Міністерство освіти і науки, молоді та спорту України
Харківський національний університет радіоелектроніки
Приватне акціонерне товариство «Інститут інформаційних технологій»

ГОРБЕНКО І. Д., ГОРБЕНКО Ю. І.

ПРИКЛАДНА КРИПТОЛОГІЯ
ТЕОРІЯ. ПРАКТИКА. ЗАСТОСУВАННЯ

МОНОГРАФІЯ

Харків
Видавництво «Форт»
2012

УДК 003.26
ББК 32.81
Г67

Рекомендовано до видання Науково-методичною радою
Харківського національного університету радіоелектроніки
(Протокол №14 від 23.11.2011)

Рекомендовано до друку Вченою радою
Харківського національного університету радіоелектроніки
(Протокол №6 від 25.11.2011)

Р е ц е н з е н т и:

Скрипник Л.В. – доктор технічних наук, професор, Заслужений діяч науки і техніки, Лауреат державної премії, начальник спеціальної кафедри інституту державної служби спеціального зв'язку та захисту інформації НТТУ КПІ;

Корченко О.Г. – доктор технічних наук, професор, Завідувач кафедри БІТ Національного авіаційного університету, м. Київ;

Стасєв Ю.В. – доктор технічних наук, професор, Заслужений діяч науки і техніки, заступник начальника Харківського університету Повітряних Сил ім. І. Кожедуба.

Горбенко І. Д., Горбенко Ю. І.
Г67 Прикладна криптологія. Теорія. Практика. Застосування: монографія. – Харків: Видавництво «Форт», 2012. – 870 с.

Горбенко І.Д. (Вступ, розділи 1, 2, 3, 4, 7, 8, 9).
Горбенко Ю.І. (Вступ, розділи 1, 5, 6, 7, 8, 9, 10).

ISBN 978-966-8599-99-6

У монографії викладено стан, сутність і сучасні проблемні питання теорії та практики аналізу, синтезу та застосування механізмів, методів і засобів криптографічних перетворень в інформаційних та інформаційно-телекомунікаційних системах різноманітного призначення. Подано методологічні, математичні та прикладні основи криптографічного аналізу, а також теоретичні та практичні основи синтезу й аналізу безпечних механізмів і протоколів. Основними завданнями цієї монографії автори вважають викладення сучасного стану та оцінки напрямів розвитку механізмів, методів, протоколів, систем і засобів криптографічного захисту інформації.

Викладений у монографії матеріал ґрунтується на матеріалі підручника (1989 р.), навчальних посібників, ряду монографій та більш ніж 120 статей і патентів авторів, а також, найголовніше, на більш ніж 70 НДДКР, що виконані авторами практично за сучасними вимогами. Крім того, у монографії використовуються матеріали (з посиланнями на них), отримані у співавторстві або під керівництвом авторів монографії. Автори розуміють, що в наш час стрімкого розвитку інформаційних технологій в сучасній криптографії та криптоаналізі, у тому числі й у галузі криптології практично за менше ніж 10 років змінювалися навіть математичні методи, що застосовуються в даній роботі, але використовуються й раніше розроблені [1–20].

Для науковців, розробників і спеціалістів у галузі криптології, підготовки аспірантів, магістрів і бакалаврів у галузі «Інформаційна безпека», користувачів сучасними інформаційно-телекомунікаційними системами, системами електронних документів та електронного документообігу.

УДК 003.26
ББК 32.81

ISBN 978-966-8599-99-6

ВСТУП

«По-справжньому безпечною можна вважати лише систему, що вимкнена, замурована в бетонний корпус, замкнена в приміщенні зі свинцевими стінами й охороняється збройною вартою, – але й у цьому випадку сумніви не залишають мене».
Юджин Х. Спаффорд

Загально визнаним і безумовним є той факт, що стан розвитку земної цивілізації більшою мірою визначається станом розвитку й застосуванням інформаційних технологій та інформаційно-телекомунікаційних систем у різних сферах нашого буття, здійснення стосунків у межах земної цивілізації.

При цьому основним призначенням і застосуванням інформаційних технологій та інформаційно-телекомунікаційних систем є обробка інформації у відповідності з певними вимогами. Вона здійснюється засобом створення та застосування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, а також автоматизованих систем управління різного призначення. Безумовно, можна також стверджувати, що вказані технології та системи відіграють перш за все суттєву роль у таких сферах, як економіка, інтеграція на міжнародному рівні, виробництво, освіта, наука, державне управління, оборона, безпека життєдіяльності людини, і в цілому визначають національну безпеку. Тобто при функціонуванні вказаних технологій і систем через доступ до інформації та інформаційних ресурсів здійснюється обробка інформації.

Згідно [21, 24, 25, 12], *під обробкою інформації в системі чи технології будемо розуміти «виконання однієї або декількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрацію, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів»*. Тобто обробка інформації є найбільш широким поняттям, яке на теперішній час у явному вигляді не включає тільки механізми та протоколи архівування й архівного зберігання інформації.

На наш погляд, в області стандартизації та уніфікації визначень і понять є ряд протиріч та невизначеностей. Автори цієї монографії вважають за необхідне взяти за основу міжнародні підходи та принципи стандартизації визначень і понять, орієнтуючись на [30–56]. При цьому безпосередньо у вступі ми наводимо базові в галузі криптології визначення й поняття.

