3 Забезпечення захисту інформації в системах зв'язку. Технічні засоби системи захисту інформації

УДК 681.31

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЯХ

Микола Будько, Вячеслав Василенко
ВАТ "КП ОТІ"

Анотація: **запропоновано шляхи та механізми підвищення ефективності телекомунікаційних систем за рахунок використання в їх системах технічного захисту інформації процедур завадо- та імітостійкого корегуючого ЛУ - коду.**
Summary: **were proposed ways and mechanisms of increasing of television service systems efficacy at the expense of using procedures of interference and imitation insensitive correcting LU-code in their system of technical information protection.**
Ключові слова: **технічний захист інформації, імітостійкість,корегуючі коди.**
Key words: **technical information protection, interference insensitive, imitation insensitive, correcting codes.**

Сучасні автоматизовані системи (АС) будуються найчастіше як ієрархічні, розподілені комп'ютерні системи. При цьому задача забезпечення усіх основних функціональних властивостей захищених систем, в тому числі і цілісності, може вирішуватися як загальносистемними засобами технічного захисту інформації (ТЗІ) та її інших (ресурсів, так і засобами, які є вбудованими в елементи таких АС. Тобто можна і слід говорити про необхідність забезпечення цих функціональних властивостей по відношенню до кожного з елементів АС, в тому числі по відношенню до телекомунікаційної підсистеми АС, та застосування засобів забезпечення захисту проти загроз, в даному випадку цілісності інформації, у складі цієї підсистеми. Тому далі в статті розглядаються проблеми забезпечення цілісності інформації саме в телекомунікаційних підсистемах (ТКПС).

Сукупність загроз тій чи іншій функціональній властивості захищеної системи чи її елементам можна розглядати як їх потік, який, в свою чергу, складається з потоків штучних та природних впливів. Потік штучних впливів породжується користувачами - ненавмисними чи навмисними діями авторизованих користувачів, тобто таких, що мають дозвіл на використання певного ресурсу АС, та неавторизованих користувачів (злонавмисників, що мають за мету завдати якоїсь шкоди АС, інформації чи її власникам). Потік природних впливів виникає внаслідок недостатньої спроможності первинних технічних засобів запобігти дії таких впливів, недостатньої надійності елементів, з яких складається телекомунікаційна підсистема, порушення умов та режимів їх експлуатації, наявності впливів зовнішніх електромагнітних полів (завад) на елементи підсистеми, середовище передачі інформації та інших причин.

Таким чином, на ресурси ТКПС можуть впливати як спроби несанкціонованого доступу, при умові подолання системи управління доступом до її ресурсів, так і безпосередньо природні впливи.

При цьому слід очікувати, що в загальну інтенсивність потоку загроз для телекомунікаційних підсистем (див. рисунок 1), в яких мережа передачі даних (МПД) складається з сукупності вузлів комутації та каналів зв'язку і побудована на загальних принципах [1-3], найбільший внесок дає потік природних впливів, тобто природні впливи є найбільш імовірними. Це пов'язано, по-перше, із підкресленим уже фактом зниження інтенсивності штучних впливів за рахунок їх проріджения засобами управління доступом, а, по-друге, із значною інтенсивністю в ТКПС (принаймні в її каналах передачі даних) природних впливів. По відношенню до інформації слід говорити про те, що наслідком впливів усіх загроз є те чи інше її викривлення-порушення правильності (в термінах російської мови - *верности*) чи цілісності інформації. Топологія МПД при цьому, принаймні для проблеми, що розглядається, принципового значення не має і може бути такою, як це представлено на запозиченому з [4] рисунку 2.

Найчастіше під правильністю розуміють стійкість інформації щодо викривлень поодинокого символу, групи символів в наслідок природних впливів, а під цілісністю - видалення чи модифікація певної кількості символів чи усього повідомлення в наслідок штучних впливів). Авторами пропонується дещо змінити наведені визначення і застосувати визначення, які є близькими до розподілу способів забезпечення конфіденційності в МПД [4] за рахунок чи то канального, чи то абонентського шифрування.

При цьому пропонується розподілити взагалі єдину задачу забезпечення цілісності в ТКПС на:

1. ***Задачу забезпечення цілісності інформації в каналах (*****канальна цілісність*****)*** - задачу забезпечення правильності інформації шляхом подолання наслідків природних впливів на елементи канального обладнання;

