УДК 681.3

О. Я. Матов[1], В. С. Василенко[2], О. К. Юдін[2]
[1]Інститут проблем реєстрації інформації НАН України
вул. М. Шпака, 2, 03113 Київ, Україна
[2]Національний авіаційний університет
вул. Космонавта Комарова, 1, 03058 Київ, Україна

Цілісність інформації в багатофазних системах захисту телекомунікаційних мереж

Запропоновано підхід щодо визначення характеристик цілісності інформаційних об'єктів як для багатофазних (багаторівневих) телекомунікаційних систем у цілому, так і для їхніх окремих рівнів (фаз).

***Ключові слова**: завада, інформаційний обмін, повідомлення, протоколи обміну, телекомунікаційна система, цілісність інформації.*

Вступ

Під цілісністю, як однією з функціональних властивостей захищеності інформації в телекомунікаційній мережі (ТКМ), розглядається [1−3] властивість інформації, яка полягає в тому, що інформація не може бути модифікованою неавторизованим користувачем або процесом. У свою чергу, під модифікацією розуміється зміна користувачем або процесом інформації, що міститься в об'єкті. Зрозуміло, що зміна інформації може здійснюватися внаслідок тих чи інших впливів, які можуть призвести до несанкціонованого авторизованим користувачем викривлення інформаційного об'єкта, чи будь-якої його частини, незалежно від джерел, чи причин виникнення цих впливів.

Викривлення інформації можливі на будь-якому етапі її циркуляції в телекомунікаційних та обчислювальних мережах: при зберіганні, передачі або обробці. Причини таких викривлень можуть бути випадковими або навмисними (умисними). У свою чергу, випадкові викривлення можуть бути як природними, пов'язаними з дією природних чинників, так і штучними. До числа природних чинників відносяться космічні та теплові шуми, атмосферні електромагнітні розряди, іскріння контактів в автомобілях, електротранспорті, недостатня надійність електронних елементів і елементів електричних ланцюгів, порушення реєструвального шару магнітних, або оптичних носіїв тощо. Випадкові штучні викривлення пов'язані з діяльністю людей, тобто з випадковими помилками персоналу. Навмисні

викривлення завжди пов'язані з умисними діями порушників. Прикладами таких умисних дій можуть бути завади в середовищі розповсюдження радіо- чи електричних сигналів.

Використання викривленої інформації чревате наслідками (часто надзвичайно важкими) для власників або користувачів цієї інформації. Тому задача забезпечення цілісності інформаційних ресурсів є однією з найактуальніших при розробці й експлуатації ТКМ і їхніх елементів. Така задача покладається на низку заходів, методів, механізмів та протоколів, які в сукупності створюють систему захисту інформації певної ТКМ. Система захисту інформації забезпечує цілісність інформації, якщо вона зберігається або передається своєчасно (із мінімальним часом затримки повідомлень), достовірною й повною, тобто захищеною від ненавмисних і зловмисних викривлень. Дана стаття як раз і призначена для розгляду проблематики, пов'язаної з оцінкою здатності системи захисту забезпечити цілісність інформаційних ресурсів ТКМ.

Боротьба з викривленнями інформаційних об'єктів, що виникають, ведеться на різних рівнях (в основному на перших чотирьох) семирівневої моделі взаємодії відкритих систем (ВВС). Нижче в таблиці наведено спробу класифікації окремих типів загроз та способів їхньої нейтралізації для перших чотирьох рівнів моделі ВВС. Звернемо увагу, що наведені в таблиці приклади не претендують на абсолютну повноту, а є, безумовно, лише малою часткою можливих загроз (навмисних дій) з їхньої множини (їхній повний аналіз виходить за межі статті).

На *фізичному рівні* цієї моделі (в середовищі розповсюдження сигналів) загрози створюються як штучними впливами (завадами), так і природними чинниками — шумами. Наслідком штучних впливів у ТКМ є збільшення інтегральної потужності суміші завада + шум $U^2_{з.еф}$, а отже, і спектральної щільності потужності цієї суміші $N_з = U^2_{з.еф}/\Delta F$, де ΔF — смуга пропускання приймальних пристроїв відповідних модемів (елементів апаратури передачі даних). Це, у свою чергу, може призводити до зменшення співвідношення $h^2 = E_c / N_з$ сигнал/завада (сигнал/шум), а отже, до збільшення ймовірності викривлень двійкових символів (біт) $P_{пом}$ та інтенсивності цих викривлень (див. нижче вирази (2), (3)).

