УДК 681.322.067

В.В. Гніліцький, к.т.н., доц.
Житомирський інженерно-технологічний інститут
Ю.П. Жураковський, д.т.н., проф.
В.П. Полторак, к.т.н., доц.
Національний технічний університет України "КПІ"

КРИПТОГРАФІЯ – ПОТЕНЦІЙНА МОЖЛИВІСТЬ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМАХ УПРАВЛІННЯ. ОСНОВНІ ПОНЯТТЯ ТА ПОЛОЖЕННЯ

Викладено основні поняття та положення щодо організації захисту інформації від несанкціонованого доступу. Особлива увага звернена на криптографічні методи захисту інформації.

В основі успішної діяльності будь-якого підприємства, організації, приватної особи лежить вірогідна інформація, яку необхідно зібрати, проаналізувати, перетворити в обгрунтоване рішення та захистити від несанкціонованих дій. При цьому зростаючі потоки інформації, з якими мають справу в системах управління, банківських, спеціалізованих та телекомунікаційних системах і мережах, потребують впровадження таких систем збору, обробки, зберігання та передачі інформації, які б забезпечували гарантовану безпеку цих процесів. Дані, що знаходяться в пам'яті комп'ютера, передаються по лініях зв'язку і є конфіденційною інформацією ділового, комерційного або приватного характеру, можуть зазнавати таких дій з боку зловмисників, як несанкціоноване читання, модифікація, крадіжка. В зв'язку з цим, сьогодні питання захисту інформації від несанкціонованого доступу (НСД) стають все більш актуальними. Засоби забезпечення інформаційної безпеки є однією з найважливіших складових частин в усіх інформаційних системах та системах управління: від електронної пошти – до стільникового зв'язку, від доступу до мережі Internet – до електронної комерції, від систем управління виробничою ділянкою – до управління космічним об'єктом.

Загроза інформаційної безпеки – це будь-яка обставина чи подія, що може призвести до нанесення збитків системі, організації, приватній особі у вигляді руйнування, розкриття, модифікації даних або відмови в обслуговуванні.

Можливі загрози інформації залежать від її характеру та сфери застосування. Одним з видів таких загроз є промислове, або комерційне, шпигунство, що проводиться з метою завоювання ринків збуту, усунення конкурентів, зриву домовленостей по контрактах, перепродажу фірмових таємниць і т. д. Зловмисники як інформаційну зброю можуть застосовувати засоби для: знищення, перекручення або викрадення інформації; подолання систем захисту; обмеження доступу законних користувачів; для дезорганізації роботи технічного обладнання, комп'ютерних систем.

Можна виділити такі способи впливу загроз на інформаційні об'єкти (рис. 1): інформаційні, програмно-технічні, фізичні, радіоелектронні, організаційно-правові [1]. До інформаційних способів відносяться незаконний збір та використання інформації, незаконне копіювання даних в інформаційних системах і т. д. До програмно-технічних способів відносять: застосування комп'ютерних вірусів, здатних розмножуватися та передаватися через лінії зв'язку, мережі передачі даних, виводити з ладу системи управління; встановлення програмних чи апаратних закладних пристроїв, які починають діяти в зазначений час тощо. До фізичних способів відносять: знищення або руйнацію засобів обробки інформації та зв'язку; викрадення програмних чи апаратних ключів та систем криптографічного захисту. До радіоелектронних способів відносять: перехоплення інформації в технічних каналах її можливого витікання; перехоплення, дешифрування та фальсифікацію інформації в мережах передачі даних та лініях зв'язку. До організаційно-правових способів відносять невиконання вимог законодавства у вигляді нормативно-правових положень в інформаційній сфері тощо.

Для вирішення питань інформаційної безпеки розроблено та використовується багато технологій, способів та засобів захисту інформації. Це свідчить про зростаючу актуальність питань захисту інформації від НСД. Але, разом з тим, далеко не кожен легко може визначити, як повинна бути побудована система захисту, які засоби захисту потрібно застосовувати. Насамперед, потрібно зазначити, що всі зусилля та заходи щодо захисту інформації повинні бути об'єднані в єдину систему – комплексну систему інформаційної безпеки (СІБ) [2].

СІБ повинна включати в себе ряд базових методів комплексного захисту інформації (рис. 2), до яких відносяться правові, організаційно-економічні та програмно-технічні методи забезпечення інформаційної безпеки.

Правові методи передбачають розробку нормативно-правових актів, що стосуються порядку використання інформаційних ресурсів та різноманітних компонентів комп'ютерних систем та мереж.