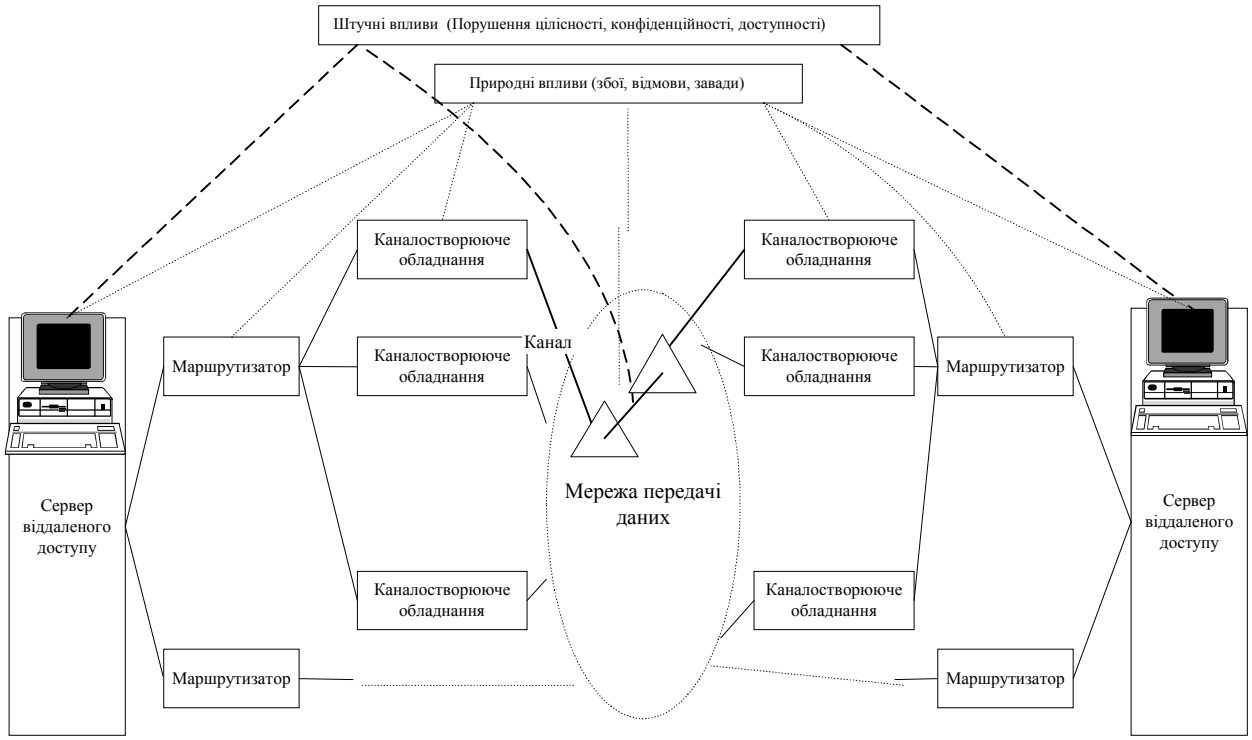

Рисунок 1 - Модель впливів на елементи ТКПС

2. ***Задачу забезпечення цілісності інформації в ТКПС (*абонентська цілісність*)*** - задачу забезпечення цілісності інформації шляхом подолання наслідків усіх штучних впливів та тих природних впливів на елементи ТКПС канального обладнання, які не усунені засобами забезпечення правильності в елементах канального обладнання.

Можливість будь-яких викривлень прийнято оцінювати через ймовірність того, що прийняті дані будуть мати помилки (викривлення), - через ймовірність викривлення повідомлення $P_п$, чи через пов'язану з нею середню ймовірність помилки символу $P_{пом}$. Ці ймовірності є одними з основних і найпоширеніших характеристик телекомунікаційних систем, які, до речі, можуть служити і характеристиками як канальної, так і абонентської цілісності інформації в цих системах. Відомо [1-3], що величина цих імовірностей визначається інтенсивністю впливів та тривалістю часового інтервалу, під час якого ці впливи діють на ресурси телекомунікаційної системи.

Слід підкреслити, що інтенсивність природних впливів, яка визначається, в основному, співвідношенням сигнал/ шум (сигнал/ завада) в каналі, є настільки значною, що лише за їх рахунок, без урахування можливостей злонавмисників по створенню загроз, наприклад різного роду завад, середня ймовірність помилки символу $P_{пом}$ (при, хоча б задовільній 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 в даному каналі. Задовільною найчастіше вважають таку узгодженість, коли $П \approx 2B$) для телефонних кабельних каналів ТКПС складає [1-3] від 2×10^{-3} до $1{,}29\times10^{-4}$; для радіорелейних телефонних – від $2{,}66\times10^{-4}$ до $7{,}3\times10^{-4}$ відповідно. Відомо також, що з часом такі помилки групуються в пакунки двох видів: "короткі" – тривалістю 2…10 мс та "довгі" – помилок зосереджено в "довгих" групах (75 - 90%) [2].

Порушення правильності та цілісності прийнятих даних призводить до різноманітних негативних наслідків, що потребує забезпечення правильності та цілісності інформації, яка досягається захистом від будь-яких її викривлень. Ця необхідність підтверджується і вимогами щодо припустимої ймовірності помилок в повідомленнях $P_п$, що обробляються. Наприклад, вона може задаватися [1-4] від 10^{-4} (в завданнях оперативно-виробничого планування) до 10^{-6} (в завданнях бухгалтерського обліку, де передача та обробка інформації здійснюється у вигляді повідомлень). Використовуючи зв'язок поміж потрібною вірністю інформації $P_п$ та середньою імовірністю помилки символу $P_{пом}$ [2] ($P_{пом} = P_п/n$, де n – розрядність повідомлення), отримаємо, що середня припустима ймовірність помилки символу, у випадку відсутності засобів захисту від помилок, складе значення від 10^{-8} до 10^{-6} – при обробці повідомлень з довжиною 100 символів, та від 10^{-9} до 10^{-7} – при обробці повідомлень з довжиною 1000 символів. Слід підкреслити, що ці вимоги є не найвищими. Наприклад, у системах з криптографічним захистом, наслідки викривлень є рівноцінними втраті повідомлення, не говорячи уже про втрати, що пов'язані з навмисним викривленням фінансової інформації, навмисним викривленням команд,

розпоряджень та т.п. Останнє іноді призводить до постановки задачі передачі інформації з абсолютною вірністю.

При цьому стає зрозумілим, що задачі забезпечення загальної (як канальної, так і абонентської) цілісності інформації є однією з основних задач системи ТЗІ в телекомунікаційних підсистемах.

