DOI: https://doi.org/10.32836/2521-6643-2018.2-56.6
УДК 004.056.2

В. Я. Пєвнєв, кандидат технічних наук, доцент кафедри комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету ім. Н. Є. Жуковського "Харківський авіаційний інститут"

МОДЕЛІ ЗАГРОЗ І ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ІНФОРМАЦІЇ

Проведено аналіз визначення поняття цілісності інформації в різних галузях науки і прикладних дисциплінах. Запропоновано визначення цілісності інформації для інфокомунікаційних систем. Розглянуто можливі загрози цілісності інформації протягом її життєвого циклу. Проведено аналіз загроз цілісності інформації щодо об'єктів інфокомунікаційних систем та методів забезпечення цілісності. Розглянуто методи забезпечення та контролю цілісності з подальшим відновленням в інфокомунікаційних системах.

Ключові слова: *цілініcть інформації; модель цілісності; загрози; об'єкти загроз; методи забезпечення; контроль цілісності.*

Проведен анализ определения понятия целостности информации в различных областях науки и прикладных дисциплинах. Предложено определение целостности информации для инфокоммуникационных систем. Рассмотрены возможные угрозы целостности информации в течение её жизненного цикла. Проведен анализ угроз целостности информации по объектам инфокоммуникационных систем и методов обеспечения целостности. Рассмотрены методы обеспечения и контроля целостности с последующим восстановлением в инфокоммуникационных системах.

Ключевые слова: *целостность информации; модель целостности; угрозы; объекты угроз, методы обеспечения; контроль целостности.*

The analysis presented in the paper shows that there is no unambiguous interpretation of many terms in the modern community of scientists and practitioners. On this basis, one can conclude that there is a need for uniform interpretation of terms. This will allow representatives of different fields to communicate more closely. The integrity model and threats in the infocommunication systems makes it possible to understand the place of information integrity in modern systems. Currently,

violation of information integrity is the most dangerous impact on all systems, including critical ones. The impact on information, from the point of view of integrity, can be its distortion and imposition. For the purpose of protection, both organizational and technical methods. From the economic point of view, the construction of technical means of protection systems is unprofitable. However, the cost of these systems of defense in oftentimes can be less than, than possible damage that can be inflicted as a result of attacks. The threat model proposed in the article reflects both the objects targeted by the threats and the threats themselves. Based on the results of the analysis, we can conclude that the most vulnerable elements are software. The number of attacks on software is more than 53 percent. The paper describes the possible methods and means of providing and monitoring the information integrity. Among them it is possible to allocate both well known methods (for example, noise proof coding), and methods which are rather seldom used for maintenance of information integrity (steganography). The methods of providing of integrity of information can be divided into two large groups. To the first group will be belongs methods that directly provide to integrity of information. Methods that allow you to control the integrity of information and, if necessary, restore the message belong to the second group. Some methods are used both in the first and in second groups. For example, facilities of anti-virus defense allow both to protect a computer from a virus (first group) and recover the damaged file (second group). The analysis which has been spent, shows variety of forms and methods of construction of systems of maintenance of information integrity.

Key words: *model of information integrity; threat; objects of threats; methods of providing; control of integrity.*

Постановка проблеми. Забезпечення інформаційної безпеки під час використання інфокомунікаційних систем (ІКС) передбачає розв'язання проблем забезпечення цілісності, доступності та конфіденційності, хоча в останніх публікаціях і європейських стандартах до цих трьох китів додаються автентичність, підзвітність, безвідмовність і надійність [1]. У більшості систем, включаючи системи, в яких циркулює інформація з обмеженим доступом, найбільш гострою проблемою є забезпечення цілісності інформації (ЦІ).

Аналіз останніх досліджень і публікацій. Що таке цілісність інформації? На жаль, нинішнього часу в різних галузях науки і прикладних дисциплінах немає єдиного поняття цілісності. Необхідність єдиного визначення обумовлюється тим, що в системі потрібно мати один термін для позначення одного явища, дії або предмета дослідження. У якості цього терміна можна було використанне поняття достовірності, але цей термін більш підходить, коли йдеться про відповідність даних явищу, яке вони описують.

Цілісність повинна відноситьсь і прив'язуватись до системи, в якій проводиться обробка інформації, і забезпечується її незмінність. У табл. 1 подано визначення поняття цілісності в різних галузях [1–4].

Таблиця 1

Порівняння поняття цілісності

Найменування галузі	Поняття цілісності	Синоніми
Теорія інформації	Відсутня	Достовірність і повнота
Теорія зв'язку	Відсутня	Достовірність
Теорія інформаційної безпеки	Властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення	
Теорія функціональної безпеки	Властивість виключати непередбачені зміни системи і послуг, що надаються	
Теорія баз даних	Коректність даних та їх несуперечність, а також повнота і правильність інформації, яка вміщується в БД	
Представлена робота	Здатність системи за допомогою вбудованих засобів протягом заданого часу протидіяти несанкціонованій зміні інформації та (або) відновлювати викривлену інформацію	

Виходячи з вищенаведеного, можна зробити висновок про актуальність розгляду методів досягнення ЦІ в ІКС.