Викривлення символів інформаційних кадрів (пакетів, вікон, комірок або узагальнених кодових слів) внаслідок розглянутих впливів утворюють деякий потік із загальною інтенсивністю λ_1. Цей потік можна розглядати як такий, що складається з потоку викривлень під впливом природних чинників з інтенсивністю $\lambda_{п1}$ та потоку викривлень під впливом шумів (завад) з інтенсивністю $\lambda_{ш1}$ так, що $\lambda_1 = \lambda_{п1} + \lambda_{ш1}$.

На *канальному рівні* ТКМ сумарний потік впливів (природних та штучних) складається з потоку викривлень, що не усунені на фізичному рівні λ_1, і штучних викривлень, що сформовані на канальному рівні внаслідок перехоплення інформації канального рівня з наступною її модифікацією та генерацією несправжніх інформаційних об'єктів.

Найбільш поширені загрози та способи їхньої нейтралізації в ТКМ

№ з/п	Рівень моделі ВВС	Загрози цілісності	Способи захисту від загроз
1.	Фізичний	Завади (природні — шуми та штучні) у середовищі розповсюдження сигналу, наслідком чого є викривлення сигналів для перенесення інформаційних символів.	1. Забезпечення потрібного співвідношення сигнал/завада. 2. Використання ефективних методів модуляції сигналів. 3. Управління шириною смуги пропускання та ін.
2.	Канальний	1. Викривлення символів інформаційних кадрів у наслідок викривлення сигналів на фізичному рівні. 2. Перехоплення, модифікація, генерація несправжніх інформаційних об'єктів.	1. Використання групових методів захисту. 2. Застосування завадостійких кодів в модемах (апаратурі передачі даних та відповідних протоколах).
3.	Мережний	1. Завади (природні та штучні викривлення) на рівні окремих символів інформаційних кадрів, блоків, пакетів, комірок, вікон. 2. Створення та генерація несправжніх мережних об'єктів та запитів, перехоплення, модифікація інформаційних об'єктів.	1. Використання протоколів мережного рівня з виявленням із виправленням викривлень. 2. Управління доступом на мережному рівні (ідентифікація, автентифікація мережних та інформаційних об'єктів), управління маршрутизацією інформаційних об'єктів.
4.	Транспортний та сеансовий	Завади (природні та штучні викривлення) та дублювання на рівні інформаційних кадрів, блоків, пакетів, комірок, вікон	Протоколи обміну транспортного рівня із контролем цілісності повідомлень та відсутності дублювання кадрів
5.	Представницький, прикладний	Підміна, модифікація інформаційних об'єктів та генерація несправжніх інформаційних об'єктів, створення несправжніх мережних об'єктів.	Використанням кодів справжності, кодів перевірки достовірності даних (MAC — Message Autentification Code) і цифрового підпису важливих об'єктів, надання прав доступу щодо читання та модифікації об'єктів.

Таке перехоплення може бути здійснене шляхом гальванічного чи індукційного підключення до кабельних мереж, аж до врізання в кабельну мережу пари модем–модем, а генерація несправжніх інформаційних об'єктів — шляхом використання згаданої пари модем–модем, гальванічного чи індукційного нав'язування та ін. Інтенсивність таких впливів може бути описаною величиною $\lambda_{ш2}$.

На мережному рівні до викривлень, які пропущені засобами захисту попередніх рівнів, додаються зловмисні впливи $\lambda_{ш3}$, які можуть бути пов'язані з перехопленням інформаційних об'єктів з їхньою наступною модифікацією (внесенням

навмисних викривлень), створенням несправжніх мережних об'єктів із подальшою генерацією несправжніх запитів та інформаційних об'єктів.

На *транспортному рівні* окрім уже розглянутих чинників (природних і штучних викривлень) слід урахувати можливості навмисної модифікації, вилучень та дублювання інформаційних об'єктів на рівні кадрів (блоків, пакетів, комірок, вікон).

Оцінка загальної цілісності інформаційних об'єктів у системі багатофазного захисту

Отже, з викладеного витікає доцільність здійснення контролю (а, по можливості, і поновлення) цілісності інформаційних об'єктів на декількох рівнях, тобто необхідність використання систем захисту інформаційних об'єктів, які дозволяли б, наприклад, окрім задачі забезпечення цілісності інформації в ТКМ на нижніх рівнях, обов'язково вирішувати й задачі забезпечення цілісності інформації хоча б на одному з вищих рівнів, так, щоб забезпечити цілісність інформації, яка безпосередньо надається одержувачу.