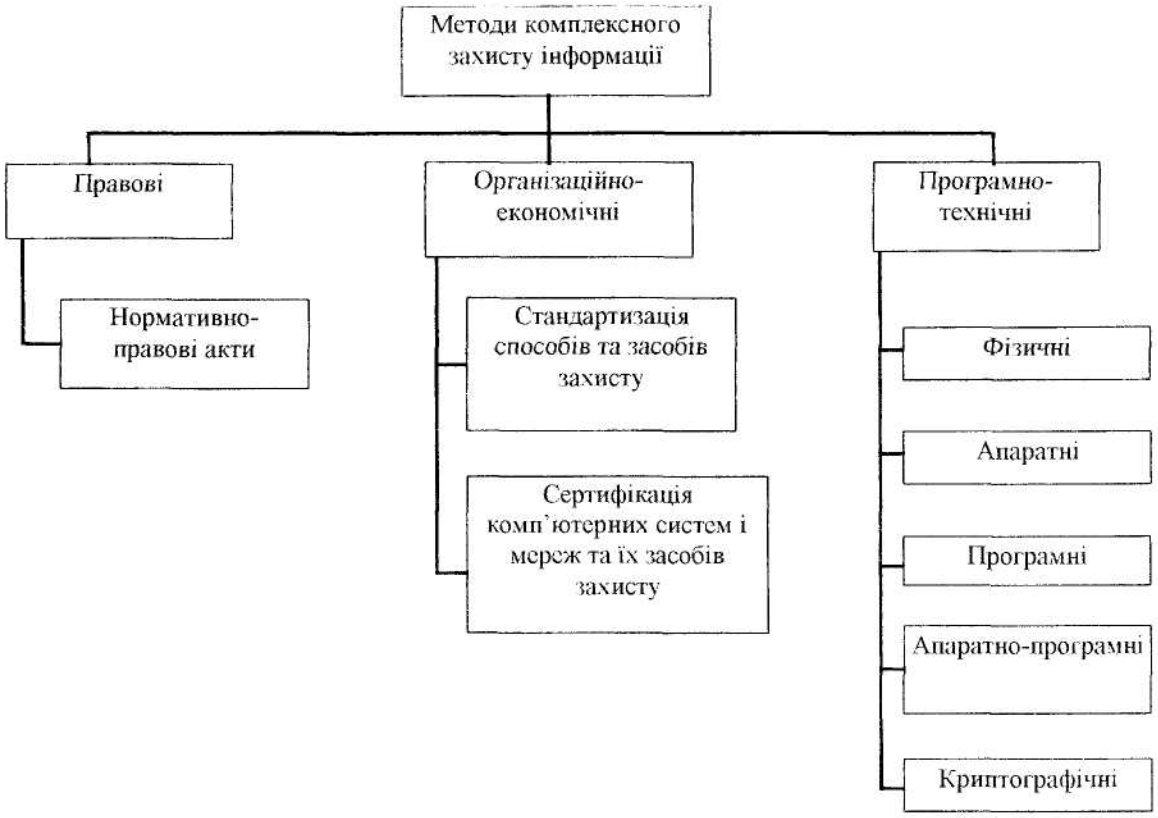

Рис. 2

Організаційно-економічні методи дозволяють вирішувати питання стандартизації способів та засобів захисту інформації, сертифікації комп'ютерних систем та мереж та їх засобів захисту, а також питання ліцензування діяльності в сфері захисту інформації. Зазначимо, що існують міжнародні стандарти (критерії) безпеки комп'ютерних систем. До них відносяться:

- TCSEC («Оранжева книга», США, 1983 р.),
- ITSEC (Європейські критерії, 1991 р.),
- Документи ГТК Росії (1992 р.),
- FCITS (федеральні критерії, 1992 р.),
- CTCPEC (Канадські критерії, 1993 р.),
- CCITSE (Єдині критерії, 1993 р.).

Порівняльна оцінка цих стандартів за показниками якості п'яти рівнів наведена в [3].

Програмно-технічна підсистема комплексного захисту об'єктів інформаційної безпеки включає фізичні, апаратні, програмні, апаратно-програмні, криптографічні методи та засоби захисту інформації.

Фізичні засоби захисту призначені для зовнішньої охорони території об'єктів, захисту ЕОМ, систем та об'єктів на базі обчислювальної техніки.

Апаратні засоби захисту – це різноманітні електронні, електронно-механічні та інші пристрої, безпосередньо вмонтовані в серійні блоки електронних систем обробки та передачі даних або зроблені у вигляді самостійних пристроїв та сполучені з цими блоками. Вони призначені для внутрішнього захисту структурних елементів ЕОМ, засобів та систем обчислювальної техніки: терміналів, пристроїв вводу–виводу, процесорів, периферійного обладнання, ліній зв'язку.

