8. *General vulnerability assessment system, version 3.1, Technical document, Revision 1.* Available at: https://www.first.org/cvss/v3.1/specification-document (accessed 19.01.2020).

9. *Prikaz FSTEK Rossii ot 11.02.2013 №17 "Ob ytvergdenii trebovanii o zashchite informatsii, ne sostavlayushchey gosudarstvennuyu tayny, sodergashcheysya v gosydarstvennykh informatsionnykh sistemakh"* [FSTEC order no. 17.11.2013 «On approval of requirements for the protection of information that does not constitute a state secret contained in state information systems»]. Available at: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702 (accessed 19.01.2020).

10. *Prikaz FSTEK Rossii ot 31.03.2014 № 31 "Ob utverzhdenii trebovaniy o zashchite informatii v avtomatizirovannykh sistemakh upravleniya proizvodstvennymmi i tekhnologicheskimi protsessami na kriticheskihh vazhnykh obektakh, potentsialno opasnykh obektakh, a takzhe obektakh predstavlayushikh povyshennuyu opasnost dlya zhizni izdorovya ludey i dlya okruzhaiyshchey prirodnoy sredy"* [FSTEC order no. 31 of March 14, 2014 «On approval of requirements for ensuring information security in automated production and process control systems at critical facilities, potentially dangerous facilities, as well as objects that pose an increased risk to human life and health and the environment»]. Available at: https://fstec.ru/index?id=868:prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (accessed 19.01.2020).

11. *Sayt bazy dannykh uyazvimostey* [Vulnerability database site]. Available at: https://nvd.nist.gov/vuln-metrics/cvss (accessed 20.01.2020).

12. *Sayt bazy dannykh uyazvimostey* [Vulnerability database site]. Available at: https://nvd.nist.gov/vuln/ (accessed 20.01.2020).

13. *Sayt bazy dannykh uyazvimostey* [Vulnerability database site]. Available at: http://www.cvedetails.com (accessed 20.01.2020).

14. *Sayt bazy dannykh uyazvimostey* [Vulnerability database site]. Available at: http://www.securityfocus.com (accessed 20.01.2020).

DOI 10.21672/2074-1707.2020.49.4.169-178
УДК 004.056

ОПРЕДЕЛЕНИЕ АКТУАЛЬНОСТИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ МАТЕМАТИЧЕСКОГО АППАРАТА НЕЙРОННЫХ СЕТЕЙ

Статья поступила в редакцию 04.02.2020, в окончательном варианте – 09.03.2020.

Жук Роман Владимирович, Филиал «Макрорегион Юг» ООО ИК «СИБИНТЕК», 352800, Российская Федерация, г. Туапсе, ул. Карла Маркса, 36,

главный специалист, e-mail: goonerkrd@gmail.com

Дзьобан Павел Игоревич, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,

кандидат технических наук, доцент кафедры компьютерных технологий и информационной безопасности Института компьютерных систем и информационной безопасности, e-mail: antiemoboy@mail.ru

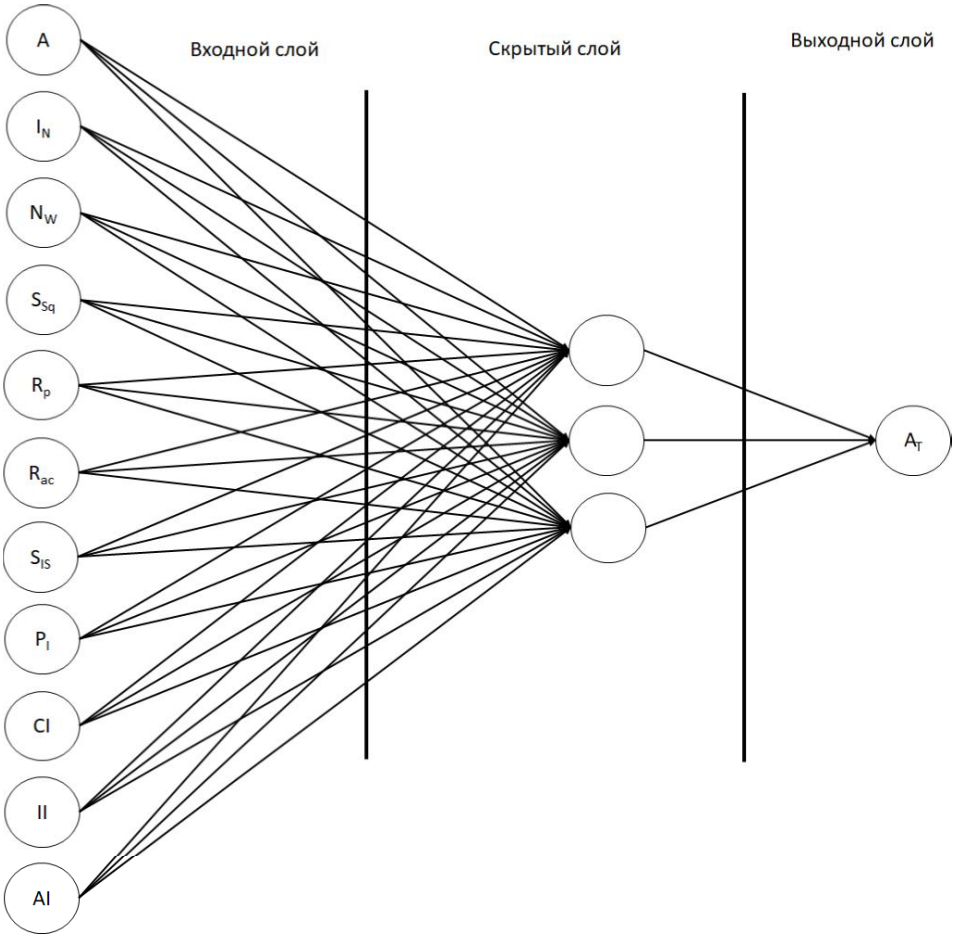
Власенко Александра Владимировна, Кубанский государственный технологический университет, 50072, г. Краснодар, ул. Московская, 2,

