ПРИМЕНЕНИЕ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ ПРИ ОЦЕНКЕ АКТУАЛЬНОСТИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИОНЫХ СИСТЕМ

А. Г. Якунин, А.С. Ефимов
Алтайский государственный технический университет, г. Барнаул

Проблема анализа и оценки угроз безопасности информации (УБИ), обрабатываемой в информационных системах (ИС), в настоящее время приобрела особую актуальность. С каждым годом в программном обеспечении, применяемом в ИС, выявляется все больше и больше уязвимостей. Статистика выявления уязвимостей по данным Банка данных угроз ФСТЭК и NVD (National Vulnerability Database – Национальная база уязвимостей США) приведена на рисунке 1. Исследование уязвимостей в программном обеспечении (ПО), применяемом в ИС различного уровня, становится актуальной задачей с каждым годом в связи с увеличением количества ИС как в государственных структурах, так и в коммерческих организациях.

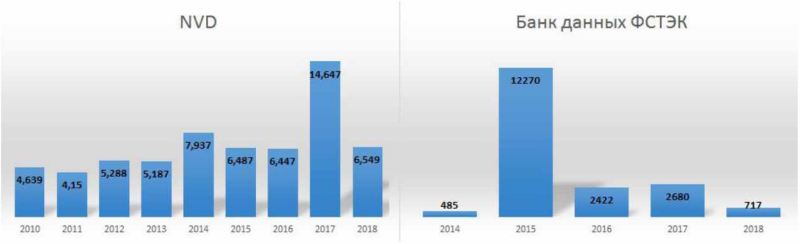

Рис. 1. Статистика количества уязвимостей по годам

Под уязвимостью ПО понимается недостаток программного средства или ИС в целом, который может быть использован для реализации УБИ [1]. Под угрозой понимается совокупность условий и факторов, создающих потенциальную и реально существующую опасность нарушения безопасности информации [1].

Наиболее важным этапом при построении защищенных ИС является формирование требований к защите информации. Согласно положениям нормативного правового акта ФСТЭК России [2], одной из задач формирования требований к защите информации, содержащейся в этих системах, является определение актуальных УБИ, а также разработка на этой основе модели угроз безопасности информации.

В соответствии с указанным документом, перечень актуальных УБИ и их описания используются при определении требований к системе защиты информации, обрабатываемой в ИС, на этапе уточнения базового набора мер защиты информации, определенного исходя из класса защищенности ИС и адаптированного под ее структурно-функциональные характеристики [2].

В настоящее время оценка актуальности УБИ для ИС осуществляется экспертным путем на основе использования такого методическом документе ФСТЭК России, как «Базовая модели угроз безопасности информации в информационных системах персональных данных» и банка угроз и уязвимостей приведенных в [3], где содержится информация как по угрозам, так и по уязвимостям, а также на основе иных зарубежных баз данных по уязвимостям и угрозам. Однако, использование зарубежных баз данных проблематично в связи с отсутствием в них информации об уязвимостях отечественных программных и программно-аппаратных разработок, поэтому более предпочтительным является использование сведений, приведенных в базе ФСТЭК [3]. Данный информационный ресурс содержит информацию не только о зарубежных продуктах, но и об отечественных разработках, которые широко применяются как в государственных структурах, так и в коммерческих организациях.

Исходя из выше сказанного, располагая информацией об уязвимостях для конкретной информационной системы, можно определить актуальные для нее угрозы, реализация которых зависит от этих уязвимостей. На сегодняшний день сведения об уязвимостях в «Банке данных угроз безопасности информации» существуют отдельно от угроз безопасности информации. Произвести экспертную оценку актуальности угрозы на основе данных об уязвимостях практически нереально, т.к. количество выявленных уязвимостей, выявленных с 2014 года, насчитывается более 18000.