Класичним шляхом вирішення такої задачі є, наприклад, застосування в ТКМ згідно з еталонною моделлю взаємодії відкритих систем OSI/ISO (міжнародний стандарт ISO 7498) ієрархічної послідовності протоколів організації обміну для кожного з рівнів цієї моделі. Згідно із цим стандартом забезпечення потрібної вірності обміну інформацією здійснюється шляхом її контролю на декількох рівнях, принаймні за протоколами транспортного (TCP), мережного (IP) та канального рівнів тощо з відповідною реакцією на виявлені викривлення. Для усунення таких викривлень використовують різні способи (механізми, протоколи). Усіх їх можна підрозділити на дві групи: такі, що не використовують зворотний зв'язок, і такі, що використовують його.

У першому випадку при передачі дані кодуються одним із відомих кодів із виправленням помилок. При прийомі, відповідно, здійснюється декодування інформації, що приймається, і виправлення знайдених помилок. Іноді, наприклад, у системах мобільного радіозв'язку, застосовується комбінація двох підходів, яка полягає в реалізації на передавальній стороні як кодування з виправленням помилок, так і кодування лише з виявленням помилок, коли пакети, у яких виявлені викривлення, ігноруються. Такі методи особливо ефективні при передачі даних каналами дуже низької якості.

Другим прикладом є застосування в системах мобільного радіозв'язку стандарту GSM перемежування певної глибини й послідовного (наприклад, двофазного) завадостійкого кодування (так званих каскадних кодів) з тією ж самою задачею — забезпечити одержувача інформацією з припустимим рівнем викривлень (з потрібним рівнем цілісності) для умов низьких співвідношень сигнал/шум.

На погляд авторів, як *основну характеристику цілісності* інформаційних об'єктів для системи багатофазного захисту цілісності можна розглядати ймовірність $Q_{пц}$ подолання порушником (деякою особою чи деяким процесом) системи захисту цілісності інформаційних об'єктів, яку з урахуванням [4] через характеристики цілісності кожного з рівнів (фази захисту) такої системи можна записати у вигляді:

$$Q_{пц} = 1 - \prod_{i=1}^{n} (1 - q_i), \qquad (1)$$

де q_i — ймовірність подолання порушником засобів забезпечення цілісності інформаційного об'єкта на *i*-му рівні системи багатофазного захисту; *n* — число рівнів (фаз) захисту. Зрозуміло, що для визначення шуканого значення $P_{пц}$ слід визначити величини q_i для всіх відповідних рівнів. Нижче пропонуються підходи щодо визначення цих ймовірностей для деяких рівнів системи багатофазного захисту.

Цілісність інформації на фізичному рівні

Задача забезпечення цілісності інформації *на фізичному рівні* в умовах впливів природних чи штучних завад (проблема завадостійкості) у каналах ТКМ є давно відомою й розв'язується шляхом підвищення якості передавальних, приймальних пристроїв, а також якості передачі сигналів у середовищі розповсюдження. Основними напрямами останнього є наступні.

1. Збільшення співвідношення сигнал/завада за рахунок підвищення енергетики сигналу (велика початкова потужність, регенерація на проміжних пунктах (пунктах ретрансляції чи підсилення як з обслуговуванням, так і без обслуговування) тощо), що вимагає значних енергетичних або матеріальних витрат.

2. Збільшення енергетики сигналу за рахунок збільшення його тривалості при тій же потужності, використання складних широкосмугових сигналів (ШСС) як зі збереженням потужності одиничного сигналу, так і з її зменшенням аж до рівня природних завад (приклад — застосування ШСС у системах мобільного радіозв'язку).

3. Забезпечення хоча б задовільної узгодженості смуги пропускання $П$ каналу зі спектром сигналу при змінах технічної швидкості B передачі інформації (а отже, при зміні тривалості сигналу τ ($B \approx 1/\tau$)) у даному каналі. Задовільною найчастіше вважають таку узгодженість, якщо $П \geq 2B$.

4. Збільшення співвідношення сигнал/завада за рахунок зниження рівня завад (шумів) шляхом використовування спеціальних ліній зв'язку, кабельних ліній зв'язку з низьким рівнем власних шумів, наприклад, оптоволоконних, що також вимагає значних матеріальних витрат.

5. Використання найбільш ефективних у даних умовах видів модуляції тощо.

Вплив сумарного потоку завад (природних та штучних) *на фізичному рівні*, як уже згадувалося, можна описати ймовірністю викривлення символу. Як відомо з [5], цей вплив можна врахувати через імовірність викривлення символу:

$$P_{пом} = 0{,}5 \exp(-\alpha^2 h^2/2), \qquad (2)$$

де $\alpha^2 = 1/\sqrt{2}$ при амплітудній модуляції (сигнали з пасивною паузою); $\alpha^2 = 1$ при частотній і фазовій модуляції на кут $\pi/2$ (ортогональні сигнали); $\alpha^2 = \sqrt{2}$ при фазовій модуляції на кут π (протилежні сигнали); h^2 — співвідношення енергетики

сигналу E_c та сумарної енергетики $N_з$ завади, яка впливає на інтервалі тривалості сигналу.