Під цілісністю розуміється здатність системи за допомогою вбудованих засобів протягом заданого часу протидіяти несанкціонованій зміні інформації та/або відновлювати викривлену інформацію

Слід зазначити, що ні доступності, а тим більше конфіденційності, без забезпечення ЦІ досягти неможливо. Наприклад, за сучасними вимогами до криптосистем, незначна зміна вихідного тексту повинна приводити до значної зміни шифрованої послідовності. Якщо в процесі передачі спотвориться один біт переданої шифрограми, то після розшифровки отриманий текст дуже відрізнятиметься від початкового. Отже, можна говорити про проблему забезпечення ЦІ, яка нині не розв'язана повною мірою.

Мета статті – розробка моделі цілісності інформації в ІКС та аналіз сучасних методів і засобів забезпечення цілісності інформації.

Виклад основного матеріалу. Виходячи з визначення ЦІ, можна виділити такі впливи на інформацію [5]:

– модифікацію інформації;

– підміну інформації;

– знищення інформації.

Модифікація передбачає зміни будь-якої частини інформації. Ці зміни можуть бути як випадковим, так і навмисними. В даному випадку вони можуть бути санкціонованими або несанкціонованими.

Підміна передбачає нав'язування неправдивої інформації шляхом заміни істинної (первісної) інформації. Знищення найчастіше пов'язується зі знищенням фізичного носія інформації та/або розмагнічуванням (форматуванням) електронних носіїв.

Розглянемо можливі загрози ЦІ протягом її життєвого циклу. При використанні неповних та/або помилкових даних під час створення (появи) інформації можна отримати інформацію, що не відповідає дійсності, про ті чи інші події. Адекватність прийнятого рішення, заснованого на такій інформації, викликає сумніви.

Під час обробки інформації порушення ЦІ може виникнути внаслідок технічних несправностей, алгоритмічних і програмних помилок, помилок і деструктивних дій обслуговуючого персоналу, зовнішнього втручання, шкідливих і програм, що руйнують (вірусів, троянів, черв'яків, логічних бомб).

У ході передачі на інформацію можуть впливати різні завади як природного, так і штучного походження. При цьому можливо її спотворення або стирання (знищення). Крім цього, можливе перехоплення інформації з метою її модифікації і подальшого нав'язування.

У ході зберігання основними загрозами є несанкціонований доступ з метою модифікації (аж до знищення) інформації, шкідливі програми (віруси, трояни, черв'яки, логічні бомби) і технічні несправності.

В процесі старіння основними загрозами інформації, поряд з погрозами під час зберігання, можна вважати втрату технологій, здатних відтворити ту чи іншу інформацію, і фізичне старіння носіїв інформації.

Слід зазначити, що на всіх етапах життєвого циклу існує загроза ЦІ через технічні системи, що використовуються. Це банальні несправності, збої електроживлення, електромагнітні імпульси тощо.

Під час утилізації про забезпечення ЦІ не йдеться.

Тому можна зробити висновок про те, що загрози ЦІ виникають протягом усього життєвого циклу інформації з моменту її появи до початку утилізації.

Якщо класифікувати загрози ЦІ за ознакою частоти загроз, то можна зробити такий висновок. У ході розгляду 128 загроз цілісності [6–9] 21 загрозу представляли несанкціоновані дії щодо всіх складових ІКС. Наприклад, існують загрози:

– несанкціонованого доступу до системи зберігання даних з віртуальної та (або) фізичної мережі;

– несанкціонованого редагування реєстру;

– несанкціонованого доступу до локального комп'ютера через клієнта грід-системи;

– перехоплення управління середовищем віртуалізації.

За кількістю ці загрози були на першому місці. Другу групу загроз становили шкідливі програми. До них нлежать і так звані віруси. Загальна кількість цих загроз дорівнює 20. Серед них:

– загроза спотворення інформації, що вводиться і виводиться на периферійні пристрої;

– загроза впровадження шкідливого коду в BIOS;

– загроза несанкціонованого вимкнення або обходу механізму захисту від запису в BIOS;

– загроза зараження комп'ютера під час відвідування неблагонадійних сайтів;

– загроза поширення "поштових черв'яків".

На третьому місці – загрози, які виникають у мережі. Кількість цих загроз дорівнює 15. У діапазоні 8–6 загроз містяться загрози виходу процесу за межі віртуальних машин, порушення в хмарних технологіях, зміни конфігурації програмного забезпечення та апаратних засобів, незаконне використання привілеїв, зміни формату даних і використання слабих криптографічних даних. У кінці списку загроз ще 6 загроз, які трапляються 1–3 рази.

Під час аналізу загроз ЦІ були розглянуті елементи ІКС. Серед них виділено програмну складову, що являла собою сукупність прикладного програмного забезпечення, системного програмного забезпечення, в якому був окремо виділений BIOS, і мережного програмного забезпечення. Окремо розглядалися апаратне забезпечення і апаратні пристрої, грід-системи й робочі станції. Також було виділено об'єкти мережної структури, до яких належать: мережний вузол, мережний трафік і вся сукупність інформаційної системи. Окремо було розглянуто сховище великих даних і хмарна система, а також окремі об'єкти (об'єкти файлової системи, віртуальні машини, облікові дані користувачів, носії обміну інформацією та ін.), на які було спрямовано різноманітні загрози. Перелік цих об'єктів і кількість загроз, спрямованих на ці об'єкти, подано в табл. 2.

