УДК 004.056

Б. В. Дурняк
Українська академія друкарства
І. М. Лях
Закарпатський державний університет

СПОСОБИ ЗАХИСТУ ІНФОРМАЦІЇ У ЗАСОБАХ МАСОВОЇ ІНФОРМАЦІЇ

Аналізуються основні види небезпеки щодо захисту інформації. Розглядається метод скремблювання як один із базових методів захисту даних у засобах масової інформації.

Засоби масової інформації, небезпека, ідентифікація

Залежно від можливостей систем масової інформації та алгоритму послуг, які можна отримати внаслідок використання систем масової інформації, можна створити небезпеки різного типу, з якими можуть зіткнутися як окремий користувач, так і власники систем масової інформації. Для того, щоб систематичніше визначитися з їхніми типами стосовно абонентів, визначимо базові типи небезпек, які можуть впливати на роботу системи масової інформації у проекції на проблеми захисту інформації, що передається каналами систем масової інформації. Основні небезпеки, що стосуються інформації, визначені у межах систем, які використовують криптографію як один з важливих способів захисту інформації і є стандартизованими поняттями, наприклад:

аутентифікація;

конфіденційність інформації, що передається;

інтегральність інформації, яка передається;

доступність до засобів інформації.

Забезпечення аутентифікації джерел інформації реалізується різними механізмами ідентифікації, найпоширенішим серед яких є використання паролів, кодів, таємних ключів. Крім того, для цього у галузі інформаційних технологій використовуються механізми ідентифікації, що полягають у:

ідентифікації мітками часу;

ідентифікації, що ґрунтуються на використанні алгоритмів шифрування тощо.

Ідентифікація мітками часу реалізується кількома методами. У першому випадку використовується фіксований інтервал часу, за який отримана інформація повинна бути розпізнана як така, що дійсно походить від легального абонента. Цей час використовується на дешифрацію, якщо повідомлення було зашифроване, чи реалізацію інших алгоритмів, які застосовуються для забезпечення контролю даних, що передаються. Другий

спосіб використання часу полягає у приписуванні переданим даним мітки часу, яка відповідає часу надання даних відповідним джерелом. Для зазначених способів ідентифікації характерною є вимога, яка полягає у тому, щоб дотримуватися режиму реального часу під час роботи відповідних апаратних та програмних засобів.

Другий спосіб аутентифікації, що ґрунтується на використанні шифрування з симетричним ключем, хоч і має свої недоліки, але доволі широко застосовується при передачі даних. Доволі часто для таких цілей використовуються асиметричні шифри, які мають таємний ключ і явний ключ, найвідомішим асиметричним алгоритмом шифрування є алгоритм RSA [2]. Процес аутентифікації можна реалізувати, використовуючи код MAC разом з ключами шифрування. У цьому разі до повідомлення додається код MAC, що формується на основі використання цього повідомлення і разом з ними передається до адресата. Адресат на основі отриманого повідомлення за відомим йому алгоритмом вираховує код MAC і порівнює його з кодом MAC, який передано адресату разом з повідомленням. Якщо порівнювані коди збігаються, то повідомлення приймається як таке, що відповідає оригіналу.

Одним з основних методів забезпечення конфіденційності інформації, що передається каналами систем масової інформації, полягає у шифруванні даних. У кожній з областей захисту інформації використовуються різні класи шифрів, починаючи від переставних шифрів та закінчуючи складними шифрами, які ґрунтуються на застосуванні модульної арифметики, теорії груп та інших математичних дисциплін, що дають можливість розв'язувати основні задачі шифрування. До таких задач належать:

перетворення кодів, що шифруються таким способом, який не дозволяє без знання таємних ключів виконати операцію дешифрації за актуальний період часу;

вибір чисел, які б можна було використовувати як ключі шифрування;

мінімізація часу, потрібного для реалізації шифрувальних функцій;

доведення необхідної міри стійкості розроблених алгоритмів та методів шифрування стосовно атак на системи шифрування, що є гарантією безпеки кожної окремої криптосистеми.

Інтегральність інформації, яка передається, означає, що в отриманій адресатом інформації немає частин, які не відповідають оригіналу. Найактуальнішим є забезпечення інтегральності у сферах фінансової діяльності, де зміна одного фрагмента даних може призвести до катастрофічних наслідків для легальних абонентів. До методів забезпечення інтегральності належить метод, що ґрунтується на використанні MAC, про що зазначалося вище.

