УДК 004.057.4(045)

ЗАХИСТ ІНФОРМАЦІЙНИХ ОБ'ЄКТІВ НА БАЗІ ЛИШКОВИХ КЛАСІВ

Василенко В. С., канд. техн. наук, доц., ***Дубчак О. В.***

Національний авіаційний університет

kszi@ukr.net

Розглянуто механізми забезпечення конфіденційності, цілісності та доступності інформаційних потоків телекомунікаційних мереж, що використовують один із методів завадостійкого кодування – код на основі лишкових класів.

Ключові слова: цілісність, конфіденційність, доступність інформації, завадостійке кодування, лишкові класи, контрольна ознака, криптографічні перетворення.

Mechanisms of maintenance of confidentiality, integrity and availability of information streams of telecommunication networks are considered; the noiseproof code on the basis of conditional classes is presented as a basis of methods of information safety.

Keywords: integrity, confidentiality, availability of information, noiceproof coding, residual classes, control sig, cryptographic transformations.

Постановка проблеми

Обмін інформаційними об'єктами в телекомунікаційних мережах (ТКМ) може відбуватися, як відомо, в умовах негативного впливу природних чи штучних загроз. Зазвичай загрози виникають унаслідок, наприклад: недостатнього співвідношення сигнал/завада в точці приймання через багатопроменевість, ослаблення сигналу на межі та, особливо, за межами зон упевненого приймання; навмисних дій неавторизованих користувачів тощо. У результаті з'являються різні викривлення інформації, а отже, порушення таких її функціональних властивостей захищеності, як цілісність і доступність. Слід урахувати, що, оскільки частина інформаційних потоків може мати витоки, також виникає завдання убезпечення їх від перехоплення, чи, іншими словами, від загроз конфіденційності.

Зрозуміло, що викривлення інформації можливі не тільки при її передачі, але й на будь-якому етапі — зберіганні або обробці в ТКМ. Причинами таких викривлень можуть бути випадкові або навмисні дії. Випадкові викривлення, у свою чергу, можна класифікувати як штучні та природні, пов'язані з дією природних чинників, до числа яких належать атмосферні електромагнітні розряди, іскріння контактів в автомобілях або електротранспорті, недостатня надійність електронних елементів й елементів електричних ланцюгів тощо. Випадкові штучні викривлення пов'язані з діяльністю людей — з випадковими помилками персоналу. Навмисні викривлення завжди пов'язані з умисними діями порушників. Наслідком будь-яких із перелічених дій є викривлення того або іншого числа символів в цифровому представленні інформації, незалежно від використовуваної системи числення або форми представлення інформації.

Отже, будь-які дії, що спричиняють порушення інформаційних об'єктів, є загрозами функціональним властивостям захищеності інформаційних ресурсів – їх цілісності та доступності.

Як результат природних впливів у каналах ТКМ є зменшення співвідношення енергетик сигнал/шум — сигнал/завада. Це співвідношення визначає правільність інформації, яку можна подати, наприклад, через імовірність $P_{\text{ïîì}}$ помилок у двійкових символах — бітах, а також інтенсивність цих помилок. Слід зазначити, що інтенсивність природних дій в каналах деяких ТКМ, яка визначається, в основному, цим співвідношенням, може бути достатньо значною.

Для забезпечення контролю та поновлення цілісності інформаційних об'єктів — відновлення викривлених чи зруйнованих даних, до складу інформаційних ресурсів, що потребують захисту, включають надмірну інформацію — ознаку цілісності або контрольну ознаку.

Відповідну назву використовують залежно від термінології, прийнятої в задачах контролю цілісності або завадостійкого кодування. Ця ознака, процедура формування якої відома, є способом відображення інформації, що захищається, і з достатньо високою вірогідністю відповідає останній.

При цьому між інформацією, що захищається, і ознаками цілісності або контрольними ознаками встановлюється регулярний (функціональний) односторонній зв'язок: процедури розрахунку контрольної ознаки за початковою інфор-мацією, що захищається, відомі, а процедури розрахунку початкової інформації за контрольними ознаками найчастіше відсутні.

Контроль цілісності, тобто виявлення відсутності викривлень, зводиться при цьому до деяких процедур перевірки наявності вказаного функці-

© В.С. Василенко, О.В. Дубчак, 2010

онального одностороннього зв'язку між ознаками цілісності і прийнятою з каналу зв'язку інформацією.

