О выявленных в ходе научных исследований по вопросам автоматизации управления защитой информации в ИССН некоторых проблемных вопросах и предлагаемых путях их решения ведется речь в докладе.

Литература

1. Интеллектуальные системы управления организационно-техническими системами / А.Н. Антамошин и [др.]; под ред. проф. А.А.Большакова. – М.: Горячая линия – Телеком, 2006. – 160 с.: ил.

ЗАЩИТА ИТКС ОТ УГРОЗ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

А.С. Мешков, В.П. Ширинский, И.Г. Некрашевич

Для современного этапа развития общества характерен непрерывный процесс информатизации. Сфера внедрения телекоммуникаций и вычислительных систем постоянно расширяется. В связи с этим важной задачей является обеспечение достаточной защищенности таких систем. При рассмотрении вопроса безопасности функционирования информационно-телекоммуникационной системы (ИТКС) определяющую роль играют угрозы, реализуемые посредством удаленного воздействия с объектом взаимодействия, или так называемые сетевые атаки. Большинство распределенных систем функционируют и проектируются с учетом использования в них технологии межсетевого взаимодействия, реализованной в Интернет. При этом ИТКС базируется на применении протоколов межсетевого воздействия TCP/IP. Поэтому в РТКС могут реализовываться большинство атак, характерных для Интернет.

Для оценки систем защищенности ИТКС в условиях воздействия на ее компоненты некоторого набора угроз необходимо перейти к категории риска. Риск – это сочетание величины ущерба и возможности реализации исхода, влекущего за собой такой ущерб.

Угрозы информационной безопасности имеют вероятный характер. Анализ возможных угроз и анализ рисков служит основой для выбора мер по защите ИТКС, которые должны быть осуществлены для снижения риска до приемлемого уровня.

Предполагаемая работа заключается в исследовании и разработке методики анализа информационных рисков и управления защищенностью ИТКС от угроз несанкционированного доступа к ее компонентам.

Литература

1. Бобов, М.Н. Протоколы аутентификации в сетях телекоммуникаций / М.Н. Бобов. – Мн.: БГУИР, 2004. – 26 с.

2. Мельников, Д.А. Информационные процессы в компьютерных сетях: протоколы, стандарты, интерфейсы, модели / Д.А. Мельников. – М.: Кудиц-образ, 1999. – 256 с.

3. Щербаков, А.Ю. Современная компьютерная безопасность: теоретические основы, практические аспекты / А.Ю. Щербаков. – М.: Книжный мир, 2009. – 351 с.

4. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах / В.Ф. Шаньгин. – М.: Форум, 2016. – 591 с.

ОБРАБОТКА ДАННЫХ ИДЕНТИФИКАЦИИ ПО СЕТЧАТКЕ ГЛАЗА

А.И. Митюхин, Р.П. Гришель

Изображение кровеносных сосудов глазного дна является биометрическим параметром индивидуального организма человека и может использоваться для решения задачи идентификации человека с помощью технической системы с особыми требованиями по надежности или в криминалистике. В сравнении с другими биометрическими параметрами, используемыми для идентификации личности (например, отпечатки пальцев – качество отпечатков зависит от возраста; распознавания по лицу – систему распознавания можно обмануть с помощью маскировки и пр.), достоинством распознавания по сетчатке глаза является постоянство биометрического параметра. Уникальное изображение отдельных фрагментов сосудистой сети глазного дна описывается совокупностью элементов (пикселями), представляющими эту сеть.

В работе приводятся результаты исследования, связанные с цифровой обработкой и распознаванием по изображению кровеносных сосудов глазного дна на основе статистического подхода и энтропийного кодирования. Для этого рассчитывались статистические характеристики изображения сети кровеносных сосудов. Сеть представлялась рядом цифровых последовательностей с числом точек (отсчетов), количество которых определялось размером обрабатываемого фрагмента или длиной линии, описывающей кровеносный сосуд. Определенная степень линейной зависимости между совокупностями данных, описывающих сеть, и применение в качестве дескрипторов распознавания коэффициентов разложения по базису собственных функций позволила уменьшить размерность области распознавания. Фильтрация значений дескрипторов осуществлялась на основе дисперсионного критерия [1]. Такая процедура выбора признаков распознавания позволила упростить процесс правильной классификации, измерения сходства биометрических образцов.

Литература

1. Мультиспектральное наблюдение / А.И. Митюхин // Технические средства защиты информации материалы XI Белорусско-российской науч.-техн. конф. Минск, 4–5 июня 2013 г. – С. 44–45.

ПОДДЕРЖКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНТЕГРИРОВАННОЙ КИС С ИСПОЛЬЗОВАНИЕМ НЕЙРОННОЙ СЕТИ

М.Г. Моздурани Шираз, В.А. Вишняков

Наиболее распространенной нейросетевой структурой, используемой для решения задач защиты информации, является многослойный персептрон. Построена обучающая выборка для многослойного персептрона, определяющего, содержит ли данная программа (ее исполняемый файл) вредоносный код или нет. В ходе работы было проведено обучение данной нейросетевой структуры при помощи специально построенной выборки исполняемых файлов двух состояний: «отсутствие вредоносного кода» и «наличие вредоносного кода». Обучение проводилось в SPSS Statistics – программе, произведенной компанией IBM. Для обучения многослойного персептрона данные обучающей выборки приведены к десятичному представлению. Для автоматизации решения данной задачи на языке JavaScript был написан конвертер чисел между различными системами счисления.

Исследована эффективность работы нейронной сети с помощью контрольной выборки исполняемых файлов после ее обучения. Относительная погрешность классификации файлов составила 5 %, однако, следует отметить, что при обучении данной нейронной сети использовалась относительно небольшая выборка исполняемых файлов; для использования же нейронной сети при решении реальных задач защиты информации, например, во внутрикорпоративных системах, выборка файлов должна быть больше, и вредоносные коды, которые внедряются в часть файлов из выборки, должны быть более разнообразными.

СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНТЕГРИРОВАННОЙ КИС НА БАЗЕ СОВ И МСЭ

М.Г. Моздурани Шираз, В.А. Вишняков

Представлено два подхода к реализации системы предотвращения вторжений: первые при выявлении атаки реконфигурируют активное сетевое оборудование (например, Snort SAM); вторые при выявлении атаки принимают решения, на основе правил, о дальнейшем действии с пакета (например, Snort inline). Недостатком первого подхода является то, что на создание правила, передачу его межсетевому экрану, реконфигурирование самого межсетевого экрана уходит время. Система Snort_inline при обнаружении следов атаки в пакете сама уничтожает пакет, что эффективней первого решения.

Представлена структура защищаемой сети. Сервер работает под управлением Slackware Linux 10.2 с ядром версии 2.4.31. Данная версия ядра является наиболее исследованной, стабильной и содержит минимальное число обнаруживаемых уязвимостей. Сервер защищен с помощью межсетевого экрана IPTables (v1.3.3).