Як *значення ймовірності подолання порушником засобів забезпечення цілісності інформаційного об'єкта* на фізичному рівні пропонується розглядати ймовірність викривлення хоча б одного символу кадру (блоку, пакету, комірки, вікна) під впливом сумарної завади, яка впливає на сигнали в середовищі їхнього розповсюдження.

Тоді в разі, коли на першому (фізичному) рівні кадр складається з N_1 символів, імовірність викривлення хоча б одного символу кадру q_1 (ймовірність подолання засобів забезпечення цілісності інформаційного об'єкта на фізичному рівні) визначається як:

$$q_1 = 1 - \prod_{i=1}^{N_1} (1 - P_{помі}) = 1 - (1 - P_{пом})^{N_1}.$$

Окрім розглянутого показника, який характеризує вплив сумарних завад на цілісність інформаційних об'єктів ТКМ, наразі можна ввести ще одну похідну від співвідношення сигнал/шум характеристику — *інтенсивність впливів* λ_1 цих завад на фізичному рівні. З цією метою відмітимо, що ця інтенсивність визначає середню кількість завад, а отже, і кількість викривлених символів у кадрі (блоці, пакеті, комірці, вікні) за час його передачі в лінії зв'язку $t_{бл}$:

$$n_{викр} = \lambda_1 \cdot t_{бл} = \lambda_1 \cdot N_1 / B,$$

де N_1, як і вище, — кількість символів у складі кадру на фізичному рівні; B — технічна швидкість передачі інформації.

З іншого боку, відомо, що кількість викривлених символів у кадрі (блоці, пакеті, комірці, вікні) з урахуванням імовірності викривлення символу $P_{пом}$ визначається як:

$$n_{викр} = N_1 \cdot P_{пом}.$$

Отже,

$$n_{викр} = \lambda_1 \cdot N_1 / B = N_1 \cdot P_{пом},$$

звідки:

$$\lambda_1 = B \cdot P_{пом}. \qquad (3)$$

Зауваження 1. Слід підкреслити, що значення величин імовірності викривлення символу $P_{пом}$ та інтенсивностей впливів, а отже, і характеристик цілісності

інформаційних об'єктів, що циркулюють в тому чи іншому середовищі, залежать від характеристик кожного із конкретної сукупності факторів, таких як:

1) наявність та активність (агресивність) зловмисників (інтенсивність їх впливів), їх спроможність по створенню завад того чи іншого типу (прицільні, загороджувальні, їхні характеристики, наприклад закони розподілу, спектральна щільність та ін.);

2) потужність, рівень (значення амплітуд та інтенсивності, закони розподілу, спектральна щільність тощо) природних (теплових, космічних, атмосферних, індустріальних) шумів;

3) характеристика середовища розповсюдження сигналів (вільний простір, дротяні лінії, кабельні (скручені пари, коаксіальний кабель, оптоволоконний кабель, ступень їх екранування від зовнішніх впливів (категорія) та ін.);

4) тип та характеристика застосованих модемів (апаратури передачі даних чи її окремих елементів) тощо;

5) потужність (спектр, спектральна щільність, значення амплітуд, закони розподілу, вид та характеристики модуляції тощо) сигналів, що забезпечують перенесення інформації, та інших. Тому визначити заздалегідь точні значення величин імовірності викривлення символу $P_{пом}$ та інтенсивностей впливів не є можливим. Для їхнього визначення слід здійснити всі необхідні вимірювання в точці прийому сигналу, визначити всі потрібні (див. зазначені вище фактори) і скористатися відповідними формульними співвідношеннями. Лише іноді ці характеристики можна визначити опосередковано. Наприклад, якщо відомо, що конкретний тип модему (апаратури передачі даних), у конкретних умовах (наприклад, для умов телефонного каналу без впливу зовнішніх (у тому числі й зловмисних) завад на певній швидкості передачі, наприклад, B = 9800 біт/с забезпечує ймовірність викривлення символу $P_{пом} = 10^{-4}$, то значення інтенсивності в даному випадку природних впливів може бути оціненим як $\lambda_1 = B \cdot P_{пом} = 0,\ 98$ 1/с. У разі, якщо для умов оптоволоконного кабелю при B = 100 Мбіт/с забезпечується $P_{пом} = 10^{-9}$, то значення інтенсивності $\lambda_1 = B \cdot P_{пом} = 0,\ 1$ 1/с.