Програмні засоби захисту призначені для виконання логічних та інтелектуальних функцій захисту і є найбільш поширеним видом захисту, чому сприяють універсальність, гнучкість, простота реалізації, можливість зміни та розвитку.

Апаратно програмні засоби захисту пов'язані з одночасним використанням програмних та апаратних засобів захисту.

Криптографічні методи захисту – це методи захисту даних через криптографічні перетворення.

Таким чином, до СІБ повинні бути включені відповідні організації, що здійснюють розробку та реалізацію організаційних заходів на основі нормативних документів. Крім того, в СІБ повинні входити різноманітні засоби, за допомогою яких здійснюється захист апаратного та програмного забезпечення інформаційної системи (ІС) – фізичні, програмні, апаратні, апаратно-програмні, криптографічні.

Враховуючи значну кількість варіантів побудови ІС, до вибору систем захисту потрібно підходити усвідомлено, проаналізувавши особливості конкретної ІС. Насамперед, потрібно визначити, які конкретно відомості мають конфіденційний характер і підлягають захисту. Важливо також для чого, від кого їх потрібно захищати і впродовж якого часу. Крім того, слід виявити потенційні загрози та найбільш ймовірні канали витікання інформації для конкретної ІС. Наступний крок полягає у виборі таких заходів та засобів, які підходять для даної ІС. Слід також зазначити, що краще аналізувати можливі небезпеки на стадії проектування ІС, оскільки впровадження системи захисту в функціонуючу ІС пов'язано з введенням певних обмежень, що зменшує ефективність роботи системи в цілому.

В даній роботі розглянуті *криптографічні методи* захисту інформації від НСД. Ці методи дозволяють здійснювати: шифрування інформації для захисту від несанкціонованого доступу з боку зловмисника та від комп'ютерних вірусів; контроль цілісності даних і програм для виявлення випадкових та навмисних перекручень; реалізацію цифрового підпису для вирішення суперечливих питань щодо авторства документів; захист програм від несанкціонованого копіювання та поширення; генерацію паролів в комп'ютерних мережах.

Розглянемо основні поняття та визначення криптографічного захисту інформації. Насамперед, зазначимо, що в основі криптографічного перетворення лежить процес зміни форми подання тексту, що захищається, – символи тексту замінюються іншими символами того же алфавіту або символами нового алфавіту. *Шифрування* – це таке перетворення початкового повідомлення (воно ще називається відкритим текстом) в шифроване (шифр, шифртекст, шифрограма, криптограма), яке характеризується значною обчислювальною складністю оберненого перетворення (дешифрування) без знання секретного елемента – ключа. Під *ключем* розуміють послідовність символів, на основі яких здійснюється шифрування та дешифрування конфіденційних даних. *Криптосистема* – це набір криптографічних перетворень або алгоритмів, що перетворюють відкритий текст в шифртекст і навпаки. *Стійкість криптосистеми* визначається стійкістю криптографічного алгоритму до його криптоаналізу, тобто до спроб отримання початкового тексту з зашифрованого без знання ключа. При розробці алгоритмів криптографічного перетворення інформації керуються *правилом Керкхоффа* (голландський математик, кінець XIX ст.): стійкість шифра повинна визначатись лише стійкістю ключа. Іншими словами, передбачається, що механізм шифрування відомий криптоаналітику. Таким чином, для надійного захисту інформації від НСД необхідно використовувати практично стійкі криптографічні алгоритми, тобто такі, які базуються на практичній складності їх розкриття, а не на неможливості такого. При цьому практично стійким вважається такий алгоритм, обчислювальна складність та економічні витрати на злом якого перевищують цінність інформації, що розкривається. Як правило, *криптостійкість* визначається середньою кількістю годин, необхідних для отримання ключа, і, отже, відкритого тексту, на основі аналізу шифртексту.

В криптографії використовується два типи криптосистем (рис. 3): *симетричні криптосистеми*, що базуються на використанні одного секретного ключа, та *асиметричні*, або *криптосистеми з відкритим ключем*, що базуються на використанні пари ключів – закритого та відкритого.

В *симетричних криптосистемах*, які називаються одноключовими (класичними, з секретним ключем), один і той же ключ використовується як для прямого перетворення (шифрування), так і для оберненого (дешифрування). Цей ключ і є секретною інформацією. В таких криптосистемах потрібен секретний канал для передачі ключа від відправника до отримувача для того, щоб останній міг скористатися ним для розшифрування отриманого повідомлення.

