2. Копытов Е., Иванова С., Птицина И. *Структуры данных и их обработка на компьютере: Учебное пособие/* Под ред. Е. Копытова. Рига: Институт транспорта и связи, 2003. 128 с.

3. В. Столлингс Криптография и защита сетей: принципы и практика, 2-е изд. : пер. с англ. — М.: издательский дом «Вильям», 2001. — 672 с.

4. Шефановский Д.Б. ГОСТ Р 34.11- 94. Функция хеширования. Краткий анализ.

5. ГОСТ Р 34.11- 94. "Информационная технология. Криптографическая защита. Функция хеширования".

6. M. Bellare, R. Canetti, and H. Krawczyk. Keying hash functions for message authentication. Advances in Cryptology - Crypto 96 Proceedings, Lecture Notes in Computer Science Vol. 1109, N. Koblitz ed, Springer-Verlag, 1996.

7. Євсеєв С.П., Чевардин В.Е., Радковский С.А. Механизмы обеспечения аутентичности банковских данных во внутриплатежных системах комерческого банка. / Збірник наукових статей ХНЕУ. – Харків: ХНЕУ. – 2008. – Вип. 6. – С. 40-44.

8. Кузнецов А.А., Король О.Г., Ткачов А.М. Анализ механизмов обеспечения безопасности банковской информации во внутриплатежных системах коммерческого банка / Матеріали І міжнародної науково-практичної конференції «Безпека та захист інформації в інформаційних і телекомунікаційних системах» 28 – 29 травня 2008 р. Зб. наук. статей «Управління розвитком». ХНЕУ. № 6 – Х.: 2008. – С. 28 – 35.

9. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 2.5-004-99.— [Чинний від 1999-28-04].]. — К. : Держспоживстандарт України 1999. — 53 с.

10. http://www.cryptopro.ru

11. http://e-signature.com.ua

12. http://www.ict.com.ua

13. http://www.vano-zhuk.narod.ru

14. http://bezpeka.ladimir.kiev.ua

15. http://www.infocity.kiev.ua

16. http://www.jetinfo.ru/2005/10/1/article1.9.200518.html

УДК 629.07.5

Дудикевич[1] В.Б., Томашевський[2] Б.В., Сергієнко[2] Р.В.

[1]Національний університет "Львівська Політехніка"
[2]Львівський Військовий інститут
Сухопутних військ імені гетьмана Петра Сагайдачного

ПРОТОКОЛИ І МЕХАНІЗМИ БЕЗПЕКИ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ І МЕРЕЖАХ

В умовах стрімкої інформатизації суспільства, широкого застосування засобів обчислювальної техніки і комп'ютерних систем особливої актуальності набувають питання інформаційної безпеки, найбільш складними з яких є необхідність захисту цінної конфіденційної і секретної інформації в державних і приватних підприємствах, в органах і установах державного управління, у банківській і інших системах [1-5].

Задля безпеки (автентичності, конфіденційності і цілісності) інформації з обмеженим доступом застосовуються різні криптографічні послуги і механізми безпеки [3-6].

Метою статті є аналіз існуючих протоколів і механізмів забезпечення автентичності,

конфіденційності і цілісності інформації в комп'ютерних системах і мережах, обґрунтування перспективних напрямів у розвитку криптографічних перетворень у ділянці безпеки сучасних інформаційних технологій.

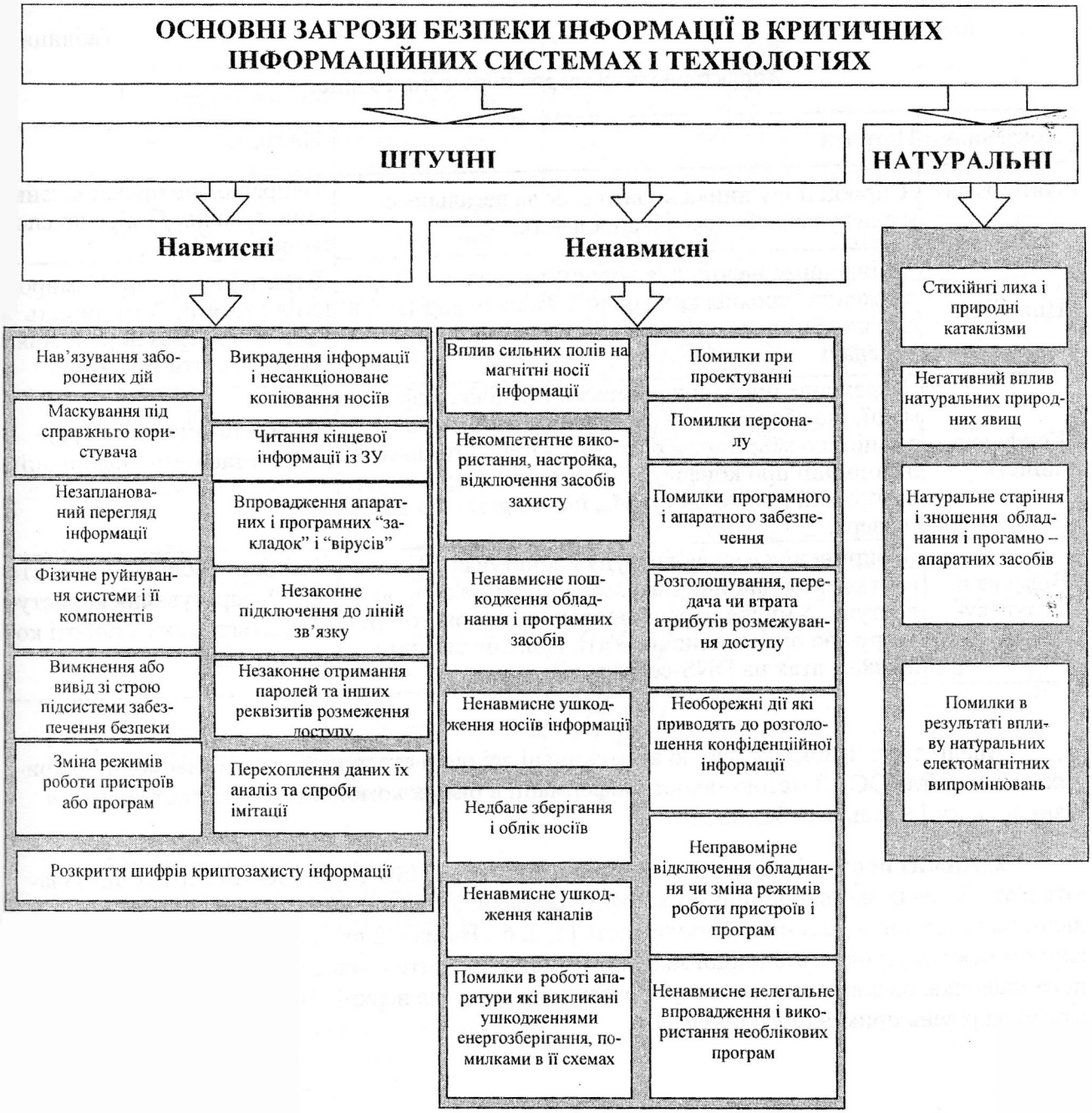
1. Аналіз загроз безпеці інформації. Збільшення об'ємів обробки і передачі інформації в комп'ютерних системах і мережах, перш за все, у банківських системах, у системах управління великими фінансовими і промисловими організаціями, підприємствами енергетичного сектору, транспорту, в системах управління і зв'язку військового призначення вимагає нових підходів до протоколів і механізмів забезпечення безпеки у процесі передачі даних.