В цілому виділено 18 об'єктів, на які було спрямовано 128 загроз ЦІ. Велика частина загроз була спрямована на програмне забезпечення діяльності ІКС. Слід зазначити, що невисокий відсоток загроз, спрямований на мережну складову, не повинен викликати подив. Тут не враховувалося використання мережних механізмів для проникнення в комп'ютери, програмну складову або в хмарні системи.

Таблиця 2

Об’єкти загроз

Об’єкти загроз	Кількість загроз			
	Спрямовані	Багатовекторні	Разом	Разом у відсотках
Апаратне забезпечення, апаратний пристрій	4	16	20	7,4
Грід-системи	2	1	3	1,1
Робоча станція		2	2	0,7
Прикладне програмне забезпечення	3	35	38	14,0
Системне програмне забезпечення	9	43	52	19,1
BIOS	12	3	15	5,5
Мережне програмне забезпечення	4	36	40	14,7
Програмне забезпечення (взагалі)	28	117	145	53,3
Об’єкти файлової системи	1	13	14	5,1
Віртуальна машина	4	7	11	4,0
Мережний вузол		11	11	4,0
Інформаційна система	1	10	11	4,0
Мережний трафік	1	6	7	2,6
Мережна система (взагалі)	2	27	29	10,7
Хмарна система	5	8	13	4,8
Сховище великих даних, метадані, база даних		11	11	4,0
Облікові дані користувача		5	5	1,8
Носій обміну інформацією	1	7	8	2,9
Реєстр		8	8	2,9
Засоби захисту інформації		3	3	1,1
Взагалі	47	225	272	100,0

У табл. 2 виділено загрози, спрямовані на конкретні об’єкти, серед яких виділяється за кількістю цих загроз BIOS, і загрози, спрямовані одночасно на кілька об’єктів.

Проаналізуємо сучасні методи й засоби забезпечення цілісності інформації. Методи забезпечення ЦІ можна розбити на дві великі групи. До першої групи зараховуємо методи, які безпосередньо забезпечують ЦІ. До другої групи – методи, які дозволяють контролювати ЦІ і, в разі необхідності, відновлювати повідомлення (рис. 1).

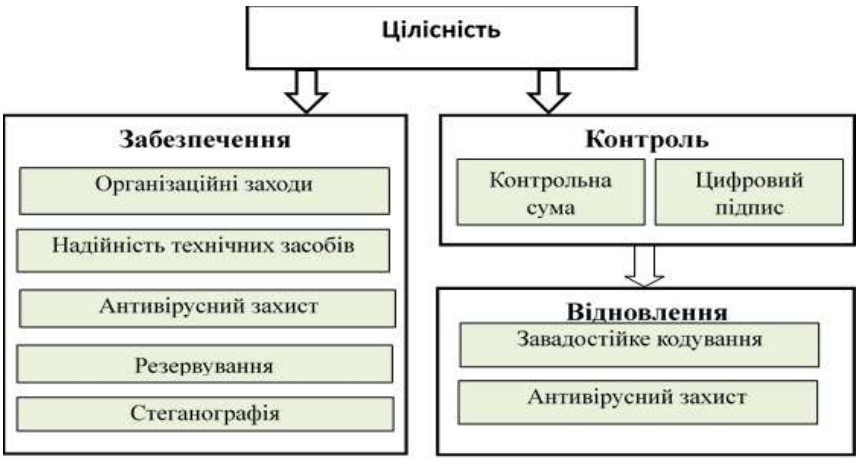

Рис. 1. Методи забезпечення ЦІ

Поширеним і досить ефективним методом забезпечення ЦІ є організація доступу до інформації та обладнання, що використовується. Даний метод належить до організаційних і передбачає досить великий перелік заходів, починаючи від добору співробітників і закінчуючи роботою з технікою і документами [10].

Серед них можна виділити технології захисту, обробки та зберігання документів, атестацію приміщень і робочих зон, порядок ЦІ від випадкових та/або несанкціонованих дій персоналу тощо. Для забезпечення ЦІ в ІКС особливу увагу слід приділити захисту операційних систем (ОС), що забезпечують функціонування практично всіх складових системи. Найбільш дієвим механізмом розмежування доступу для ОС є ізольоване програмне середовище (ІПС) [11]. ІПС підвищує стійкість ІКС до різних шкідливих програм і програм, що руйнують, дозволяючи забезпечити ЦІ.

Надійність технічних засобів. Необхідною умовою забезпечення ЦІ є наявність високонадійних технічних засобів (ТЗ), які включають в себе як апаратну, так та/або програмну складові [12]. Таке обладнання повинно забезпечувати як високу відмовостійкість, так і ЗІ від можливих загроз.

