Mashkina I. V., Sentsova A. U.* The methodology of expert audit in the cloud computing system // Information technology security 2013. № 4. P. 63—70.
4. *Osovskiy S.* Neyronnye seti dlya obrabotki informacii / Per. s polskogo I. D. Rudinskogo. M.: Financy i statistika, 2002. — 344 s.
5. *Guzairov M. B., Mashkina, I. V., Stepanova E. S.* The treats model development by fuzzy cognitive maps formation on the bases of security policy // Information technology security 2011. № 2. P. 37—49.