зависит от конкретной языковой среды и используемых в системе типов криптографических алгоритмов, что позволяет создавать программные модули, которые на уровне исходного текста не зависят от конкретных механизмов безопасности, применяемых в системе. Тем самым реализуется открытость прикладных систем и соответствующих средств защиты. В качестве внешних модулей могут выступать продукты, основанные на симметричных методах шифрования (например, система аутентификации Kerberos), а также реализующие спецификации X.509 на основе открытых ключей. Совместно с подсистемой SNC обычно используется сервер-шлюз системы SAProuter, который используется совместно с межсетевым экраном и предназначен для управления сетевыми соединениями, устанавливаемыми с серверами приложений SAP R/3.

Подсистема аудита предназначена для сбора информации о событиях системы и содержит два типа регистрационных журналов – системный и аудита безопасности. Системный журнал содержит сведения о функционировании ERP-системы, журнал аудита безопасности – данные, связанные с информационной безопасностью системы. Дополнительно подсистема аудита может включать в себя регистрационный журнал сервера SAProuter с данными по всем сетевым соединениям, которые были установлены через этот сервер. Для каждого события подсистема регистрирует дату и время возникновения события, порядковый номер события, категорию события, источник события и другую информацию, связанную с этим событием. Перечень событий, подлежащих аудиту, может быть определен администратором безопасности при помощи фильтров. В соответствии с настройками администратора безопасности при возникновении событий определенного типа подсистема аудита безопасности может выводить информацию об этих событиях на консоль администратора системы.

Подсистема идентификации и аутентификации предназначена для защиты SAP R/3 от НСД путем проверки аутентификационных данных, предоставляемых пользователями системы. Процедуры идентификации и аутентификации подсистемы могут быть реализованы следующими способами:

1. при помощи регистрационных имен и паролей, вводимых пользователями на этапе получения доступа к системе;
2. посредством подсистемы SNC;
3. с использованием сертификатов X.509. При реализации данного механизма аутентификации вместо регистрационных имен и паролей пользователь предоставляет свой сертификат. Аутентификация с использованием сертификатов X.509 в основном используется при удаленном подключении пользователей к системе через сеть Internet;
4. при помощи механизма SAP Logon ticket позволяющего реализовать единую процедуру регистрации в системе.

В заключение можно подчеркнуть, что SAP R/3 должны быть оснащены модулями защиты с криптографическими функциями, основанными на отечественных стандартах. Кроме того, функциональные возможности системы безопасности (SSF, SNC) должны быть дополнены специализированными средствами защиты (например, межсетевыми экранами, системами обнаружения атак, активного мониторинга, антивирусными системами и др.). Лишь при решении этих задач информационная безопасность SAP R/3 и других ERP-систем данного класса будет соответствовать требованиям, предъявляемым к системам защиты.

Литература: ***1.*** *PKCS #7: Cryptographic Message Syntax Standard* ***2.*** *J. Linn. RFC 1421: Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures. February 1993.* ***3.*** *НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно - телекомунікаційній системі. Утверджено приказом ДСТСЗИ СБ Украины от 08.11.2005 №125.* ***4.*** *НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Утверджено приказом ДСТСЗИ СБ Украины от 28.04.1999 №22.*

УДК 004.056.5 (076.5)

МЕХАНІЗМ КОДУВАННЯ ТА ОБРОБКИ ІНФОРМАЦІЇ В СИСТЕМАХ ІЗ ХАОСОМ

Богдан Корнієнко, Олександр Неділько
Національний авіаційний університет

Анотація: **В комунікаційних системах хаос може використовуватися як носій інформації і як динамічний процес, що забезпечує перетворення інформації до нового вигляду. Методи хаотичного кодування є зручним засобом організації віртуальних корпоративних мереж із забезпеченням заданого рівня конфіденційності інформації. В статті досліджується можливість використання хаосу для обробки інформації, розглядається модель хаотичного процесора.**

Summary: **In communication systems chaos can be used as a carrier of information and as a dynamic process, which provides conversion information for the new type. Methods chaotic coding is a convenient tool for organizing virtual corporate networks with a given level of confidentiality of information. This article explores the possibility of using chaos for information processing, is considered a model chaotic processor.**
Ключові слова: **Хаос, кодування інформації, хаотичний процесор**

I Вступ

В комунікаційних системах хаос може використовуватися як носій інформації, як динамічний процес, що забезпечує перетворення інформації до нового вигляду, і як комбінація першого і другого. Пристрій, що перетворює за допомогою хаотичних кодувань сигнал в передавачі, називається хаотичним процесором. Із його допомогою можна змінювати інформацію таким чином, що вона виявиться недоступною сторонньому спостерігачеві, але в той же час буде легко повернена до початкового вигляду спеціальною динамічною системою - хаотичним процесором, що знаходиться на приймальній стороні комунікаційної системи.