Задача забезпечення канальної цілісності інформації в умовах природних впливів (проблема завадостійкості) для ТКПС (взагалі для мереж передачі даних) є давно відомою і дуже важливою [1, 2] і вирішується, як уже підкреслено, на канальному рівні шляхом підвищення якості та умов передавання сигналу. Основними напрямками цього є:

1. Збільшення уже згаданого співвідношення сигнал/ завада за рахунок підвищення енергетики сигналу (велика початкова потужність, регенерація на пунктах як з обслуговуванням, так і без обслуговування та т.п.), що потребує значних енергетичних чи матеріальних витрат;

2. Збільшення співвідношення сигнал/завада за рахунок зниження рівня завад (шумів) шляхом використання спеціальних кабельних ліній зв'язку, в тому числі оптоволоконних, що потребує значних матеріальних витрат;

3. Застосування мажоритарних методів захисту, що базуються на використанні декількох фізично (найчастіше, навіть, географічно) рознесених каналів зв'язку (3…5), по яких передається одна і та ж сама інформація, або на багатократному передаванні (3…5 разів) однієї і тієї ж інформації по одному каналу зв'язку. В першому випадку необхідні суттєві матеріальні витрати, а в другому – значно зменшується перепускна спроможність каналу зв'язку (у 3…5 разів). З цих причин, в системах передачі даних (СПД) використання цих методів є не завжди доцільним;

4. Застосування програмних, апаратурних чи програмно-апаратурних засобів виявлення та усунення викривлень - застосування каналів із різного роду зворотним зв'язком (інформаційним - деякий аналог мажоритарного методу з на багатократним передаванням інформації та прийманням рішення щодо правильності передачі на боці передавача, або з зворотним вирішуючим зв'язком (ЗВЗ) - при необхідності багатократному передаванню з прийманням рішення щодо правильності передачі на боці приймача) та каналів з завадостійкими корегуючими кодами (ЗКК)). Для організації такого зв'язку широко застосовуються сучасні модеми – елементи каналостворюючого обладнання (див. рисунок 1).

5. Методи з застосуванням зворотного зв'язку завжди потребують наявності другого, тим чи іншим чином організованого, каналу зв'язку, що звичайно збільшує матеріальні витрати. Крім того, проведені авторами дослідження [4] показують, що для каналів із значною інтенсивністю завад більшу ефективність (окрім зменшення матеріальних витрат) мають канали з використанням завадостійких корегуючих кодів. Тому доцільно говорити про доречність вибору, як найбільш ефективних, з багатьох точок погляду, каналів з використанням

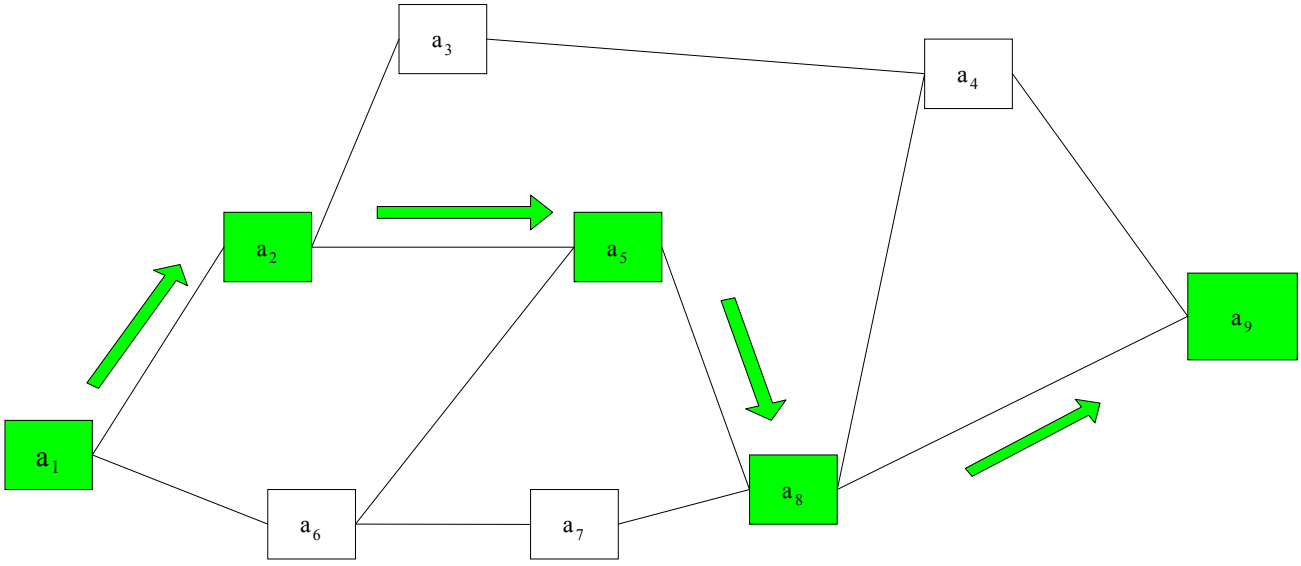

Рисунок 2 - Приклад топології мережі передачі даних

завадостійких корегуючих кодів. Як напрямок в цій же роботі розглянуто використання адаптивних комбінованих систем передачі даних, в яких залежно від інтенсивності завад використовується режим роботи із ЗВЗ, або із ЗКК. Будемо вважати, що задача забезпечення канальної цілісності вирішена і відповідні засоби забезпечують захист від природних впливів з ймовірністю $p_{кц}$.