кандидат технических наук, доцент, заведующая кафедрой компьютерных технологий и информационной безопасности института компьютерных систем и информационной безопасности, e-mail: Alex_Vlasenko@list.ru

Рассмотрены методики определения угроз информационной безопасности в информационных системах обработки персональных данных. В связи с отсутствием согласованности существующей утвержденной методики с применяемой банком данных угроз информационной безопасности (https://bdu.fstec.ru/) был проведен анализ параметров актуальности угроз информационной безопасности и предложен способ определения актуальности угроз информационной безопасности с использованием математического аппарата искусственных нейронных сетей. Для реализации этого способа был выполнен анализ топологий искусственных нейронных сетей и методов вычисления ошибок в них. Разработана искусственная нейронная сеть на основании топологии многослойного перцептрона с обратным распространением ошибки. Проведено обучение разработанной искусственной нейронной сети путем подготовки и использования обучающей выборки. Осуществлено сравнение быстродействия функционирования разработанной искусственной нейронной сети с быстродействием привлеченной группы экспертов, действующих по существующей утвержденной методике определения актуальности угроз информационной безопасности в информационных системах обработки персональных данных.

Ключевые слова: показатель исходной защищенности, потенциал нарушителя информационной безопасности, искусственная нейронная сеть, перцептрон, искусственный нейрон, слой, входной сигнал, выходной сигнал, функция активации, сигмоидальная функция, обучающая выборка, угроза информационной безопасности

Графическая аннотация (Grapchical annotation)



DETERMINING THE RELEVANCE OF INFORMATION SECURITY THREATS IN INFORMATION SYSTEMS FOR PROCESSING PERSONAL DATA USING THE MATHEMATICAL APPARATUS OF NEURAL NETWORKS

The article was received by the editorial board on 04.02.2020, in the final version – 09.03.2020.

Zhuk Roman V., Branch «Macroregion South» Ltd Co IC «SIBINTEK», 36 Karl Marks St., Tuapse, 352800, Russian Federation,

chief specialist, e-mail: goonerkrd@gmail.com

Dzoban Pavel I., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,

Cand. Sci. (Engineering), Associate Professor of the Department of Computer Technologies and Information Security of the Institute of Computer Systems and Information Security, e-mail: antiemoboy@mail.ru

Vlasenko Alexandra V., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,

Cand. Sci. (Engineering), Head of the Department of Computer Technologies and Information Security of the Institute of computer systems and information security, e-mail: Vlasenko@kubstu.ru

Describes methods of determining threats to the information security in information systems of personal data processing. Due to the lack of consistency of the existing approved methodology with the one used by the information security threat data Bank (https://bdu.fstec.ru/) the analysis of the parameters of the relevance of threats is carried out and a method for determining the relevance of is threats using the mathematical apparatus of artificial neural networks is proposed. To implement the method, the analysis of artificial neural networks topologies and methods for calculating errors in artificial neural networks is performed. The artificial neural network was developed based on the topology of a multi-layer perceptron with reverse error propagation. Training of the developed information systems was conducted by preparing a training sample. The performance of the developed information

systems was compared with the performance of the involved group of experts acting on the existing approved methodology for determining the relevance of is threats in the personal data processing.