Зрозуміло, що наше викладення матеріалу ґрунтується на суттєвих досягненнях світової криптографії. Перш за все в історичному плані хотілося б відзначити історичні постаті й отримані ними результати. Монографія Уільяма Ф. Фрідмана «Індекс співпадання та його застосування в криптографії» стала однією з визначальних праць у криптоаналізі. Наступною найбільш значущою в криптографії є робота К. Шеннона «Теория связи в секретных системах» [1], що була надрукована у відкритому вигляді в 1949 році. Необхідно відзначити й роботу Девіда Канна «Взломщики кодов». У цьому ряді необхідно назвати Хорста Файстеля, Мартина Геллмана, Брюса Шнайєра, Neal Koblitza та ін. Надалі, незважаючи на завіси секретності, ми будемо посилатися на відомих спеціалістів та відмічати їх внески в різні напрями досліджень і розробок. Також необхідно відмітити деяке збурення в криптології, що пов'язане з розвитком та впровадженням новітніх або «просунутих» методів і механізмів: як приклад можна назвати криптосистему NTRU (N-th degree truncated polynomial ring).

З орієнтацією на вищевказане, у монографії будемо використовувати як основну таку систему визначень і понять.

Інформаційна (автоматизована) система *– система, у якій реалізується технологія обробки інформації за допомогою технічних і програмних засобів [21, 12, 13].*

Телекомунікаційна система *– сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи іншим способом [21].*

Інформаційно-телекомунікаційна система *– сукупність взаємопов'язаних інформаційних і телекомунікаційних систем, які в процесі обробки інформації діють як єдина система [21].*

Інформаційно-телекомунікаційна система *– організаційно-технічна сукупність, що складається з автоматизованої системи та мережі передачі даних (наказ СБУ №25 від 13.03.2006).*

Особливо дискусійними при обробці інформації є поняття й визначення, що стосуються інформації та інформаційних ресурсів. Ми не будемо розгортати щодо них дискусій, а вчинимо прагматично – будемо використовувати такі, що визнані й закріплені в стандартах і нормативних документах [31–56].

Інформація в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, інформаційних технологіях – сукупність даних, програм, повідомлень, команд сигналів тощо, які використовуються або передаються в них, незалежно від способу їх фізичного чи логічного подання. Також керівна, науково-дослідна та науково-технічна, проектно-експлуатаційна й інша документація життєвого циклу вказаних систем і технологій.

Інформація – привселюдно оголошені чи опубліковані зведення про події та явища, що відбуваються в суспільстві, природному середовищі і т.д. (Закон України про інформацію) [24].

Таким чином, під *інформацією* будемо розуміти довільні відомості про будь-яку подію, процес, об'єкт, які є предметом сприйняття, передавання, перетворення, збереження чи використання. Інформація може бути кількісною і якісною. *Кількісна інформація* відображається числами. *Якісна інформація* – це візуальні

чи інші враження від розмов, телевізійних програм, газетних повідомлень. Інформація відображає об'єктивну реальність і фіксується на фізичних носіях.

При визначенні поняття інформаційних ресурсів необхідно враховувати ряд факторів та особливостей інформації, що міститься в них. Інформаційні ресурси є об'єктами відносин фізичних, юридичних осіб держави. Розрізняють державні та недержавні інформаційні ресурси.

Державні інформаційні ресурси – інформація, яка є власністю держави та (або) необхідність захисту якої визначено законодавством [21]. Вони складають інформаційні ресурси України і захищаються законом так само, як і інформація.

Інформаційні ресурси підприємства – це сукупність інформації, яку можна отримати на підприємстві.

Інформаційний ресурс також може бути визначений як сукупність документів в інформаційних системах (бібліотеках, архівах, банках даних тощо) [421]. Інформаційні ресурси можуть бути реальними і віртуальними. *Реальні* – це ті ресурси, які на момент потреби в них є в наявності на підприємстві. *Віртуальні* – це ті, яких на момент потреби в них на підприємстві немає, але вони можуть бути отримані ззовні або розраховані за допомогою інформаційної системи управління підприємством.

Дані – інформація, що передається мережею передачі даних, незалежно від способу її фізичного та логічного подання.

На сучасному етапі розвитку суспільства широкого розповсюдження набуло використання специфічно поданої інформації – електронних документів і здійснення на їх основі електронного документообігу, у тому числі електронного врядування, електронної звітності тощо.

Під ***електронним документом*** розуміють інформацію, зафіксовану у вигляді електронних даних, включаючи обов'язкові реквізити документа [23]. Уже перші впровадження підтверджують, що електронний документообіг є найбільш результативним підходом до суттєвого підвищення ефективності роботи органів державної влади та місцевого самоврядування. Також надзвичайно важливим фактором є впровадження електронного документообігу в час розбудови інформаційного суспільства, функціонування технологій електронного управління для забезпечення прозорості відносин «громадянин – держава», «підприємство – держава» та високої якості надання державних, комерційних і банківських послуг.

Великий досвід створення й застосування інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем і різноманітних технологій підтверджує, що користувачам і власникам інформації та електронних ресурсів необхідні якісні послуги із забезпечення безпеки оброблюваної інформації, які мають надаватися їм за їхнім замовленням. Достатньо повно ці послуги визначені в [21–29]. Значною мірою їх якість визначається механізмами, методами, протоколами й засобами криптографічного захисту інформації та ресурсів, які надалі будемо розглядати як послуги криптографічного захисту інформації.

Згідно із [27–30] ***під послугами криптографічної системи будемо розуміти послуги цілісності, автентичності (справжності), неспростовності (спостережливості), доступності, конфіденційності та надійності.***

Нині є декілька визначень указаних послуг з безпеки інформації. Як основні приймемо і будемо враховувати та/або використовувати такі [27–30, 11–13].

