Таблица 2

Эффективность фильтрации на реальном почтовом ящике

Фильтр	Всего сообщений	Легитимных сообщений	Спам-сообщений	Отфильтровано спама	Ложные срабатывания
На основе двухслойного персептрона	164	34	130	109 (83,85 %)	0 (0 %)
На основе персептрона Розенблатта	164	34	130	112 (86,27 %)	0 (0 %)
На основе карт Кохонена	164	34	130	107 (82,36 %)	0 (0 %)

Как видно из таблиц, все три нейросети дают близкие значения, из чего можно сделать вывод о малой чувствительности предложенного алгоритма фильтрации к выбору типа нейронной сети. Следовательно, в практике можно выбирать нейросеть наиболее простую в реализации и обладающую наибольшей скоростью работы.

Практическая значимость исследования заключается в возможности на его основе разработки прикладных систем индивидуальной защиты от нежелательной корреспонденции для персональных компьютеров.

Библиографические ссылки

1. Burges C. J. C. A tutorial on Support Vector Machines for Pattern Recognition // Data Mining and Knowledge Discovery, 1998. P. 955–974.

2. Мкртчян С. О. Нейроны и нейронные сети (Введение в теорию формальных нейронов и нейронных сетей). М. : Энергия, 1971. С. 232.

3. Загоруйко Н. Г. Прикладные методы анализа данных и знаний. Новосибирск : ИМ СО РАН, 1999.

A. N. Mironenko

Omsk state university of F. M. Dostoevsky, Russia, Omsk.

CLASSIFICATION ALGORITHM OF INCOMING E-MAIL BASED ON A COMBINAION METHOD OF SUPPORT VECTOR AND NEURAL NETWORK APPROACH

The incorporation of support vector and neural network approach for solving the problem of spam filtering is performed. This allows to reduce significantly both the dimension of the space of support vectors and the number of input synapses of neural network. As a result, a significant reduction in the time of the filter is obtained.

УДК 004.056

В. Г. Миронова

Томский государственный университет систем управления и радиоэлектроники, Россия, Томск

ВЫЯВЛЕНИЕ ВЕРОЯТНОСТНЫХ НАРУШИТЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Выявление вероятностных нарушителей безопасности конфиденциальной информации является одним из основных этапов проведения предпроектного обследования и формирования требований по защите информации, обрабатываемой и хранимой в информационных системах.

Важной проблемой, которая затрудняет использование современных информационных технологий, является обеспечение их информационной безопасности (ИБ). Системы обработки информации приобретают популярность и используются повсеместно. Информационные системы (ИС), предназначенные для обеспечения работоспособности информационной инфраструктуры организации, предоставления различных видов информационных сервисов, автоматизации финансовой и производственной деятельности, а также бизнес-процессов организации, позволяют сократить как временные, финансовые, так и трудовые затраты. В ИС хранятся и обрабатываются значительные объемы информации разной степени секретности, поэтому вопрос защищенности этих ИС от различных угроз безопасности информации стоит остро [1].

Защищенность ИС обеспечивается с помощью системы защиты информации (СЗИ), которая представляет собой комплекс организационных и технических мероприятий. Построение СЗИ осуществляется в три этапа:

– предпроектное обследование ИС;

– проектирование СЗИ;

– внедрение СЗИ.

На этапе предпроектного обследования определяются технические средства и системы, участвующие в обработке информации, проводится анализ технологии обработки информации в ИС, выявляются вероятностные нарушители и угрозы.

Одной из основных стадий проведения предпроектного обследования является формирование модели вероятностного нарушителя ИБ в ИС.

Под нарушителем безопасности информации понимают «физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации при их обработке техническими средствами в ИС» (URL: http://www.fstec.ru/_docs/doc_3_3_001.htm).

Модель вероятностного нарушителя безопасности ИС необходима для систематизации информации о типах и возможностях субъектов, целях несанкционированных воздействий и выработки адекватных организационных и технических мер противодействия им.

Модель нарушителей безопасности информации – совокупность сведений о нарушителях, их целях, квалификации, технической оснащенности, возможности реализации угроз, мотивации, применяемых ими способах (методах) реализации угроз и используемых при этом уязвимостях в отношении информационных объектов защиты (активов).

Нарушителей ИБ различают по следующим критериям:

– расположение нарушителя ИБ относительно компонент ИС (в пределах контролируемой зоны (КЗ), либо за ее пределами);

– возможности, которыми обладает нарушитель ИБ относительно ИС (например, нарушитель может осуществлять несанкционированный доступ (НСД) к каналам связи, выходящим за пределы служебных помещений; нарушитель может осуществлять НСД к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок);

– сведения об ИС, которые могут быть известны нарушителю ИБ (например, нарушителю известна информация о размещении и технических характеристиках технических средств и систем ИС).

Модель нарушителя ИБ и угроз безопасности информации позволяет сформировать перечень требований к СЗИ.

Используя основные критерии, формируется множество нарушителей ИБ в ИС. Предложенные автором критерии классификации нарушителей позволяют выделить вероятностных нарушителей ИБ для конкретных условий функционирования ИС и организовать СЗИ в целом.

Следующим шагом на этапе предпроектного обследования строится модель угроз безопасности конфиденциальной информации, результатом которой является перечень актуальных угроз ИБ.

Адекватная модель нарушителя ИБ, в которой отражаются его практические и теоретические возможности, априорные знания, время и место действия и другие характеристики позволит правильно сориентировать и определить требования к СЗИ, тем самым повысить уровень защищенности хранимой и обрабатываемой информации в ИС.

Библиографическая ссылка

1. Информационная безопасность систем // Информатика и системы управления. 2012. № 1(31). С. 28–35.

V. G. Mironova

Tomsk state university of control systems and radioelectronics (TUSUR), Russia, Tomsk

IDENTIFICATION OF INFORMATION SECURITY VIOLATORS IN INFORMATION SYSTEMS PROCESSING CONFIDENTIAL INFORMATION

Identification of probabilistic safety intruders of confidential information is one of the main stages of the pre-examination formation and the requirements for protection of information processed and stored in information systems.