Але реалізація розглянутих напрямків забезпечення канальної цілісності (правильності) не забезпечує вирішення другої із задач – задачі забезпечення абонентської цілісності інформації. Дійсно, достатньо в каналі

зв'язку між абонентами (між модемами з боку передавача та приймача інформації) підключити ще одну пару модем - модем (а це, безумовно є лише одним із можливих способів штучного впливу із їх множини), в якій застосовуються ті ж самі методи забезпечення правильності, щоб забезпечити неконтрольоване методами підвищення правильності порушення як конфіденційності, так і, особливо, цілісності інформації, а також доступності ресурсів ТКПС. Цьому, безумовно, сприяє проходження ліній зв'язку, в яких організуються потрібні канали, як правило, за межами контролюємої території. Підключення такої пари модемів гарантує формування контрольних ознак відсутності викривлень інформації незалежно від того, наскільки є модифікованою інформація перед другим модемом згаданої пари. Тобто можливим є не тільки модифікація інформації (що є метою злонавмисника при порушенні її цілісності), а і вилучення повідомлень чи, навпаки, генерація будь-якого числа додаткових (несправжніх) повідомлень з метою, наприклад, перевантаження системи передачі даних і блокування, за рахунок цього, процесу обміну справжніми повідомленнями - порушення доступності ТКПС. Зрозуміло, що це вимагає застосування окремих способів забезпечення і конфіденційності інформації (застосування різного роду криптографічних перетворень), але розгляд засобів забезпечення конфіденційності інформації (частково вони викладені в [5]) виходить за межі поставленої в статті мети.

Таким чином, з викладеного витікає необхідність окрім задачі забезпечення канальної цілісності (правильності обміну) інформацією в ТКПС обов'язкового вирішення і задачі забезпечення абонентської цілісності інформації. Модель взаємодії засобів в процесі ТЗІ в телекомунікаційних системах, на думку авторів з урахуванням викладених нижче міркувань, можна уявити так, як це представлено на рисунку 3. Зрозуміло, що вирішення задачі забезпечення абонентської цілісності інформації доцільно здійснювати в ланці сервер - сервер (рис.1), причому шляхом застосування окремих, відмінних від канальних, методів, механізмів, засобів.

З моделі взаємодії засобів в процесі ТЗІ (рисунок 3) випливає, що штучні впливи на абонентському рівні з інтенсивністю $\lambda_{ша}$ дають наслідки лише при умові подолання ними системи управління доступом