Цілісність інформації – властивість захищеності інформації, яка полягає в тому, що інформація практично не може бути змінена випадково чи навмисне неавторизованими суб'єктами (порушниками) чи об'єктами (процесами), причому факт можливості порушення цілісності може бути визначений з наперед заданою ймовірністю.

Цілісність інформації – захист від несанкціонованої модифікації чи знищення інформації.

Автентифікація – заходи захисту, що призначені для встановлення достовірності передачі повідомлення чи відправника або засобів верифікації санкціонування індивідуума для отримання конкретних категорій інформації.

Автентифікація – процедура чи процес встановлення достовірності твердження, що суб'єкт або об'єкт має заявлені (очікувані) властивості.

Як правило, автентифікація має дві складові – ідентифікацію та верифікацію.

Конфіденційність інформації – властивість захищеності інформації з наперед заданою якістю (імовірністю) від неавторизованого доступу до неї та спроб розкриття (отримання змісту) неавторизованими користувачами та (або) процесами.

Конфіденційність інформації – властивість захищеної інформації забезпечувати з наперед гарантованою стійкістю (ймовірністю) захист від неавторизованого доступу до неї та спроб розкриття змісту неавторизованими суб'єктами чи об'єктами (порушниками).

Конфіденційність інформації – гарантія нерозголошування інформації для несанкціонованих об'єктів або процесів.

Доступність – властивість ресурсу системи (інформації, послуги, об'єкта інформаційної та (або) телекомунікаційної системи або ІТС, КСЗІ ІТ тощо), яка полягає в тому, що авторизований користувач і (або) процес, наділений відповідними повноваженнями, може використовувати ресурс згідно з правилами та з певною якістю, у тому числі за рахунок виконання криптографічних перетворень.

Доступність – властивість криптографічної системи, яка полягає в тому, що уповноважений суб'єкт (користувач) чи об'єкт (процес) може здійснювати криптографічний захист інформації згідно з правилами та наперед визначеною якістю (криптостійкістю, імітостійкістю тощо). Доступність криптографічної системи є складовою (як правило, основною, в сенсі рівня гарантій) забезпечення доступності в інформаційних, телекомунікаційних, інформаційно-телекомунікаційних системах тощо.

Неспростовність – властивість запобігання можливості заперечення реальними суб'єктами (користувачами) та об'єктами (процесами) фактів повного або часткового взяття участі в інформаційному обміні або інформаційній взаємодії. Як правило, включає формування, надання та передавання доказів реальної участі в інформаційному обміні чи інформаційній взаємодії і в основному ґрунтується на виконанні криптографічних перетворень з використанням особистих ключів.

Спостережливість – властивість ресурсу системи (комп'ютерної системи, об'єкта комп'ютерної системи, КСЗІ ІТ тощо), що дозволяє реєструвати (фіксувати) роботу та дії користувачів і процесів, використання ресурсу системи, однозначно встановлювати ідентифікатори (імена) причетних до певних подій користувачів та процесів, а також реагувати на ці події з метою мінімізації можливих втрат у системі, що здійснюється, в тому числі, за рахунок використання криптографічних перетворень.

Надійність – властивість незмінності певної поведінки та результатів.

Указані послуги повною мірою можуть бути надані засобом використання як основних симетричних та асиметричних криптографічних перетворень, наприклад, типу шифр, «електронний цифровий підпис», «направлений шифр», а також криптографічних механізмів розподілення таємниці та ключа, встановлення й підтвердження ключа тощо. Однією з фундаментальних системних проблем у цьому напрямку є генерування симетричних і асиметричних пар ключів та відповідне їх зберігання й використання. Розв'язання цієї проблеми ґрунтується на створенні, а також застосуванні на рівні держав, союзів, а то й на міжнародному рівні, симетричних шифрів та інфраструктури відкритих ключів (ІВК). Також особливе місце в наданні перелічених послуг посідають криптографічні перетворення типу «електронний цифровий підпис» [12, 22–26, 31–37, 44–54].

Наступні основні поняття та визначення нами пов'язуються з криптологією, тобто по суті криптографією та криптоаналізом.

Криптологія (en cryptology) – галузь науки, що вивчає основні закономірності, протиріччя, принципи, механізми, методи, протоколи, моделі, системи та засоби криптографічного захисту інформації, здійснення криптоаналізу та приховування фактів обробки інформації та її змісту.

Криптографія (en cryptography) – напрям у криптології, що вивчає основні закономірності, протиріччя, механізми, методи, протоколи, системи, комплекси, алгоритми та засоби криптографічного захисту інформації в ході її обробки.

Криптографічний аналіз (en cryptanalysis) – напрям у криптології, що вивчає основні закономірності, протиріччя, методи, алгоритми, системи й засоби аналізу криптографічних систем, ґрунтуючись на їх вхідних та вихідних даних, алгоритмах чи засобах криптографічних перетворень, у тому числі можливо на частині ключових даних, що здійснюється з метою визначення спеціальних (ключових) даних та значущої інформації.

Криптографічне перетворення (en cryptographic transformation) – перетворення інформації з метою приховування або відновлення її змісту, підтвердження дійсності, цілісності, авторства, захисту від несанкціонованого доступу тощо, що здійснюється з використанням спеціальних (ключових) даних.

Асиметричне криптографічне перетворення (en asymmetric cryptographic technique) – пряме та однозначне йому зворотне криптографічні перетворення інформації, що виконуються з метою криптографічного захисту інформації (приховування її змісту, підтвердження дійсності, цілісності, авторства, захисту від несанкціонованого доступу до інформації тощо), яке здійснюється за допомогою пов'язаних між собою перетворень ключів – особистого та відкритого. Пряме і зворотне перетворення мають таку властивість, що для заданого відкритого перетворення (ключа) обчислювально неможливе одержання особистого перетворення (ключа).