Шифри, що використовуються в симетричних криптосистемах, поділяються на потокові та блочні. В потокових шифрах шифруюче перетворення елемента відкритого тексту змінюється від одного елемента до іншого, тобто відбувається поелементне шифрування потоку даних, при якому кожен символ відкритого тексту шифрується, передається та дешифрується незалежно від інших. Для блочних шифрів характерно розбиття початкового тексту на блоки фіксованої довжини, кожен з яких шифрується окремо.

Потокові шифри базуються на псевдовипадкових послідовностях, що генеруються певним чином за допомогою датчиків псевдовипадкових чисел (ПВЧ). Як датчики ПВЧ використовуються конгруентні датчики, датчики М-послідовностей і т. д. Виділяють потокові шифри з одноразовим або нескінченним ключем та шифри з обмеженим ключем (наприклад, система Вернама).

Багато *блочних шифрів* в криптосистемах з секретним ключем базуються на двох методах – перестановок та підстановок (метод заміни). Метод заміни характерний як для моноалфавітних підстановок (шифр Цезаря), так і для поліалфавітних (шифр Тритеміуса, шифр Віжинера, циліндр Джефферсона, диск Уетстоуна).

Крім того, серед більшості блочних шифрів виділяють складені шифри, які отримуються при багаторазовому чергуванні простих перестановок та підстановок. Це досить стійкі шифри з добрим розсіюванням та перемішуванням – необхідними складовими частинами для побудови стійких алгоритмів шифрування [4, 5].

Прикладами криптографічних алгоритмів з секретним ключем є DES, ГОСТ 28147-89, FEAL, IDEA, CAST, RC2, RC4, RC5, B-Crypt, Blowfish, Scipjack та інші.

Основні переваги симетричних криптосистем:

- простота алгоритмів та їх реалізації;
- висока швидкість процесів шифрування/дешифрування;
- висока криптостійкість, пов'язана з розміром ключа.

Основним недоліком симетричних криптосистем є необхідність наявності секретного каналу зв'язку для передачі секретного ключа.

В *криптосистемах з відкритим ключем* є два математичні ключі, що використовуються для шифрування та дешифрування даних. Ці ключі називаються відкритим та закритим. Кожен користувач криптосистеми з відкритим ключем володіє двома взаємодоповнюючими ключами: відкритим та закритим (приватним). Відкритий ключ доступний для всіх користувачів системи, він може бути опублікований і широко розповсюджений через мережі комунікацій. Закритий ключ є власно секретною інформацією та зберігається в таємниці. Будь-хто може використати відкритий ключ отримувача для того, щоб зашифрувати повідомлення, яке йому відправляє. Отримувач же застосовує свій закритий ключ для розшифрування повідомлення.

Як правило, кожен з цих ключів підходить для розшифрування повідомлення, зашифрованого з використанням іншого ключа, однак розшифрувати повідомлення тим же ключем, яким воно було зашифроване, неможливо. Це пов'язано з використанням так званих необоротних (односторонніх) математичних функцій для реалізації алгоритмів шифрування, а також з високою обчислювальною складністю отримання закритого ключа за відомим відкритим. Неможливість обчислити будь-який з ключів при наявності іншого з прийнятними витратами – одна з основних властивостей систем з відкритим ключем.

Під час звичайної передачі конфіденційної інформації *відправник* зашифровує дані відкритим ключем отримувача, а *отримувач* розшифровує їх своїм закритим ключем.

Багато криптоалгоритмів з відкритим ключем мають ще один важливий засіб захисту – так званий *цифровий підпис*. Останній свідчить, що файл не був змінений з того часу, як був підписаний, і дає отримувачу інформацію про те, хто саме підписав цей файл. При використанні цифрового підпису *відправник* зашифровує частину повідомлення (ставить підпис) своїм закритим ключем, а *отримувач* має можливість ідентифікувати підпис відправника, використовуючи його відкритий ключ.

На сьогодні найбільш поширеними є два алгоритми створення цифрового підпису: перший належить компанії RSA, другий – стандарт DSS (Digital Signature Standart – "стандарт цифрового підпису"). В обох варіантах схема обчислення підпису передбачає отримання ускладненого еквівалента контрольної суми – так званої хеш-суми. Для цього використовується одна з двох стандартних методик – MD5 або SHA (Secure Hash Algorithm).

До досить поширених на сьогодні систем з відкритим ключем відносяться криптосистеми RSA, Диффі-Хелмана, Ель-Гамаля, криптосистеми на основі еліптичних рівнянь.

Алгоритм RSA базується на множенні та піднесенні до степеня за модулем простого числа. Криптостійкість його грунтується на недоведеному ще (хоча й досить правдоподібному) припущенні, що розкладення великих чисел на множники в сучасних умовах обчислювально нездійсненно (так звана проблема факторизації чисел). Це позбавляє зловмисника можливості дешифрувати криптограму без знання закритого ключа.

