Висновки. В системі СНеП реалізовано механізм нечіткого логічного виводу, що дозволяє максимально точно розв'язувати задачі, що складно формалізуються, розвинуто і розширено принцип найдовшої умови – це відношення на множині продукцій «загальне правило – окреме правило». Цим система відрізняється від існуючих аналогічних систем.

1. Нечеткие множества в моделях управления и искусственного интеллекта / Под ред. *Д.А. Поспелова*. – М.: Наука. Гл. ред. физ.-мат лит., 1986.
2. Нечеткие множества и теория возможностей. Последние достижения. Пер. с англ. / Под ред. *Р.Р. Ягера*. – М.: Радио и связь, 1986.
3. *Заде Л.А*. Понятие лингвистической переменной и его применение к принятию приближенных решений. – М.: Мир, 1976.
4. Искусственный интеллект. Книга 2. Модели и методы: Справочник. Под ред. *Д.А. Поспелова*. – М.,Радио и связь, 1990.
5. *Кузнецов В.Е.* Представление в ЭВМ неформальных процедур. – М.: Наука, 1989.
6. *Марков С.В.* Продукционное программирование процессов автоматизированного проектирования конструкторской документации печатных плат: Дис. канд. техн. наук / Воронеж. НИИ полупр. машин-я. Воронеж, 1988.
7. *Попов Э. В.* Экспертные системы. Решение неформализованных задач в диалоге с ЭВМ. М.,Наука, гл. редакция физико-математической литературы, 1987

Поступила 27.01.2010р.

УДК 681.3

В.С. Василенко

МОДЕЛІ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ІНФОРМАЦІЙНИХ ОБ'ЄКТІВ

Summary: Considered most widespread models of providing of integrity of information's holding object.

Відповідно до термінології нормативних документів Державної служби спеціального зв'язку і захисту інформації України [1] під цілісністю інформації розуміється її властивість, яка полягає у тому, що інформація не може бути модифікована неавторизованим користувачем або процесом. Іншими словами, під цілісністю інформації розуміється відсутність в ній будь-яких викривлень (модифікацій), які не були санкціоновані її власником, не залежно від причин або джерел виникнення таких викривлень.

Причини таких викривлень можуть бути випадковими або навмисними. Випадкові викривлення можуть бути як природними, пов'язаними з дією природних чинників, так і штучними. До числа природних чинників

відносяться атмосферні електромагнітні розряди, іскріння контактів в автомобілях, електротранспорті, недостатня надійність електронних елементів і елементів електричних ланцюгів, порушення реєструючого шару магнітних або оптичних носіїв і багато що інше. Випадкові штучні викривлення пов'язані з діяльністю людей − з випадковими помилками персоналу. Навмисні викривлення завжди пов'язані з умисними діями порушників. І ті, і інші дії мають своїм слідством викривлення того або іншого числа символів в цифровому представленні інформації, незалежно від використовуваної системи числення або форми представлення інформації і, в цьому значенні, є загрозами функціональним властивостям захищеності інформаційних ресурсів – їх цілісності і доступності. Надалі розглядаються задачі забезпечення цілісності інформаційних об'єктів в умовах природних впливів.

Наслідком природних впливів в каналах телекомунікаційних мереж (ТКМ) є зменшення співвідношення енергетик сигнал/ шум (сигнал/завада). Це відношення визначає вірність інформації, визначувану, наприклад, через ймовірність помилок двійкових символів (біт) $P_{пом}$, а також інтенсивність цих помилок.

Тому задача забезпечення цілісності і доступності інформаційних ресурсів є однією з найактуальніших при розробці і експлуатації АС і їх елементів. Ця необхідність підтверджується і вимогами щодо допустимої імовірності $P_{пом}$ помилок в повідомленнях, яку слід трактувати як вірогідність порушення цілісності інформаційних об'єктів, які обробляються (якщо передача і обробка інформації здійснюється у вигляді повідомлень). Наприклад, вона може задаватися від 10^{-4} (у задачах оперативно − виробничого планування) до 10^{-6} (у задачах бухгалтерського обліку).

Як правило, в моделях забезпечення контролю та поновлення цілісності інформаційних об'єктів до складу інформації, яка захищається, додають надмірну інформацію – ознаку цілісності або контрольну ознаку (залежно від прийнятої в задачах контролю цілісності або завадостійкого кодування термінології) − своєрідний образ, відображення цієї інформації, процедура формування якого відома, і який з дуже високою вірогідністю відповідає інформації, що захищається.