Одним із найбільш поширених засобів підвищення надійності ТЗ є резервування. Якщо розглядати ТЗ з точки зору інформаційної складової, то підвищення надійності досягається за рахунок послідовного з'єднання елементів системи, що відповідають за дану складову. Якщо послідовно з'єднати два комп'ютери, поставивши на кожен із них свій антивірус, то ймовірність проникнення шкідливої програми зменшується. Однак при цьому зменшується ймовірність безвідмовної роботи ТЗ, що складається з двох комп'ютерів, які послідовно з'єднані.

Для забезпечення заданої надійності (гарантоздатності) такого інформаційно-технічного комплексу необхідно застосовувати послідовно-паралельну архітектуру побудови систем ТЗ.

ТЗ припускають і можливість використання виділених та/або фізично захищених лінії зв'язку, наприклад броньовані кабелі з контролем цілісності оболонки.

До ТС забезпечення ЦІ належать також і засоби захисту від електромагнітного імпульсу (ЕМІ). Вражаючими факторами ЕМІ є високоінтенсивні електромагнітні поля, які або безпосередньо впливають на радіоелектронні засоби (РЕЗ), або трансформуються в небезпечних трактах цих засобів у наведені струми й напруги [13]. Найбільш ефективним методом зменшення інтенсивності ЕМІ є екранування – розміщення обладнання в електропровідному корпусі, який перешкоджає проникненню електромагнітного поля від джерела до обладнання, що захищається. Однак в більшості випадків обладнання, яке захищають, має зовнішні комунікації, що призводить до проникнення в екранований простір наведених завадових струмів і напруги, що викликають пошкодження елементної бази РЕЗ. Рішенням є методи обмеження наведених напруг і струмів за амплітудою і спектром у зовнішніх трактах РЕЗ і електромагнітна розв'язка зовнішніх ланцюгів РЕЗ від екранованих пристроїв. Для обмеження наведень за амплітудою і спектром використовуються іскрові і газорозрядні розрядники, напівпровідникові обмежувальні пристрої, варистори і спеціальні нелінійні опори. До обмежувача спектра належать прохідні конденсатори, дроселі та фільтри [13].

Електромагнітна розв'язка досягається за допомогою ізолювальних трансформаторів, дроселів, оптронів, елементів оптоелектроніки. Застосування оптоелектронних схем дозволяє зменшити число замкнутих контурів і забезпечити електричну розв'язку кола. Крім цього, системи на базі оптоелектроніки некритичні до впливу перешкоджаючих електромагнітних полів унаслідок того, що носіями інформації в цих системах є електрично нейтральні фотони. Ще однією перевагою оптоелектронних систем стало обмеження смуги пропускання, особливо на високих частотах, й що тим самим є бездротовими обмежувачами високочастотних завадових наведень на вхідні кола РЕЗ, які властиві ЕМІ [13].

Стиснення даних. Як відомо [14], стиснення це заміна послідовності символів іншою послідовністю меншої довжини або оптимальне кодування. Забезпечення ЦІ досягається за рахунок зменшення обсягу інформації, що передається. Це зменшення можна досягти за рахунок оптимального кодування джерела. Однак такий метод у даний час практично не використовується з огляду на те, що під час цифрової обробки сигналу вигідніше, з точки зору організації обчислювального процесу, під кожен символ виділяти однакову кількість біт.

Найчастіше використовується метод динамічного стиснення. За такого підходу структура стисненого повідомлення включає в себе словник і стислу інформацію. Зменшення обсягу переданої інформації досягає 20 разів (залежно від типу інформації, що передається). Однак, якщо під час передачі або зберігання виявляється помилка, особливо в словнику, то виникає ефект розмноження помилок, що призводить до значного спотворення або знищення інформації.

У працях [15–16] подано спосіб стиснення інформації, що дозволяє зменшити розмір файлів невеликої довжини (менше 1000 біт) до 75 відсотків. Основна ідея даного способу – використання шести біт для кодування переданого символу й декількох кодових таблиць, попередньо розміщених у користувачів ІКС.

Стеганографія. З цим терміном знайомі всі, хто займається питаннями ЗІ. Нині можна виділити три тісно пов'язаних між собою напрямки стеганографії: приховування даних, цифрові водяні знаки і заголовки. За прихованої передачі інформації одночасно із забезпеченням конфіденційності [17] вирішується й питання забезпечення ЦІ. Не можна змінити того, чого не бачиш – головний аргумент використання стеганографії для забезпечення ЦІ.

Одним із найпростіших способів прихованої передачі є відправлення повідомлення всередині іншого повідомлення. Це може бути якийсь контейнер, наприклад, у згрупованому об'єкті що на другому плані міститься текстове повідомлення, написане білим по білому. До цього методу можна зарахувати і використання спеціальних сигналів, наприклад широкосмугових шумоподібних або ортогональних.

Головним недоліком використання стеганографії для забезпечення ЦІ є значно більшим обсягом контейнера в порівнянні з обсягом повідомлення. Але цей недолік можна нівелювати, передаючи в якості контейнера корисну інформацію, не критичну до ЦІ.

Про використання методів стеганографії з метою забезпечення ЦІ не прийнято говорити, хоча вони є найбільш ефективними для досягнення поставленої мети.