Key words: initial security indicator, potential of information security intruder, artificial neural network, perceptron, artificial neuron, layer, input signal, output signal, activation function, sigmoid function, training sample, information security threat

Введение. В настоящее время математический аппарат искусственных нейронных сетей (ИНС) применяется в различных областях науки для решения широкого спектра задач, оперирующих со значительными объемами данных. В частности, широкое распространение ИНС получили в рамках решения задач машинного обучения. Основными направлениями аппарата ИНС сейчас являются распознавание образов в изображениях и классификация объектов.

Также ИНС активно применяются в различных областях деятельности, связанных с информационной безопасностью (ИБ) [1].

- идентификация и аутентификация объектов (в частном случае – биометрия);
- методы обнаружения и предотвращения вторжений;
- механизмы обнаружения и классификации вирусной активности;
- анализ защищенности информационных систем (ИС);
- выявление и классификация уязвимостей программного обеспечения (далее – уязвимости ПО);
- оценка рисков ИБ, направленных на информационные активы

К последнему пункту также может быть отнесена задача подготовка модели угроз ИБ для ИС. Частной подзадачей такой задачи является подготовка перечня угроз ИБ для ИС обработки персональных данных (далее – ИСПДн).

Многие эксперты в области ИБ при разработке модели угроз ИБ для ИСПДн сталкиваются с рядом проблем, решение которых отсутствует на протяжении долгого времени.

1. Существующие методики определения актуальных угроз ИБ в ИСПДн [4, 6] морально устарели.

2. Использование разработанного регуляторами в области ИБ банка угроз ИБ [5] противоречит утвержденным методикам [4, 6].

3. В банке данных угроз ИБ (https://bdu.fstec.ru/) отсутствует утвержденная методика определения потенциала нарушителя ИБ.

4. В банке данных угроз ИБ (https://bdu.fstec.ru/) отсутствует взаимосвязь между уязвимостями ПО и угрозами ИБ.

Целью данной работы является анализ и выбор параметров актуальности угрозы ИБ в ИСПДн, а также разработка механизма определения актуальности угроз ИБ посредством применения математического аппарата ИНС. Для достижения данной цели необходимо ***решить следующие задачи***:

- произвести анализ и подготовить перечень параметров актуальности угрозы ИБ ИСПДн;
- разработать модель ИНС и осуществить ее обучение.

Анализ существующих методик определения актуальных угроз ИБ в ИСПДн. Проблема построения взаимосвязи между уязвимостями ПО и угрозами ИБ в «банке данных угроз ИБ» является фундаментальной – ранее на нее было обращено внимание множества экспертов в области ИБ. Один из способов решения данной проблемы был предложен в [2] и заключается в применении математического аппарата ИНС для определения вероятности угрозы ИБ. При этом входными сигналами для создаваемой ИНС являются формализованные параметры записи об уязвимости ПО в «банке данных угроз ИБ», например:

- класс уязвимости ПО;
- тип ошибки ПО;
- тип ПО.

Веса для нейронов входного слоя ИНС назначаются в случайном порядке. Выходными параметрами данной ИНС являются числовые значения вероятности реализации угрозы ИБ в интервале от 0 до 1. Способ обучения разработанной ИНС предложен на примере угроз ИБ из «банка данных угроз ИБ», входящих в перечень OWASP Top 10 [9]. Для каждой выбранной угрозы ИБ формируется отдельная ИНС. Обучение ИНС проводится на основе выборки параметров из записей уязвимостей ПО в банке угроз ИБ. Для проведения обучения ИНС формируются две обучающие выборки для уязвимостей ПО:

- эксплуатация которых может повлечь реализацию угрозы ИБ;
- эксплуатация которых не может повлечь реализацию угрозы ИБ.

Недостатком данного подхода является отсутствие алгоритма подготовки перечня уязвимостей ПО и угроз ИБ для ИСПДн. Первоначально перечень угроз ИБ готовится на основании выбранного потенциала нарушителя ИБ и статистической информации из открытых источников интернета. Дополнительно в [2] не рассмотрено отсутствие статистической информации при обучении ИНС.

На следующем этапе выбранные угрозы ИБ экспертным путем сопоставляются с уязвимостями ПО. Затем осуществляется выборка актуальных угроз ИБ посредством ИНС, на вход которой подаются параметры выбранных экспертом уязвимостей ПО. Таким образом, мерой выбора угрозы ИБ является потенциал нарушителя ИБ. При этом выбор уязвимостей ПО полностью зависит от квалификации привлекаемого эксперта.

В [4] и [6] актуальность угрозы ИБ в ИСПДн представлена как соотношение «вероятности или возможности ее реализации нарушителем ИБ» со «степенью возможного ущерба от реализации данной угрозы ИБ». Возможность реализации угрозы ИБ определяется в зависимости от уровня защищенности для двух видов ИСПДн:

- проектируемых;
- введенных в эксплуатацию (эксплуатируемых).