За допомогою хаотичних кодувань можливо принципово по новому організувати інформаційний простір, створюючи в ньому більше відкритих груп користувачів − підпросторів. В рамках кожної групи вводиться своя "мова" спілкування − одні для всіх учасників правила, протоколи і інші ознаки даної "інформаційної субкультури". Для бажаючих опанувати цю "мову" і стати членом співтовариства є відносно прості засоби доступу. В той же час для сторонніх спостерігачів участь у подібному обміні буде ускладнена. Отже, хаотичне кодування може слугувати засобом структуризації спільного інформаційного простору.

Подібним чином можна організувати багатокористувачевий доступ до інформації. Наявність глобальної мережі Інтернет і магістральних інформаційних потоків передбачає існування спільних протоколів, що забезпечують проходження інформації одними каналами. Але в рамках визначених груп учасників (наприклад, в рамках корпоративних мереж) існує необхідність доставки інформації конкретним споживачам без дозволу доступа сторонніх учасників. Методи хаотичного кодування є зручним засобом організації таких віртуальних корпоративних мереж. Крім цього, вони можуть використовуватися і безпосередньо для забезпечення заданого рівня конфіденційності інформації.

II Постановка задачі

В статті досліджується можливість використання хаотичних кодувань для обробки інформації, розглядається модель хаотичного процесора.

III Гнучкий контроль якості інформаційних потоків

У зв'язку з розвитком електронної комерції й загостренням проблеми авторських прав в Інтернеті дуже актуальною є ще одна функція хаотичного кодування. Особливо це стосується продажу через мережу мультимедійних товарів (музики, відео, цифрової фотографії й ін.). На основі детермінованого хаосу можна забезпечити такий спосіб захисту авторських прав і прав на інтелектуальну власність, як зниження якості інформаційного продукту при загальному доступі. Наприклад, музичні треки, закодовані за допомогою хаосу, будуть поширюватися в мережі без яких-небудь обмежень, так що кожен користувач зможе скористатися ними. Однак при прослуховуванні без спеціального хаотичного процесора якість звуку буде низькою. Розповсюджувана інформація залишається відкритою і не підпадає під обмеження, що накладають застосування криптографічних методів захисту. Крім того, потенційний покупець має можливість ознайомитися із продуктом, а вже потім вирішити, чи варто придбати його високоякісну версію. При захисті від копіювання цифрових фотографій, музичної і відеоінформації, що циркулює в мережі, немає необхідності в тому, щоб інформація була повністю недоступна для «зловмисника». Цілком досить просто знизити якість її відтворення до рівня, неприйнятного для її використання (рис. 1). Законні одержувачі забезпечуються процесорами, що дозволяють відновити якість інформації [1].

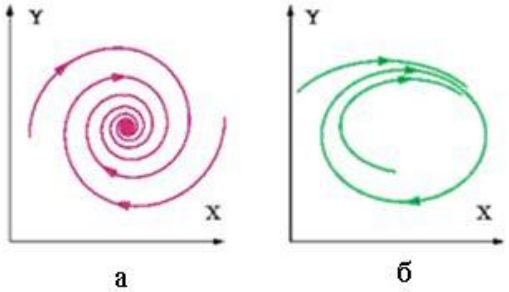
а б в

Рисунок 1 − Зображення з різними ступенями деградації в результаті хаотичного кодування
а − початкова фотографія
б − фотографія спотворена до неприйнятного для споживача рівня
в − ознаки початкового зображення відсутні

IV Захищеність інформаційного обміну

Хаотичне кодування може безпосередньо виконувати завдання забезпечення певного рівня конфіденційності інформації, що передається [2]. Ці методи переходять в область традиційної криптографії. До теперішнього часу запропоновано і апробовано ряд конкретних алгоритмів і схем хаотичного кодування, що забезпечують різну ступінь конфіденційності. З їх допомогою досягаються: вища ефективність захисту мультимедійної інформації, ніж у поширеного алгоритму DES, великі швидкості кодування та стійкість відносно шуму.