Антивірусний захист. Однією із загроз ІБ є шкідливі програми, в яких окремим класом виділяються віруси. Їх безліч видів і типів, вони відрізняються між собою способами впливу на різні файли, розміщенням у пам'яті ЕОМ або програмах, об'єктами впливу. Але головна властивість вірусів – здатність до розмноження. Це властивість виділяє їх серед безлічі шкідливих програм і робить найбільш небезпечними.

Одним із найбільш дієвих способів забезпечення ЦІ є добре продуманий і надійний захист від вірусів. Найбільш поширеним способом захисту від вірусів є використання антивірусних програм, яких у даний час достатня кількість. Однак необхідно пам'ятати, що жодна програма не гарантує виявлення невідомого вірусу.

Евристичні сканери, що застосовуються, теоретично можуть виявити невідомі віруси за непрямими ознаками, не завжди дають правильний діагноз. Прикладом подібних помилок можуть служити дві антивірусні програми, які запущені на одному комп'ютері. Практично будь-який користувач стикався з ситуацією, коли файли одного антивірусу приймалися за шкідливу програму іншим антивірусом.

Найкращим засобом захисту від вірусів є використання локальних мереж, які не мають зв'язку з інтернетом. При цьому необхідно жорстко контролювати різні носії інформації з прикладними програмами, за допомогою яких можна занести вірус.

Резервування. Під резервуванням розуміється в даному контексті можливість програмних засобів створювати свої копії в процесі виконання програм. Створюються так звані точки відкоту, до яких програма працювала правильно. Якщо в результаті збоїв або інших причин сталося порушення ходу виконання програми, то вона відкочується до заздалегідь визначеної точки і продовжує своє виконання. Найчастіше точки відкоту створюються користувачем шляхом вибору часу створення такої точки.

Аналіз сучасних методів і засобів контролю цілісності інформації. Перевірку цілісності повідомлення можна проводити двома методами. До першого методу належать контрольна сума, в якій виділяються безпосередньо контрольна сума і хеш сума. До другого методу – цифровий підпис.

Контрольна сума. Під терміном "контрольна сума" розуміється метод перевірки цілісності прийнятої інформації на приймальній стороні. Суть контрольної суми полягає в діленні повідомлення на деяку, заздалегідь визначену константу, де сумою виступає залишок від ділення. Найбільш проста контрольна сума – перевірка на парність, що відповідає діленню на два. Зазвичай в якості дільника використовують поліноми 8, 16 або 32 ступенів.

Контрольною сумою може бути перевірка на парність різних комбінацій переданих біт. У цьому випадку можна говорити не тільки про виявлення помилок, а й про їх виправлення. Цей принцип лежить в основі систем завадостійкого кодування, що дозволяє відновлювати як поодинокі, так і кратні помилки в прийнятих повідомленнях. В цьому випадку можна говорити не тільки про контроль цілісності, а й про забезпечення цілісності.

Подальшим розвитком контрольних сум стало використання хеш функцій, які мають деякі відмінності від перевірки на парність. Найголовніша відмінність – це наявність лавинного ефекту, коли результат застосування хеш функції залежить від кожного біта повідомлення. Окрім цього, ці функції мають постійний розмір, незалежно від довжини повідомлення, обчислювальне неможливо згенерувати два різних повідомлення з однаковими хешами, обчислюванням неможливо відновити повідомлення зі значення хешу.

У деяких випадках як хеш функції використовуються алгоритми блокового шифрування, при цьому значення хешу залежатиме не лише від самого повідомлення, але й від секретного ключа, використовуваного в алгоритмі шифрування.

Електронний підпис. Електронний підпис – це механізм перевірки ЦІ, котра приймається. Електронний підпис – електронні дані, які додаються підписувачем до других електронних даних або логічно з ними пов'язуються і використовуються ним як підпис [18]. Документ, який підписується, представляється у відкритому вигляді, тобто незашифрованим. На стороні відправника обчислюється хеш документа, який необхідно передати. Отриманий хеш шифрується за допомогою особистого ключа відправника і відсилається разом із документом, що передається. На приймальній стороні обчислюється хеш документа, розшифровується отриманий разом з документом хеш за допомогою відкритого ключа і порівнюються два отриманих хеша. Якщо вони збігаються, то документ у процесі передачі не був спотворений, в іншому випадку він відкидається.

Головною проблемою отримання пари ключів є знаходження простих чисел великої розмірності, на яких ґрунтується побудова асиметричної системи шифрування. Нині розміри ключів сягають чотирьох кілобіт, що відповідає десятковим числам розміром приблизно в 1300D. Це означає, що прості числа, які використовуються які основа системи, повинні мати розмір не менше 650D. Побудова простих чисел таких розмірів складна обчислювальна задача. У працях [19–21] пропонується підхід до побудови простих чисел великої розмірності.

Аналіз сучасних методів і засобів відновлення цілісності інформації. Завадостійке кодування. Найуразливішою інформація буває в процесі її передачі. Це можна пояснити тим, що така міра забезпечення ЦІ, як розмежування доступу знімає багато загроз, але вона неможлива у використанні в каналі зв'язку бездротових ліній. Інформація найбільш вразлива саме на таких ділянках ІКС. Очевидно, що при навмисному впливі на сигнал, котрий передається, забезпечити ЦІ неможливо. Для виправлення помилок, що виникли в результаті природних явищ, технічних збоїв, використовується завадостійке кодування інформації (ЗКІ).