Симетричне криптографічне перетворення (en symmetric cryptographic technique) – пряме та однозначне йому зворотне криптографічні перетворення інформації, що виконуються з метою криптографічного захисту інформації (приховування її змісту, підтвердження дійсності, цілісності, авторства, захисту від несанкціонованого доступу до інформації тощо), які здійснюються з використанням одного й того ж таємного ключа. Пряме і зворотне перетворення мають таку

властивість, що вони виконуються з використанням одного й того ж ключа, або ключів, що зв'язані між собою і один може бути обчислений, якщо відомий інший з поліноміальною складністю.

Криптографічний захист інформації (en cryptographic information security) – вид захисту інформації, що реалізується за допомогою її криптографічного перетворення з метою забезпечення її конфіденційності, дійсності, цілісності, справжності, неспростовності, доступності, спостережливості тощо.

Криптографічний протокол (en cryptographic protocol) – розподілений алгоритм дії чи взаємодії $N \geq 2$ суб'єктів та(чи) об'єктів при обробці інформації, тобто сукупність алгоритмів, які виконуються за допомогою хоча б одного криптографічного перетворення інформації (як кожним із них окремо, так і при обміні між собою), що здійснюються ними з метою мінімізації ризиків унаслідок дії загроз.

Криптографічний алгоритм (en cryptographic algorithm) – набір специфікацій, математичних правил і процедур, за допомогою яких здійснюються криптографічні перетворення, розгортання ключів та управління ключовими даними тощо у межах окремого засобу криптографічного захисту інформації.

Криптографічна стійкість (en cryptographic strength) – здатність криптографічної системи або криптографічного алгоритму протистояти спробам здійснення успішного криптоаналізу з розкриттям або підробленням ключових даних та(або) ключової інформації і, як наслідок, можливості реалізації загроз порушення конфіденційності, цілісності, дійсності, доступності, спостережливості тощо.

Ключові дані (ключ) (en key) – сукупність випадкових або псевдовипадкових значень змінних параметрів криптографічного перетворення інформації, за рахунок яких досягається мета цього перетворення (наприклад: зашифровування, розшифровування, обчислення криптографічного контрольного значення, обчислення електронного цифрового підпису, перевіряння електронного цифрового підпису, формування сертифіката відкритого ключа тощо).

Управління ключовими даними (en key management) – дії, що пов'язані з генеруванням або придбанням, реєструванням, розподіленням (розповсюдженням), сертифікацією, доставкою, уведенням в дію (інсталюванням), зміненням, зберіганням, архівуванням, скасуванням, блокуванням, поновленням, зняттям з реєстрації, обліком та знищенням ключової інформації (даних), а також носіїв ключових даних.

Засіб криптографічного захисту (en security cryptographic facility) – програмний, апаратно-програмний і апаратний засіб, що призначений для здійснення криптографічного захисту інформації.

Залежно від способу реалізації, засоби криптографічного захисту інформації розрізняють за такими типами:

- програмні засоби, що функціонують у середовищі операційних систем електронно-обчислювальної техніки та взаємодіють із прикладним програмним забезпеченням;
- апаратно-програмні засоби, у яких частину або всі криптографічні функції реалізовано в спеціальному апаратному пристрої, що може функціонувати у складі електронно-обчислювальної техніки, керування та використ-

тання якого здійснюється за допомогою спеціального програмного забезпечення;

- апаратні засоби, алгоритми функціонування яких (включаючи криптографічні перетворення та управління ключами) реалізуються в мікроелектронних, механічних, оптичних або інших спеціалізованих пристроях.

Ключові документи (en key document) – матеріальні документи із зафіксованими відповідним чином ключовими даними, що призначені для подальшого практичного їх застосування в процесі криптографічних перетворень інформації та управління ключовими даними.

Криптографічна система (en cryptographic scheme (cryptosystem)) – сукупність засобів криптографічного захисту інформації, необхідної ключової, нормативної, експлуатаційної, а також іншої документації, використання яких забезпечує необхідний рівень конфіденційності, цілісності, дійсності, доступності та спостережливості інформації, що захищається.

Шифрування (en encryption) – процеси криптографічного перетворення інформації, що складаються із взаємно однозначних процесів зашифровування, у результаті виконання якого відкрита інформація відображається у шифр-текст, та розшифровування, у результаті виконання якого шифр-текст відображається у відкриту інформацію.

Електронний підпис (en signature) – дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних.

(Електронний) цифровий підпис (en digital signature) – вид електронного підпису, що отримано за результатами криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити цілісність і справжність даних та ідентифікувати підписувача. Електронний цифровий підпис обчислюється за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

Геш-функція (en hash-function) – функція, яка відображає бітові рядки довільної довжини у бітові рядки фіксованої довжини, що мають щонайменше такі властивості:

1) для заданих вихідних даних обчислювально неможливо знайти відповідні вхідні дані;

2) для заданих вхідних даних обчислювально неможливо знайти інші вхідні дані, що відображаються геш-функцією на ті ж вихідні дані.

Геш-значення (en hash-code) – бітовий рядок, що є вихідним значенням геш-функції.

Генератор випадкової послідовності (en random bit (number) – апаратний або апаратно-програмний засіб, який на засаді процесів випадкової природи походження (фізичних, хімічних, фізико-хімічних тощо) забезпечує формування послідовності символів, яка за статистичними властивостями практично не відрізняється від випадкової послідовності.

