0.1. *Антонов Р.А., Хандожко Г.В.* Применение искусственных нейронных сетей для оценки вероятности реализации угроз безопасности информации

В соответствии с ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования» [1], оценка актуальности угроз безопасности информации является одним из этапов идентификации рисков. Актуальность угрозы, в свою очередь, является показателем уровня защищенности объекта информатизации, информационных средств и систем. Формирование перечня актуальных угроз по определенному алгоритму используется как метод создания эффективной системы защиты информации, средств и систем. Эффективность системы защиты определяется отношением затраченных ресурсов (времени, сил и средств) к уровню защищенности информации. При определении актуальности угрозы эксперты используют вербальные показатели. Например, эксперт может определить угрозу, как маловероятную, или угрозу с низкой, средней или высокой вероятности, а также определить опасности реализации угрозы: низкую, среднюю или высокую. При составлении перечня актуальных угроз безопасности информации каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент. Таким образом, вербальные показатели вероятности реализации угроз интерпретируются в числовые градации этого показателя, теоретически воспринимаемые компьютером. С другой стороны, при оценке вероятности реализации угроз эксперт может рассматривать множество ситуаций и множество возможных ответов: два разных эксперта, разные по своему опыту или компетенциям, могут дать разные вербальные характеристики. С использованием методов экспертной оценки, производится итоговое определение вероятности реализации угроз. Для автоматизации процесса определения вероятности реализации угроз требуется определить некоторую зависимость между совокупностью условий обработки информации в системе и итоговыми значениями вероятностей реализации каждой угрозы, то есть построить алгоритм, способный для любой возможной совокупности входных объектов выдать достаточно точный классифицирующий ответ. Таким образом, экспертное определение вероятности реализации угрозы можно рассматривать, как задачу распознавания. Одним из наиболее эффективных и распространенных способов представления и решения таких типов задач являются искусственные нейронные сети [2–4].

В ходе исследования был разработан программный продукт, рассчитывающий вероятность реализации угроз безопасности информации на основе имеющейся обучающей выборки с применением искусственной нейронной сети. Для оценки качества распознавания проводится тестирование полученной модели искусственной нейронной сети на независимой выборке примеров, состоящей из 500 векторов, сформированных по аналогии с искусственным набором обучающих данных. При должном обучении нейронной сети программный продукт показывает хороший результат.

Список литературы

[1] ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования.

[2] Бодянский Е.В., Руденко О.Г. Искусственные нейронные сети: архитектуры, обучение, применения. Харьков: ТЕЛЕТЕХ, 2004. 362 с.

[3] Анисимов В.В. Искусственные нейронные сети: Методические материалы для выполнения курсового проекта. ДВГУПС, 2011г.

[4] Хайкин С. Нейронные сети: полный курс. 2-е изд. М., 2008.