Система Діффі-Хелмана базується на дискретному піднесенні до степеня. Стійкість її грунтується на обчислювальній складності процедур дискретного логарифмування.

Метод Ель-Гамаля також грунтується на проблемі дискретного логарифмування.

Стійкість криптосистем на основі еліптичних рівнянь базується на проблемі обчислення дискретного логарифма на еліптичній кривій. Прикладом такої криптосистеми є ECC (Elliptic Curve Cryptography) [6].

Класифікувати криптосистеми з відкритим ключем можна за типом важковиріщуваної математичної задачі, що лежить в їх основі:

- системи розкладення цілих чисел на множники (RSA);
- дискретні логарифмічні системи (Діффі-Хелмана, Ель-Гамаля);
- дискретні логарифмічні системи еліптичних кривих (криптосистеми на основі еліптичних рівнянь).

Основні переваги асиметричних криптосистем:

- відсутність необхідності передавати ключ дешифрування (закритий) будь-кому взагалі та відсутність необхідності в секретному каналі зв'язку;
- неможливість визначити закритий ключ за відкритим.

Основним недоліком асиметричних криптосистем є велика тривалість процедур шифрування/дешифрування.

Аналіз наведених вище переваг та недоліків двох криптосистем показує доцільність використання так званого гібридного або каскадного методу в конкретних реалізаціях систем захисту інформації від НСД. Важливо, що при цьому можна досягти поєднання переваг симетричних криптосистем та криптосистем з відкритим ключем. Оптимальною є побудова такої каскадної системи, в якій криптосистеми з відкритим ключем використовуються для розподілу ключів та створення спільних секретних ключів, які потім застосовуються для шифрування/дешифрування конфіденційної інформації в симетричних (класичних) криптосистемах. Таке поєднання криптосистем дає можливість обійтись без секретного каналу зв'язку і при цьому використати криптостійкі та швидкісні симетричні алгоритми для шифрування конфіденційної інформації.

Наведемо деякі *приклади* розроблених комерційних програм, побудованих на об'єднанні двох типів криптографічних перетворень [7]. Так в програмі SecretAgent фірми AT&T управління ключами повністю базується на шифруванні з відкритим ключем. Користувачеві пропонуються на вибір ключі типу RSA або DSA (Digital Signature Algorithm – алгоритм цифрового підпису). Крім того, програма передбачає декілька алгоритмів шифрування: DES, Triple DES, EA2 – власну розробку AT&T. Підтримуються такі апаратні засоби шифрування, як карти Smartcard компаній Datakey та Fortezza. Крім шифрування файлів, SecretAgent дозволяє ставити цифрові підписи в стандарті DSS, але тільки на попередньо зашифровані файли.

В пакеті Norton Your Eyes Only корпорації Symantec реалізовані такі алгоритми шифрування з симетричним ключем: RC4, RC5, Triple DES и Blowfish. Секретний ключ зашифровується на основі відкритого. Ставлення цифрового підпису не забезпечується.

Програма RSA Secure базується на алгоритмі шифрування RC4, розробленому компанією RSA.

В програмі ViaCrypt PGP компанії Pretty Good Privacy реалізований алгоритм Pretty Good Privacy, шифрування з секретним ключем проводиться за алгоритмом IDEA, а секретні ключі зашифровуються за допомогою системи RSA. В цій програмі є можливість ставити цифровий підпис під незашифрованим документом.

Порівняльний аналіз наведеного в літературі досить великого матеріалу з криптографічних шифрів дав можливість отримати компактне подання їх основних властивостей, що наведено в двох таблицях: табл. 1 – для симетричних і табл. 2 – для асиметричних криптосистем. На жаль, різні криптосистеми в літературі описані різними авторами і не на однаковому рівні, що призводить до неможливості вказати значення одних і тих самих або порівняних параметрів для різних шифрів. Тому згадані таблиці не претендують на глибину та повноту висвітлення матеріалу, що в деякій мірі ускладнює об'єктивну оцінку шифрів. Однак за розглянутими даними можна зробити деякі висновки.

Всі криптосистеми діляться на два великих класи: симетричні (з єдиним секретним) ключем та асиметричні (з двома ключами – відкритим та закритим).

Немає шифрів, які абсолютно не можна розкрити. Будь-який шифр вносить або неприпустимо великі витрати часу на несанкціоноване дешифрування без знання ключа, або неприпустимо великі витрати матеріальних засобів (коли вартість розкриття повідомлень виявляється значно вищою за очікувану користь від знання тексту такого повідомлення).