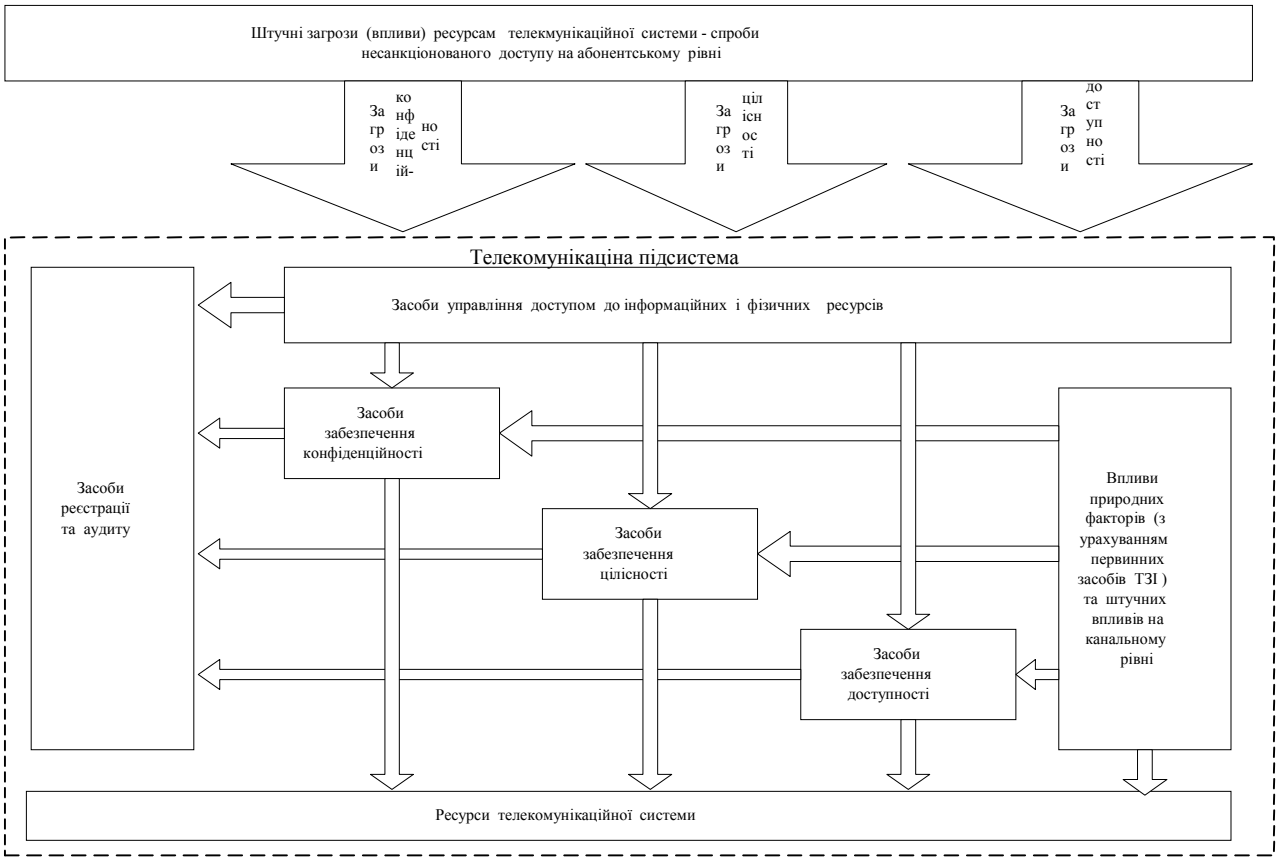

Рисунок 3 - Модель взаємодії засобів в процесі технічного захисту інформації

до

інформаційних та фізичних ресурсів, тобто тільки в разі їх невиявлення засобами управління доступом. Тоді інтенсивність таких штучних загроз, які впливають на засоби забезпечення відповідної функціональної послуги ТКПС, зменшується (за рахунок проріджєння, фільтрації штучних загроз засобами управління доступом) до $\lambda_{ша}(1-p_д)$, де $p_д$ - ймовірність запобігання впливу загроз системою управління доступом. Штучні ж впливи на

канальному рівні, у багатьох випадках, протидії не мають, тому впливають на відповідні ресурси ТКПС з інтенсивністю $\lambda_{шк}$. Природні впливи, також впливають на ресурси ТКПС, але лише в разі неспроможності виявити та усунути їх засобами канального забезпечення цілісності. Тобто, інтенсивність природних загроз, які впливають на засоби забезпечення відповідної функціональної послуги ТКПС, також зменшується (за рахунок проріджєння, фільтрації природних загроз канальними засобами) до $\lambda(1-p_{кц})$, де $p_{кц}$ - ймовірність виявлення та усунення загроз засобами канального забезпечення цілісності. Тоді результуюча інтенсивність загроз $\lambda_р$ може бути розрахована як

$$\lambda_р = \lambda_ш(1- p_д)+ \lambda_{шк} +\lambda(1- p_{кц}),$$

а **з урахуванням застосування відповідних засобів захисту - засобів забезпечення цілісності ресурсів ТКПС (на абонентському рівні), які дозволяють виявити (і, зрозуміло, усунути) загрозу з імовірністю $p_в$**, результуюча інтенсивність загроз неусунутих системою ТЗІ $\lambda_н$ може бути розрахованою як

$$\lambda_н = \lambda_р \cdot(1-p_в)= (\lambda_ш(1- p_д))+ \lambda_{шк} +\lambda(1- p_{кц}))\cdot(1-p_в). \qquad (1)$$

Звернемо увагу на те, що найбільший вплив на ресурси ТКПС, як видно з виразу (1), слід очікувати від штучних впливів на канальному рівні, оскільки вони не зменшуються (не проріджуються) ніякими засобами, окрім засобів забезпечення цілісності ресурсів ТКПС на абонентському рівні та особливу необхідність при цьому збільшення ймовірності $p_в$.

Нехай система ТЗІ здійснює свої функції шляхом періодичного (з періодом T_k) контролю цілісності, що формулюється як її спроможність надавати власну функціональну послугу - *спостереженість* шляхом застосування відповідних засобів забезпечення спостереженості (ЗЗС). Будемо вважати, що такий контроль потребує ΔT_{ki} одиниць часу. Періодичність контролю визначається власниками ресурсів, які захищаються, чи технічними характеристиками ТКПС (наприклад, часом передачі одного повідомлення, чи тривалістю одного сеансу обміну), чи якимось нормативними документами (наприклад, планом ТЗІ, в якому сформульована політика безпеки в даній АС взагалі, чи ТКПС, зокрема). Під час контролю здійснюється перевірка наявності порушень цілісності, її поновлення, необхідне переналагодження параметрів засобу забезпечення цілісності (наприклад, зміна ідентифікаторів, паролів, ключових наборів, за допомогою яких забезпечується управління доступом, необхідні криптографічна та імітостійкість та т.п.). Тривалість контролю залежить від способу його реалізації (наприклад, контроль цілісності може відбуватися шляхом використання спеціальних швидкодіючих процедур (алгоритмів) перевірки цілісності [3] та т.п.). Порушення , які виявлені під час контролю, усуваються. Для цього також можливе застосування різноманітних засобів - тих же швидкодіючих процедур (алгоритмів) поновлення цілісності та інше. Зрозуміло, що від якості застосованих засобів контролю та усунення порушень (поновлення роботоспроможності) залежать тривалість відповідних процедур та ймовірність правільного вирішення цих завдань.

Тривалість впливу загрози $T_з$ є випадковою величиною з часового інтервалу $(0; (T_k-\Delta T_k))$, тобто може бути різною - від нуля до $(T_k-\Delta T_k)$ одиниць часу, При чьому, T_k - тривалість часу між двома суміжними перевірками роботоспроможності ТКПС (період контролю) засобу захисту від загроз, а ΔT_k - тривалість контролю та поновлення цілісності (вважаємо, що під час контролю система є нероботоспроможною). Можна припустити, що $T_з = (T_k-\Delta T_k)$, якщо порушнику вдалося реалізувати загрозу одразу ж після закінчення процедури відповідного контролю, та $T_з = 0$ у випадку спроби реалізації загрози безпосередньо перед її початком. Найгірші умови створюються при $T_з = (T_k-\Delta T_k)$, тому при розробці системи ТЗІ доцільно орієнтуватися саме на цю тривалість реалізації загрози.