В связи с отсутствием статистической информации по введенным в эксплуатацию ИСПДн, предлагается использовать структурно-функциональные характеристики ИСПДн уровня проектной защищенности [7]. Для подготовки исчерпывающего перечня данных характеристик осуществим сравнение предлагаемых в [7] параметров с аналогичными показателями уровня исходной защищенности [4]. Результат сравнения и оптимизации данных параметров представлен в таблице.

Таблица – Показатели исходной защищенности ИСПДн

№ п/п	Показатель	Влияние на уровень исходной защищенности		
		Высокий	Средний	Низкий
1	***Архитектура ИС***:			
	Тонкий клиент	+		
	Одноранговая сеть		+	
	Файл-серверная			+
	ЦОД			+
	Удаленный доступ			+
	Разные типы ОС (гетерогенность среды)		+	
	ППО, независимое от ОС		+	
2	***Взаимодействие ИСПДн со сторонними ИСПДн***:			
	Взаимодействует			+
	Не взаимодействует		+	
3	***Взаимодействие ИСПДн с сетями общего пользования:***			
	Подключена;			+
	Подключена через выделенную инфраструктуру		+	
	Не подключена	+		
4	***Территориальное размещение ИСПДн:***			
	Распределенная			+
	Локальная в пределах одной КЗ		+	
	Локальная на одном АРМ, не подключенном к сети	+		
5	***Режим обработки информации в ИСПДн:***			
	Многопользовательский			+
	Однопользовательский	+		

Продолжение таблицы

6	***Разграничение прав доступа в ИСПДн:***			
	Без разграничения			+
	С разграничением		+	
7	***Наличие сегментирования ИС***			
	Отсутствует			+
	Имеется		+	

Количественно потенциал нарушителя ИБ также может быть представлен путем проецирования метрик уязвимостей ПО [10] на возможности нарушителя ИБ [6].

ИНС является одной из реализаций систем искусственного интеллекта и представляет собой совокупность искусственных нейронов (ИН), объединённых синапсами (имеющими определенные «веса») и размещенных на определенном количестве слоев (входной, скрытый, выходной). Необходимо отметить, что количество скрытых слоев является произвольным и может быть выбрано в соответствии с решаемой задачей.

Основной теорией построения ИНС является представление об ИН как о логическом элементе, имеющим множество входных сигналов x(ti) и выходных сигналов y(ti+1) в момент времени, который работает по принципу «все или ничего» [1]. Данные сигналы аппроксимируются единичными импульсами прямоугольной формы или единичными потенциалами, которые могут быть представлены булевыми переменными x(ti), y(ti+1) в интервале от 0 до 1.

По результатам анализа для определения актуальных угроз ИБ с использованием математического аппарата ИНС предлагается использовать в качестве искусственных нейронов (ИН) входного слоя следующие показатели актуальности угрозы ИБ:

- уровень проектной защищенности;
- потенциал нарушителя ИБ;
- нарушение свойств защищенности, используемые при расчете возможного ущерба от реализации угрозы ИБ для ИСПДн.

На основании вышеизложенного параметры показателей актуальности угрозы ИБ на входном слое ИНС представляются как перечень следующих ИН:

- архитектура ИС (A);
- взаимодействие со сторонними ИСПДн (I_N);
- взаимодействие с сетями общего пользования (N_W);
- территориальное размещение ИСПДн (S_{Sq});
- режим обработки информации в ИСПДн (R_p);
- разграничение прав доступа (R_{ac});
- наличие сегментирования ИС (S_{IS})
- потенциал нарушителя (P_i);
- нарушение конфиденциальности (CI);
- нарушение целостности (II);
- нарушение доступности (AI).

Таким образом, общее количество ИН во входном слое ИНС составляет «11». На основании методик, приведенных в [4, 6], можно считать, что данный перечень является необходимым и достаточным для определения актуальности угроз ИБ в ИСПДн.

Выходным ИН будет являться величина актуальности угрозы ИБ (A_T).

Все значения для входных и выходных ИН будут принадлежать интервалу [0, 1].

В процессе выбора топологии был проведен анализ следующих типов ИНС:

- однослойная сеть;
- многослойная сеть;
- рекуррентная сеть;
- сеть латеральными связями;
- сеть с локальными связями.