Вивчення ЗКІ почалося практично відразу після виходу в світ праці [22]. Найбільш відомими в нашій країні є дослідження [23–25], де представлені й проаналізовані різні методи ЗКІ. Головною ідеєю виправлення помилок, що виникають у процесі передачі, є введення надмірності в повідомлення, що передається. Чим більше необхідно виправити помилок, тим більшою має бути надмірність.

Нині все більшу популярність завойовує "м'яке" декодування, яке ґрунтується на спільному конструюванні коду й багатьох сигнальних точок.

Така сигнально кодова конструкція забезпечує вищу ефективність і більший енергетичний виграш від кодування, ніж послідовне застосування ЗКІ і модуляції [26].

У працях [27–28] запропоновано та обґрунтовано метод забезпечення ЦІ в системах передачі інформації, що базується на контролі парності в мініблоках та контрольній сумі. Даний метод найбільш ефективний під час роботи з кратними помилками, має високу швидкість відновлення інформації.

Резервування. Даний метод забезпечення ЦІ використовується в основному при передачі і зберіганні інформації. Під час передачі можливий багатократний повтор повідомлення в один напрям або розсилка повідомлень в усі можливі напрями. Даний підхід можна розглядати як один із методів ЗКІ.

При зберіганні ідея резервування досить проста – створення копій отриманих файлів та їх зберігання окремо від первинних документів. Найчастіше такі сховища створюються в географічно рознесених місцях. Як приклад можна розглянути сучасні хмарні технології.

Одним із головних недоліків резервування інформації є підвищення можливості її несанкціонованого зняття, тому що інформація, яка розміщується на зовнішніх пристроях зберігання, є незахищеною.

Антивірусний захист. На відміну від застосування антивірусного захисту при забезпеченні ЦІ за якого антивірусна програма виявляє вірус до моменту зараження, в даному випадку ці засоби виступають як засоби відновлення інформації. Якщо в результаті сканування виявляється файл, пошкоджений вірусом, то в багатьох випадках такі файли відновлюються. Відновлення відбувається шляхом знищення коду віруса, який був поміщений у тіло файлу і на його місце переписується оригінальний код. У деяких випадках файл відновленню не підлягає, і він поміщається в карантин. Відновлення таких файлів можливо тільки за рахунок резервування.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. Аналіз, який був представлений в роботі, показує, що в сучасній спільності вчених і практиків немає однозначного тлумачення багатьох термінів. Виходячи з цього, можна зробити висновок про необхідність уніфікованого тлумачення термінів. Це дозволить тісніше спілкуватися представникам різних напрямків.

Модель цілісності і загроз в ІКС дозволяє усвідомити місце ЦІ в сучасних системах. В даний час порушення ЦІ є найбільш небезпечним впливом на всі системи, включаючи і критичні. Для забезпечення ЦІ використовуються як організаційні, так і технічні методи і засоби. Побудова систем ТЗІ, з економічної точки зору, є збитковою. Проте вартість цих систем захисту в багато разів може бути менше, ніж можливі збитки, що можуть бути завдані в результаті атак.

В роботі наведені можливі методи і засоби забезпечення та контролю ЦІ. Серед них можна виділити як добре відомі методи (наприклад, завадостійкого кодування), так і методи, які порівняно рідко використовуються для забезпечення ЦІ (стеганографія). Аналіз, який було проведено, показує різноманітність форм і методів побудови систем забезпечення ЦІ.

Список використаних джерел:

1. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги [Чинний від 2015.12.18]. – Київ: Держспоживстандарт України, 2016. – 22 с.
2. Шеннон К. Работы по теории информации и кибернетике. / К. Шеннон – М. : Изд-во иностранной литературы, 1963. 830 с.
3. Kharchenko V. S. Multiversion Systems: Models, Reliability, Design Technologies // Proceeding of 10th European Conference on Safety and Reliability, Munich, Germany, 13-17 September, 1999, vol. 1. – P. 73–77.
4. ISO/IEC 2382:2015. Information technology. Vocabulary [Електронний ресурс] – Режим доступа: https://www.iso.org/standard/63598.html – 3.01.2018 р.
5. Певнев В. Я. Методы обеспечения целостности информации в инфокоммуникационных системах / В. Я. Певнев // Вісник Національного технічного університету “ХПІ”. Серія: Техніка та електрофізика високих напруг. - 2015. - № 51. - С. 74-77.
6. Karlsson J. Routing Security in Ad-hoc Networks / J. Karlsson, L. S. Dooley, G. Pulkkis // Issues in Informing Science and Information Technology. Vol. 9. – 2012. P. 369–383.
7. Luna, J. Leveraging the Potential of Cloud Security Service-Level Agreements through Standards [Text] / J. Luna, N. Suri, M. Iorga and A. Karmel // IEEE Cloud Computing. – 2015. – Vol. 2, Issue 3. – P. 32–40. doi: 10.1109/mcc.2015.52
8. Juliadotter, N. Cloud Attack and Risk Assessment Taxonomy [Text] / N. Juliadotter, K. Choo // IEEE Cloud Computing. – 2015. – Vol. 1, Issue 2. – P. 14–20. doi: 10.1109/mcc.2015.2
9. Комаров М. Ю. Аналіз і дослідження загроз для захищеного вузла інтернет доступу / М. Ю. Комаров, С. Ф. Гончар // Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія : Технічні науки. – 2018. – Т. 29 (68), № 4 (1). – С. 165–168.
10. Цуранов М. В., Струков В. М., Пєвнєв В. Я. Методи та засоби боротьби з правопорушеннями в інформаційної сфері : навч посібник. / Цуранов М. В., Струков В. М., Пєвнєв В. Я. – Харків : ХНУВС, 2015. – 256 с.
11. Проскурин В. Г., Крутов С. В., Мацкевич И. В. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных система : учеб.пособие для вузов / Проскурин В. Г., Крутов С. В., Мацкевич И. В. – М. : Радио и связь. 2000. – 168 с