Інструментарій забезпечення цілісності інформації істотно залежить від умов його застосування, а саме від характеру впливу випадкових природних або штучних зловмисних викривлень.

До характерних особливостей випадкових викривлень слід віднести передусім те, що через відсутність навмисності вони порушують функціональний односторонній зв'язок між прийнятою інформацією та ознаками цілісності, сформованими перед передачею. Тому в разі виявлення подібного порушення зв'язку встановлюється факт наявності таких викривлень, а за певних умов, і їх місця та величини. За відсутності порушення зв'язку встановлюється факт відсутності викривлень.

Характерною ж особливістю навмисних викривлень є прагнення зловмисника забезпечити наявність регулярного зв'язку між модифікованою їм початковою інформацією та ознаками її цілісності. Знаючи процедуру формування контрольних ознак, після необхідної для його цілей модифікації початкової інформації перед передачею її одержувачу, порушник забезпечує їх формування з метою імітації. Розкриття наявності модифікації при успішному формуванні вказаних ознак унеможливлюється. Для захисту інформаційних ресурсів їх власнику або авторизованому користувачу необхідно використовувати: приховані, тобто невідомі потенційним порушникам, процедури формування контрольних ознак, забезпечення чого суттєво ускладнено; уведення в загальновідомі процедури формування контрольних ознак таємних параметрів — ключів перетворення. Не знаючи ключів перетворення, порушник не зуміє забезпечити, зімітувати наявність регулярного зв'язку між модифікова-ною їм початковою інформацією та ознаками цілісності.

У процесі обігу інформації в ТКМ виділяють дві основні причини виникнення природних викривлень:

— збої в якійсь частині устаткування мережі або виникнення несприятливих об'єктивних подій у мережі, наприклад, колізії при використанні методу випадкового доступу в мережу тощо. Як правило, система передачі даних готова до такого роду проявів і містить планово передбачені засоби для їх усунення;

— завади, викликані зовнішніми чинниками, атмосферними явищами й джерелами, наприклад, багатопроменевість, яка згадувалася вище.

Певні ускладнення боротьби із завадами полягають у їх безладді, нерегулярності та структурній подібності з корисними інформаційними сигналами. З огляду на це, однією з найсерйозніших сучасних проблем теорії та техніки інформаційного обміну в каналах ТКМ стає захист інформації від викривлень унаслідок шкідливого впливу завад.

Вирішення проблеми завадостійкості має суттєве практичне значення. Для цього використовуються певні механізми забезпечення цілісності, й у певному значенні — доступності, інформації в умовах природних дій для каналів ТКМ, і взагалі для мереж передачі даних. Серед таких механізмів слід виділити:

1) збільшення згаданого вище співвідношення сигнал/завада за рахунок підвищення енергетики сигналу, наприклад, шляхом збільшення початкової потужності, регенерації на пунктах підсилення та ретрансляції, що потребує значних енергетичних або матеріальних витрат. Слід зауважити, що у деяких випадках, наприклад в радіоканалах, такі дії демаскують наявність трафіку та полегшують перехоплення інформаційних потоків;

2) збільшення співвідношення сигнал/завада за рахунок зниження рівня завад шляхом використання спеціальних ліній зв'язку з низьким рівнем власних шумів, наприклад, кабельних, передусім оптоволоконних, що також може вимагати значних матеріальних витрат, або не може бути реалізованим взагалі, наприклад, у радіоканалах;

3) забезпечення хоча б задовільної узгодженості смуги пропускання Π каналу із спектром сигналу, який визначається параметрами сигналу, в першу чергу, його тривалістю $\tau \approx \frac{1}{B}$; тут τ — тривалість сигналу; B — технічна швидкість передачі інформації або швидкість посимвольної передачі в даному каналі; найчастіше задовільною вважають таку узгодженість, коли $\Pi \geq 2B$;

4) застосування групових (мажоритарних) методів захисту; вони ґрунтуються на використанні: декількох каналів зв'язку (від 3 — до 5), що є фізично і найчастіше, навіть, географічно рознесеними, якими передається одна й та сама інформація; багатократної передачі (від 3 — до 5 разів) однієї й тієї самої інформації одним каналом зв'язку. У першому випадку необхідні істотні матеріальні витрати, в другому — значно зменшується пропускна спроможність каналу зв'язку (від 3 — до 5 разів), а час затримки передавання інформаційних об'єктів може стати неприпустимо великим. Із зрозумілих причин у системах