Применение однослойной ИНС является невозможным в связи с представлением весовых коэффициентов ИН в виде матрицы, что ограничивает возможности ее обучения [1]. Также задача определения актуальности угроз ИБ в ИСПДн не является линейной. ИН выходного слоя рекуррентной ИНС подаются на ИН входного слоя и участвуют в обработке следующего входного век-

тора. Процесс определения угроз ИБ носит постоянный, но не динамический характер – поэтому применение рекуррентных ИНС нецелесообразно. ИНС с латеральными связями используют боковые связи ИН в слое и чаще всего применяются для построения сетей распознавания графических объектов [1]. ИНС с локальными связями ориентированы на обработку и восстановление изображений. По результатам выполненного обзора было принято решение использовать модель многослойной ИНС обратного распространения ошибки [1].

Для сравнения и выбора количества скрытых слоев ИНС экспериментальным путем созданы две ИНС. Первая – с учетом количества скрытых слоев ИНС представлена в [2], т.е. входным, двумя скрытыми и выходном слоем. Вторая ИНС – с одним скрытым слоем.

Количество ИН на каждом слое определяются по эвристическому правилу геометрической пирамиды. Суть данного правила заключается в сопоставлении слоев ИНС с формой пирамиды, т.е. количество ИН от входного к выходному слою должно уменьшаться в геометрической прогрессии.

Расчет количества ИН на скрытых слоях для первой ИНС осуществлялся по следующим формулам [11]:

$$r = \sqrt[3]{\frac{n}{m}}, \quad (1)$$

$$k_1 = mr^2, \quad (2)$$

$$k_2 = mr, \quad (3)$$

где n – число ИН входного слоя; m – число ИН выходного слоя; k_1 – число ИН в первом скрытом слое; k_2 – число ИН во втором скрытом слое. Исходя из количества ИН входного слоя n = 11 и выходного слоя m = 1, k_1 = 4,9, округляется в большую сторону до целого числа 5, k_2 = 2,22, округляется в меньшую сторону до целого числа 2.

Расчет количества ИН в скрытом слое для второй ИНС осуществляется по формуле для трехслойной сети [11]:

$$r = \sqrt{nm}, \quad (4)$$

вследствие чего количество нейронов на скрытом слое r = 3,31, округляется в меньшую сторону до целого числа 3.

Для осуществления выбора топологии была разработана обучающая выборка, параметры уровня проектной защищенности и потенциал нарушителя ИБ (8 «единиц»), выбираются с привлечением эксперта. В связи с этим количество комбинаций ограничено. Параметры нарушения свойств защищенности (конфиденциальности, целостности, доступности) для подготовки обучающей выборки были выбраны из ранее подготовленного экспертным путем перечня угроз ИБ.

Проблемным вопросом при формировании обучающей выборки является отсутствие статистической информации в банке данных угроз ИБ.

Для решения данной проблемы проведен анализ статистической информации из реестра операторов, осуществляющих обработку персональных данных [8]. Установлено, что юридические лица в среднем регистрируют порядка трех ИСПДн в реестре, в то время как государственные и муниципальные учреждения – от 5 до 15 (с учетом учреждений здравоохранения).

На основании вышеизложенного была подготовлена обучающая выборка для усредненного количества ИСПДн – 5 шт. В нее была включена информация о параметрах нарушения свойств защищенности 8-ми различных угроз ИБ (рис. 1).

```
# Тренировочный сет.
training_set_inputs = array([[0.2, 0.2, 0.6, 0.6, 0.6, 0.6, 0.6, 0.25, 0.9, 0.6, 0.6],
                             [0.6, 0.6, 0.6, 0.6, 0.6, 0.6, 0.6, 0.25, 0.9, 0.6, 0.6],
                             [0.2, 0.2, 0.6, 0.6, 0.6, 0.6, 0.6, 0.25, 0.2, 0.3, 0.4],
                             [0.8, 0.2, 0.8, 0.2, 0.6, 0.6, 0.6, 0.25, 0.4, 0.4, 0.2],
                             [0.2, 0.6, 0.8, 0.8, 0.6, 0.6, 0.6, 0.25, 0.9, 0.6, 0.6],
                             [0.2, 0.2, 0.6, 0.6, 0.6, 0.6, 0.6, 0.25, 0.4, 0.8, 0.3],
                             [0.6, 0.6, 0.6, 0.6, 0.6, 0.6, 0.6, 0.25, 0.2, 0.8, 0.3],
                             [0.2, 0.2, 0.6, 0.6, 0.6, 0.6, 0.6, 0.25, 0.9, 0.9, 0.4],
                             [0.8, 0.2, 0.8, 0.2, 0.6, 0.6, 0.6, 0.25, 0.2, 0.6, 0.1],
                             [0.2, 0.6, 0.8, 0.8, 0.6, 0.6, 0.6, 0.25, 0.3, 0.2, 0.3]])
training_set_outputs = array([[1, 1, 0, 0, 1, 1, 1, 1, 1, 0]]).T
```

Рисунок 1 – Обучающая выборка для ИНС

Для обучения ИНС используется скрипт, написанный на языке программирования Python (https://github.com/miloharper/simple-neural-network/blob/master/main.py).