Цілісність інформації на канальному рівні

Механізми контролю та поновлення цілісності істотно залежать від умов їхнього застосування, а саме від впливу випадкових (природних) або штучних (зловмисних) викривлень. Існує багато методів забезпечення вірності передачі інформації (методів захисту від помилок), які розрізняються за використовуваними для їхньої реалізації засобами, за витратами часу на їхнє застосування на передавальному й приймальному пунктах, за витратами додаткового часу на передачу фіксованого об'єму даних (воно обумовлене зміною об'єму трафіку користувача при реалізації даного методу), за ступенем забезпечення достовірності передачі інформації.

Для реалізації обміну інформацією дані організовуються в спеціальні блоки, які називаються кадрами, вікнами, пакетами, комірками або узагальненими кодовими словами, які, у свою чергу можуть складатися з базових кодових слів — порцій інформації певної довжини (у бітах або для узагальнених символів у гру-

пах біт, найчастіше в байтах), по відношенню до яких реалізуються механізми забезпечення цілісності: контролю цілісності (в термінах завадостійкого кодування — виявлення помилок) або контролю з відновленням цілісності (у термінах завадостійкого кодування — виявлення та виправлення помилок).

Для забезпечення контролю цілісності інформаційних об'єктів із використанням завадостійких кодів, включаючи й відновлення зруйнованої інформації, до складу інформації, яка захищається, вводять надмірну інформацію — ознаку цілісності або контрольну ознаку (залежно від прийнятої термінології та призначення — у задачах контролю цілісності або завадостійкого кодування) — своєрідний образ, відображення цієї інформації, процедура формування якого відома, і який із дуже високою вірогідністю відповідає інформації, що захищається. Цим 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 за контрольними ознаками найчастіше не існує). Контроль цілісності (на відсутність викривлень) зводиться при цьому до тих або інших процедур перевірки відповідності між ознаками цілісності, і власне прийнятою з каналу зв'язку (або зчитаної із запам'ятовуючого пристрою (ЗП)) інформацією.

Характерною особливістю випадкових викривлень є те, що вони, через відсутність навмисності, порушують регулярний (функціональний) односторонній зв'язок між прийнятою (або зчитаною з ЗП) інформацією й ознаками цілісності, що сформовані перед передачею (перед записом у ЗП). Тому при виявленні порушення вказаного зв'язку встановлюється факт наявності таких викривлень, а за певних умов, і їхні місця, і величини (характеру). Якщо ж порушення такого зв'язку не виявлено, то робиться висновок про відсутність викривлень.

Як *характеристику цілісності* інформаційного об'єкта на канальному рівні пропонується розглядати ймовірність подолання порушником засобів забезпечення цілісності q_2 (ймовірність неусунення засобами захисту цього рівня сумарного потоку викривлень). Інтенсивність сумарного потоку викривлень λ_2 складається з інтенсивностей викривлень на фізичному рівні λ_1, і штучних викривлень, що сформовані вже на канальному рівні $\lambda_{ш2}$, $\lambda_2 = \lambda_1 + \lambda_{ш2}$.

Серед основних способів (механізмів) забезпечення цілісності інформації, які визначають імовірність q_2 подолання засобів забезпечення цілісності інформаційного об'єкта на канальному рівні ТКМ, слід виділяти наступні.

1. Застосування групових (мажоритарних) методів захисту, що ґрунтуються на використовуванні декількох каналів зв'язку (3...5), що є фізично (найчастіше, навіть, географічно) рознесеними, якими передається одна й та ж інформація, або на багатократній передачі (3...5 разів) однієї й тієї ж інформації одним каналом зв'язку. У першому випадку необхідні істотні матеріальні витрати, а в другому значно зменшується пропускна можливість каналу зв'язку (у 3...5 разів). З цих причин, у системах передачі даних використовування цих методів є не завжди доцільним.

2. Застосування у відповідних модемах (апаратурі передачі даних) різного роду протоколів із використанням завадостійких кодів із виявленням помилок у