Нехай потік загроз, що впливають на інформацію ТКПС, є найпростішим. Тоді ймовірність впливу на ресурси хоча б однієї загрози, тобто ймовірність хоча б одного викривлення інформації (помилки символу) за рахунок впливу на інтервалі $(T_к- \Delta T_к)$ будь-якої загрози при умові застосування системи ТЗІ, тобто коли система захисту не виявила і, зрозуміло, не протидіяла цій загрозі, дорівнює

$$p_з= 1- \exp\{-(T_к- \Delta T_к)\cdot\lambda_н\}=1-\exp\{-(T_к- \Delta T_к)\cdot (\lambda_ш(1- p_д))+ \lambda_{шк} +\lambda(1- p_{кц}))\cdot(1-p_в)\}. \qquad (2)$$

Зрозуміло, що для підвищення ефективності системи ТЗІ в ТКПС слід здійснювати заходи по зменшенню величини ймовірності $p_з$ впливу будь-якої загрози на інформацію чи інші ресурси ТКПС. Для цього, як видно з виразу (2) необхідно застосовувати швидкодіючі процедури контролю цілісності (з малою тривалістю - $\Delta T_к$), збільшувати $p_д$ - ймовірність запобігання впливу загроз системою управління доступом, $p_{кц}$ - ймовірність виявлення та усунення загроз засобами канального забезпечення цілісності та $p_в$ - ймовірність виявлення і усунення загрози засобами забезпечення цілісності ресурсів ТКПС на абонентському рівні (на збільшенні останньої ймовірності уже наголошено раніше).

При аналізі шляхів збільшення величини $p_в$ виявлення і усунення загрози засобами забезпечення цілісності ресурсів ТКПС слід підкреслити, що ця ймовірність є ймовірністю складної події, яка складається з події виявлення порушення абонентської цілісності та події з її усунення. При цьому **основною задачею засобів контролю цілісності** інформаційних ресурсів є забезпечення такого стану системи, коли **унеможливлюється приховування факту будь-якої** несанкціонованої **модифікації** захищеної інформації (вставки, вилучення, підміна та т.п.). З цією метою до складу інформації, що захищається, включають надлишкову інформацію -

своєрідний образ, відображення цієї інформації, процедура формування якого є відомою лише власнику інформації та авторизованим користувачам. Тобто образи, що формуються, повинні мати певну стійкість щодо підробок - імітостійкість. До цих механізмів захисту відносяться такі відомі механізми захисту [6] з використанням: сигнатур важливих об'єктів, хеш–функцій важливих об'єктів, процедур завадостійкого кодування для забезпечення цілісності архівної інформації в тому числі і резервних копій програмних засобів та баз даних.

На цей час для контролю цілісності інформації в Україні міждержавним стандартом (ГОСТ 34.311 – 95) передбачено застосування процедури формування хеш–функції, імітостійкість яких забезпечується використанням процедур криптографічного перетворення з використанням стандарту - ГОСТ 28147-89. При цьому відомі механізми захисту з використанням сигнатур чи хеш–функцій важливих об'єктів грунтуються на застосуванні швидкодіючих процедур виявлення порушення цілісності та подальшому поновленні викривленої інформації за рахунок повторної передачі непошкодженої інформації, що є своєрідним аналогом систем ЗВЗ і потребує [4] значних часових витрат.

З розглянутого можна зробити висновок про те, що **потрібним є не тільки забезпечення високого значення ймовірності виявлення і усунення загрози засобами забезпечення цілісності ресурсів ТКПС, а і підвищення оперативності процесів забезпечення цілісності, що, в свою чергу , є можливим за рахунок розробки і застосування погоджених між собою швидкодіючих процедур як виявлення порушення цілісності інформації, так і її поновлення.** Такими процедурами є процедури, що грунтуються на застосуванні корегуючих завадостійких кодів.

Однак відомі завадостійкі коди не в змозі забезпечити головну із необхідних при цьому властивостей - імітостійкість, в наслідок чого їх використання в механізмах контролю цілісності є неможливим. **На відміну від цього, завадостійкий код умовних лишків (лишків умовних код – ЛУ – код), який пропонується авторами [6], забезпечує одночасно контроль та поновлення цілісності і потрібний рівень імітостійкості.**

В цьому коді, як і в інших, для контролю цілісності, а в подальшому і поновлення цілісності базових кодових слів, з яких в подальшому складається повідомлення чи узагальнене кодове слово, потрібно мати додаткові (надлишкові) символи, які зберігають в собі в специфічному вигляді – у вигляді чи контрольної ознаки (в термінах завадостійкого кодування), чи хеш–функції (в термінах криптографічних перетворень) образ - відображення інформації, яка контролюється, за її станом на час формування цього образу (а не після порушення цілісності!).

В загальному випадку базовим кодовим словом називається частка повідомлення (узагальненого кодового слова), довжина якого в символах, наприклад в байтах, задовольняє рівнянню

$$N = n1 \cdot \lambda ,$$

де: N-число байтів в повідомленні (узагальненому кодовому слові), яка визначається відповідними протоколами обміну в даній ТКПС; λ –число базових кодових слів (глибина перемежування) в повідомленні; n1 – число байтів в базовому кодовому слові (довжина базового кодового слова).

Контрольна ознака H кожного з базових кодових слів при застосуванні процедур ЛУ - коду формується як s - байтове двійкове число[6].Після формування контрольної ознаки її значення для кожного з базових кодових слів записується чи після інформаційних наборів, чи в іншому місці файлу, який контролюється, чи в окремому файлі та зберігається для наступного контролю цілісності цих же базових кодових слів. Контрольна ознака повідомлення формується як конкатенація контрольних ознак усіх базових кодових слів.