При запуске скрипта через среду разработки Python – IDLE было установлено, что разница в вычислении ошибок между ИНС с одним скрытым слоем и ИНС с двумя скрытыми слоями, составляет менее 1 %.

Однако ИНС с одним скрытым слоем функционирует на 1 (одну) секунду быстрее, что является преимуществом при дальнейшем увеличении объемов обучающей выборки. В связи с отсутствием статистической информации, каждый новый случай предлагается добавлять в обучающую выборку и проводить переобучение ИНС.

Для упрощения обучения ИНС, а также осуществления вычислений, было принято решение использовать ИНС с одним скрытым слоем, состоящим из трех ИН.

Все значения ИН входного слоя предлагается использовать на интервале от 0 до 1 в соответствии с предлагаемой в [10] градацией.

После обучения ИНС с помощью вышеуказанного скрипта было проведено определение актуальности выбранной тестовой угрозы ИБ для смоделированной ИСПДн.

Проблемами, вытекающими из результатов функционирования ИНС, является зависимость результата ИНС от следующих факторов: 1) объема обучающей выборки; 2) от квалификации учителя, либо источника, который используется для сопоставления входных и выходных сигналов.

Решение вышеуказанных проблем может быть достигнуто посредством создания дополнительной площадки для банка данных угроз ИБ. Целью ее создания будет являться сбор и накопление статистической информации об угрозах ИБ в ИСПДН операторов и калькуляция актуальности угроз ИБ. Удобство данного способа будет заключаться в обезличенной передаче значений входных ИН для общего перечня угроз ИБ и получении выгрузки по актуальности выбранных оператором угроз ИБ также в обезличенной виде.

Визуализация функционирования ИНС при определении актуальности выбранной тестовой угрозы ИБ для смоделированной ИСПДн на основании представленной на рисунке 1 обучающей выборки представлена на рисунках 2 и 3. Точность функционирования ИНС вычисляется (оценивается) по результатам прохождения каждой итерации, и включает в себя: вычисление погрешности методом обратного распространения ошибки текущей итерации и корректировку весов слоев ИНС после прохождения итерации.

Для визуализации последовательного увеличения точности определения актуальности угроз ИБ в ИСПДн посредством ИНС на рисунках 2 и 3 на основании проведенного эксперимента, было принято решение отобразить 5950 итерацией (шагов). Данное количество итераций позволяет визуализировать вычисление ошибки ИНС. Однако дальнейшее отображение итераций делает график точности ИНС не информативным.

Обучение ИНС проводилось с помощью одной эпохи, состоящей из 10000 итераций. Данное количество было установлено экспериментально и является достаточным для достижения результата с приемлемой ошибкой. Также экспертным путем для контроля результатов функционирования ИНС была установлена градация актуальности угрозы ИБ в ИСПДн на уровне значения ИН выходного слоя равного 0,51. В рамках дальнейшей работы планируется провести декомпозицию ИН выходного слоя в соответствии с таблицей оценки уязвимостей ПО [10].

Скорость функционирования скрипта при определении актуальности тестовой угрозы ИБ для смоделированной ИСПДн на основании подготовленной обучающей выборки, составляет 2 (две) секунды. Наряду с этим, определение актуальности угрозы ИБ в ИСПДн по методикам, представленным в [6], а также с применением банка данных угроз ИБ требует создания рабочей группы и проведения анкетирования экспертов, что является достаточно трудоемким и продолжительным по времени процессом. По результатам проведенного эксперимента с привлечением группы экспертов в составе 5-ти человек, время, затраченное на определение актуальности тестовой угроз ИБ в смоделированной ИСПДн, равняется приблизительно 30 минутам.