При цьому між інформацією, що захищається, і ознаками цілісності або контрольними ознаками встановлюється регулярний (функціональний) односторонній зв'язок (процедури розрахунку контрольної ознаки за початковою інформацією, що захищається, відомі, а процедури розрахунку початкової інформації по контрольних ознаках найчастіше не існує). Контроль цілісності (відсутність викривлень) зводиться при цьому до тих або інших процедур перевірки наявності вказаного регулярного (функціональної) одностороннього зв'язку між ознаками цілісності і прийнятої з каналу зв'язку (або зчитаної із запам'ятовуючого (ЗП) пристрою) інформацією.

Моделі забезпечення цілісності істотно залежать від умов їх застосування, а саме від впливу випадкових (природних) або штучних

(зловмисних) викривлень.

Характерною особливістю випадкових викривлень є те, що вони, через відсутність навмисності, порушують регулярний (функціональний) односторонній зв'язок між прийнятою (або зчитаною із ЗП) інформацією і ознаками цілісності, сформованими перед передачею (перед записом в ЗП). Тому при виявленні порушення вказаного зв'язку встановлюється факт наявності таких викривлень, а за певних умов, і їх місця і величини (характер). За відсутності порушення цього зв'язку встановлюється факт відсутності викривлень.

Характерною ж особливістю навмисних викривлень є те, що зловмисник прагне забезпечити, зімітувати наявність регулярного (функціонального) зв'язку між модифікованою їм початковою інформацією, прийнятою (або зчитаною із ЗП), і ознаками цілісності. З цією метою порушник, використовуючи знання процедур формування контрольних ознак, після необхідної для його цілей модифікації початкової інформації перед передачею одержувачу (перед записом в ЗП) забезпечує формування відповідних ознак. При успішному формуванні вказаних ознак, розкрити наявність модифікації неможливо. Для боротьби з цим власнику (або авторизованому користувачу) необхідно використовувати або секретні (невідомі потенційним порушникам) процедури формування контрольних ознак (що дуже складно забезпечити), або вводити в загальновідомі процедури формування контрольних ознак секретні параметри (ключі перетворення). Не знаючи цих секретних параметрів (ключів перетворення), порушник не зуміє забезпечити, зімітувати наявність регулярного (функціонального) зв'язку між модифікованою їм початковою інформацією, прийнятою (або зчитаною із ЗП), і ознаками цілісності.

Виділяють дві основні причини виникнення природних викривлень в процесі циркуляції інформації в мережах:

• збої в якійсь частині устаткування мережі або виникнення несприятливих об'єктивних подій в мережі (наприклад, колізій при використовуванні методу випадкового доступу в мережу). Як правило, система передачі даних готова до такого роду проявів і усуває їх за допомогою планово передбачених засобів;

• завади, викликані зовнішніми джерелами і атмосферними явищами.

Труднощі боротьби з завадами полягають в безладності, нерегулярності і в структурній схожості завад з інформаційними сигналами. Тому захист інформації від викривлень і шкідливого впливу завад має велике практичне значення і є однією з серйозних проблем сучасної теорії і техніки інформаційного обміну в каналах ТКМ.

Серед основних моделей забезпечення цілісності інформації в умовах природних дій (проблема завадостійкості) для каналів ТКМ (взагалі для мереж передачі даних) слід виділяти:

1. Збільшення вже згаданого співвідношення сигнал/завада за рахунок підвищення енергетики сигналу (велика початкова потужність, регенерація

на пунктах підсилення та ретрансляції, що вимагає значних енергетичних або матеріальних витрат;

2. Збільшення співвідношення сигнал/завада за рахунок зниження рівня завад (шумів) шляхом заміни існуючих кабельних ліній зв'язку на спеціальні з низьким рівнем власних шумів, наприклад, на оптоволоконні, що також вимагає значних матеріальних витрат, і може бути реалізованим лише в окремих випадках;

3. Забезпечення хоча б задовільної узгодженості смуги пропускання П каналу із спектром сигналу, який визначається параметрами сигналу, в першу чергу його тривалістю $\tau \approx 1/B$, де τ − тривалість сигналу, а В − технічна швидкість передачі інформації (швидкість по символьної передачі) в даному каналі. Задовільною найчастіше вважають таку узгодженість, коли $П \geq 2B$;