ЛІТЕРАТУРА:

1. *Леонов А.П., Леонов К.А., Фролов Г.В.* Безопасность автоматизированных банковских и офисных систем. – Минск: Национальная книжная палата Беларуси, 1996. – 262 с.
2. *Домарев В.В.* Бизнес и информационная безопасность // Мир связи, 1998. – № 1. – С. 64–67.
3. *Шорошев В.В., Ильницкий А.Е.* Международные стандарты безопасности компьютерных систем: эволюция развития, проблемы, рекомендации //- Бизнес и безопасность, 1998. – № 5. – С. 2–3.
4. Защита информации в персональных ЭВМ // Спесивцев А.В., Вегнер В.А. и др. – М.: Радио и связь, 1992. – 192 с.
5. *Жельников В.* Криптография от папируса до компьютера. – М.: ABF, 1997. – 336 с.
6. *Горша Л.* Эллиптические кривые // ComputerWorld / Киев, 1996. – № 34 (200). – С. 22.
7. *Willie Schatz.* The secret to encryption // Computer Week. – М., 1995 – № 24 (182).

ГНЛІЦЬКИЙ Віталій Васильович – кандидат технічних наук, доцент, завідувач кафедри автоматики та управління в технічних системах Житомирського інженерно-технологічного інституту.

Наукові інтереси:
- цифрова обробка сигналів;
- інформаційні системи.

ЖУРАКОВСЬКИЙ Юрій Павлович – доктор технічних наук, професор кафедри АУТС Національного технічного університету України "Київський політехнічний інститут".

Наукові інтереси:
- теорія інформації;
- кодування та захист інформації.

ПОЛТОРАК Вадим Петрович – кандидат технічних наук, доцент кафедри АУТС Національного технічного університету України "Київський політехнічний інститут".

Наукові інтереси:
- передача, обробка та захист інформації.

Подано 23.11.1999.

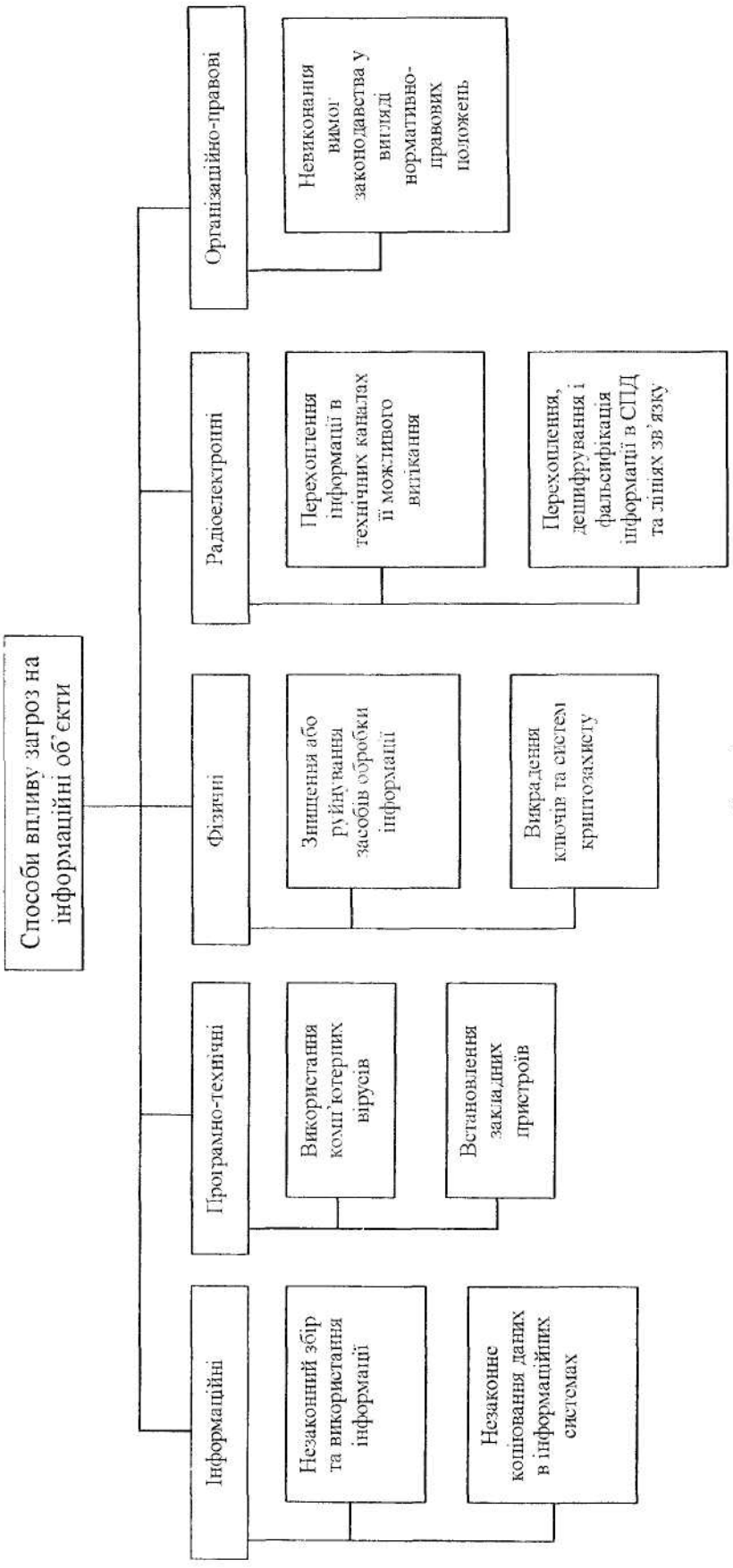
Способи впливу загроз на інформаційні об'єкти
Організаційно-правові
Невиконання вимог законодавства у вигляді нормативно-правових положень
Радіоелектронні
Перехоплення інформації в технічних каналах її можливого витікання
Перехоплення, дешифрування і фальсифікація інформації в СПД та лініях зв'язку
Фізичні
Знищення або руйнування засобів обробки інформації
Викрадення ключів та систем криптозахисту
Програмно-технічні
Використання комп'ютерних вірусів
Встановлення закладних пристроїв
Інформаційні
Незаконний збір та використання інформації
Незаконне копіювання даних в інформаційних системах