Рух динамічної системи можна наглядно зобразити як траєкторію на фазовій площині (рис. 2), де осі X і Y − узагальнені координати.



а б

Рисунок 2 − Траєкторії на фазовій площині
а − коливання маятника, що затухають
б − періодичні автоколивання

Траєкторії сходяться до однієї точки, що відповідає положенню рівноваги − повній зупинці маятника. Всі траєкторії "намотуються" на граничний цикл − замкнену криву, відповідну сталому процесу. Основним елементом хаотичної системи зв'язку є генератор хаосу. Сенс процедури полягає в переході від спрощеної математичної моделі до використання спеціальних симулюючих пакетів типу ADS (Advanced Design System). Моделі активних елементів є в самих пакетах. Крім того, в симулюючих пакетах використовуються моделі як активних, так і пасивних компонентів, що враховують появи артефактів на високих і понад високих частотах.

V Волоконно-оптичний зв'язок із застосуванням динамічного хаосу

Хаотичні коливання використовуються також для кодування інформації при передачі від лазера-передавача до лазера-приймача через волоконно-оптический кабель (рис. 3). При передачі від лазера-передавача до лазера-приймача через волоконно-оптичний кабель у макеті «повідомлення» генерували сигнал типу меандра напівпровідниковим лазерним діодом. Потім сигнал потрапляв на волоконно-оптичний підсилювач і вводився в хаотичний сигнал, що генерується кільцевим волоконно-оптичним лазером.

Результуючий комбінований сигнал, що складається з суміші повідомлення і хаотичного носія, передавався через оптичний кабель до другого підсилювача. При отриманні комбінованого сигналу підсилювач приймача відтворював хаотичні коливання, синхронізовані з тими, які надсилалися лазером-передавачем. Повідомлення для одержувача отримано так: хаотична складова сигналу, що виміряна цифровим осцилографом, віднімалася від комбінованого сигналу і обмежувалася фільтром низьких частот.

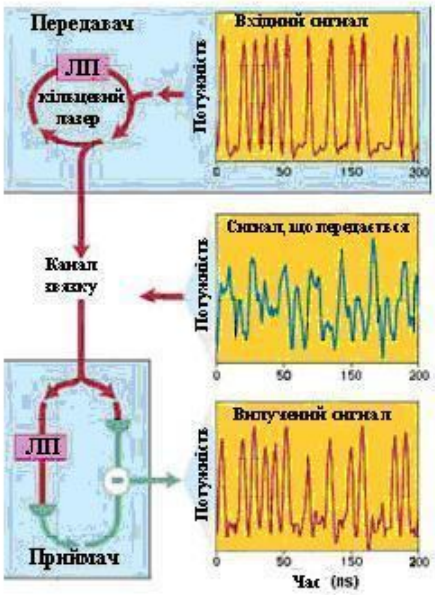


Рисунок 3 − Використання хаотичних коливань для кодування інформації

VI Модель хаотичного процесора

Для генерування псевдовипадкової послідовності використовуємо систему рівнянь [3]:

$$\begin{aligned} dx/dt &= a(y-x), \\ dy/dt &= x(z-\beta), \\ dz/dt &= \gamma - xy, \end{aligned} \qquad (1)$$

де a, β, γ - додатні коєфіцієнти. Особливістю цих рівнянь як системи, що володіє хаотичною динамікою, є висока чутливість до зміни параметрів. Саме це перешкоджає несанкціонованому дешифруванню при використанні для кодування інформації детирмінованого хаосу.

Для ілюстрації чутливості системи до зміни параметрів, проведемо порівняння коливань двох автономних систем, кожна з яких описується рівняннями (1), які відрізняються індексами *i* (1,2) при змінних коефіцієнтах. В такому випадку:

$$\begin{aligned} dx_1/dt &= a_1(y_1-x_1), \quad & dx_2/dt &= a_2(y_2-x_2), \\ dy_1/dt &= x_1(z_1-\beta_1), \quad & dy_2/dt &= x_2(z_2-\beta_2), \\ dz_1/dt &= \gamma_1 - x_1y_1, \quad & dz_2/dt &= \gamma_2 - x_2y_2. \end{aligned} \qquad (2)$$

На рис. 4. наведені фрагменти реалізації різниці коливань $x_1(t)-x_2(t)$ за незначної різниці параметрів a_1 і a_2; при цьому $a_1=1,\ \beta_1=\beta_2=0.8,\ \gamma_1=\gamma_2=1.2.$ Початкові умови для всіх змінних дорівнюють 0.1.