Вимога до безпеки і достовірності оброблюваної і передаваної інформації в таких системах є дуже суворими, оскільки відмова системи або вихід за встановлені обмеження вказаних власти-востей може привести до значних фінансових і матеріальних втрат, зниження обороноздатності країни, збитків екологічного характеру, загрози життю і здоров'ю людей.

Доведено [8 - 10], що за останній час загальний об'єм оброблюваної і передаваної інформа-ції в комп'ютерних системах і мережах зріс у багато разів (збільшується на два-три порядки кожні п'ять-десять років) і загальні тенденції свідчать, що така динаміка зберігається. Сучасні криптографічні засоби захисту інформації повинні забезпечувати своєчасну обробку величезних об'ємів даних (десятки-сотні Мбіт/с) і відповідати жорстким вимогам щодо достовірності і безпеки інформації. В умовах великої кількості різнотипних джерел інформації і можливої швидкої компрометації секретних ключових даних найбільш доцільним є використання криптографічних засобів, що допускають функціонування в інфраструктурі відкритих ключів.

Крім того, сучасний розвиток інформаційних технологій, високий рівень комп'ютеризації і інформатизації суспільства зумовили виникнення нових погроз безпеці інформації [1-5].

Загальна класифікація загроз безпеці інформації в комп'ютерних системах і мережах представлена на мал. 1. В процесі зберігання і обробки інформація може зазнавати дії чинників, як випадкових, так і навмисних. Найчастішими і найнебезпечнішими щодо розміру збитку є ненавмисні помилки користувачів, операторів, системних адміністраторів та інших осіб, що обслуговують інформаційні системи у процесі обробки і передачі інформації. Відповідно до статистики 65% втрат - наслідок ненавмисних помилок [5 - 7]. Особливу небезпеку останнім часом набули навмисні загрози, реалізація яких доступна терористичним групам і організаціям [6, 7]. Потенційною мішенню злочинних намірів можуть служити інформаційні системи міністерства оборони та інших силових структур, системи управління атомних, хімічних і інших небезпечних виробництв, обчислювальні системи банків і великих промислових підприємств.



Мал. 1. Загрози інформації в компютерних системах і мережах

Для запобігання ненавмисним і навмисним погрозам необхідні спеціальні засоби ідентифікації користувачів в мережі, що забезпечують доступ до інформації лише у разі повної упевненості в наявності у користувача прав доступу до неї.

У табл. 1 приведений взаємозв'язок механізмів забезпечення безпеки і основних типів загроз порушення захисту, що виникають при використанні комп'ютерних систем і мереж.

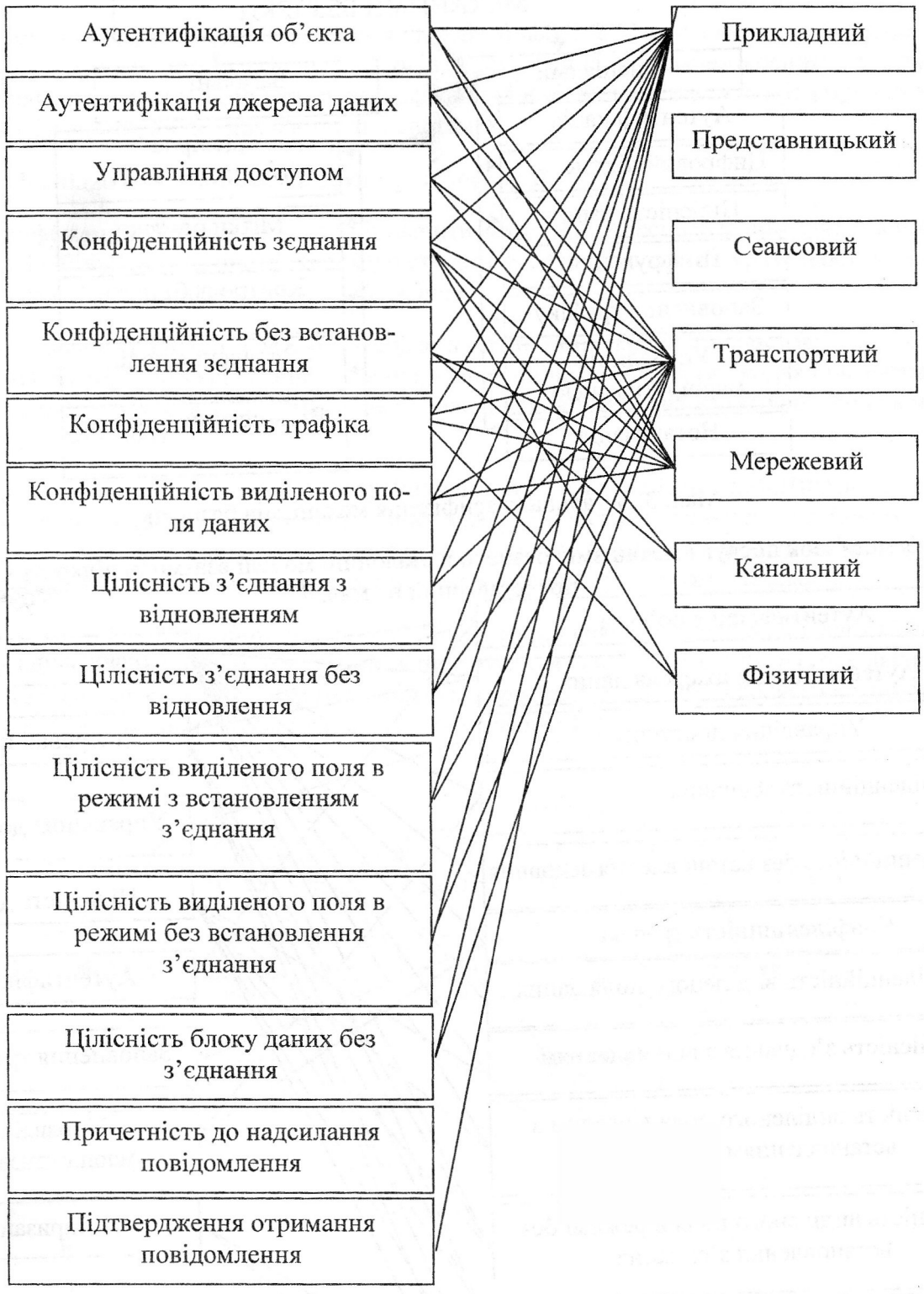
Таблиця 1

Характеристики загроз порушення захисту

Показники	Погрози	Наслідки
Автентифікація	Спроби порушника видати себе за легального користувача. Фальсифікація даних.	Неправильне представлення користувачів. Довіра до спотворених даних .
Цілісність	Зміна призначених для користувача даних. Впровадження "троянських коней". Зміна інформації в пам'яті. Зміна потоку повідомлень на шляху їх передачі	Втрата інформації Компрометація системи. Уразливість відносно погроз порушення захисту решти всіх типів
Конфіденційність	Перехоплення даних в мережі. Крадіжка інформації, що зберігається на сервері. Крадіжка інформації, що зберігається на комп'ютері. Отримання інформації про конфігурацію мережі. Отримання інформації про користувача, що звертається до сервера.	Втрата інформації. Порушення таємниці інформації
Відмова в обслуговуванні	Припинення сеансу доступу користувача. Перевантаження машини потоком фальшивих спроб доступу. Умисне переповнювання дискового простору або оперативної пам'яті. Ізоляція системи шляхом атак на DNS-сервер.	Руйнівні наслідки для системи. Роздратування користувачів. Затримки в роботі користувачів.