4. Застосування мажоритарних (групових) методів захисту, які ґрунтуються на використовуванні декількох каналів зв'язку (3...5), що є фізично (найчастіше, навіть, географічно) рознесеними, по яким передається одна і та ж інформація, або на багатократній передачі (3...5 раз) однієї і тієї ж інформації по одному каналу зв'язку. У першому випадку необхідні істотні матеріальні витрати, а в другому значно зменшується пропускна можливість каналу зв'язку (у 3...5 раз), а час затримки передавання інформаційних об'єктів може стати неприпустимо великим. З цих причин, в системах передачі даних використовування цих методів не завжди доцільне;

5. Застосування різного роду завадостійких кодів з виявленням помилок в прийнятій (зчитаній) інформації, які дозволяють реалізувати програмні, апаратурні або програмно-апаратурні засобів виявлення викривлень. Це, в свою чергу дає можливість застосування способів передачі повідомлень з різного роду зворотним зв'язком. Недоліки таких способів забезпечення цілісності зводяться до необхідності організації другого (зворотного) каналу зв'язку, тобто до істотних матеріальних витрат, а також до збільшення часу затримки передавання інформаційних об'єктів, який може бути неприпустимо великим;

6. Застосування різного роду завадостійких корегуючих кодів (ЗКК), які дозволяють реалізувати програмні, апаратурні або програмно-апаратурні засобів виявлення і усунення викривлень.

Остання із моделей забезпечення цілісності інформаційних об'єктів − із застосуванням завадостійких корегуючих кодів наразі знайшов широке застосування в стандартах радіозв'язку, стільникового зв'язку. Вона не потребує зворотного каналу і забезпечує, як правило, прийнятне значення часу затримки передавання інформаційних об'єктів. Тому, чи не єдиною проблемою в цих та інших ТКМ з використанням телефонних кабельних та радіоканалів є проблема забезпечення цілісності інформаційних об'єктів в умовах впливу навіть природних (не говорячи уже про штучні, навмисні завади) пакетних викривлень, як "коротких" (тривалістю 2...10 мс) так і особливо "довгих" (тривалістю 100…200 мс). Це є особливо актуальним і для

уже згаданих систем стільникового зв'язку. Наприклад, в стандартах CDMA базовий цифровий потік розбивається на пакети тривалістю по 20 мс и подається на згорточний кодер с половинною швидкістю [2]. При цьому тривалість пакету викривлень може бути порівняною чи, навіть, значно перевищувати тривалість інформаційного пакету, що може суттєво вплинути на результативність процедур обміну інформацією.

Як вихід із таких ситуацій може розглядатися можливість збільшення тривалості інформаційних пактів із одночасним застосуванням перемежування потрібної глибини та завадостійких корегуючих кодів, які були б спроможними забезпечити виявлення та виправлення пакетів викривлень значної тривалості. Як такі коди в статті пропонуються узагальнені завадостійкі корегуючі коди.

Остання із моделей забезпечення цілісності інформаційних об'єктів − із застосуванням завадостійких корегуючих кодів наразі знайшов широке застосування в стандартах радіозв'язку, стільникового зв'язку. Він не потребує зворотного каналу і забезпечує, як правило, прийнятне значення часу затримки передавання інформаційних об'єктів. Тому, чи не єдиною проблемою в цих та інших ТКМ з використанням телефонних кабельних та радіоканалів є проблема забезпечення цілісності інформаційних об'єктів в умовах впливу навіть природних (не говорячи уже про штучні, навмисні завади) пакетних викривлень, як "коротких" (тривалістю 2...10 мс) так і особливо "довгих" (тривалістю 100…200 мс). Це є особливо актуальним і для уже згаданих систем стільникового зв'язку. Наприклад, в стандартах CDMA базовий цифровий потік розбивається на пакети тривалістю по 20 мс и подається на згорточний кодер с половинною швидкістю [2]. При цьому тривалість пакету викривлень може бути порівняною чи, навіть, значно перевищувати тривалість інформаційного пакету, що може суттєво вплинути на результативність процедур обміну інформацією.

На закінчення слід відмітити, що як вихід із таких ситуацій може розглядатися модель із збільшенням тривалості інформаційних пакетів із одночасним застосуванням перемежування потрібної глибини та застосуванням завадостійких корегуючих кодів, які були б спроможними забезпечити виявлення та виправлення пакетів викривлень значної тривалості. До таких кодів відносяться завадостійкі узагальнені коди, розгляд яких виходить за межі даної статті.

1. НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу".
2. *Дубровский В.В.* CDMA − взгляд глазами профессионала. // mailto:v_dubrovskii@mail.ru.

Поступила 15.02.2010р.