Примітка 1. **Під конкатенацією** двох хеш–функцій (символів) розуміється слово, довжина якого в бітах (байтах) дорівнює сумі чисел біт (байтів) кожної з хеш–функцій (кожного з символів). При цьому ліва половина даного нового слова є першою хеш–функцією (словом), а права – другою хеш–функцією (словом).

У випадку, коли кількість базових кодових слів у повідомленні є величиною не цілою, меншою ніж λ, або коли довжина повідомлення є невеликою, за контрольні ознаки відсутніх базових кодових слів приймаються нульові контрольні ознаки, тобто контрольні ознаки, в яких кожен з s байтів, що входять до їх складу, є арифметичним нулем.

При організації контролю цілісності також використовуються властивості ЛУ – коду.

Поновлення цілісності інформації при контролі цілісності з використанням властивостей ЛУ – коду не потребує використання резервних копій, а є суто розрахунковим процесом з повним використанням інформації, яка зосереджена в надлишкових символах – в контрольних ознаках кожного з базових кодових слів.

Під імітостійкістю запропонованих механізмів контролю цілісності інформації розуміється здатність бути нерозкриваємими використовуємих ключових наборів (наборів p_i) а також здатність не допускати приховування навмисних порушень цілісності інформації (імітацію відсутності порушень) з боку неавторизованих користувачів (злонавмисників).

При цьому стійкість механізмів контролю цілісності інформації визначається стійкістю обчислень хеш-функцій, яка залежить від довжини вибраних ключів криптозахисту а також від статистичної пов'язаності початкового тексту (інформаційного блоку) з його криптографічним відображенням.

Під ключем криптозахисту в запропонованих механізмах контролю цілісності інформації розуміється набір

чисел, які є чи номерами основ (i), чи власне основами (p_i). Основи в першому випадку вибираються за їх номерами з набору простих чисел. При цьому формується ключовий набір, інакше, таким ключовим набором є набір, який задано у вигляді сукупності основ (p_i). Кількість цих основ визначає згадану вище довжину ключового набору.

Процес обчислення хеш–функцій за відомим алгоритмом, але за невідомим ключем чи ключовим набором **є по суті криптографічним перетворенням** інформації, цілісність якої повинна контролюватися, в хеш-функцію. При цьому неавторизований користувач, не знаючи ключового набору, не має змоги замаскувати порушення цілісності інформації шляхом формування такої хеш–функції, яка б приховувала це порушення.

Примітка 2. Звернемо увагу на те, що в запропонованих механізмах контролю цілісності інформації доступною для аналізу неавторизованими користувачами є лише частка інформації – хеш–функція та відповідна частина (при n1=32, s=3 це близько 8%) ключового набору для їх формування (основи для формування надлишкової інформації - хеш-функції). Основна ж частина (для тих же умов - близько 92%) ключового набору є недоступною для аналізу, оскільки не є представленою в явному вигляді в результаті перетворення інформації – в хеш–функціях.

Тобто суттєвою перевагою, відмінністю цього механізму контролю цілісності інформації є прихованість ключа чи результатів перетворення інформації у відповідності з цим ключем. Це пов'язане з тим, що хеш–функції, що формуються, навіть найпростіші, є відображенням результатів перетворення інформації лише за незначною кількістю елементів ключа. Така особливість є не чим іншим, як додатковою можливістю підвищення імітостійкості запропонованих механізмів контролю цілісності інформації за рахунок відсутності безпосереднього статистичного зв'язку між первинним текстом та його хеш–функцією, та дає змогу говорити про відсутність можливості чи значне утруднення з'ясування такої статистичної пов'язаності початкового тексту (інформаційного блоку) з його криптографічним відображенням – хеш–функцією. Останнє, в свою чергу, дозволяє говорити про можливість визначення ключа тільки шляхом прямого перебору та визначати стійкість запропонованого механізму контролю цілісності інформації лише через кількість варіантів ключів.

В таблиці 1 для порівняння наведено кількість варіантів ключів для відомих механізмів формування цифрового підпису (за стандартом ГОСТ 34.310 – 94), та функції хешування (за стандартом ГОСТ 34.311-95), а також запропонованого механізму [6]. До речі при застосуванні цього механізму лише для контролю цілісності можна суттєво зменшити об'єм надлишкової інформації та спростити саму процедуру формування хеш-функції. Це пов'язане з тим, що сформована за розглянутою процедурою надлишкова сукупність контрольних ознак містить в собі інформацію, потрібну для визначення в подальшому наявності викривлення, його місця та величини. При контролі ж лише цілісності достатньо мати інформацію, потрібну для визначення в подальшому тільки наявності викривлення. Тому під час формування хеш-функції можна поруч з конкатенацією використовувати і операції порозрядного додавання за модулем 2. За рахунок цього довжина хеш-функції (об'єм надлишкової інформації) легко доводиться до довжини, визначеної міждержавним стандартом ГОСТ 34.311-95.

Як видно з таблиці, запропонований механізм забезпечує кількість варіантів ключів, яка суттєво перевищує кількість варіантів ключів відомих механізмів, та має, відповідно, значно вищу імітостійкість. У наведених прикладах кількість варіантів ключів задовольняє вимогам навіть гарантованого криптозахисту.