Аналіз табл. 1 показує, що до атак схильні всі рівні еталонної моделі взаємодії відкритих систем (ЕМВОС). З метою захисту інформації в різних комбінаціях використовуються різні послуги і механізми безпеки.

2. Аналіз послуг і механізмів безпеки. Стандарти ISO 7498, ISO/IEC 10181 визначають п'ять базових загальноприйнятих послуг безпеки: автентифікація, конфіденційність, цілісність, управління доступом і причетність [1, 2, 6]. На мал. 2 представлений розподіл послуг безпеки за рівнями еталонної моделі взаємодії відкритих мереж. Як випливає з наведеного малюнка, велика частина послуг безпеки припадає на верхні рівні моделі ЕВОС, переважно на рівень прикладного процесу.

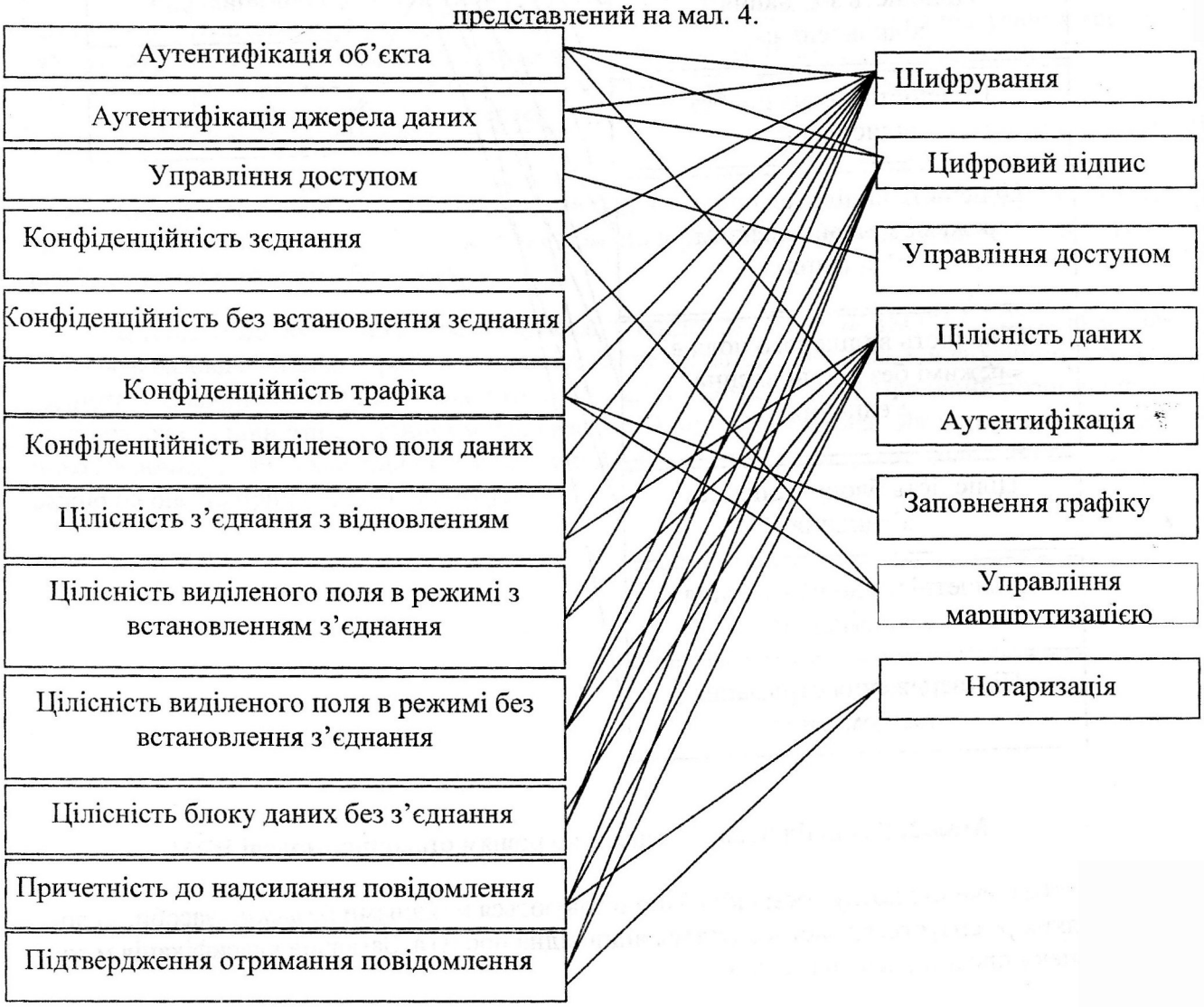


Мал.2. Розподіл послуг безпеки по рівням еталонної моделі ВВМ

Для забезпечення послуг безпеки використовуються механізми *безпеки* - засоби, за допомогою яких реалізується і застосовується відповідна послуга. Загальна класифікація механізмів безпеки представлена на мал. 3.

Мал. 3. Загальна класифікація механізмів безпеки

Взаємозв'язок послуг і механізмів безпеки в еталонній моделі взаємодії відкритих мереж представлений на мал. 4.



Мал. 4. Взаємозв'язок послуг і механізмів безпеки

Таким чином, як показав проведений аналіз, більшість послуг і механізмів безпеки реалізуються на основі криптографічних методів перетворення. Розглянемо основні протоколи, що забезпечують конфіденційність, автентифікацію і цілісність передаваної інформації в критичних інформаційних і комп'ютерних системах.

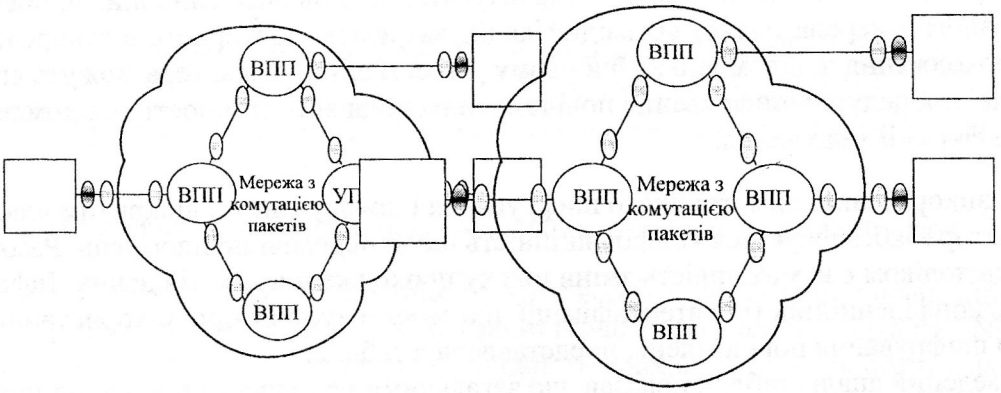
3. Дослідження протоколів захисту інформації.