За незначної різниці параметрів a_1 і a_2 (a_1 - a_2=0.01) різні коливання виникають із помітною затримкою, яка збільшується зі зменшенням величини a_1 - a_2 (в). У випадку рис. 4 (б), затримка займає інтервал часу $t\in[0,20],$ а в випадку рис. 4 (в), – інтервал часу $t\in[0,52]$. Цю затримку (її умови можна розглядати як «перехідний» процес) легко виправити шляхом виключення початкової ділянки реалізації. Це необхідно при кодуванні інформації.

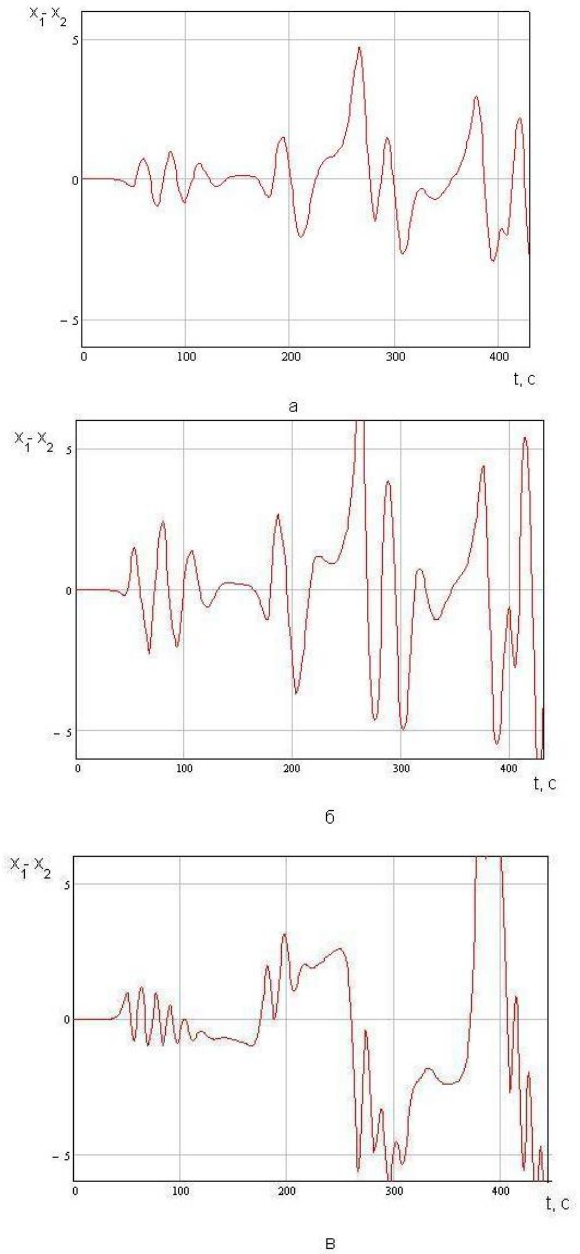


Рисунок 4 − Фрагменти реалізації коливань для різних значень коефіцієнта a_2

а − a_2 =1.1, б − a_2 = 1.01, в − a_2 =1.000001

Використання хаотичних рішень розглянутої системи рівнянь дозволяє побудувати складний шифр, який не піддається розкриттю, якщо не відомі точні значення початкових умов і параметрів динамічної системи, за яких можна отримати розв`язок даного рівня.

VII Висновки

Таким чином, розглянуто можливості використання хаотичних коливань для обробки інформації. Проведено дослідження математичної моделі для різних режимів роботи хаотичного процесора. Дослідження шифрування та дешифрування свідчать про те, що при кодуванні символів, які формують зображення, можуть використовуватися псевдовипадкові послідовності цілих чисел, одержані після розв`язання нелінійних диференціальних рівнянь із хаотичною динамікою.

Отже, інформація може бути прихована і в сигналах, що виглядають шумоподібними. Інформація може бути ефективно передана і прийнята за допомогою хаотичного кодування.