прийнятій (зчитаній) інформації, які дозволяють реалізувати програмні, апаратурні або програмно-апаратурні засоби виявлення викривлень. За способами організації обміну все різноманіття можливих механізмів (процедур, протоколів) обміну може бути розподіленим на два типи: протоколи із забезпеченням лише високої швидкості обміну без «турботи» про вірність переданих даних та на протоколи із забезпеченням певного рівня вірності переданих даних [6]. Протоколи першого типу взагалі не здійснюють такого контролю (приклади — протоколи обміну мережного рівня frame relay, транспортного рівня UDP), чи в разі виявлення викривлень інформаційного об'єкта вилучають його з мережі (приклади — протоколи обміну мережного рівня IP) або підміняють викривлену інформацію, наприклад, її лінійним прогнозом (приклад — протоколи обміну в стандарті мобільного зв'язку GSM [7]). Протоколи другого типу забезпечують корекцію можливих викривлень за рахунок використання кодів, які виявляють наявність викривлень, з наступним перезапитом викривленої інформації — протоколи зі зворотним зв'язком. Це, у свою чергу, дає можливість застосування способів передачі повідомлень із різного роду зворотним зв'язком: інформаційним — деяким аналогом мажоритарного методу з багатократною передачею інформації й зворотним прийомом й ухваленням рішення щодо правильності передачі на стороні передавача, або з вирішальним зворотним зв'язком (ВЗЗ) — багатократній, за необхідності, передачі з ухваленням рішення щодо правильності передачі на стороні приймача (приклад — протоколи транспортного рівня TCP). У цьому випадку код застосовується тільки в режимі виявлення помилок, що дозволяє досягти високої ймовірності виявлення викривлень при незначному рівні надмірності, що вводиться.

Імовірність q_2 подолання засобів забезпечення цілісності інформаційного об'єкта для таких засобів практично не залежить від кратності викривлень і залежить лише від кількості k надлишкових символів, яка використана при побудові коду:

$$q_2 = 1/2^k.$$

3. Застосування в модемах різного роду протоколів, що забезпечують корекцію можливих викривлень за рахунок використання завадостійких корегувальних кодів (ЗКК), які дозволяють реалізувати програмні, апаратурні або програмно-апаратурні засоби виявлення й усунення викривлень (приклад — протоколи обміну в стандарті GSM).

При використанні механізмів виявлення та виправлення викривлень із застосуванням у межах кадру перемежування кратності λ_n та ЗКК, які в межах базового кодового слова здатні виявляти лише поодинокі викривлення, можливим є виявлення і виправлення викривлень такої ж кратності, як і λ_n. Отже, засоби забезпечення цілісності інформаційного об'єкта будуть подолані з імовірністю q_2 у разі, коли кількість викривлень u за час t_n доставляння повідомлення (кадру), перевищить величину λ_n. Вважаючи, що кількість викривлень підпорядкована закону Пуассона, при інтенсивності впливів $\lambda_2 = \lambda_1 + \lambda_{ш2}$, ймовірність того, що кількість викривлень u за час t_n перевищить можливості застосованого ЗКК із пере-

межуванням, а отже, і ймовірність q_2 подолання засобів забезпечення цілісності інформаційного об'єкта може бути розрахованою з виразу:

$$q_2 = P_{u>\lambda_n}(t_n) = 1 - \sum_{s=0}^{\lambda_n} (\lambda_2 \cdot t_n)^s \exp(-\lambda_2 \cdot t_n)/s!$$

У цьому виразі час t_n доставляння повідомлень у протоколах організації обміну телекомунікаційних мереж із ЗКК може бути визначеним, у свою чергу, як [8]:

$$t_{n\text{ЗКК}} = N_2/[(1+ \lambda_2 t_к)\exp(-\lambda_2 t_к)\cdot m_{\text{ЗКК}}/\{t_к + \Delta t_{к2} + \Delta t_{n2}\cdot(1 - \exp(-\lambda_2 t_к))\}],$$

де $\Delta t_{к2}$ — час, необхідний для контролю цілісності кадрів; Δt_{n2} — час, необхідний для виправлення викривлень у кадрах (у випадку їхнього виявлення); $t_к$ — часова тривалість ($t_к = N_2/B$) кадру; $m_{\text{ЗКК}}$ — кількість суто інформаційних символів у складі кадру; N_2 — загальна кількість символів у складі кадру на канальному рівні, а B — технічна швидкість передачі інформації.

Зауваження 2. Значення величин інтенсивностей впливів $\lambda_{ш2}$, як і розглянутих вище величин інтенсивностей впливів λ_1, залежать від наявності та активності (агресивності) зловмисників, їхньої спроможності щодо перехоплення інформації канального рівня із наступною її модифікацією та генерацією несправжніх інформаційних об'єктів (інтенсивності їхніх впливів). Їхнє визначення слід здійснювати шляхом необхідних вимірювань на приймальному боці каналу. *Це стосується й інших рівнів, розглянутих у даній статті*.