Конфіденційність покликана забезпечити захист в процесі передачі даних від пасивних атак. Найбільш загальним підходом до створення безпеки в точках уразливості комп'ютерних мереж (КМ) є використання *шифрування*.

При передачі даних в КМ з комутацією пакетів, як правило, використовується або канальне шифрування, або крізне шифрування, засновані на симетричних кодах (алгоритми CAST-128, IDEA або 3DES. На мал. 5 представлені основні можливості шифрування в мережі з комутацією пакетів.

Для протидії порушенням захисту використовується *канальне* і *наскрізне шифрування*. При *канальному шифруванні* весь потік даних в каналі виявляється захищеним. Одним з недоліків є необхідність дешифрування пакету даних при кожному його проходженні через пакетний перемикач, при цьому повідомлення стає вразливим у кожному перемикачі.

При *наскрізному шифруванні* процес шифрування виконується тільки в двох кінцевих системах. Істотним недоліком є відсутність шифрування всього потоку даних, оскільки заголовки пакетів передаються у відкритому вигляді (протокол X.25). Щоб досягти кращого захисту, потрібне як канальне, так і наскрізне шифрування [5].



Мал. 5. Основні можливості шифрування в мережі з комутацією пакетів

- пристрій наскрізного шифрування

- пристрій канального шифрування

ВПП - вузол перемикання пакетів

При використанні обох форм шифрування провідний вузол шифрує порцію пакету даних, використовуючи ключ наскрізного шифрування. При русі пакету по мережі кожен світч розшифровує заголовок, а потім знову шифрує весь пакет. Проте у момент часу, коли пакет знаходиться в пам'яті світча, заголовок пакету є відкритим. Стосовно моделі взаємодії відкритих систем це означає, що канальне шифрування здійснюється або на фізичному рівні, або на рівні ланки передачі (канальному рівні). При наскрізному шифруванні функцію шифрування можна розмістити на мережному рівні. Розміщення засобів шифрування в протоколах наскрізної передачі даних, наприклад у протоколах мережного рівня X.25 або TCP забезпечує наскрізну безпеку передачі даних у рамках будь-якої окремо даної мережі. Проте таке шифрування не може забезпечити необхідну безпеку для обміну даними між мережами, наприклад, при використанні електронної пошти, електронного обміну даними або при передачі файлів.

Тому для додатків типу електронної пошти єдиною можливістю для розміщення засобів наскрізного шифрування є рівень додатків. Недоліком шифрування на рівні додатків є створення і розподіл величезної кількості секретних ключів.

Автентифікація гарантує, що повідомлення дійсно поступило з передбачуваного джерела, а також захист від модифікацій, затримок, повторного відтворення і зміни порядку проходження повідомлень [4, 5]. Для забезпечення автентифікації використовуються алгоритми *шифрування, цифровий підпис, коди автентичності повідомлення (MAC) і функції хешування.* Розглянемо механізми і протоколи, що забезпечують автентифікацію повідомлень, докладніше.

Одним з важливих засобів *автентифікації* є *цифровий підпис,* що забезпечує заходи протидії можливості оспорити джерелом або адресатом факт відправки і отримання повідомлення. Крім того, автентифікація здатна гарантувати, що повідомлення дійсно поступило з передбачуваного джерела, захист від модифікацій, затримок, повторного відтворення і зміни порядку проходження повідомлень. При цьому у якості автентифікатора можуть використовуватися такі процедури: шифрування повідомлення, коди автентичності повідомлення (MAC) або функції хешування.

При використанні симетричного шифрування і шифрування з відкритим ключем як автентифікатора забезпечується конфіденційність щодо передачі повідомлень. Разом з тим, загальним недоліком є неможливість зміни шляху проходження пакетів даних. Інформація про ступінь конфіденційності і автентифікації, що забезпечується при використанні різних підходів до шифрування повідомлень, представлена в табл. 2.

Проведений аналіз табл. 2 показав, що загальними недоліками при використанні симетричного шифрування і шифрування з відкритим ключем є неможливість зміни шляху проходження пакетів даних, і відкритий доступ до всієї порції даних при її обробці в проміжних блоках (маршрутизаторах, шлюзах і т. ін).

Альтернативним варіантом автентифікації є MAC-коди (криптографічна контрольна сума, або код автентичності повідомлення **MAC** (MAC - Message Authentication Code).- невеликий блок даних фіксованого розміру, що приєднується до повідомлення, і створюваний з використанням секретного ключа. При цьому забезпечується тільки автентифікація, оскільки повідомлення передається у відкритому вигляді.

Таблиця 2

Конфіденційність і аутентифікація повідомлень при шифруванні

Симетричне шифрування (A→B: E_K [M])
забезпечує конфіденційність - тільки сторони А і В знають ключ К (секретний ключ).
Забезпечує певний рівень аутентифікації: джерелом може бути тільки сторона А; зміни на шляху проходження неможливі; потрібне форматування /надлишковість.
Не забезпечує ЦП: одержувач має можливість фальсифікувати отримане повідомлення; абонент має можливість заперечувати відправку повідомлення.
Шифрування з відкритим ключем (A→B: E_{KR_a} [M])
Забезпечує конфіденційність - тільки сторона В має закритий ключ (Krb), щоб розшифрувати повідомлення
Не забезпечує аутентифікацію - будь-який абонент може скористатися відкритим ключем (Kub), щоб оголосити себе абонентом А.
Шифрування з відкритим ключем (A→B: E_{KR_a} [M])
Забезпечує аутентифікацію і цифровий підпис: тільки сторона А має закритий ключ (KRa), щоб зашифрувати повідомлення; зміни на шляху проходження неможливі; потрібне форматування /надлишковість; хто завгодно може використовувати відкритий ключ (RUa), щоб перевірити підпис.
Шифрування з відкритим ключем (A→B: E_{KU_b} [E_{KU_a} M])
Забезпечує конфіденційність і цифровий підпис, оскільки використовується відкритий ключ (KUb) Забезпечує автентифікацію і підпис, оскільки використовується закритий ключ (Kra)

Прикладом може служити **протокол SNMP** версії 3, де функції конфіденційності і автентифікації розділяються. У цьому застосуванні гарантується автентифікація SNMP-повідомлень, що поступають, водночас необхідність приховувати потік обміну даними SNMP може бути зайвою.

Варіацією ідеї використання коду автентичності повідомлень є *одностороння функція хешування,* що забезпечує автентифікацію, цифровий підпис і конфіденційність.

