В связи с этим целью работы является разработка эффективного алгоритма обнаружения сетевых аномалий, основанного на использовании анализа главных компонент и технологии опорных векторов.

Предложенный алгоритм основан на анализе главных компонентов тестовых пакетов данных трафика TCP/IP, выборе оптимального числа значимых главных компонент на каждую категорию сетевого поведения по энергетическому критерию, формировании матриц PCA преобразования трафика, вычислении векторов признаков для каждой категории и эталонных векторов признаков и их сравнении с использованием метрики евклидового расстояния, принятия предварительного решения о типе категории с использованием порогового сравнения и классификация типов вторжений на основе ансамбля классификаторов SVM (10 классификаторов). Использование метода анализа главных компонент уменьшает пространство с 41-го до 6-ти признаков. Установлено, что предложенный алгоритм обеспечивает приблизительно 98% точность классификации или обнаружения атак с использованием базы пакетов сетевых трафиков 1999 DARPA, разделенной на 5 категорий: Normal, DoS, R2L, U2R и Probe.

ИТЕРАТИВНЫЙ АЛГОРИТМ ОБНАРУЖЕНИЯ НИЗКОКОНТРАСТНЫХ ОБЪЕКТОВ НА ОСНОВЕ ИЗБЫТОЧНОГО ДИСКРЕТНОГО ЛИФТИНГ ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ В УСЛОВИЯХ НЕСТАБИЛЬНОСТИ ВИДЕОСЪЕМКИ

И.А. БОРИСКЕВИЧ

Традиционные подходы к обнаружению низкоконтрастных объектов на видеопоследовательности в условиях нестабильности видеосъемки требует значительных вычислительно-временных затрат на предварительную стабилизацию соседних видеокадров. Известные алгоритмы не позволяют осуществлять эффективное обнаружение целей в реальном масштабе времени. В связи с этим предложен итеративный алгоритм обнаружения объектов в видеопоследовательности, основанный на вычислении избыточного дискретного лифтинг вейвлет-преобразования, гистограммных метрик сходства окна поиска и эталонного целевого изображения и модифицированной процедуры оптимизации множества частиц. Он позволяет обнаружить низкоконтрастные динамические объекты за счет использования свойств избыточного дискретного вейвлет-преобразования и выбранного правила объединения вейвлет-матриц. Избыточное дискретное вейвлет-преобразование производит локализацию компонент исходного изображения в пространственно-частотной области с сохранением его энергии, что гарантирует отсутствие искажения значимых деталей и обеспечивает адаптацию к изменению контрастности. Гистограммные метрики обладают свойством инвариантности к масштабу и положению объектов поиска на изображении.

Моделирование проведено в среде MATLAB для первого уровня разложения вейвлет-функции Хаара. Последовательность тестовых кадров аэросъемки содержит низкоконтрастные объекты размером 200–300 пикселов. Определено оптимальное количество частиц и характер их распределения. Установлено, что наилучшими характеристиками по критериям эффективности обнаружения и времени выполнения алгоритма обладает расстояние Бхаттачария для объединенных аппроксимирующей и диагональной детализирующей вейвлет-матриц.

СПОСОБЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ РАБОТЕ С ПАРОЛЯМИ В СЕТИ ИНТЕРНЕТ

А.А. БОРКУН

Информационная безопасность в сети Интернет постоянно снижается, что является одной из основных проблем, с которой столкнулось современное общество. Даже такое

нововведение в сетевой безопасности, как двухфакторная аутентификация, всё равно полагается на один из факторов — пароль.

В этой связи обязательным является использование следующих требований, которые существенно повысят информационную безопасность при работе с паролями в сети Интернет:

Пароль должен быть выбран таким образом, чтобы злоумышленнику было невозможно подобрать его по словарю.

Для каждого сайта, где регистрируется пользователь, должен быть использован уникальный пароль, так как после получения пароля от одного из сайтов, где зарегистрирован пользователь, злоумышленники получат доступ к его e-mail, системе интернет-банкинга и другой частной информации.

Рекомендуется использовать длинные пароли со случайными символами разного регистра, которые будут храниться в зашифрованном виде на USB флэш-накопителе, защищенном паролем. Для шифрации данных рекомендуется к использованию решение TrueCrypt. При использовании пароля пользователь будет копировать его через буфер обмена, что позволит избежать утечки информации с помощью ПО, которое логирует нажатия клавиш.

Для работы с особо важной информацией (интернет-банкинг, оплата с помощью электронного платежного средства) рекомендуется использовать отдельный браузер, что позволит избежать кражи информации после открытия сайта, содержащего вредоносный код.

При работе с малоизвестными сайтами рекомендуется использовать одноразовые e-mail, созданные с помощью http://10minutemail.com. Через 10 минут после создания e-mail будет удалён.

Использование вышеперечисленных требований позволит существенно повысить информационную безопасность пользователя при работе в сети интернет и затруднит кражу информации третьими лицами.

ИМИТАЦИОННАЯ МОДЕЛЬ СИНХРОНИЗИРУЕМЫХ СЕТЕЙ КИНЦЕЛЯ

Н.В. БРИЧ

На сегодняшний день актуальна задача доставки секретной ключевой информации. Использование синхронизируемых искусственных нейронных сетей (ИНС) является одним из перспективных решений задачи формирования общего секретного ключа. Для изучения особенностей сетей Кинцеля создана имитационная модель на языке высокого уровня Python 3.2. Программа является консольным приложением, позволяющим анализировать свойства ИНС и моделировать основные типы атак. Результаты моделирования сохраняются в файл. Пользователь имеет возможность устанавливать значение количества необходимых испытаний. Достоинствами разработанной модели является скорость вычислений, которая соизмерима со скоростью работы программ, написанных на языке С.

АВТОМАТИЗАЦИЯ ПРОЦЕССА КОРРЕЛЯЦИИ СОБЫТИЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

С.М. ДОВГУЧИЦ

На сегодняшний день не существует универсальных систем обнаружения и предотвращения атак в связи с огромным разнообразием защищаемых информационных систем и ресурсов. Процесс обнаружения атак можно усовершенствовать путем комбинации различных программ обнаружения. Сложности связаны с различием типов и форматов информации на выходе таких систем. Также все тревожные события, сгенерированные системами контроля доступа к ресурсам на серверах и рабочих станциях, не отражают непосредственно атаки. Они описывают действия пользователя, работающего