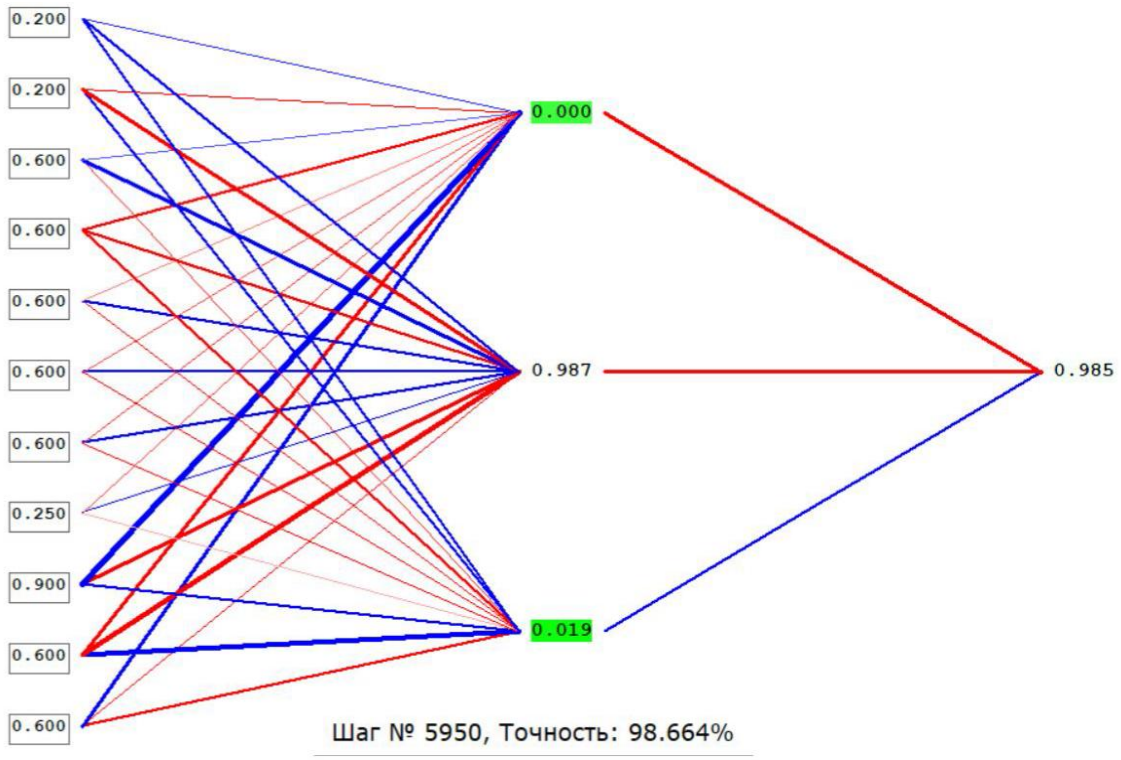


Рисунок 2 – Визуализация определения актуальности тестовой угрозы ИБ для смоделированной ИСПДн на основании обучающей выборки

Рисунок 3 – Изменение точности применяемой ИНС в зависимости от количества шагов

На основании вышеизложенного делаем вывод, что применение математического аппарата ИНС позволит существенно сократить время, затрачиваемое на определение актуальности угрозы ИБ в ИСПДн по сравнению со способом основанном на экспертной оценке. Для расчета сравнительного эффекта сокращения времени используем следующую формулу:

$$T = T_{Э}/T_{ИНС}, \quad (5)$$

где $T_{Э}$ – время, затраченное на определение актуальности угрозы ИБ в ИСПДн группой экспертов; а $T_{ИНС}$ – время, затраченное на определение актуальности угрозы ИБ в ИСПДн с помощью ИНС. Таким образом, в рамках конкретного эксперимента на основании времени функционирования скрипта, указанного выше, и времени, затрачиваемого группой экспертов, эффект применения ИНС представляет собой сокращение времени, затрачиваемого на определение актуальности тестовой угрозы ИБ в смоделированной ИСПДн и составляет 900 раз.

Учитывая предложенный подход к решению проблем накопления статистической информации об актуальных угрозах ИБ в ИСПДн и дополнению обучающей выборки с переобучением, математический аппарат ИНС позволит определять актуальность угроз ИБ в динамике изменения входных параметров, например, показателей защищенности.

Научной новизной представленого подхода, в том числе в сравнении с [2], является унификация состава ИН входного слоя; организация связи угроз ИБ с уязвимостями ИБ через значения нарушения свойств защищенности. Существенным отличием представленного метода от [2] является возможность применения одной ИНС для определения актуальности множества угроз ИБ в отличие от подхода, требующего формирования отдельных ИНС для отдельных угроз ИБ.

Заключение. Таким образом, используя параметры уровня проектной защищенности, потенциал нарушителя ИБ и нарушение свойств защищенности, можно разработать простую для реализации ИНС, с минимальным значением ошибки сети. Данная ИНС позволит минимизировать участие эксперта в процессе определения угроз ИБ в ИСПДн.

Библиографический список

1. Брюхомицкий Ю. А. Нейросетевые модели для систем информационной безопасности : учебное пособие / Ю. А. Брюхомицкий. – Таганрог : Изд-во ТРТУ, 2005. – 160 с.

2. Соловьев С. В. Применение аппарата нейронных сетей для определения актуальных угроз безопасности информации информационных систем / С. В. Соловьев, В. В. Мамута // Наукоемкие технологии в космических исследованиях Земли. – 2016 – Т. 8, № 5 – С.78-82.