Генератор ключових даних (ключів) (en key generator) – засіб, що складається з послідовно об'єднаних генератора (генераторів) випадкової послідовності та засобів формування і тестування ключів певної криптографічної системи або алгоритму.

Функція обчислення криптографічного контрольного значення (en cryptographic check function) – криптографічне перетворення, у якому вхідними даними є таємний ключ і довільний рядок даних, а вихідними даними є результат криптографічного перетворення – криптографічне контрольне значення. Обчислення правильного криптографічного контрольного значення без знання таємного ключа має бути неможливим з наперед визначеною ймовірністю.

Криптографічне контрольне значення (en cryptographic check value) – інформація, що отримана шляхом виконання криптографічного перетворення над блоком вхідних даних через застосування (роботи) функції обчислення криптографічного контрольного значення.

Однобічна функція (en one-way function) – функція з властивістю, що дозволяє з поліноміальною складністю обчислювати для заданих вхідних даних вихідні дані і в той же час робить обчислювально неможливим (експоненційно складним) знаходження для заданих вихідних даних відповідних вхідних даних.

Функція $f(x)$, у якої для всіх x зі скінченної області визначення існує поліноміальний алгоритм обчислення значення $y = f(x)$, але практично для всіх y не існує поліноміального алгоритму обернення функції, тобто знаходження $x = f - 1(y)$.

Криптографічна живучість (en forward security) – властивість криптографічної системи забезпечувати необхідний рівень криптографічної стійкості криптографічних перетворень в умовах компрометації призупинених в дії, заархівованих, чергових, а також часток діючих ключових даних і ключової інформації.

Ключова інформація (en key information) – ключові дані (ключі), значення розділюваного таємного ключа, значення для ініціалізації криптографічних засобів та їх елементів, синхронізуючі послідовності тощо.

Автентифікація (en authentication) – процедура або процес встановлення достовірності твердження, що суб'єкт або об'єкт має заявлені (очікувані) властивості.

Як правило, автентифікація має дві складові – ідентифікацію та верифікацію.

Ідентифікація (en identification) – процеси присвоєння суб'єкту чи об'єкту унікального позначення, імені чи коду (ідентифікатора), характерної ознаки, наявність яких дозволяє однозначно виділити даний суб'єкт чи об'єкт серед множини йому подібних, а також процес пред'явлення суб'єктом чи об'єктом цього ідентифікатора.

Верифікація (en verification) – процеси встановлення відповідності засобу криптографічного захисту інформації чи алгоритму криптографічних перетворень еталонному засобу чи алгоритму, причому еталонним вважається засіб, що пройшов спеціальні дослідження. Реалізація алгоритму криптоперетворень вважається еталонною, якщо вона перевірена на правильність.

Захист від несанкціонованого доступу (з обов'язковим застосуванням засобів криптографічного захисту) (en protection from unavtorized access) – гарантоване запобігання або забезпечення необхідної ймовірності захисту від несанкціонованого доступу до інформації засобом забезпечення необхідного рівня надання таких послуг, як конфіденційність, доступність, спостережливість, цілісність, дійсність тощо, перш за все за рахунок виконання криптографічних перетворень інформації, що захищається.

Імітостійкість (en imitation insertion) – здатність криптографічної системи, що застосовується в інформаційній, телекомунікаційній чи інформаційно-

телекомунікаційній системах, протистояти нав'язуванню хибної чи викривленої інформації будь-якими порушниками будь-якими способами та засобами. У вузькому розумінні чисельні характеристики складності та ймовірності нав'язування неправдивої (хибної, викривленої тощо) інформації, з урахуванням методів і потужності засобів, що застосовуються порушниками.

Вхідний алфавіт криптографічного перетворення (en plain text) – сукупність символів алфавіту, у якому подається інформація (дані), що підлягає криптографічному перетворенню. Вхідний алфавіт може бути літерний, цифровий літерно-цифровий, символьний тощо.

Вихідний алфавіт криптографічного перетворення (en ciper text) – сукупність символів алфавіту, у якому подано результат криптографічного перетворення інформації (даних). Вихідний алфавіт може бути літерний, цифровий, літерно-цифровий, символьний тощо. Вихідний алфавіт може відрізнятися від вхідного алфавіту криптографічного перетворення.

Примітка. Результатом криптографічного перетворення може бути шифр-текст, криптографічне контрольне значення, електронний цифровий підпис, імітоприкладка, геш-значення тощо.

Відкритий текст (en plain text) – результат подання інформації (даних, текстів), що підлягає захисту, у вхідному алфавіті криптографічного перетворення.

Шифр-текст (зашифровані дані) (en cipher text) – результат криптографічного перетворення відкритого тексту (даних), що поданий у вихідному алфавіті криптографічного перетворення.

Шифр (en cipher) – сукупність взаємно однозначних відображень за допомогою криптографічних перетворень відкритого тексту (даних) у шифр-текст (зашифровані дані), і навпаки, шифр-тексту (зашифрованих даних) у відкритий текст (дані).

Блоковий шифр (en block cipher) – шифр, у якому криптографічне перетворення здійснюється при зашифровуванні на блоках відкритих даних (тексту), а при розшифровуванні – на блоках зашифрованих даних (текстів).

Потоковий шифр (en stream cipher) – шифр, у якому криптографічні перетворення зашифровування та розшифровування символів здійснюються послідовно.

Зашифровування (en encryption) – вид криптографічного перетворення інформації, що здійснюється з метою приховування змісту інформації, яка захищається, у результаті виконання якого відкрита інформація відображається в зашифровану (шифр-текст).