Здатність функції хешування протистояти атакам з перебором усіх варіантів залежить виключно від довжини хеш-коду, що породжується алгоритмом. Одними з перспективних алгоритмів хэш-функцій є Sha-1 і Ripemd-160. Основні їх характеристики представлені в табл. 3 у порівнянні з алгоритмом хеш-функції Md-5. Всі три алгоритми невразливі відносно атак, заснованих на порушенні слабкої опірності колізіям. При 128-бітовій довжині Md-5 алгоритм вельми вразливий до атак, спрямованих на порушення сильної опірності колізіям, в цій ситуації використовують парадокс про дні народження, тоді як Sha-1 і Ripemd-160 виявляються надійними в перспективі передбачуваного майбутнього.

Таблиця 3

Основні характеристики алгоритмів хеш-функцій

Параметри	MD-5	SHA-1	RIPEMD-160
Довжина профілю	128 бітів	160 бітів	160 бітів
Базова довжина блоків які обробляються	512 бітов	512 бітов	512 бітов
Число кроків	64 (4 раунди по 16 кроків)	80 (4 раунди по 20 кроків)	160 (5 спарених раунду по 16 кроків)
Максимальна довжина повідомлення	–	2^{64} - 1 бітів	2^{64} - 1 бітів
Число прим. логічних функцій	4	4	5
Число аддітивних констант	64	4	9
Порядок проходження бітів	Прямий	Зворотній	Прямий

Таким чином, MD-5 значно схильний до криптоаналізу. Разом з тим, додаткова складність SHA-1 і RIPEMD-160 приводить до уповільнення обробки алгоритмів.

Функція хешування типу MD-5не була розроблена для використання для обчислення значень MAC, оскільки не залежить від секретного ключа. Подальшим її застосуванням, прийнятим у якості обов'язкового алгоритму в протоколі безпеки IP, є **алгоритм HMAC**.

Алгоритм HMAC забезпечує гарантовану захищеність за умови, що вбудована функція хешування володіє певною криптографічною стійкістю.

Для забезпечення тільки функції цифрового підпису використовується **стандарт DSS** (Digital Signature Standards - стандарт цифрового підпису), заснований на алгоритмі хешування SHA.

Алгоритм цифрового підпису **DSA** (Digital Signature Algorithm) створений на основі деко-дування NP-повної завдання обчислення дискретних алгоритмів і спирається на схеми Ель-гамаля і Шнорра. Разом з тим, істотним його недоліком є складність обчислення при піднесенні до ступеня $g^k mod p$.

Для забезпечення автентифікації на кожному сервері використовується **система Kerberos**, що пропонує централізований сервер автентифікації, її функціями є ідентифікація користувачів для серверів і серверів для користувачів. У системі Kerberos використовуються прості протоколи вида-леного доступу *PAP* (Password Authentication Protocol) і *CHAP* (Challenge Handshake Authentication Protocol). Недоліком застосування *PAP* є можливість перехоплення порушником відомостей про пароль. Тому протокол PAP використовується спільно з протоколом *S/key*, заснованому на моделі одноразових паролів, що отримуються послідовним застосуванням еоборотної функції.

До переваг протоколу Kerberos належать швидке під'єднання клієнта до сервера, можливість делегування клієнтом своїх повноважень серверу для виконання запиту, спрощення адміністрування розподіленої КС.

Основними недоліками протоколу є відсутність виділеного каналу зв'язку між об'єктами розподіленої КС, що дозволяє порушникові аналізувати мережний трафік у подібних сис-

темах; можливість взаємодії об'єктів розподіленої КС без встановлення віртуального каналу між ними, що не дозволяє надійно ідентифікувати об'єкт або суб'єкт розподіленої КС і організувати захист передаваної інформації; використання недостатньо надійних протоколів ідентифікації об'єктів розподіленої КС перед встановленням віртуального каналу між ними, що дозволяє порушникові при перехопленні повідомлень видати себе за одну зі сторін з'єднання [5].

Для забезпечення конфіденційності і сервісу автентифікації на прикладному рівні в комп'ютерних системах і мережах використовуються *схеми PGP* (Pretty Good Privacy) і *S/mime* (Secure/multipurpose Internet Mail Extension).

Система S/MIME забезпечує можливість упаковки даних і цифровий підпис, що формується за допомогою шифрування профілю повідомлення, з використанням особистого ключа відправника. У табл. 4. представлені криптографічні алгоритми, використовувані в системі S/MIME.

Таблиця 4

Криптографічні алгоритми в системі S/MIME

Функція	Вимоги
Створення профілю повідомлення, використовуваного при формуванні цифрового підпису	ОБОВ'ЯЗКОВА підтримка SHA-1 і MD-5 РЕКОМЕНДУЄТЬСЯ використання SHA-1
Шифрування профілю повідомлення для формування цифрового підпису	Для агентів відсилання і прийому ОБОВ'ЯЗКОВА підтримка DSS. Для агентів відсилання РЕКОМЕНДУЄТЬСЯ підтримка шифрування RSA. Для агентів прийому РЕКОМЕНДУЄТЬСЯ підтримка верифікації RSA з довжиною ключа від 512 до 1024 бітів
Шифрування сеансового ключа для передачі з повідомленням	Для агентів відсилання і прийому ОБОВ'ЯЗКОВА підтримка алгоритму Діффі-Хеллмана. Для агентів відсилання РЕКОМЕНДУЄТЬСЯ підтримка шифрування RSA з довжиною ключа від 512 до 1024 бітів. Для агентів прийому РЕКОМЕНДУЄТЬСЯ підтримка дешифровки RSA.
Продовження таблиці №4.	
Шифрування повідомлення для передачі з використанням сеансового ключа	Для агентів відсилання РЕКОМЕНДУЄТЬСЯ підтримка шифрування triple DES і RC2/40. Для агентів прийому ОБОВ'ЯЗКОВА підтримка дешифровки triple DES і РЕКОМЕНДУЄТЬСЯ підтримка дешифровки RC2/40.

Розглянемо механізми захисту за допомогою *протоколу IP* (Internet Protocol - протокол міжмережної взаємодії), що забезпечують автентифікацію, конфіденційність і управління ключами. Захист на рівні IP охоплює автентифікацію, конфіденційність і управління ключами. До найбільш серйозних типів атак на мережу TCP/IP належать:

- обман IP, при якому порушники створюють пакети з помилковими IP-адресами і використовують додатки, що пропонують автентифікацію на основі IP;

- різні форми перехоплення інформації і пакетів з даними, коли порушники читали передавану інформацію, включаючи інформацію автентифікації і вміст баз даних.

Для забезпечення захисту обміну даними в локальних мережах (LAN), корпоративних і відкритих глобальних мережах (WAN) і в Internet використовується *протокол IPSec*. Головною властивістю протоколу є можливість шифрування і/або автентифікації *всього* потоку обміну даними на рівні IP.

Ключовим об'єктом в механізмах автентифікації і конфіденційності для IP є захищений зв'язок (Security Association). Зв'язок забезпечує односторонній захист потоку даних на транспортному рівні і використовує при цьому або протокол AH, або ESP.