Цілісність інформації на мережному та транспортному рівнях

З викладеного вище витікає, що на мережному рівні впливають викривлення, які пропущені засобами захисту канального рівня в кількості $\lambda_2 \cdot q_2$, до яких додаються зловмисні впливи $\lambda_{ш3}$, що можуть бути пов'язаними із перехопленням інформаційних об'єктів з їхньою наступною модифікацією (внесенням навмисних викривлень), створенням несправжніх мережних об'єктів із подальшою генерацією несправжніх запитів та інформаційних об'єктів так, що:

$$\lambda_3 = \lambda_2 \cdot q_2 + \lambda_{ш3}.$$

Як *значення ймовірності подолання порушником засобів забезпечення цілісності* інформаційного об'єкта на мережному та транспортному рівнях пропонується розглядати також імовірності подолання порушником засобів забезпечення цілісності на мережному q_3 та транспортному q_4 рівнях (ймовірність неусунення засобами захисту відповідного рівня сумарного потоку викривлень). Інтенсивності сумарних потоків λ_3 та λ_4, як і вище, розглядатимемо у вигляді сум інтенсивностей природних викривлень, що не усунені на попередніх рівнях, і штучних ви-

кривлень, що сформовані уже на мережному $\lambda_{ш3}$ та канальному $\lambda_{ш4}$ рівнях відповідно. Для цих рівнів пропонується врахувати, що після фільтрації природних викривлень протоколами канального рівня та застосування можливостей щодо динамічної маршрутизації (із переходом на канали з меншим рівнем завад) потік на вході мережного рівня у своїй інтенсивності λ_3 може мати досить низьку природну складову. З цієї причини й на цьому рівні, і на транспортному рівні природні викривлення можна не враховувати. Отже, для даних рівнів можна вважати: $\lambda_3 = \lambda_{ш3}$, $\lambda_4 = \lambda_{ш4}$. У подальших міркуваннях це припущення враховане.

Тоді в протоколах *мережного й транспортного рівнів* доцільним є застосування засобів захисту від таких впливів, коли порушник маскує здійснену ним модифікацію інформаційних об'єктів. Зрозуміло, що окрім таких впливів можливим є застосування зловмисниками потоків несправжніх об'єктів, але їхній вплив є спрямованим на порушення іншої функціональної властивості захищеності — доступності, а її розгляд виходить за межі даної статті.

Звернемо увагу на те, що, на відміну від випадкових викривлень, характерною особливістю навмисних викривлень є те, що зловмисник прагне забезпечити, зімітувати наявність згаданого вище регулярного (функціонального) зв'язку між модифікованою ним початковою інформацією, прийнятою (або зчитаною зі 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 у ЗП) забезпечує формування відповідних ознак. *При успішному формуванні вказаних ознак, розкрити наявність модифікації неможливо.* Для боротьби із цим власнику (або авторизованому користувачеві) 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, порушник не зуміє забезпечити, зімітувати наявність регулярного (функціонального) зв'язку між модифікованою ним початковою інформацією, прийнятою (або зчитаною зі ЗП), і ознаками цілісності.

З викладеного витікає істотна відмінність задач захисту цілісності інформаційних об'єктів у телекомунікаційних мережах при виявленні випадкових і навмисних викривлень, і відповідно процедур формування контрольних ознак. Окрім того, можна зробити висновок про те, що процедури формування контрольних ознак (ознак цілісності) для виявлення навмисних викривлень можуть, звичайно ж, використовуватися й для виявлення випадкових викривлень, але це не завжди виправдано економічно, оскільки такі процедури потребують більших витрат на свою реалізацію й використання, ніж процедури формування контрольних ознак для виявлення випадкових викривлень.

Наступне зауваження стосується того, що навмисні впливи типу модифікації аж до підміни інформаційних об'єктів можливі як на мережному, так і на транспортному рівнях. При цьому задачу захисту від модифікацій також можна вирішувати на кожному із цих рівнів, але її вирішення на транспортному рівні є обов'язковим. У зв'язку із цим для підвищення загальної продуктивності багато-

фазної системи захисту задачу контролю цілісності інформаційних об'єктів доцільно вирішувати якраз на транспортному рівні.

На мережному рівні для забезпечення цілісності інформації потрібно використовувати наступні заходи.

1. Для захисту від викривлень, які пропущені засобами захисту попередніх рівнів і мають інтенсивність $\lambda_2 \cdot q_2$, стає можливим використання протоколів із застосуванням механізмів виявлення (а, можливо, і корекції), що аналогічні протоколам канального рівня з імовірністю їхнього подолання q_3. Але, враховуючи те, що після їхньої фільтрації протоколами канального рівня цей потік має досить низьку інтенсивність, у протоколах даного рівня можна допустити відсутність механізмів виявлення (а, тим більше, виправлення) викривлень (такими протоколами є, наприклад, протоколи IP та frame relay). В останньому випадку $q_3 = 1$. У будь-якому випадку інтенсивність цих викривлень на вході протоколів транспортного рівня можна розраховувати з виразу: $\lambda_{n3} = \lambda_2 \cdot q_2 \cdot q_3$.