передачі даних використовування цих методів не завжди є доцільним;

5) застосування різного роду завадостійких кодів з виявленням помилок у прийнятій або зчитаній з відповідних пристроїв інформації. Ці коди дають змогу реалізувати програмні, апаратурні або програмно-апаратурні засоби виявлення викривлень. Це, в свою чергу, дає можливість застосування способів передачі повідомлень з різноманітним зворотним зв'язком: інформаційним — деяким аналогом мажоритарного методу з багатократною передачею інформації, зворотним її прийомом і ухваленням рішення щодо правильності передачі на стороні передавача; з вирішальним зворотним зв'язком (ВЗЗ) — багатократній, за необхідності, передачі з ухваленням рішення щодо її правильності на стороні приймача. Недоліком таких способів забезпечення цілісності є необхідність організації зворотного (другого) каналу зв'язку, що призводить до істотних матеріальних витрат, а також до збільшення часу затримки передавання інформаційних об'єктів, який може бути неприпустимо великим;

6) застосування різного роду завадостійких коригуючих кодів (ЗКК), які дозволяють реалізувати програмні, апаратурні або програмно-апаратурні засоби виявлення та усунення викривлень.

Останній із механізмів забезпечення цілісності інформаційних об'єктів, із застосуванням завадостійких корегуючих кодів, є найбільш прийнятним в стандартах радіозв'язку, в тому числі — в системах мобільного, стільникового зв'язку. Він не потребує наявності зворотного каналу і забезпечує, як правило, прийнятний час затримки передавання інформаційних об'єктів. Слід зауважити, що такий механізм у мережах, в яких використовується невідомий для сторонніх завадостійкий коригуючий код — код із прихованими параметрами, дає певний енергетичний виграш: застосування коду для абонентів еквівалентно збільшенню співвідношення сигнал/завада. Відомо [1], що такий асимптотичний енергетичний виграш від кодування дорівнює

$$g = R(t+1),$$

де R — відносна швидкість коду; t — кратність викривлень, що виявляються кодом, або в децибелах

$$G = 10 \cdot \log[R(t+1)].$$

Наприклад, у стандарті *GSM* [2] забезпечується $t = 5,\ R = 0{,}5,\ g = 3\,(2\ Äá)$, що є еквівалентним можливості збільшення у 2,5 разу потужності передавача — базової чи мобільної станції — і, відповідно, збільшенню дальності радіозв'язку в 1,58 разу. Якщо ж забезпечити $t = 16,\ R = 0{,}875,\ g = 14\ (11{,}5\ Äá)$, то це є еквівалентним можливості збільшення дальності радіозв'язку вже у 3,7 разу.

Отже, вирішення проблеми забезпечення цілісності інформаційних об'єктів у таких та подібних ТКМ, з використанням телефонних радіо- та кабельних каналів, займає суттєве місце. Даними кодами цілісність забезпечується навіть в умовах впливу природних пакетних викривлень, як тривалістю 2...10 мс, так званих «коротких», так і особливо «довгих» — тривалістю 100…200 мс, не кажучи вже про штучні навмисні завади. Особливу актуальність даний механізм набуває для згаданих систем стільникового зв'язку. Наприклад, у стандартах *CDMA*, *GSM* базовий цифровий потік розбивається на пакети певної тривалості, відносно до яких реалізується згорточне кодування із певним перемежуванням [2]. При цьому тривалість пакету викривлень може дорівнювати чи, навіть, значно перевищувати тривалість інформаційного пакету, що може мати суттєвий вплив на результативність процедур інформаційного обміну.

Задача убезпечення інформаційних об'єктів від перехоплення в умовах передачі її каналами, що пролягають за межами контрольованої території, передусім радіоканалами, вирішується застосуванням засобів криптографічного перетворення. Наприклад, при застосуванні засобу шифрування з відкритими ключами [3], блок інформації, що сформований з використанням завадостійкого кодування, шифрується відповідними засобами. З цього витікає, що одночасне забезпечення конфіденційності та цілісності інформаційних об'єктів потребується достатньо часто. Отже, слід акцентувати увагу на необхідності забезпечення одночасного захисту від загроз конфіденційності, цілісності та доступності інформаційних потоків.