3. Цветкова О. Л. О применении теории искусственных нейронных сетей в решении задач обеспечения информационной безопасности / О. Л. Цветкова, А. И. Крепер // Символ науки. – 2017. – № 04-2 – С. 105–107.

4. Методический документ ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка)» – 2008. – 69 с. – Режим доступа: https://fstec.ru/component/attachments/download/289, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 27.12.2019).

5. Информационное сообщение ФСТЭК России от 6 марта 2015 г. № 240/22/879 «О банке данных угроз безопасности информации». – Режим доступа: https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/956-informatsionnoe-soobshchenie-fstek-rossii-ot-6-marta-2015-g-240-22-879, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 24.12.2019).

6. Методический документ ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных». – 2008. – 10 с. – Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 27.12.2019).

7. Методический документ ФСТЭК России «Методика определения угроз безопасности информации в информационных системах» (проект). – 2015. – 43 с. – Режим доступа: https://fstec.ru/component/attachments/download/812, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 20.12.2019).

8. Реестр операторов, осуществляющих обработку персональных данных. – Режим доступа: http://rkn.gov.ru/personal-data/register/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 25.01.2020).

9. Сайт OWASP – Режим доступа: https://owasp.org/www-project-top-ten/, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 25.01.2020).

10. Common Vulnerability Scoring System v3.0: Specification Document. – Режим доступа: https://www.first.org/cvss/specification-document свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 20.01.2020).

11. Masters T. Practical Neural Network Recipes in C++ / T. Masters. – Academic Press, 1993. – 504 p.

References

1. Bryukhomitskiy Yu. A. *Neyrosetevie modeli dlya system informatsionnoy bezopasnosti* [Neural network models for information security systems]. Taganrog, Taganrog State Radioengineering University, 2005. 160 p.

2. Soloviev S. V., Mamuta V. V. Priminenie apparata neyronnykh setey dlya opredeleniya aktyalnykh ugroz bezopasnosti informatsii informatsionnykh system [The use of the apparatus of neural networks to determine the current threats to the security of information of information systems]. *Naukoemkie tekhnologii v kosmicheskikh issledovaniyakh zemli* [High Technology in Space Research of the Earth], 2016, vol. 8, issue 5, pp. 78–82.

3. Tsvetkova O. L., Kreper A. I. O primenenii teorii neyronnykh setey v reshenii zadach obespecheniya informatsionnoy bezopasnosti [On the application of the theory of artificial neural networks in solving problems of ensuring information security]. *Simvol nauki* [Symbol of Science], 2017, issue 04-2, pp. 105–107.

4. *Metodicheskiy dokument FSTEK Rossii "Bazovaya model ugroz bezopasnosti personalnykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personalnykh dannykh (vypiska)"* [Guidance document of the FSTEC of Russia "The basic model of personal data security threats when they are processed in personal data information systems (extract)"], 2008. 69 p. Available at: https://fstec.ru/component/attachments/download/289 (accessed 27.12.2019).

5. *Informatsionnoe pismo FSTEK Rossii ot 6 marta 2015 g. № 240/22/879 "O banke dannykh ugroz bezopasnosti informatsii"* [FSTEC information message no. 240/22/879 of March 6, 2015 «On the data bank of information security threats»]. Available at: https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/956-informatsionnoe-soobshchenie-fstek-rossii-ot-6-marta-2015-g-240-22-879 (accessed 24.12.2019).

6. *Metodicheskiy dokument FSTEK Rossii "Methodika opredeleniya aktualnykh ugroz bezopasnosti personalnykh dannykh v informatsionnykh sistemakh personalnykh dannykh"* [Guidance document of the FSTEC of Russia "Methodology for determining current threats to the security of personal data when they are processed in personal data information systems"], 2008. 10 p. Available at: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380 (accessed 27.12.2019).

7. *Metodicheskiy dokument FSTEK Rossii "Methodika opredeleniya ugroz bezopasnosti informatsii v informatsionnykh sistemakh" (proekt)* [Methods for determining information security threats in information systems (project)]. Available at: https://fstec.ru/component/attachments/download/812 (accessed 20.12.2019).

8. *Reestr operatorov personalnykh dannykh* [Register of operators that process personal data]. Available at: http://rkn.gov.ru/personal-data/register/ (accessed 01/25/2020).

9. *OWASP website.* Available at: https://owasp.org/www-project-top-ten/ (accessed 01.25.2020).

10. *Common Vulnerability Scoring System v3.0: Specification Document.* Available at: https://www.first.org/cvss/specification-document (accessed 01.20.2020).

11. Masters T. *Practical Neural Network Recipes in C++*. Academic Press, 1993. 504 p.