Рис. 1

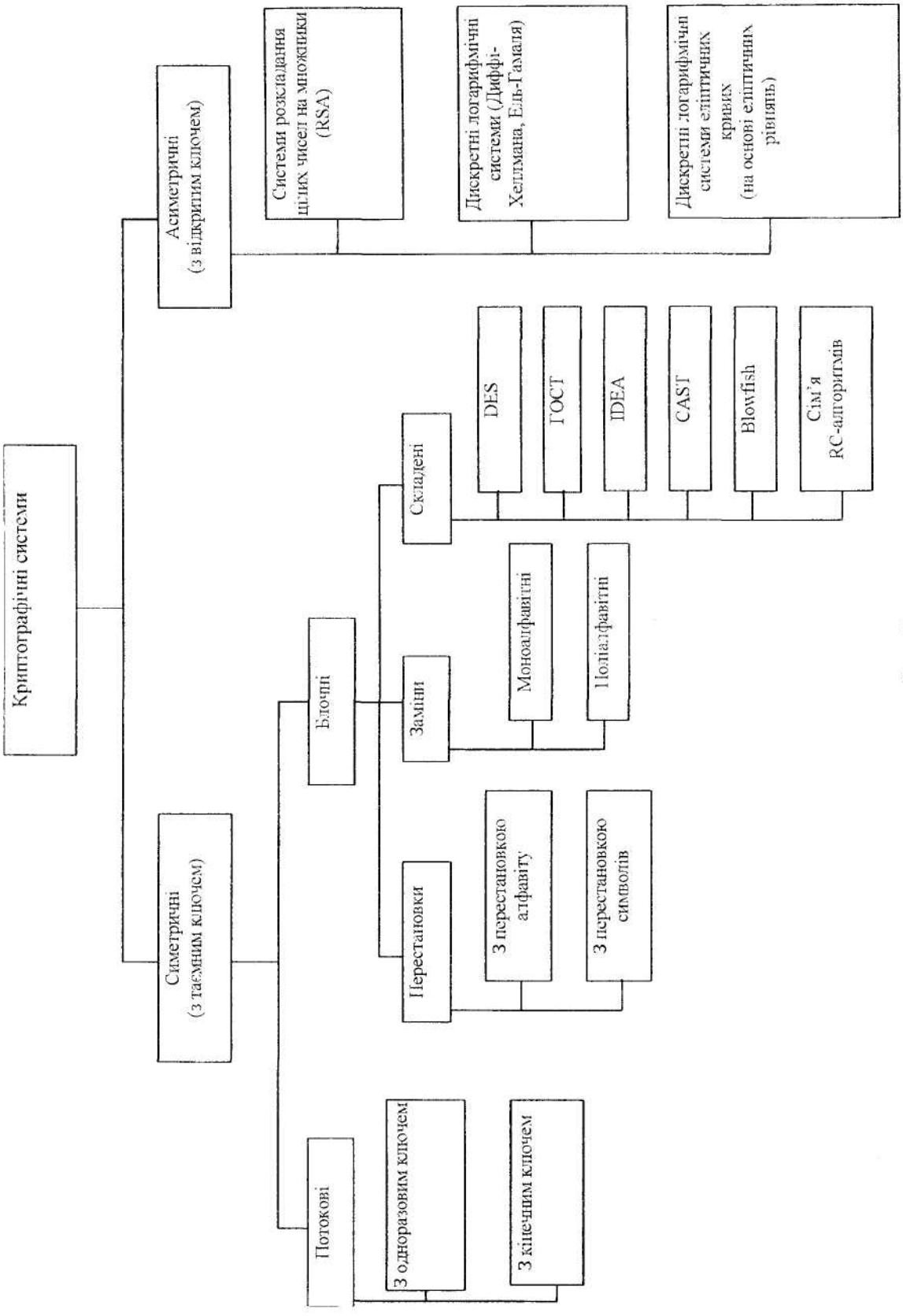
Криптографічні системи
Асиметричні (з відкритим ключем)
Системи розкладання цілих чисел на множники (RSA)
Дискретні логарифмічні системи (Діффі-Хеллмана, Ель-Гамаля)
Дискретні логарифмічні системи еліптичних кривих (на основі еліптичних рівнянь)
Симетричні (з таємним ключем)
Блочні
Складені
DES
ГОСТ
IDEA
CAST
Blowfish
Сім'я RC-алгоритмів
Замини
Моноалфавітні
Поліалфавітні
Перестановки
З перестановкою алфавіту
З перестановкою символів
Потокові
З одноразовим ключем
З кінечним ключем