Розшифровування (en decipherment) – вид криптографічного перетворення інформації, що здійснюється з метою відновлення змісту інформації, яка прихована в зашифрованій інформації (шифр-тексті), у результаті виконання якого зашифрована інформація (шифр-текст) відображається у відкриту інформацію, тобто з доступним семантичним змістом.

Шифратор (en krypton, ciphermachien) – програмний, апаратно-програмний або апаратний засіб, що забезпечує виконання операцій введення, захищеного зберігання, вироблення, контролювання, використання та знищення ключових даних, зашифровування відкритих даних (текстів) та розшифровування зашифрованих даних (текстів).

Простір ключів (en key space) – множина $\{K\}$ усіх ключів, що дозволені для використання в даній криптосистемі. Головними вимогами до ключів є випадковий, рівноймовірний та незалежний вибір із повного простору, а у деяких випадках і максимальна кількість нееквівалентних ключів.

Слабкий ключ (en weak key) – ключ, при застосуванні якого стійкість криптографічного перетворення знижується до неприпустимого рівня або просто знижується.

Еквівалентні ключі (en equivalent keys) – два ключі $K1$ та $K2$ із простору ключів $\{K\}$ вважаються еквівалентними, якщо для прямих криптоперетворень $F(K1)$ та $F(K2)$ зворотні перетворення $F-(K1)$ та $F-(K2)$ мають таку властивість: $F-(K1)(x) = F-(K2)(x)$ для будь-яких криптографічно захищених даних $x \in X$ (наприклад, для будь-яких зашифрованих даних $x \in X$).

Стійкість криптографічного перетворення (en cryptographic technique strength) – абсолютні або відносні чисельні характеристики оцінки складності та ймовірності здійснення успішного криптоаналізу з урахуванням рівня порушника, математичних методів та потужності засобів криптоаналізу, що застосовуються.

Безпечний час (en secure time) – математичне сподівання часу здійснення успішного криптоаналізу з урахуванням методів та потужності засобів криптоаналізу, що застосовуються.

Досконала (безумовна) стійкість шифрування (en proved encryption strength) – криптографічна стійкість шифру, за якої у криптоаналітика не існує можливостей отримати будь-яку інформацію щодо відкритого тексту (даних) і ключа, що застосований при зашифровуванні, незалежно від методів і потужності засобів криптоаналізу.

Примітка. Необхідною й достатньою умовою безумовної стійкості є $P(C_J / M_i) = P(C_J)$, тобто ймовірність появи в системі C_J шифр-тексту не повинна залежати від відкритого тексту M_i, що зашифровується.

Обчислювальна стійкість криптографічного перетворення (en computationallystrength cryptographic technique) – стійкість криптографічних перетворень, для яких безпечний час криптосистеми $t_б$ набагато більше часу цінності інформації $t_{ці}$, що захищається, і при цьому не існує жодного методу криптоаналізу, складність якого може бути меншою, ніж складність атаки перебирання всіх ключів.

Примітка. Складність криптоаналізу в обчислювально стійких криптосистемах має експоненційний характер.

Імовірно стійкі криптографічні перетворення (en probabilistic strong cryptographic technique) – стійкість криптографічних перетворень, для яких безпечний час $t_б$ на багато більше часу цінності інформації $t_{ці}$, що захищається, причому криптоаналіз таких систем зводиться до розв'язання деяких математичних задач, складність яких є меншою, ніж складність атаки перебирання всіх ключів.

Примітка. Для ймовірно стійких криптосистем можуть існувати методи криптоаналізу, складність яких є набагато меншою ніж тих, що відомі на цей час. Складність криптоаналізу ймовірно стійких криптосистем має субекспоненційний характер.

Обчислювально нестійкі криптографічні перетворення (en computationally strong cryptographic technique) – стійкість криптографічних перетворень, для

яких безпечний час t_6 криптосистеми одного порядку або менше часу цінності інформації, що захищається.

Відстань єдності шифру (en proved encryption strength) – мінімально необхідне число символів шифр-тексту (зашифрованих даних), наявність яких дозволяє однозначно визначити відкритий текст (дані) без знання ключових даних.

Примітка. Як правило, необхідно 10 підряд розміщених символів шифр-тексту (зашифрованих даних).

Гама шифрування (en encryption gamma) – псевдовипадкова послідовність символів довільного алфавіту m з наперед відомими статистичними властивостями та періодом повторення, конкретна реалізація якої залежить від ключової інформації, що вводиться в засіб формування гами шифрування.

Одноразова гама шифрування (en one-time encryption gamma) – послідовність символів довільного алфавіту m, яка сформована на основі процесів випадкової природи і за статистичними властивостями практично не відрізняється від випадкової послідовності. Використовується один раз для зашифровування та розшифровування і має бути знищена після кожного використання.

Імітоприкладка (імітовставка, код автентифікації повідомлення) – криптографічне контрольне значення у вигляді рядка бітів фіксованої довжини, що додається до інформації, яка захищається (повідомлення, даних, команд, програм тощо), для забезпечення імітозахисту.

Повідомлення (en message) – бітовий рядок будь-якої довжини.

Ключ сеансу (сеансовий) (en randomizer) – елемент таємних даних, який виробляється суб'єктом, що підписує, у підготовчому процесі вироблення підпису і який не може бути передбачений іншими суб'єктами.

Функція вироблення ключових даних (ключа) (en key generating function) – функція, яка приймає на вході декілька параметрів, щонайменше один з яких має бути таємним, та видає на виході ключові дані, які відповідають заданому криптографічному перетворенню та умовам застосування. Функція повинна мати таку властивість, що обчислювально неможливо встановити вихідні (ключові) дані без попереднього знання таємних вхідних (вхідного) параметрів.