Література ***1.*** *Дмитриев А. С., Клецов А. В., Лактюшкин А. М., Панас А. И., Старков С. О. "Сверхширокополосные коммуникационные системы на основе динамического хаоса", Успехи современной радиоэлектроники, 2008, №1, С. 4–18.* ***2.*** *Дмитриев А. С., Ефремова Е. В., Максимов Н. А., Григорьев Е. В. "Генератор хаотических колебаний сверхвысокочастотного диапазона на основе автоколебательной системы с 2,5 степенями свободы", Радиотехника и электроника, 2007, Т. 52. № 10, С. 1232-1240.* ***3.*** *Кальянов Г. Н., Кальянов Э. В. // Письма в ЖТФ. 2005. Т. 31. В. 24. С. 45-50.*

УДК 621.391:519.7:510.5

ОПТИМАЛЬНЫЕ ПРОТОКОЛЫ МНОЖЕСТВЕННОГО РАЗДЕЛЕНИЯ СЕКРЕТА С МНОГОАДРЕСНЫМ СООБЩЕНИЕМ, ОСНОВАННЫЕ НА ЛИНЕЙНЫХ ПРЕОБРАЗОВАНИЯХ НАД КОЛЬЦАМИ ВЫЧЕТОВ

Антон Алексейчук, Андрей Волошин
Институт специальной связи и защиты информации НТУУ «КПИ»

Анотація: **Отримані достатні умови оптимальності (за критерієм максимуму інформаційних відношень) протоколів множинного розподілу секрету з багатоадресним повідомленням, що реалізують певні ієрархії доступу. Наведено низку конструкцій зазначених протоколів, які задовольняють отриманим умовам оптимальності.**
Summary: **The sufficient conditions of optimality (i. e. of information rates maximality) of multi-secret sharing schemes with broadcast message for certain access hierarchies are obtained. Some constructions of such schemes satisfied the described conditions are presented.**
Ключевые слова: **криптографическая защита информации, протокол множественного разделения секрета с многоадресным сообщением, иерархия доступа, кольцо вычетов.**

Введение

Как известно, при разработке современных информационно-телекоммуникационных систем (ИТС) особое внимание уделяется вопросам разграничения доступа к их ресурсам [1]. Согласно принятой мировой и отечественной практике [2, 3], решение задач разграничение доступа к ресурсам таких систем возлагают на подсистему управления доступом. При этом расширение функциональных возможностей ИТС, как правило, приводит к необходимости значительного повышения гибкости и надежности используемых подсистем управления доступом [4]. Для решения последней задачи, наряду с другими методами, применяют так называемые протоколы разделения секрета (ПРС), позволяющие получать приемлемые решения, как с точки зрения надежности, так и с точки зрения гибкости подсистемы управления доступом [5, 6].

Из анализа результатов статей [5 – 7] и ряда других публикаций следует, что повышение надежности и гибкости подсистем управления доступом современных ИТС может быть достигнуто при применении ПРС, обладающих следующими свойствами:

1) возможность одновременного разделения нескольких секретных ключей (секретов);
2) безусловная (совершенная) стойкость ПРС;
3) возможность реализации процедур восстановления секретов с использованием многоадресных сообщений, в том числе, для семейств иерархий доступа на множестве участников протокола;
4) вычислительная эффективность процедур формирования секретной информации, передаваемой участникам протокола, и восстановления секретов соответствующими коалициями участников.

В [8 – 10] предложены и исследованы протоколы разделения секрета, обладающие перечисленными свойствами. Указанные ПРС, названные линейными протоколами множественного разделения секрета с многоадресным сообщением (ПМРС с МС), строятся на основе линейных преобразований над кольцами вычетов целых чисел и обобщают классические векторные схемы разделения секрета над конечными полями [11, 12] и линейные ПРС над кольцами вычетов примарного порядка [13].

Для оценки эффективности ПМРС с МС, как правило, используют два показателя: информационное отношение и многоадресное информационное отношение. Первый из них определяется как отношение суммарной длины разделяемых секретных ключей к максимуму длин сообщений, передаваемых участникам протокола на первом этапе, а второй – как отношение суммарной длины секретов к длине многоадресного сообщения, необходимого для восстановления секретных ключей соответствующими коалициями участников [14]. Протокол множественного разделения секрета с многоадресным сообщением называется оптимальным в заданном классе ПМРС с МС, если он имеет наибольшее информационное отношение и