2. Для захисту від перехоплень і генерації модифікованих пакетів і несправжніх запитів й інформаційних об'єктів з інтенсивністю потоку $\lambda_{ш3}$ необхідним є використання механізмів управління доступом (фільтрації пакетів, ідентифікації та автентифікації мережних інформаційних об'єктів, перевірки істинності та ін.), управління маршрутизацією інформаційних об'єктів тощо. Управління доступом до ресурсів ТКМ може включати, наприклад, контроль доступу мережними адресами та фільтрацію пакетів. Управління доступом на мережному рівні реалізується програмно-технічними засобами розмежування, управління та контролю доступу (міжмережні екрани, маршрутизатори та ін.). Управління маршрутизацією інформаційних об'єктів полягає у визначенні таких маршрутів передачі, у каналах передачі яких інтенсивність як природних, так і штучних впливів, є мінімальними.

Будемо вважати, що ймовірність подолання сукупності таких механізмів дорівнює $q_{3ш}$. Тоді результуюча інтенсивність впливів, які здатні подолати засоби захисту мережного рівня, може бути визначена як: $\lambda_3 = \lambda_2 \cdot q_2 \cdot q_3 + q_{3ш} \cdot \lambda_{ш3}$.

На *транспортному рівні* для забезпечення цілісності інформаційних об'єктів, окрім уже розглянутих механізмів контролю (і поновлення) цілісності інформаційних об'єктів на рівні кадрів (блоків, пакетів, комірок, вікон), необхідно застосовувати механізми контролю цілісності повідомлень (їхньої повноти, одержання в повному обсязі) та відсутності дублювання кадрів (блоків, пакетів, комірок, вікон). Вважаючи, що ймовірність подолання цих засобів дорівнює q_4, результуюча інтенсивність впливів на виході даного може бути визначена як: $\lambda_4 = \lambda_3 \cdot q_4$.

На більш високих рівнях моделі ВВС вирішуються задачі управління доступом паролями, задачі розподілу повноважень суб'єктів (користувачів), надання рівнів доступу до об'єктів (ресурсів), решта задач контролю цілісності інформаційних об'єктів (файлів, інформації при її обробці й передачі), програмних засобів і баз даних, архівної інформації, і резервних копій програмних засобів, і баз даних. Оскільки визначення відповідних характеристик цілісності на цих рівнях (фазах) захисту (q_5, q_6, q_7) виходить за межі даної статті, відзначимо лише, що ймовірність $Q_{пц}$ подолання семифазної системи захисту цілісності інформаційних об'єктів на підставі (1) може бути визначеною як:

$$Q_{пц} = 1 - \prod_{i=1}^{7} (1 - q_i) .$$

Таким чином, у статті розглянуті задачі забезпечення багатофазного захисту цілісності інформації, яка надається користувачам ТКМ, запропоновано вирази для розрахунку характеристик цілісності інформаційних об'єктів для систем багатофазного захисту, а також характеристик цілісності кожного з рівнів (фаз) захисту у вигляді ймовірностей подолання порушником системи захисту цілісності інформаційних об'єктів у цілому, чи її окремих фаз.

1. «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу» (НД ТЗІ 1.1-002-99).

2. «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» (НД ТЗІ 2.5-004-99).

3. «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» (НД ТЗІ 2.5-005-99).

4. *Антонюк А.А., Волощук А.Г., Заславская Е.А., Суслов В.Ю.* Об одном подходе в моделировании защиты информации // Перша міжнародна науково-практична конференція з програмування УкрПРОГ, 1998. — С. 505–510.

5. *Бунин С.Г., Войтер А.П.* Вычислительные системы с пакетной радиосвязью. — К.: Техніка, 1989. — 223 с.

6. *Василенко В.С., Будько М.М., Короленко М.П.* Механізми контролю цілісності інформації та її поновлення // Правове, нормативне та метрологічне забезпечення Системи захисту інформації в Україні // К.: НТУУ «КПІ», 2000. — С. 130–139.

7. Особенности сотовой системы подвижной связи стандарта GSM // на сайті http://astra.pp.ru/doc/hard/GSM,

8. *Василенко В.С., Матов О.А., Будько М.М.* Оцінка часу доставки повідомлень у протоколах організації обміну в телекомунікаційних системах // Реєстрація, зберігання і оброб. даних. — 2004. — Т. 7, № 2. — С. 66–76.

Надійшла до редакції 20.02.2006