Другим методом забезпечення інтегральності є метод, що полягає у використанні цифрового підпису. Цифровий підпис створюється шляхом редукції тексту, який передбачається передавати за допомогою односпрямованих функцій, типу H-функцій, та шифрування H-образу тексту з допомогою

несиметричних алгоритмів. При шифруванні абонент використовує приватний таємний ключ і скорочений зашифрований текст, тобто цифровий підпис, що передається адресату разом з текстом зашифрованим за допомогою симетричного шифру або відкритим. Адресат, використовуючи публічний ключ, розшифровує Н-образ тексту повідомлення через прийнятий по каналу зв'язку текст, формує його скорочений образ і, якщо цей образ збігається із скороченим, який отримано з цифрового підпису, то це є гарантією, що текст повідомлення не було модифіковано.

Доступність означає можливість керування доступом до засобів масової інформації, до інформації, яка перебуває в системі масової інформації, до засобів шифрування даних, що передаються, та інших компонентів, несанкціонований доступ до яких може призвести до порушення роботи системи масової інформації та неможливості надання послуг легальним користувачам. Небезпека, що пов'язана з несанкціонованим доступом до системи масової інформації, є досить багатогранною за способами взаємодії з системою масової інформації.

Однією з компонент, що протидіє такій небезпеці, є використання паролів та ідентифікаційних номерів PIN. Розвиток електронно-апаратних засобів дає можливість використовувати складніші методи для контролю доступу. На сьогодні вже можливе використання цілого роду біометричних засобів для ідентифікації споживачів послуг перед наданням їм послуг. До таких засобів зокрема належать ідентифікація за:

райдужною оболонкою ока;

відбитком долоні;

відбитком пальців;

голосом.

Одним з базових методів захисту даних у засобах масової інформації є скремблювання мови. Методи скремблювання використовуються для аналогових систем і являють собою методи шифрування аналогового сигналу [1]. Для того, щоб шифрувати сигнал мови, потрібно поміняти кореляцію між такими параметрами, що визначають аналоговий сигнал: часом, частотою і амплітудою.

Скремблювання частоти полягає у виділенні окремих частотних смуг у сигналі й переставлянні фрагментів сигналів цих частотних смуг у зміненому порядку. Скремблювання у часі полягає у перестановці виділених фрагментів сигналу з одної часової послідовності в іншу. Скремблювання аналогового сигналу за одним параметром називається однопараметричним. Якщо скремблювання реалізується за кількома параметрами, то воно називається багатопараметричним.

1. Грушо А. А. Теоретические основы защиты информации / А. А. Грушо, Е. Е. Тимонина. — М.: Яхтсмен, 1996. — 187 с. 2. Коутинхо С. Введение в теорию чисел. Алгоритм RSA / С. Коутинхо. — М.: Постмаркет, 2001. — 328 с.

СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ В СРЕДСТВАХ МАССОВОЙ ИНФОРМАЦИИ

Анализируются основные виды опасности, которые существуют по отношению к защите информации. Рассматривается метод скремблирования как один из базовых методов защиты данных в средствах массовой информации.

INFORMATION SECURITY METHODS IN THE MEDIA

The basic kinds of danger related to the information security are analyzed here. The method of scrambling is supposed to be one of the basic methods of data protection in the media.

УДК 655.15.011.56

В. Ф. Морфлюк, А. В. Пархоменко
Видавничо-поліграфічний інститут НТУУ «КПІ»

ВИЗНАЧЕННЯ ТА СТАБІЛІЗАЦІЯ ТЕХНОЛОГІЧНИХ ПАРАМЕТРІВ РУЛОННИХ ДРУКАРСЬКИХ МАШИН У ПАРАЛЕЛЬНОМУ РЕЖИМІ ОБРОБКИ

Розробляється підхід для створення програмних засобів визначення та стабілізації технологічних параметрів рулонних друкарських машин, що забезпечує побудову процесів паралельної обробки множини технологічних параметрів у реальному масштабі часу на основі багатоядерних мікропроцесорів.

Рулонні друкарські машини, друкована продукція, мікропроцесор, технологічні параметри

У сучасних рулонних друкарських машинах наявна значна кількість технологічних параметрів, що мають суттєвий вплив на якість друкованої продукції [1–2; 6]. Серед параметрів є такі, що змінюються з невеликою частотою, і тому потребують незначних програмно-апаратних затрат під час друкування всього накладу. Однак технологічний процес включає також ряд параметрів, зміна яких відбувається зі значною частотою впродовж всього часу роботи друкарської машини, що потребує достатніх програмно-апаратних затрат для їх контролю та прийняття рішення. Згідно із цим визначені технологічні параметри потребують постійного контролю на основі об'єктивної автоматизованої системи, яка дає можливість швидко реагувати на зміну характеристик технологічних параметрів та виконати їх стабілізацію у визначений термін.

Тепер проблематика таких систем полягає в мінімізації часу витраченого на обробку інформації з датчиків технологічного процесу рулонних друкарських машин та стабілізації технологічних параметрів у реальному