Узгодження ключів (en key agreement) – процес встановлення розділюваної таємниці (ключа) між суб'єктами таким чином, щоб жоден із суб'єктів практично (з наперед заданою великою ймовірністю) не міг наперед визначити значення цієї таємниці.

Встановлення ключів (en key establishment) – процес забезпечення доступності розділюваної таємниці (ключа) для одного чи багатьох суб'єктів (об'єктів). Встановлення ключів включає узгодження та передавання ключів.

Інфраструктура відкритого ключа (en public key infrastructure) – інфраструктура, що здійснює управління відкритими ключами з метою надання послуг цілісності, дійсності (автентифікації), неспростовності та конфіденційності.

Автентифікація суб'єкта (об'єкта) (en entity authentication) – підтвердження (доказ) того, що суб'єкт (об'єкт) є тим, за кого він себе видає.

Проста автентифікація (en simple authentication) – автентифікація, що виконується за допомогою використання паролів.

Сувора автентифікація (en strong authentication) – автентифікація, що засвідчує користувача (надає посвідчення особи) з використанням засобів криптографічного захисту інформації.

Диференційний криптоаналіз (en differential cryptoanalysis) – метод криптоаналізу, що засновується на використанні залежності відмінностей між вхідними та вихідними даними в блокових і потокових шифрах.

Лінійний криптоаналіз (en linear cryptoanalysis) – метод криптоаналізу, що засновується на пошуку лінійних апроксимацій між вхідними (вихідними) та ключовими даними потокових і блокових шифрів.

Криптоаналіз «брутальна сила» (en brute force cryptanalysis) – метод криптоаналізу криптографічно захищених даних (текстів), що ґрунтується на перебиранні ключів із повного простору ключів.

Криптоаналіз методом факторизації модуля (en factorization problem) – метод визначення особистого ключа з асиметричної ключової пари (E, D), основна частка складності якого полягає у розв'язанні задачі канонічного розкладання модуля перетворення N на прості співмножники.

Криптоаналіз методом розв'язання дискретного логарифмічного рівняння (en cryptanalysis by method of discrete logarithm problem solution) – метод визначення особистого ключа X з асиметричної пари ключів (X, Y), що ґрунтується на розв'язанні дискретного логарифмічного рівняння $Y = \Theta^X (\mathrm{mod}\ P)$ відносно X.

Криптоаналіз розв'язання дискретного логарифмічного рівняння в групі точок еліптичних кривих (en cryptanalysis by method of discrete logarithm on elliptic curves problem solution) – метод визначення особистого ключа d з асиметричної пари ключів (d, Q), що ґрунтується на розв'язанні дискретного логарифмічного рівняння в групі точок еліптичних кривих $Q = d \cdot G (\mathrm{mod}\ Q)$ відносно d.

Ефективність атаки криптоаналізу (en cryptanalysis attack efficiency) – степінь зменшення складності криптоаналізу для заданого методу у порівнянні зі складністю криптоаналізу з перебиранням усіх ключів.

Засіб електронного цифрового підпису – програмний засіб, програмно-апаратний або апаратний пристрій, призначений для генерації ключів, накладення та (або) перевірки електронного цифрового підпису. Вироблення електронного цифрового підпису здійснюється з використанням особистого ключа, перевіряння підписаної інформації за допомогою відкритого ключа.

Особистий ключ – це параметр криптографічного алгоритму формування електронного цифрового підпису, доступний тільки підписувачу.

Відкритий ключ – параметр криптографічного алгоритму електронного цифрового підпису, доступний суб'єктам відносин у сфері використання електронного цифрового підпису.

Для надійного використання відкритого ключа виконується засвідчення його чинності – процедура формування сертифіката відкритого ключа. На національному рівні сертифікат відкритого ключа (далі сертифікат ключа) – документ, виданий центром сертифікації ключів, який засвідчує чинність і належність відкритого ключа підписувачу. Сертифікати ключів можуть розповсюджуватися в електронній формі документа на папері та використовуватися для ідентифікації особи підписувача.

Монографія складається з 10 розділів і переліку джерел. Поданий тут матеріал отримано за останні 12 років у практичній діяльності авторів: участі у проектуванні, експертизі, впровадженні та застосуванні систем, комплексів та засобів криптографічного захисту інформації, виконанні ряду НДР, у тому числі відносно

інфраструктур відкритих ключів, включаючи систему ЕЦП України. Також використані навчальні матеріали та електронні лекції з дисциплін «Основи теорії захисту інформації» та «Криптографічні системи та протоколи», що підготовлені й читалися на курсі професором Горбенко І.Д. в ХНУРЕ у 1995 – 2011 роках.

У монографії викладені стан, сутність і сучасні проблемні питання теорії та практики практичної криптології.

У Розділі 1 наведено основні відомості щодо перспективних математичних методів, що застосовуються або будуть, на думку авторів, застосовуватись у криптографії та криптоаналізі. По суті, основна увага приділяється математиці еліптичних та гіпереліптичних кривих, парним відображенням (спарюванню) точок еліптичних кривих, перетворенням у зрізаних кільцях поліномів тощо. У цьому розділі наведено мінімальні відомості, що потрібні для засвоєння завдань сучасної криптології. Інші математичні відомості й теоретичні положення можна знайти у джерелах, на які є посилання в тексті. Ми також наводимо основні математичні відомості з теорії та практики криптології, які стосуються криптосистеми NTRU (N-th degree truncated polynomial ring). Різні аспекти цієї криптосистеми розглядаються також у Розділах 3, 5 та 9.