12. Захист інформації. Технічний захист інформації. Терміни і визначення: ДСТУ 3396.2-97. – [Чинний від 1998.01.01]. – К. : Держстандарт України, 1998. – 20 с.

13. Кравченко В. И. Оружие на нетрадиционных принципах: Электромагнитное оружие / В. И. Кравченко – Харків : НТУ "ХПИ", 2009. – 266 с.

14. Смирнов М., Ватолин Д., Ратушняк А., Юкин В. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео./ М. Смирнов, Д. Ватолин, А. Ратушняк, В. Юкин. – М.: Диалог-МИФИ. 2002. – 384 с.

15. Певнев В. Я. Построение оптимальных кодовых таблиц / В. Я. Певнев, М. В. Цуранов // Системи обробки інформації. – 2012. – № 4(102). – С. 56–59.

16. Tsuranov M. The Method of Data Integrity Assurance for Increasing IoT Infrastructure Security / V. Pevnev, Y. Novakov, M. Tsuranov, V. Kharchenko// InfoTech-2017: proc. of the 31 th IC on Information Technologies (September 20-21, 2017, Sofia). Sofia: 2017. – P. 27–36

17. Oleshchenko V. Development of digital steganography techniques for copyright protection, based on the watermark / V. Oleshchenko, V. Pevnev // Сучасні інформаційні системи. – 2017. – Т. 1, № 1. – С. 57–60.

18. Про електронні довірчі послуги: Закон України від 05.10.2017 №2155-VIII. [Електронний ресурс]. – Режим доступа : https://zakon.rada.gov.ua/laws/show/2155-19/ed20171005 – 3.01.2018 р.

19. Певнев В. Я. Методика построения псевдопростых чисел / В. Я. Певнев // Системи обробки інформації. – 2016. – № 3(140). – С. 30–34.

20. Генератор простых чисел. Кафедра систем інформації: Зб. наукових праць / Певнев В. Я. – Харків : ТОВ "Щедра садиба плюс", 2014. – С. 140–146.

21. Pevnev V. Pseudoprime Numbers: Basic Concepts and the Problem of Security / V. Pevnev // ICTERI Applications: Integration, Harmonization and Knowledge Transfer: proc. 13th Int. Conf. ICTERI 2017 (May 15-18, 2017, Kyiv). CEUR-WS.org, online-c.583-593

23. Шеннон К. Е. Математическая теория связи. Работы по теории информации и кибернетики / К. Е. Шеннон //– М.: ИЛ. 1963. – 476 с.

24. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки / У. Питерсон, Э. Уэлдон // – М. : Мир, 1976. – 594с.

25. Галлагер Р. Теория информации и надежная связь / Р. Галлагер // – М. : Сов. радио, 1974. – 568 с.

26. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение / Р. Морелос-Сарагоса // – М. : Техносфера. 2005. – 320 с.

27. Пєвнєв В. Я. та ін. Спосіб відновлення інформації при обміні даними у телекомунікаційних системах. – Патент на корисну модель № 26778, МПК HO4L 12/00, заяв. 23.04.07, опубл. 10.10.2007, Бюл. No 16.

28. Пєвнєв В. Я. Теоретичне обґрунтування методу відновлення повідомлення, прийнятого з помилками / В. Я. Пєвнєв, М. В. Цуранов // Системи обробки інформації. – 2013. – № 2 (109). – С. 194–196.

References:

1. DSTU ISO/IEC 27001:2015 Metody zakhystu systemy upravlinnya informatsiynoyu bezpekoyu. [Chynnyy vid 2015-12-18]. Vyd. ofits. Kyyiv, DP "UkrNDNTS" 2016. 22 p.

2. Shennon K. Raboty po teorii informatsii i kibernetike. M.: Izd-vo inostrannoy literatury, 1963. 830 p.

3. . Kharchenko V. S. Multiversion systems: Models, Reliability, Design Technologies: Proc. 10th European Conference of Safety and Reliability. Munich, 1999. P. 73–77.

