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

инциденты, связанные с нарушением контроля целостности данных, хранимых на серверах предприятия.

Литература

1. Guide to Computer Security Log Management [Электронный ресурс]. – Электронные данные. – Режим доступа : http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

СТАТИСТИЧЕСКАЯ ПРОВЕРКА СЛУЧАЙНОСТИ ДВОИЧНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ТЕСТАМИ NIST DRAFT SP 800-90B

Е.В. Ставер

Одной из актуальных задач криптографии является задача исследования статистических свойств бинарных последовательностей, используемых для создания ключей криптографических алгоритмов. Разработан программный комплекс проверки последовательностей на случайность по стандарту DRAFT 800-90b. Приведены результаты разработки программного комплекса и тестирования, с помощью его четырех последовательностей последовательности bits.01, bits.02, calif.bit, germany.bit, тестами по критерию «хи-квадрат» и тестом проверки на коллизии. Проверка по критерию «хи-квадрат» позволит узнать, насколько созданный реальный ГСЧ близок к эталону ГСЧ, т.е. удовлетворяет ли он требованию равномерного распределения. Тест на коллизии измерит оцениваемое время до первой коллизии в выборке.

Цель статистики коллизий – оценка вероятности наступления наиболее желаемого состояния, основываясь на времени коллизий.

УПРАВЛЕНИЕ ЗАЩИТОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СЕТЯХ, ПРОБЛЕМЫ И ВОЗМОЖНЫЕ ПУТИ ИХ РЕШЕНИЯ

Л.Л. Утин, А.Р. Мацылевич

В целях обеспечения защищенности информационных ресурсов должна быть создана система защиты информации (СЗИ), к которой предъявляется ряд требований [1, 2]. Важным условием функционирования СЗИ, как системы, обладающей целевой функцией, является осуществление эффективного управления. Одной из особенностей управления защитой информации является то, что в основном объекты управления имеют техногенную природу, а субъекты управления — антропогенную. Данный факт в большинстве своем отрицательно сказывается на адекватном функционировании СЗИ. Кроме того, одним из критически важных факторов, оказывающим воздействие на защиту информации, является так называемый «человеческий фактор», который особенно сильно влияет на процессы управления защитой информации. Одним из путей минимизации влияния «человеческого фактора» и повышения эффективности СЗИ в целом, является организация управления защитой информации.

Проведенный анализ возможностей существующих технических средств и систем защиты информации свидетельствует о том, что они в основном являются локальными и выполняют ограниченные задачи (системы защиты от несанкционированного доступа, системы обнаружения и предотвращения вторжений, системы анализа защищенности сети и др.). При этом функции единого управления в масштабах всей сети (корпоративной сети) не реализуются.

О существующих при этом некоторых проблемах и возможных путях их решения ведется речь в докладе.

Литература

1. Защита информации. Основные термины и определения: СТБ ГОСТ Р 50922-2000. – Введ. 01.01.2001 – Мн. : Госстандарт, 2001. - 6 с.

2. О некоторых вопросах технической и криптографической защиты информации: приказ Оперативно-аналитического центра при Президенте Респ. Беларусь, 30 авг. 2013 г., № 62 // [Электронный ресурс].