Таким чином, в будь-якому пакеті IP- захищений зв'язок однозначно ідентифікується адресою одержувача і індексом параметрів захисту (AH або ESP).

Заголовки AH і ESP підтримують два режими використання: транспортний і тунельний. При цьому на транспортному режимі забезпечують захист, перш за все, для протоколів вищого рівня (захист поширюється на корисний вантаж пакету IP). Зазвичай транспортний режим забезпечує наскрізний зв'язок двох головних вузлів (клієнта і сервера або двох робочих станцій). Тунельний режим забезпечує захист всього пакету IP. Для цього після додавання до пакету IP полів AH або ESP весь пакет разом з полями захисту розглядається як корисний вантаж деякого нового "зовнішнього" пакету IP з новим зовнішнім заголовком IP. Увесь оригінальний пакет пересилається без перевірки в маршрутизаторах внутрішнього заголовку IP. Тунельний режим використовується тоді, коли один або обидва кінці захищеного зв'язку є шлюзами захисту (брандмауери або маршрутизатори, засновані на IPSec). У табл. 5 представлені функціональні можливості транспортного і тунельного режимів.

Таблиця 5

Функціональні можливості транспортного і тунельного режимів

Протоколи захисту	Транспортний режим захищеного зв'язку	Тунельний режим захищеного зв'язку
AH	Ідентифікує корисний вантаж IP, а також окремі частини заголовку IP і заголовків розширень IPv6	Ідентифікує весь внутрішній пакет IP (заголовок і корисний вантаж внутрішнього пакету IP), а також окремі частини зовнішнього заголовка IP і зовнішніх заголовків розширень IPv6
ESP	Шифрує корисний вантаж IP і всі заголовки розширень IPv6, наступні за заголовками ESP	Шифрує внутрішній пакет IP
ESP з аутентифікацією	Шифрує корисний вантаж IP і всі заголовки розширень IPv6, наступні за заголовками ESP. Ідентифікує корисний вантаж IP, але не заголовок IP.	Шифрує внутрішній пакет IP. Ідентифікує внутрішній пакет IP.

Автентифікація в протоколах AH і ESP спирається на використання кодів автентичності MAC з довжиною за умовчанням 96 бітів (схеми HMAC-MD5-96 і HMAC-SHA-1-96), а сервіс шифрування полів корисного вантажу, заповнювача, довжини заповнювача і наступного заголовку протоколом ESP використовує алгоритми шифрування: "потрійний" DES з трьома ключами, RC5, IDEA, "потрійний" IDEA з трьома ключами, CAST, Blowfish.

Таким чином, перевагою транспортного режиму є забезпечення конфіденційності для того, хто застосовує цей режим додатку, що дозволяє уникнути необхідності реалізації функцій забезпечення конфіденційності в кожному окремому застосуванні. Недоліком режиму є те, що при його використанні не виключається можливість аналізу трафіку пакетів, що пересилаються.

Тунельний режим виявляється корисним в конфігурації мережі, яка припускає наявність брандмауера або шлюзу захисту, при цьому шифрування використовується тільки для обміну між зовнішнім вузлом і шлюзом захисту.

Одним з найпоширеніших додатків критичних систем, що використовуються в локальних мережах, є web-броузери з графічним інтерфейсом. По суті **World Wide Web** можна інтерпретувати як додаток типу клієнт/сервер, що працює в мережі Internet і внутрішніх мережах підприємств на основі протоколу TCP/IP. Разом з тим, як відмічено в [4, 7], і Internet, і Web достатньо уразливі з погляду загроз різного типу.

У табл. 6 перераховані основні типи загроз порушення захисту, що виникають при використанні Web-технологий.

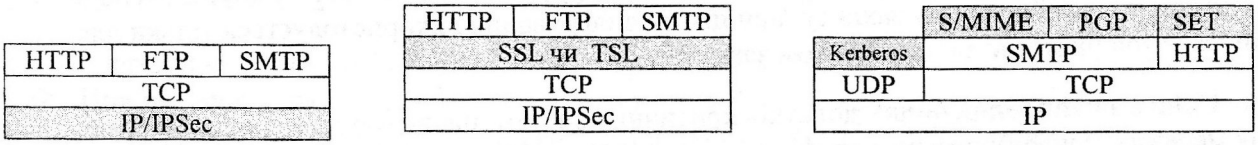
Таблиця 6

Порівняльні характеристики погроз порушення захисту Web

Показники	Погрози	Наслідки	Контрзаходи
Цілісність	• Зміна призначених для користувача даних. · • Впровадження "троянських коней". • Зміна інформації в пам'яті. • Зміна потоку повідомлень на шляху їх передачі·	• Втрата інформації · • Компрометація комп'ютерної системи. • Уразливість відносно погроз порушення захисту всіх типів	Криптографічні контрольні суми.
Конфіденційність	• Перехоплення даних в мережі. · • Крадіжка інформації, що зберігається на сервері. · • Крадіжка інформації, що зберігається на комп'ютері користувача. · • Отримання інформації про конфігурацію мережі. · • Отримання інформації про користувача, що звертається до сервера.·	• Втрата інформації. · • Порушення таємниці інформації	Шифрування, проксі-сервери Web
Відмова в обслуговуванні	• · Припинення сеансу доступу користувача. · • Перевантаження машини потоком фальшивих спроб доступу. · • Умисне переповнення дискового	• Руйнівні наслідки для системи. • Роздратування користувачів. · • Затримки в роботі	Важко запобігти.

	простору або оперативної пам'яті. Ізоляція системи шляхом атак на DNS-сервер.	користувачів.	
Аутентифікація	• Спроби порушника видати себе за легального користувача. • Фальсифікація даних.	• Неправильне представлення користувачів. • Довіра до спотворених даних	Криптографічні технології

Існує декілька підходів до забезпечення захисту даних в Web. Всі вони схожі, але розрізняються за ділянками застосування і розміщення відповідних засобів захисту в стеку протоколів PSP/IP. На мал. 6 представлені варіанти розміщення протоколів захисту в стеку протоколів TCP/IP.



(а) Мережевий рівень (б) Транспортний рівень (в) Рівень додатку

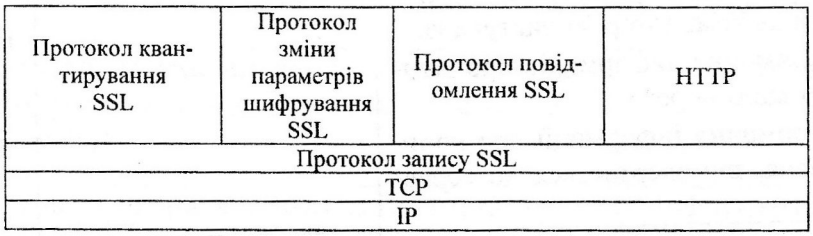
Рис. 6. Розміщення засобів захисту в стеку протоколів TCP/IP

Аналіз мал. 6 показує, що для забезпечення конфіденційності, автентичності і цілісності передачі інформації в Web необхідно використовувати комплекс протоколів, що приводить до значної втрати часу на обробку і передачу інформації.