Выходом из данной ситуации может служить автоматизация процесса оценки актуальности УБИ. Экспертную оценку можно заменить искусственной нейронной сетью [4,5]. Обучение нейронной сети предлагается проводить на примерах, полученных в результате осуществления специальных выборок данных об имеющихся уязвимостях.

Для каждой угрозы, реализация которой зависит от наличия в ИС уязвимости, следует построить нейронную сеть с количеством входов, равным выбранному количеству признаков уязвимости и

одном выходом, на котором формируется вероятность реализации угрозы (Рисунок 2).

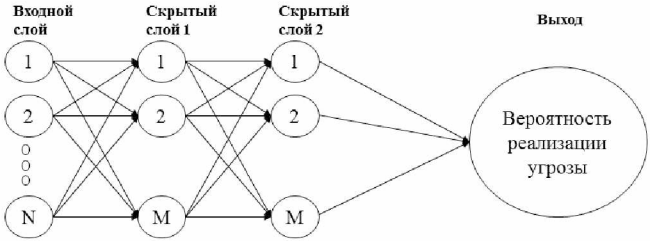

Рис. 2. Топология нейронной сети

С целью подтверждения выше сказанного было разработано программное обесчпечение, основу которого составляла реализация нейронной сети, имеющей описанную в [4,5] типовую структуру персептрона, содержащего входной, выходной (с одним выходом) и ряд скрытых слоев. Обучение нейронной сети производилось на основе метода обратного распространения ошибки. Обучение алгоритмом обратного распространения ошибки предполагает два прохода по всем слоям сети: прямого и обратного [6]. В качестве активационной функции в многослойном персептроне используется сигмоидальная активационная функция:

$$f(s) = \frac{1}{1+e^{-x}},$$

где x – параметр наклона сигмоидальной функции.

Интерфейс программы представлен на рисунках 3-5. В главном окне программы (Рисунок 3) настраивается структура сети и ведутся логи обучения. Для контроля процесса обучения и анализа качества был реализован вывод графиков, представленных на рисунке 4 и рисунке 5.

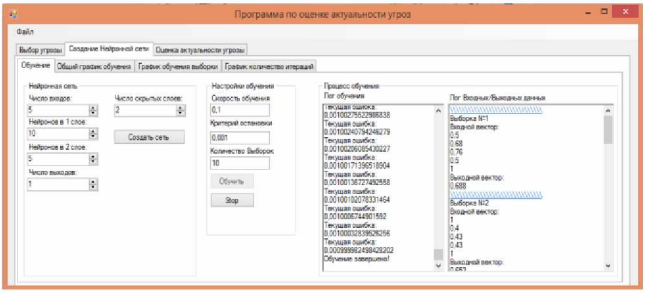

Рис. 3. Интерфейс программы

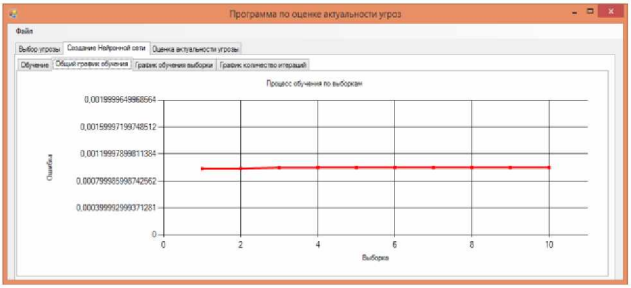

Рис. 4. График оценки качества обучения для различных выборок

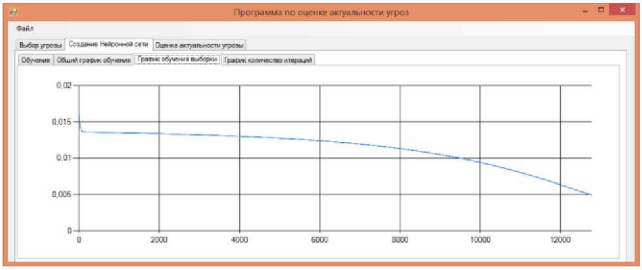

Рис. 5. График процесса обучения для конкретной выборки

Для проведения тестирования программы была привлечена группа экспертов, занимающихся аттестацией ИС, в количестве 5 человек. Для эксперимента им предъявлялись различные конфигурации ИС, которые формировались случайным образом из Банка ФСТЭК и в ориентировке сообщалось, что степень ущерба от реализации угроз минимальна, поскольку именно для этого случая в