Рис. 3

Таблиця 1

Алгоритм	Функція	Розмір блока, біт	Кількість раундів	Довжина ключа, біт	Довжина ключа на раунд, біт	Час генерації ключа	Швидкість процесів шифрування/дешифрування	Криптостійкість	Ефективний криптоаналіз	Основа безпеки
DES (1971)	перестановки та заміни	64	16	56	48	–	V_{DES}	вважається гірше, ніж у ГОСТ	диференційний та лінійний криптоаналіз	збереження ключа в таємниці
ГОСТ 28147-89	перестановки та заміни	64	32	256	32	–	2 V_{DES}	вважається краще, ніж у DES	–	Збереження ключа в таємниці
IDEA (1990)	перестановки та заміни	64	8	128	–	–	V_{DES}	більон комп'ютерів, що тестують по більону ключів за секунду протягом 10^{13} років	диференційний та лінійний криптоаналіз	використання 3-х несумісних операцій над 16-бітними словами; концепція "змішаних операцій з різних алгебраїчних груп"
CAST	перестановки та заміни	–	–	256 (128, 160, 192, 224)	–	–	–	–	–	збереження ключа в таємниці
BLOWFISH (1993)	перестановки та заміни	64	–	от 32 до 48; max 448	–	–	вище V_{DES}	вважається краще, ніж у DES	–	збереження ключа в таємниці
Сімейство RC-алгоритмів	перестановки та заміни	–	від 0 до 2048 (задається при вводі ключа)	32, 64, 128	–	–	2 V_{DES}	–	–	збереження ключа в таємниці

Примітка. – означає "немає даних".

Таблиця 2

Алгоритм	Функція	Розмір блока	Кількість раундів	Довжина ключа	Довжина ключа на раунд	Час генерації ключа	Швидкість процесів шифрування / дешифрування	Криптостійкість	Ефективний криптоаналіз	Основа безпеки
RSA (1978)	дискретне піднесення до степеня	0...N	1	250–300 десятичних розрядів	–	4708,3 мс (Bsafe 3.0 для 1024 bit RSA) T_{RSA}	0,0001 V_{DES} (в апаратній реалізації)	10^4–10^{78} MIPS-років (в залежності від розміру ключа)	розкладання цілих чисел на множники	обчислювальна складність розкладання цілих чисел на множники
Діффі-Хелмана (1976)	дискретне піднесення до степеня	0...P	1	–	–	–	–	–	обчислення дискретного логарифма	складність дискретного логарифмування в кінцевих полях
ElGamal (1985)	дискретне піднесення до степеня	–	1	–	0...P	T_{RSA} / 30	0,001 V_{DES}	вище, ніж у RSA	обчислення дискретного логарифма	складність дискретного логарифмування в кінцевих полях
Еліптичних кривих (1985)	рівняння еліптичних кривих	–	1	–	–	3,8 мс (Security Builder 1.2, 163 bit ECC)	–	–	дискретне логарифмування на еліптичній кривій	складність дискретного логарифмування на еліптичній кривій

Примітка. – означає "немає даних".