Таким чином, для забезпечення автентифікації даних в протоколах можуть застосовуватися різні алгоритми симетричного і несиметричного шифрування, MAC-коди і функції хешування. Разом з тим, для кожної окремої комп'ютерної системи (мережі) необхідне проведення оптимізації засобів автентифікації залежно від вимог конкретних застосувань, що використовуються в даних КС (мережах).

Цілісність покликана забезпечити можливість модифікації інформації, такою, що зберігається, і її передачі в КС інформації тільки користувачами, що мають на це право. При цьому під модифікацією розуміються операції запису, зміни, зміни стану, видалення, створення, затримки або повторні відтворення даних [4-5].

Протокол SSL (secure socket layer) розроблений для забезпечення надійного захисту наскрізної передачі даних з використанням протоколу TCP. Слід відзначити, SSL є не одним протоколом, а двома рівнем протоколів, як показано на мал.7.



Мал. 7. Стек протоколів SSL

Протокол SSL пропонує базовий набір засобів захисту, вживаних протоколами вищих рівнів, і забезпечує конфіденційність каналу комунікацій і автентифікацію користувача.

Протокол діалогу SSL має дві основні фази. Перша фаза використовується для встановлення конфіденційного каналу комунікацій. Друга - служить для автентифікації користувача.

Протокол TLS призначений для забезпечення конфіденційності і цілісності даних. Він має два рівні: протокол записів TLS і протокол діалогу TLS. Протокол записів TLS забезпечує конфіденційність даних з використанням симетричних алгоритмів шифрування DES, RC4 і цілісність даних з використанням хеш-функций SHA-1 або MD5.

Протокол діалогу TLS забезпечує цифровий підпис, заснований на підході RSA або DSS.

Аналіз засобів захисту цілісності повідомлень показав, що протоколи гарантовано забезпечують ухвалення повідомлення у відповідності до відправлених. Разом з тим, працюючи з потоками повідомлень, вони забезпечують тільки виявлення порушення цілісності потоку даних і не забезпечують відновлення пошкодженої або втраченої інформації.

Таким чином, протоколи і механізми забезпечення автентичності, конфіденційності і цілісності передачі даних, вживані в комп'ютерних системах і мережах, використовують криптографічні методи, засновані на використанні симетричних і несиметричних алгоритмів перетворення інформації. Разом з тим, підвищення імовірнісно-тимчасових вимог до стійкості криптографічних методів захисту інформації і оперативності обробки і передачі даних при частій зміні ключових даних вказує на необхідність розробки нових підходів криптоперетворень, що дозволили б при жорстких обмеженнях обчислювальної складності забезпечити доказовий рівень безпеки інформації.

4. Обґрунтування вибору напряму досліджень. Виходячи з основних теоретичних поло-жень сучасної криптографії, розглянуті особливості функціонування підсистеми захисту інформації в критичних комп'ютерних системах і мережах можна реалізувати такими шляхами [8 - 14]:

1. *Шляхом застосування симетричних криптоалгоритмів у поєднанні з несиметричними протоколами розповсюдження секретних ключових даних.* У цьому випадку використання симетричних криптоалгоритмів дозволяє реалізувати швидке криптографічне перетворення великих об'ємів даних. В той же час, цей напрям зв'язаний з наступними істотними недоліками:

- несиметричні протоколи обміну ключами мають передбачає самостійне формування частин секретного ключа двома різними абонентами, що порушує принцип централізованого управління і розповсюдження ключів;

- . використання несиметричних протоколів обміну ключами передбачає формування загального ключа для двох абонентів. При формуванні секретного ключа з іншими абонентами відповідні секретні ключі відмінні, що робить неможливою організацію управління і зв'язку в циркулярному режимі і, у свою чергу, утруднює своєчасне управління підпорядкованими об'єктами і, врешті, веде до зниження безперервності і оперативності управління;

- використання несиметричних протоколів обміну ключами передбачає застосування криптоалгоритмів, складність реалізації яких на 3-5 порядків перевершує складність реалізації класичних (симетричних) криптоалгоритмів, що в умовах частої зміни ключових даних може привести до значних затримок в управлінні.

2. *Шляхом застосування несиметричних алгоритмів шифрування.* В цьому випадку один загальний для групи абонентів ключ поширюється по відкритих каналах зв'язку, і немає необхідності почергового виконання алгоритмів поширення секретних ключових даних кожним абонентом інформаційного обміну окремо. В той же час, цей підхід пов'язаний з такими істотними недоліками:

- складність реалізації існуючих алгоритмів несиметричного шифрування істотно (на 3-5 порядків) вища в порівнянні з симетричними криптоалгоритмамі, що в умовах стрімкого збільшення об'ємів обробки і передачі даних і підвищення імовірнісно-тимчасових вимог до безпеки і достовірності інформації неприпустимо;

- застосування існуючих несиметричних протоколів обміну секретними повідомленнями з використанням відкритих ключів приводить до значного (у 2-4 рази) збільшення надмірності передаваних даних, що істотно знижує ефективність зв'язку.

Таким чином, існуючі (класичні) підходи до побудови підсистем обміну конфіденційними повідомленнями *не дозволяють* повною мірою забезпечити виконання сучасних вимог безпеки інформації в критичних інформаційних і комп'ютерних системах.

Виникає *суперечність* між різко збільшеними об'ємами оброблюваних і передаваних даних, підвищенням імовірнісно-тимчасових вимог до безпеки і достовірності інформації при частій зміні ключових даних і існуючими підходами теорії захисту інформації до побудови підсистем обміну конфіденційними повідомленнями.

Перспективним напрямом у розвитку методів захисту інформації є розробка і дослідження криптосистем, стійкість яких заснована на складності теоретично складної проблеми декодування випадкового коду т.зв. несиметричних теоретико-кодових схем [15, 16]. У деяких джерелах вони отримали назву теоретико-кодових схем [18, 19]. Як показує проведений аналіз, їх застосування дозволяє реалізувати швидке криптографічне перетворення із забезпеченням доказової стійкості. Складність їх реалізації розмірна з криптоалгоритмами тимчасової стійкості (БСШ). Крім того, їх практичне використання дозволяє застосувати інфраструктуру відкритих ключів і будувати інтегровані механізми криптографічного перетворення даних і канального кодування.

Таким чином, одним з перспективних шляхів вдосконалення криптографічних методів перетворення інформації є розробка криптографічних засобів доказової стійкості, побудованих з використанням блокових кодів алгебри.

5. Висновки. Проведені дослідження показали, що на сьогоднішній день для забезпечення захисту передаваних даних в комп'ютерних системах і мережах використовуються набори протоколів захисту, які не повною мірою забезпечують виконання сучасних збільшених вимог по стійкості і обчислювальній складності криптоалгоритмів.