4. ISO/IEC 2382:2015, Information technology – Vocabulary https://www.iso.org/standard/63598.html

5. Pevnev V. Ya. Metody obespechenyya tselostnosty ynformatsyy v ynfokommunykatsyonnykh systemakh. Visnyk NTU "KHPI". Seriya: Tekhnika ta elektrofizika vysokykh napruh. Kharkiv, 2015. № 51. P. 74–77

6. Karlsson J., Dooley L. S., Pulkkis G. Routing Security in Ad-hoc Networks. IISIT in Informing Science and Information Technology. 2012. Vol. 9. P. 369–383

7. Luna J., Suri N., Iorga M., Karmel A. Leveraging the Potential of Cloud Security Service-Level Agreements through Standards IEEE Cloud Computing. 2015. Vol. 2. Issue 3. P. 32–40.

8. Juliadotter N., Choo K. Cloud Attack and Risk Assessment Taxonomy.IEEE Cloud Computing. 2015. Vol. 1, Issue 2. P. 14–20.

9. Komarov M. Yu., Honchar S. F Analiz i doslidzhennya zahroz dlya zakhyshchenoho vuzla Internet dostupa. Informatyka, obchyslyuval′na tekhnika ta avtomatyzatsiya. Tom 29 (68). CH. 1 № 4. 2018. P. 165–168.

10. Tsuranov M. V., Strukov V. M., Pevnev V. Ya.. Metody ta zasoby borot′by z pravoporushennyamy v informatsiynoyi sferi: navch posibnyk. Kharkiv: KHNUVS, 2015. – 256 p.

11. Proskurin V. G., Krutov S. V., Matskevich I. V. Programmno-apparatnyye sredstva obespecheniya informatsionnoy bezopasnosti. Zashchita v operatsionnykh sistemakh: Ucheb.posobiye dlya vuzov M.:Radio i svyaz'. 2000. 168 p.

12. DSTU 3396.2-97. Zakhist ínformatsíÿ. Tekhníchniy zakhist ínformatsíÿ. Termíni ta viznachennya. [Chynnyy vid 1998.01.01]. Vyd. ofits. Kyyiv, DERZHSTANDART UKRAYINY 1997. 22 p.

13. Kravchenko V. I. Oruzhiye na netraditsionnykh printsipakh: Elektromagnitnoye oruzhiye. Kharkív: NTU "KHPI", 2009. 266 p.

14. Smirnov M., Vatolin D., Ratushnyak A., Yukin V. Metody szhatiya dannykh. Ustroystvo arkhivatorov, szhatiye izobrazheniy i video. M. : Dialog-MIFI. 2002. P. 384.

15. Pevnev V., Tsuranov M. The construction of the optimal code tables. Systemy obrobky informatsiyi. 2012. № 3 (108), p. 27–30.

16. Pevnev V., Novakov Y., Tsuranov M, Kharchenko V. The Method of Data Integrity Assurance for Increasing IoT Infrastructure Security. InfoTech-2017: proceedings of the 31 th IC on Information Technologies. Sofia, 2017. P. 27–36.

17. Oleshchenko V, Pevnev V. Development of digital steganography techniques for copyright protection, based on the watermark. Advanced information systems. 2017. № 1. P. 57–60.

18. Pro elektronni dovirchi posluhy: Zakon Ukrayiny vid 05.10.2017 №2155-VIII. Vidomosti Verkhovnoyi Rady Ukrayiny. 2017 r., № 45. P. 400

19. Pevnev V. Ya. Metodyka postroenyya psevdoprostykh chysel Systemy obrobky informatsiyi. 2016. № 140 (3). P. 30–34.

20. Pevnev V. Ya. Henerator prostykh chysel. Kafedra system ynformatsyy: sb. nauch. tr. Khar′kov, 2014. P. 140–146.

21. Pevnev V. Pseudoprime Numbers: Basic Concepts and the Problem of Security. ICTERI Applications: Integration, Harmonization and Knowledge Transfer: proc. 13th Int. Conf. ICTERI 2017 (Kyiv, May 15–18, 2017), CEUR-WS.org, online – C. 583–593

22. Matskevich I. V. M. :Radio i svyaz'. 2000. P.168

23. Shennon K. Ye. Matematicheskaya teoriya svyazi. Raboty po teorii informatsii i kibernetiki. M.: IL. 1963. P.476

24. Piterson U., Ueldon E. Kody, ispravlyayushchiye oshibki. M. : Mir, 1976. P.594

25. Gallager, R. Teoriya informatsii i nadezhnaya svyaz’. M. : Sov. radio, 1974. P. 568

26. Morelos-Saragosa R. Iskusstvo pomekhoustoychivogo kodirovaniya. Metody,algoritmy, primeneniyeM.: Tekhnosfera. 2005. P.320.

27. Pevnev V.YA. Sposíb vídnovlennya ínformatsíЇ pri obmíní danimi u telekomunікatsíynikh sistemakh / Pêvnêv V. YA. i dr. // D.p. № 26778. Byul., 2007. – № 16.

28. Pevnev V. Ya., Tsuranov M. V. Teoretichne obg̀runtuvannya metodu vídnovlennya povídomlennya, priynyatogo z pomilkami. Sistemi obrobki ínformatsíЇ . 2013. № 2 (109). P. 194–196.