АЛГОРИТМЫ ШИФРОВАНИЯ ИЗОБРАЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ ГАММЫ, ФОРМИРУЕМОЙ НА ОСНОВЕ ДИНАМИЧЕСКОГО ХАОСА

А.В. Сидоренко, В.И. Шакинко

Стремительное развитие телекоммуникационных технологий и широкое распространение фотокамер мобильной аппаратуры приводит к тому, что огромное количество изображений в цифровом виде передается по каналам связи. Поскольку часть изображений носит конфиденциальный характер, актуальной становится задача их защиты. Существующие алгоритмы шифрования не ориентированы на применение именно к изображениям, и вследствие этого не способны достаточно эффективно справиться с поставленной задачей [1]. Одним из новых подходов является использование при шифровании изображений явления динамического хаоса. Часть предлагаемых схем, основанных на данном явлении, состоит из двух процедур: перестановки элементов (пикселей) изображения и изменения значений пикселей [2]. Перестановка проводится для уменьшения корреляции между значениями соседних элементов изображения. Однако распределение значений пикселей по яркостям сохраняется после проведения данной процедуры и содержит часть информации об исходном изображении.

В данной работе для изменения значений элементов изображения используется наложение гаммы, получаемой с использованием хаотических отображений. Одна из основных особенностей предлагаемого способа формирования гаммы заключается в использовании количества итераций хаотических отображений в два раза меньшего, чем количество пикселей изображения, что позволяет повысить скорость шифрования.

Литература

1. *Cheng P.* A fast image encryption algorithm based on chaotic map and lookup table // Nonlinear Dynamics. 2015. Vol. 79, Issue 3. P. 2121–2131.

2. *Hanchinamani G., Kulakami L.* // Int. J. of Hybrid Information Technology. 2014. Vol. 7, Issue 4. P. 185–200.

АНАЛИЗ НЕОБХОДИМОСТИ ВНЕДРЕНИЯ СИСТЕМ ЦЕНТРАЛИЗОВАННОГО ХРАНЕНИЯ И АНАЛИЗА ЖУРНАЛОВ АУДИТА

Д.С. Смоляк, Т.А. Пулко

Современные информационные системы включают большое число различных устройств и прикладных систем. Источники событий ведут файлы журналов аудита, некоторые используют базы данных для хранения записей аудита, при этом число событий только на устройствах систем информационной безопасности (например, межсетевых экранах) может превышать несколько миллионов в сутки. Очевидно, что анализ полученных данных вручную без применения автоматизированных систем представляет собой практически невыполнимую задачу. Для решения этих задач предлагается использовать средства централизованного хранения и анализа событий аудита, такие как системы мониторинга и корреляции событий информационной безопасности. События информационной безопасности регистрируются с помощью встроенных механизмов безопасности информационных систем и устройств. Агент (коннектор) собирает данные с различных источников событий ИБ, причем одной записи в журнале сообщений каждого из контролируемых источников событий ИБ, соответствует одно событие зафиксированное системой ArcSightESM. После сбора агентом событий ИБ запускается процесс нормализации событий. Данные от различных средств защиты приводятся к единому виду и формату времени. В процессе нормализации используется синтаксический анализ сообщений. Правила синтаксического анализа (parsers) устанавливаются и настраиваются при инсталляции ArcSightESM и могут, при необходимости, корректироваться администратором системы мониторинга. Предлагаемый способ интеграции средств мониторинга и корреляции событий HPArcSight может успешно использоваться в корпоративных сетях, что позволит повысить защищенность серверов предприятий, сократить время реагирования на