Таблиця 1

Довжина ключа (байти)	Механізми формування хеш–функцій для контролю цілісності інформації				
	ГОСТ 34.310 – 94	ГОСТ 28147-89	ЛУ - код		
			n1=28, s=4	n1=29, s=3	n1=32, s=4
32	-	10^{76}	$>3\cdot10^{76}$	$>10^{76}$	$>10^{76}$
64	$9{,}45\cdot10^{65}$	-	$>10^{135}$	$>10^{136}$	$>10^{136}$
128	$9{,}45\cdot10^{156}$	-	$>10^{260}$	$>10^{260}$	$>10^{260}$

Примітка 3. Для другої та третьої колонок використані дані Інституту Інформаційних Технологій Харківського технічного університету радіоелектроніки (в другій колонці, виходячи з обсягу обчислень в $3\cdot10^5$ та $3\cdot10^{12}$ міпсороків відповідно). В шостій колонці наведено дані для довжини інформаційної частки базового кодового слова в 32 байти та довжині надлишкової частки базового кодового слова в 4 байти.

Цей механізм дозволяє виявити порушення цілісності інформації в межах *кожного з узагальнених кодових слів* та виправити виявлені в ньому викривлення, довжина яких B_B може бути (при їх довільному розташуванні в межах узагальненого кодового слова) від одного до

$$B_B=[(\lambda-1)\cdot b_c+1]$$

двійкових символів (біт), де b_c- довжина символів в інформації, що контролюється, в бітах, а λ - глибина перемежування (кількість базових кодових слів в одному узагальненому). Тобто найбільш можлива довжина

виправляємих довільно розташованих в межах узагальненого кодового слова викривлень дорівнює (λ-1) символів.

Таким чином, запропоновані методи дозволяють забезпечити різні, в залежності від умов застосування, процедури контролю чи контролю та оперативного поновлення цілісності інформації в ТКПС при її несанкціонованих порушеннях з забезпеченням високої імітостійкості.

При організації процесів обміну інформацією слід врахувати наступне:

1. Методи контролю цілісності інформації, з їх вище визначеними особливостями, можуть бути легко пристосованими для організації обміну без використання механізмів зворотного вирішуючого зв'язку, що, як відомо [4], призводить до підвищення швидкості обміну (довжина блоку повинна відповідати довжині повідомлення, прийнятій у відповідному протоколі. Це просто реалізується, наприклад, в протоколі X.25).
2. Контроль цілісності інформації в блоках, довжина яких перевищує довжину повідомлення (наприклад, контроль у файлах, які передаються через ТКПС), дозволяє застосовувати принципи каскадних кодів, та забезпечувати цілісність в умовах впливу чи то завад великої тривалості (кількість викривлень перевищує корегуючі властивості внутрішнього коду), чи то тривалих (в тому ж розумінні) завмирань сигналів.
3. Оскільки використання ЛУ-коду дозволяє виявляти та виправляти викривлення, обумовлені будь-якими впливами, в тому числі і впливами на канальному рівні, то принципово можливим є використання модемів з найпростішими функціями, принаймні без використання функцій виявлення в узагальненому кодовому слові місця викривлення та його виправлення, що, на думку авторів, дозволить зменшити вартість ТКПС та підвищити швидкість обміну.

Слід, крім того, звернути увагу і на те, що обчислення контрольних ознак за запропонованими методами має усі ознаки, необхідні для деяких видів *цифрового підпису*, а отже можуть в певних випадках виконувати його функції.

Література: Игнатов В.А. Теория информации и передачи сигналов. – М.: Сов. радио, 1979. – 280 с. 2. Хетагуров Д.А., Руднев Ю.П. Повышение надежности цифровых устройств методами избыточного кодирования. – М.: "Энергия", 1974. – 290 с. 3. Мамиконов А.Г. и др. Достоверность и резервирование информации в АСУ. – М.: Энергоиздат, 1986. – 304 с. 4. Бойченко А.В. Про один алгоритм захисту інформаційного обміну в комп'ютерних мережах //Реєстрація, зберігання і обробка даних. - 1999. - № 1, том 1. с. 92 - 95. 5. Бунин С.Г., Василенко В.С. Сравнительная оценка СПД с решающей обратной связью и с использованием корректирующих кодов // УСиМ. – 1992. – № 9/10. – С.30 – 35. 6. Василенко В.С., Короленко М.П. Целостность информации в автоматизированных системах // Корпоративные системы. 1999.-№ 3.-с. 52-57.

УДК 681.31

МЕХАНІЗМИ КОНТРОЛЮ ЦІЛІСНОСТІ ІНФОРМАЦІЇ ТА ЇЇ ПОНОВЛЕННЯ

Василь Василенко, Михайло Короленко
ВАТ "КП ОТІ"

Анотація: **В статті запропоновано застосування для задач контролю та поновлення цілісності інформаційних наборів процедур завадостійкого корегуючого коду умовних лишків (ЛУ - КОДУ), які при високій імітостійкості хеш-функцій, які формуються для цього, забезпечують можливість більш оперативного поновлення інформації, цілісність якої є порушеною.**

Summari: **The article presents the application of the noise-immune correcting conditional residue code (CR-code) procedures, which in case of a high imitation resistance of the formed hash functions provide the possibility for the prompt recovery of the corrupted data integrity, to the tasks of data sets integrity control and recovery.**

Ключові слова: **цілісність інформації, контроль, поновлення, імітостійкість, завадостійкий корегуючий код.**
Key words: **data integrity, control, recovery, imitation resistance, noise-immune correcting code.**

Цілісність є однією з основних функціональних властивостей захищених систем [1-4], забезпечення якої дозволяє з певною гарантією говорити про можливість викрити чи запобігти спробам будь-якої несанкціонованої модифікації чи знищення програмних засобів, інформації та інших ресурсів комп'ютерних систем.

Як відомо, цілісність інформації забезпечується або механізмами розмежування доступу, або механізмами контролю цілісності інформації, або їх сукупністю.