Цілі

Для застосування у зазначених умовах пропонується один із досить дієвих способів забезпечення даних вимог — *механізми захисту інформаційних об'єктів на основі лишкових класів.*

Нагадаємо, що для застосування таких механізмів захисту інформаційних об'єктів блок початкової інформації в цифровій формі, незалежно від застосованої системи числення чи наявності якихось попередніх перетворень, розглядається як число A у двійковій позиційній системі числення. Як символи цього числа можуть розглядатися, що і відбувається найчастіше, певні групи двійкових розрядів, наприклад,

байти. Так, блок початкової інформації можна записати у вигляді

$$A = a_1, a_2, ..., a_s, \quad (1)$$

де a_i – згадані групи двійкових розрядів $(i = 1, 2, ..., s)$; s — кількість інформаційних символів розрядністю b у блоці початкової інформації.

Щодо до такого представлення можна запропонувати викладену нижче сукупність механізмів на основі лишкових класів.

Механізми забезпечення конфіденційності інформації шляхом криптографічних перетворень на основі лишкових класів

Дані механізми ґрунтуються на переведенні первинного блоку із задекларованої позиційної системи числення (1) в систему лишкових класів за сукупністю основ цієї системи p_i $(i = 1, 2, ..., m)$, тобто подання (1) у вигляді

$$A = \alpha_1, \alpha_2, ..., \alpha_m, \quad (2)$$

де α_i — лишки від ділення числа A у формі (1) на відповідні основи p_i; m — кількість основ, за якої забезпечується умова узгодження діапазонів представлення позиційного числа розрядністю $n = s \cdot b$ двійкових символів (біт) у вигляді (1) та числа в системі лишкових класів (2):

$$\prod_{i=1}^{m} p_i \geq 2^n. \quad (3)$$

Якщо зберігати в таємниці від неавторизованих користувачів — абонентів величини цієї сукупності основ p_i та вважати їх ключами перетворення, то одержимо не що інше, як меха-нізм криптографічного перетворення із симетричними ключами.

Недоліком такого механізму забезпечення конфіденційності інформації є недостатня криптографічна стійкість, що пояснюється можливістю досить швидкого накопичення статистичної інформації щодо максимального значення величин лишків за основами системи числення, тобто величин $(p_i - 1)$, а отже і величин ключів p_i для усіх $i = 1, 2, ..., m$. Однак не важко показати, що цей недолік дуже просто усувається нескладними перетвореннями вихідного та перетвореного блоків.

Ці механізми ґрунуються на поєднанні розглянутих криптографічних властивостей системи лишкових класів із властивими для цієї системи можливостями щодо побудови завадостійких кодів.

Нагадаємо, що перевагами системи лишкових класів є можливість, у разі введення надмірності у вигляді лишку від ділення початкового числа A на ще одну надлишкову основу p_k, утворити завадостійкий код

$$A = \alpha_1, \alpha_2, ..., \alpha_m, \alpha_k. \quad (3)$$

Відомо, що такий код, за певної надлишковості, дає змогу здійснювати контроль наявності викривлень у вихідному блоці, а при її збільшенні — також і виправлення виявленого викривлення. Отже, цей механізм дозволяє органічно поєднувати можливості й крипто- і завадозахищеності інформаційних об’єктів.

В умовах секретності для зловмисників величини основ системи числення в лишкових класах механізм перетворення вихідного блоку у вигляд (3) стає *механізмом контролю чи контролю та поновлення цілісності зашифрованих інформаційних об’єктів*. Отже, виключається можливість такої несанкціонованої модифікації вихідного інформаційного об’єкта, яка б не могла бути виявлена засобами контролю.

Механізми забезпечення контролю, контролю та поновленню цілісності інформації шляхом застосування коду умовних лишків (ЛУ-коду)

Для механізмів такого класу характерно, що вихідний код деякого інформаційного блоку, незалежно від початкової системи числення, умовно розглядається як число A в лишкових класах у вигляді виразу (2). З цією метою кожний із символів цього числа подається як лишок від розподілу деякого умовного, невідомого наперед, числа на певну основу із їх сукупності p_i. Для забезпечення такого підходу, окрім умови (2), на цю умовну систему числення накладається ще одне обмеження у вигляді

$$p_i \geq 2^b$$

для усіх умовних основ та усіх символів блоку початкової інформації розрядністю b. Останнє пов’язано із зрозумілою необхідністю забезпечення перевищення величиною кожної основи p_i максимального значення можливого значення умовного лишку.