Перспективним напрямом інтегрованого вирішення завдань забезпечення необхідних показників автентифікації, конфіденційності і цілісності передачі даних в критичних комп'ютерних системах і мережах є використання теоретико-кодових схем на блокових кодах алгебри, що дозволить:

- реалізувати швидкі криптографічні перетворення великих об'ємів даних з використанням відкритих ключів, що, з одного боку, не вимагає поширення секретних ключових даних по закритих каналах зв'язку, а з іншого боку, не вимагає ускладнення існуючої апаратури передачі даних;

- забезпечити високий рівень стійкості до сучасних методів криптоаналізу за рахунок зведення завдання безключового читання до рішення теоретико-складної задачі декодування

випадкового коду; забезпечити доказову стійкість створюваних криптографічних засобів захисту інформації;

- будувати інтегровані механізми канального кодування і криптографічного перетворення даних, що дозволить комплексно вирішувати завдання створення безпеки і достовірності інформації в комп'ютерних системах і мережах.

Список літератури

1. Горбенко И.Д., Потий А.В., Терещенко П.И. Рекомендации международных стандартов по оценке безопасности информационных технологий // Материалы третьей международной научно-практической конференции "Безопасность информации в информационно-телекоммуника-ционных системах".- Киев, 2000.-С.150-160.
2. Бондаренко М.Ф., Черных С.П., Горбенко И.Д., Замула А.А., Ткач А.А. Методологические основы концепции и политики безопасности информационных технологий// Радиотехника. Всеукраинский межвед. научн.-техн. сб. – 2001. -Вып.119.-С.5-17.
3. Горбенко И.Д., Потий А.В., Терещенко П.И. Критерии и методология оценки безопасности информационных технологий // Радиотехника. Всеукраинский межвед.
4. Вильям Столингс. Криптография и защита сетей. Принципы и практика Изд. Дом "Вильямс".М.С-П.К. – 2001. – 670с.
5. Хорев П. Б. Методы и средства защиты информации в компьютерных системах. Изд. Академия.–2005. – 256 с.
6. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / Под ред. В.Ф. Шаньгина.-2-е изд., перераб. и доп.-М.: Радио и связь, 2001. – 376 с.
7. Вихорев С. В. Классификация угроз информационной безопасности // http://www2.cnews.ru/ comments/security/elvis_class.shtm.l
8. Cryptrec. Cryptrec liaison report to ISO/IEC 18033-2 and 18033-3. Technical report,Cryptography Research and Evaluation Committees, October 2002.
9. National Institute of Standards and Technology, "FIPS-197: Advanced Encryption Standard." Nov. 2001. Available at http://csrc.nist.gov/publications/ fips/fips197/fips-197.pdf
10. National Institute of Standards and Technology, "FIPS-46-3: Data Encryption Standard." Oct. 1999. Available at http://csrc.nist.gov/publications/fips/ fips46-3/fips46-3.pdf
11. Шеннон К. Теория связи в секретных системах // Шеннон К. Работы по теории информации и кибернетике. – М.: Изд-во иностранной литературы, 1963. – С.333-402.
12. Разборов А.А. Основы теории сложности вычислений // Лекция 23 апреля 1998 года.
13. Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption. April 19, 2004. – p. 836.
14. Саломаа А. Криптография с открытым ключом: Пер. с англ., – М.:Мир, 1995. – 318с.
15. Стасєв Ю.В., Кузнецов О.О., Корольов Р.В. Аналіз існуючих послуг і механізмів захисту інформації// Системи озброєння і військова техніка. – Х.: ХУПС. – 2006.4(8) – С.81-87.
16. Кузнецов А.А.,Евсеев С.П., Томашевский Б.П., Жмурко Ю.И.Исследование протоколов и механизмов защиты информации в компьютерных системах и сетях// Збірник наукових праць ХУ ПС. – Харків: ХУПС. – 2007. – Вип. 2 (14). – С. 102-111.
17. Сидельников В.М. Криптография и теория кодирования. Материалы конференции «Московский университет и развитие криптографии в России», МГУ. – 2002. – 22с.

18. Сидельников В.М., Шестаков С.О. О системе шифрования, построенной на основе обобщенных кодов Рида-Соломона.//Дискретная математика.-1992.-Т.4.№3.-С.57-63.

19. Кузнецов А.А., Евсеев С.П. Разработка теоретико-кодовых схем с использованием эллиптических кодов. // Системи обробки інформації. – Харків: ХВУ. –2004 – Вип. 5. – С. 127-132.

УДК 004.681.3

Гулак Г.М.
Державний університет
інформаційно-комунікаційних технологій

ХАРАКТЕРИСТИКА НЕБЕЗПЕЧНИХ ВІДМОВ ЗАСОБІВ, ЩО РЕАЛІЗУЮТЬ СТЕГАНОГРАФІЧНІ МЕТОДИ ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ

Ретельно обґрунтовані та досліджені методи перетворення інформації в стеганографічних системах (далі – стегосистемах) можуть не досягати поставленої мети, якщо апаратно-програмні засоби, які їх реалізують не відповідають певному рівню функціональної безпеки [1]. Це означає, що конструктивні, алгоритмічні и схемно-технічні рішення, обрані під час проектування цих засобів, не адекватні можливим збоям технічних та програмних компонент, не здатні знизити до нуля ймовірність проведення ефективної атаки на стегосистему у випадку ситуації з відмовою [2].

Оцінювання рівня безпеки та надійності засобів, що реалізують стеганографічні перетворення (ЗРСП), здійснюється шляхом проведення їх інженерного аналізу, у рамках якого виконуються реєстрація, вимірювання, впорядкування, узагальнення реальних характеристик ситуацій з відмовами та визначення їх наслідків для безпеки інформації. У підсумку проведення інженерного аналізу мають бути зроблені висновки щодо достатності обраних рішень, а також, за необхідності, сформовані пропозиції щодо вдосконалення функціональної безпеки ЗРСП.

При цьому функціональну безпеку ЗРСП на відміну від [1] будемо розуміти не в сенсі катастрофічності наслідків відмови взагалі, а лише у вузькому змісті інформаційної безпеки. Аналогічно визначенням стандартів [3] під функціональною безпекою ЗРСП будемо розуміти їх здатність тривало правильно виконувати завдання за призначенням, не утворюючі, у разі виходу з ладу їх компонентів, передумов для витоку інформації з обмеженим доступом, іншої критичної інформації. Таким чином можливо сформулювати у якості головного завдання інженерного аналізу ЗРСП визначення складових функціональної безпеки, рівня захищеності від виходу з ладу компонентів та ступеню впливу ймовірних відмов на стеганографічні якості цих засобів.

Як і у випадку інженерних досліджень надійності будь-якої складної системи [4,5], звичайно, інженерний аналіз ЗРСП повинен передбачати виявлення та оцінку загроз безпеці інформації з боку апаратних компонент, програмного забезпечення (ПЗ) та людського фактору.

Звернемо увагу, що введене поняття функціональної (інформаційної) безпеки стегосистеми та характеристики її рівня перекликаються з показниками надійності звичайної технічної системи. Суттєва різниця полягає у тому, що показники надійності враховують будь яки відмови та збої системи, а характеристики інформаційної безпеки ЗРСП повинні виходити тільки з тих відмов, наслідком яких може бути суттєве погіршення стеганографічних властивостей цих засобів.

Слід зазначити, що у наукових публікаціях [6,7,8] приділяється недостатня увага інженерно-технічним аспектам створення апаратно-програмних ЗРСП, с точки зору забезпечення надійності їхнього функціонування та безпеки інформації в умовах виникнення апаратних та