соотвествии с методикой ФСТЭК актуальность угрозы напрямую связана с вероятностью ее реализации. Всего было сформировано и предъявлено экспертам 10 конфигураций ИС. Результат их оценок, а также результат оценки вероятности реализации угрозы, полученный на выходе нейронной сети для различного объема обучающих выборок, приведен в таблице 1.

Из результатов эксперимента, представленных в этой таблице, можно сделать вывод, что оценка, данная экспертами и нейронной сетью, не сильно различаются между собой. Среднее отклонение экспертной оценки от оценки, данной нейронной сетью, не превышает 7,9%. Этот показатель говорит о большой степени адекватности оценки актуальности УБИ, получаемый на основании искуственной нейронной сети.

Таблица 1 – Результаты эксперимента по сопоставлению экспертных оценок и оценки нейронной сети (А – угроза актуальна, Н- угроза не актуальна, СО – средняя оценка)

№	Экспертная оценка						Нейронная сеть: вероятность реализации угроз для различного объема обучающих выборок		
	Эксперт №1	Эксперт №2	Эксперт №3	Эксперт №4	Эксперт №5	СО	10 выборок	20 выборок	30 выборок
1	А	Н	А	А	А	А	0,6 (А)	0,63 (А)	0,64 (А)
2	Н	А	Н	Н	Н	Н	0,29 (Н)	0,3 (Н)	0,32 (Н)
3	А	А	А	А	А	А	0,67 (А)	0,72 (А)	0,73 (А)
4	Н	Н	Н	А	А	Н	0,24 (Н)	0,28 (Н)	0,31 (Н)
5	А	А	А	А	А	А	0,81 (А)	0,82 (А)	0,85 (А)
6	А	А	А	Н	А	А	0,64 (А)	0,66 (А)	0,67 (А)
7	Н	А	А	А	А	А	0,61 (А)	0,63 (А)	0,64 (А)
8	А	А	А	А	Н	А	0,91 (А)	0,92 (А)	0,94 (А)
9	Н	Н	Н	Н	Н	Н	0,1 (Н)	0,11 (Н)	0,12 (Н)
10	А	А	Н	Н	А	А	0,71 (А)	0,72 (А)	0,72 (А)

Полученный протип программного обеспечения отличается простотой реализации. При проведении работ по аттестации объектов информации возможно его использование в качестве дополнения к экспертной оценке или даже ее полной замене для ИС невысокого класса, а также в качестве оперативного средства контролля актуальности угроз и при проведении внутренней самоаттесации ИС.

Библиографический список

1. ГОСТ Р 56546-2015. Защита информации. Уязвимости информационных систем. Классификация уязвимостей Информационных систем. – М.: Стандартинформ, 2015-12 с

2. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: [приказ: утв. ФСТЭК

России 11.02.2013 № 17 в редакции приказа ФСТЭК России от 15.02.2017 № 27].
3. Банк данных угроз безопасности информации [Электронный ресурс]. Режим доступа http://bdu.fstec.ru/threat свободный. Загл. с экрана. — Яз. рус.
4. Барский А.Б. Нейронные сети: распознавание, управление, принятие решений. / А.Б. Барнский - М.: Финансы и статистика. 2004.176.
5. Заенцев И.В. Нейронные сети: основные модели. / И.В. Заенцев - Воронеж: Изд-во Воронежского госуд. ун-та, 1999. 76с.