Тоді, з використанням алгоритмів кодування — декодування ЛУ-коду можна розрахувати значення умовного лишку α_k і за додатковою, контрольною основою p_k — контрольну ознаку чи ознаку цілісності. Отримана сукупність вихідного блоку та умовного лишку α_k може вважатися числом у системі лишкових класів видгляу (3), а отже, дозволяє здійснювати виявлення і виправлення можливих викривлень у прийнятому інформаційному об’єкті.

У разі відкритості параметрів та констант цей код може застосовуватися як звичайний завадо-

стійкий код, наприклад, для захисту інформації у логічних каналах управління стандартів мобільного зв'язку типу *GSM*. Звернемо увагу на те, що основна частина в такому представленні вихідного блоку при кодуванні не змінюється, а при розрахунках контрольної ознаки, чи ознаки цілісності, можна оперувати параметрами, прихованими від сторонніх абонентів. Для захисту інформації, у цьому випадку, такий код дає змогу реалізувати механізм забезпечення *контролю чи контролю та поновлення цілісності інформації* із використанням симетричних ключів. Наприклад, він знайшов застосування у повношвидкісному каналі передачі даних того ж стандарту мобільного зв'язку типу *GSM* із притаманним йому кодуванням та перемежуванням.

Таким чином, застосування щодо до різної інформації одного і того ж механізму контролю та поновлення інформації, але із загальновідомими чи прихованими ключами перетворення дозволить не тільки отримати відповідний енергетичний виграш від такого кодування, але й забезпечити контроль чи контроль та поновлення цілісності інформації з одночасним спрощенням, принаймні зменшенням кількості типів апаратури для реалізації означених задач.

Механізми формування імітовставок

Дані механізми використовують розглянутий вище підхід щодо забезпечення контролю цілісності інформації у разі, коли ставиться лише задача контролю цілісності інформаційних об'єктів, а завдання одержання енергетичного виграшу відсутня. Тоді застосування згаданого вище механізму дає змогу обмежитися його модифікацією та використанням секретних симетричних ключів. Власне модифікація полягає у форму-ванні ознаки цілісності, яка обчислюється не для кожного з інформаційних блоків, а є загальною для усього інформаційного об'єкта. Це є певним еквівалентом застосування відомого механізму формування геш-функцій за міждержавним стандартом ГОСТ 34.310-94. Винятком є відсут-ність секретних елементів у геш-функції та непотрібність, у свою чергу, захисту певними механізмами, наприклад, криптографічним перетворенням з відкритими ключами. А механізм, що пропонується, дозволяє здійснювати формування ознаки цілісності на симетричних ключах, тобто є більш функціональним порівняно зі стандартизованою геш-функцією. Оскільки такий механізм можна застосовувати як для усього інформаційного об'єкта, так і для його частин, то його можна називати *механізмом формування імітовставок.*

Механізми формування цифрового підпису

Ці механізми використовують можливості повного чи часткового приховування певних параметрів та змінних системи лишкових класів, унаслідок якого неавторизовані користувачі не мають можливостей ні зімітувати чужий цифровий підпис, ні розшифрувати інформацію, яка не призначена даному користувачеві.

Наприкінці зауважимо, що усі викладені механізми мають відповідне теоретичне обґрунтування, математичні моделі та розроблені алгоритми їх реалізації.

Висновок

Отже, розглянувши деякі сучасні засоби захисту інформаційних об'єктів від впливів природних та штучних загроз, можна використовувати у ТКМ механізми захисту інформації на основі лишкових класів, які забезпечують достатньо високу степінь конфіденційності, контролю, контролю та поновлення цілісності інформаційних ресурсів, формують імітовставки та цифровий підпис з метою захисту інформаційних ресурсів.

ЛІТЕРАТУРА

1. *Кларк Дж*. Кодирование с исправлением ошибок в системах цифровой связи / Дж. Кларк, Дж. Кейн; пер. с англ.: под ред. В. Герасименко. — М. : Радио и связь, 1987. — 397 с.

2. *Дубровский В. В*. CDMA — взгляд глазами профессионала. //mailto:v_ dubrovskii@mail.ru.

3. *Громаков Ю. А*. Сотовые системы подвижной радиосвязи. Режим допуску //http:-//mobile.altmaster.ru.

Стаття надійшла до редакції 14.12.2010.