перенасыщенной среде и интеллектуальное развитие. Рост хакерских атак и киберпреступлений, необходимость надежной защиты информационного актива компаний делает профессию специалиста по информационной безопасности одной из самых востребованных на рынке труда. Традиционная форма преподавания дисциплин, в которых делается упор на организационные и правовые методы, обычно не вызывает энтузиазма у студентов. На помощь приходят творческие технологии, прежде всего тризовские.

Так, метод «маленьких человечков» применим для моделирования злоумышленных атак на информационные ресурсы компании и планирования адекватных контрмер. Метод РВС развивает творческое мышление при построении надежной системы информационной безопасности предприятия. Системный оператор используется при анализе эволюции средств промышленного шпионажа для прогнозирования каналов утечки ближайшего и отдаленного будущего. Таблица основных приемов разрешения противоречий помогает при проектировании системы защиты компьютерных сетей. Опыт показывает, что студенты позитивно воспринимают деловые игры на базе творческих технологий. Внедрение тризовских методов обучения в учебный процесс позволяет выработать у студента умение ориентироваться в меняющихся условиях, навыки анализа нестандартных проблемы, самостоятельной разработки и реализации управленческих решений, что в конечном итоге позволяет существенно повысить уровень и качество профессиональной подготовки в целом.

Литература

1. Экономическая безопасность предприятия (фирмы) / В.Б. Зубик [и др.]. Минск: Вышэйшая школа, 1998. 391 с.

2. Nesbor K. Arbeit in Gruppen.Projektarbeit. – Kompetenzentrum «Hochschuldidaktik fur Niedersachsen» an der TU Braunschweig. 2010.

РЕАЛИЗАЦИЯ ШИФРОВАНИЯ С ЭЛЕМЕНТАМИ ПОДПИСИ НА ОСНОВЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Н.С. Иванин

Схема шифрования с элементами подписи (шифрование с ЭП) была предложена в [1] для одновременного решения задач конфиденциальности и аутентификации. Эта схема как правило является частью систем, использующих инфраструктуру с публичным ключом. В таких системах пользователи регистрируют свои публичные ключи вместе с удостоверяющим центром, которые являются независимыми между собой в отличии от разделяемых ключей в системах с симметричным шифрованием (в таких системах у пользователей хранится одинаковый ключ). При шифровании с ЭП для защиты коммуникации пользователю необходимо получить публичный ключ второго пользователя из удостоверяющего центра и зашифровать сообщение.

В качестве схемы была использована схема шифрования с ЭП без использования сертификата, основанная на использовании эллиптических кривых без вычисления функции пересчета пар. Эта схема основана на схеме Барбосы-Фашима, описанной в [2]. Такой подход позволяет шифровать сообщения любой длины и использовать одноразовый ключ симметричного шифрования. Используемая в схеме хэш-функция является устойчивой к коллизиям.

Полученная система состоит из 3 частей: сервера генерации ключей(СГК), отправителя и получателя. Сначала СГК вычисляет параметры, которые будут затем использованы в схеме шифрования. После чего пользователь на своей стороне вычисляет свой публичный ключ. На третьем этапе происходит извлечение частичного приватного ключа. Эта операция выполняется на сервере генерации ключей на основе идентификатора пользователя. Затем полученный приватный ключ и публичный ключ присваиваются пользователю также на основе его идентификатора. С помощью публичного и частичного приватного ключей пользователь зашифровывает сообщение и отправляет его в канал связи. Получатель с помощью своего публичного и полного приватного ключей расшифровывает и верифицирует полученное сообщение.

Литература

1. Zheng Y. Digital Signcryption or How to Achieve Cost (Signature & Encryption) << Cost(Signature) + Cost(Encryption) // Crypto'97. 1997.

2. Barbosa M., Farshim P. Certificateless Signcryption // ACM symposium on Information, computer and communications security. 2008.

РЕШЕНИЕ ЗАДАЧ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

Н.А. Искров, Д.В. Лящук

В докладе представлен обзор наиболее актуальных угроз информационной безопасности (ИБ) и основных направлений использования искусственных нейронных сетей (ИНС) при решении задач обеспечения ИБ. Описаны основная теория построения ИНС и их принцип работы.

Наиболее актуальные угрозы по мнению специалистов в области ИБ: внедрение в сеть предприятия вирусного ПО; простота реализация и распространенность DDoS-атак; снижение эффективности автоматизированных методов защиты от спама; сложности в поиске и идентификации уязвимостей ИБ; возникновение новых способов вторжения. Поэтому следует обратить внимание на перспективные методы защиты информации, в частности, на теорию ИНС.

Преимущества ИНС в решении задач ИБ: в процессе обучения ИНС могут быть выявлены новые сведения, закономерности, использование которых возможно для коррекции топологии сети, входных данных, для получения более эффективной защиты; после обучения ИНС входной сигнал становится нечувствительным к небольшим колебаниям при правильном построении архитектуры ИНС и верном выборе качества обучения; ИНС способна обратить внимание на те сведения, которые являются несущественными для интеллектуальной системы защиты.

Основные направления внедрения ИНС в защиту информации: обнаружение вторжений и защита от DDoS-атак; криптографические методы защиты информации, автоматизация процессов криптоанализа; проведение испытаний подсистем и оборудования систем защиты, моделирование возникновения внештатных ситуаций; прогрозирование шаблонных данных с целью выявления аномалий в классификации или кластеризации операций.

ДЕТЕКТИРОВАНИЕ СТЕГАНОГРАФИЧЕСКОЙ ИНФОРМАЦИИ В ИЗОБРАЖЕНИЯХ СЛЕПЫМ МЕТОДОМ

А.М. Кадан, И.А. Сазановец

Стеганографические методы позволяют скрыть одну информацию, сообщение, в другой, контейнере. В работе в качестве контейнеров рассматриваются изображения. Для реализации стеганографического сокрытия информации существует множество алгоритмов. И, зная использованный в конкретном случае стегоалгоритм, можно написать программу детектирования скрытого сообщения. В работе рассмотрен метод детектирования стеганографической информации в случаях, когда алгоритм сокрытия неизвестен. Такие способы в стегоанализе называются слепыми. И их использование возможно благодаря тому факту, что внедрение информации в контейнер оставляет после себя искажения.

Решаемая задача является задачей бинарной классификации, так как нужно, имея некое изображение, определить, содержит ли оно скрытое сообщение или нет. Для ее решения предлагается использовать методы машинного обучения. Исходное изображение раскладывается на три цветовых канала: красный, зеленый и синий. Для каждого канала строится трехуровневое двумерное вейвлет-разложение (используется вейвлет-функция Хаара) [1]. Из полученных коэффициентов разложения берутся аппроксимационный, вертикальные и диагональные коэффициенты. В частотных плоскостях этих коэффициентов вычисляются моменты третьего и четвертого порядков (коэффициент асимметрии и эксцесс). Полученные моменты рассматриваются как данные входного вектора (dataset’a) для работы