У Розділі 2 розглядаються основні положення з теорії та деякою мірою й практики симетричних криптоперетворень і симетричних криптосистем. Робиться класифікація та розглядаються основні функції криптологічних систем, а також моделі порушника та загроз. Наведено структурні схеми та моделі захищених інформаційної та інформаційно-телекомунікаційної систем. Розглядаються питання вступу в теорію криптографічної стійкості, умови та приклади реалізації криптосистем з безумовним рівнем стійкості, умови реалізації обчислювальної та ймовірної стійкості криптоперетворень. Подано математичні моделі основних симетричних криптографічних перетворень та їх властивості. Дається опис та аналіз перспективних блокових і потокових шифрів.

У Розділі 3 розглядаються теоретичні та практичні питання асиметричної криптографії. У тому числі асиметричні криптоперетворення, що реалізуються в кільцях та простих полях Галуа, групах точок еліптичних кривих та гіпереліптичних кривих, засобом спарювання точок еліптичних кривих, перетворення в кільцях урізаних поліномів тощо. Методи оцінки криптографічної стійкості та складності реалізації асиметричних криптоперетворень. Розглядаються двохключові криптографічні (асиметричні) перетворення, у тому числі методи й засоби генерування ключів для асиметричних криптоперетворень у кільцях, полях, групах точок еліптичних кривих і парних відображень, що можуть або застосовуються для направленого (асиметричного) шифрування. Розглядаються й аналізуються перспективні стандартизовані асиметричні (направлені) шифри. Наведено результати аналізу основних прикладних задач, проблемні питання і напрями розвитку теорії та практики асиметричних криптоперетворень у кільцях, полях Галуа, у групах точок еліптичних та гіпереліптичних кривих, зі спарюванням точок еліптичних кривих, у кільцях урізаних поліномів тощо.

У Розділі 4 розглядаються теоретичні положення та методи автентифікації. В якості основної вибрана модель взаємної недовіри та взаємного захисту. Обґрунтовуються та вибираються критерії та показники оцінки якості автентифікації. Наведено інформаційний підхід до оцінки та забезпечення автентичності, доско-

налі та практично реалізовані системи автентифікації та умови їх реалізації, методи автентифікації на основі використання симетричних криптосистем. Аналізуються прості та суворі системи (протоколи) автентифікації. Робиться порівняльний аналіз методів автентифікації. Розглядаються канали НСД до інформації та ресурсів, а також методи захисту від НСД. Також розглядаються питання теорії та практики криптографічного захисту інформації в радіоканалах та основні прикладні задачі, проблемні питання теорії та практики забезпечення імітозахисту.

Розділ 5 присвячений теорії та практиці управління ключами, в першу чергу генеруванню ключів. Зважаючи на важливість, матеріал, що стосується генерування ключів, ми виділяємо окремо. У ньому викладається, на наш погляд, сучасний стан генерування випадкових послідовностей (чисел). У тому числі розглядаються й аналізуються ключові системи в криптографічних системах, основні положення в частині управління ключами, дається визначення та робиться аналіз вимог до (протоколів) генерування ключів, обговорюються властивості випадкових і псевдовипадкових послідовностей, методики тестування детермінованих випадкових послідовностей. Наведено класифікацію та характеристику генераторів випадкових чисел, а також вимоги до детермінованих генераторів випадкових бітів, базова структурна схема ДГВБ. Розглядаються основні методи та алгоритми генерування ВП ПВП, у тому числі перспективні. Матеріал цього розділу, на наш погляд, є суттєво оригінальним, він підготовлений на основі серії статей Ю.І. Горбенко.

У Розділі 6 розглядаються теоретичні та практичні питання (електронного) цифрового підпису, в тому числі критерії та показники оцінки якості цифрових підписів, основні види атак та загрози цифровому підпису. Аналізуються існуючі цифрові підписи й такі, що мають нині практичне значення, з доповненням і відновленням повідомлень, кільцеві та групові підписи. Наведено основні методи оцінки криптографічної стійкості та складності цифрових підписів, питання стандартизації цифрових підписів та функцій гешування. Аналізуються основні прикладні задачі та проблемні питання теорії та практики цифрових підписів.

У Розділі 7 розглядаються основні положення теорії та практики криптографічних протоколів. Дається ґрунтовна класифікація криптографічних протоколів, у тому числі протоколи встановлення й узгодження ключів, автентифікації, автентифікація та встановлення ключів; методи ідентифікації та автентифікації з нульовими розголошеннями, протоколи розподілу таємниці. Зважаючи на особливу важливість, даються основні поняття та введення у фізику квантових обчислень, аналізуються протоколи квантового розподілу ключів та відповідні оцінки безпеки криптографічних протоколів.

У Розділі 8 розглядаються методи та алгоритми криптографічного аналізу симетричних криптосистем, у тому числі основні положення криптоаналізу. Подається класифікація методів криптоаналізу, критерії та показники оцінки складності процесів криптоаналізу. Основна орієнтація робиться на блокові та потокові симетричні шифри. Матеріал цього розділу певною мірою пов'язаний з Розділом 2, по суті, у Розділі 7 розглядаються методи криптоаналізу шифрів, які розглянуто в Розділі 3.

У Розділі 9 розглядаються методи й алгоритми криптоаналізу асиметричних криптосистем, у тому числі методи й алгоритми криптоаналізу асиметричних криптосистем у кільцях, полях і групах точок еліптичних і деякою мірою гіпер-

еліптичних кривих. Також наведено методи криптоаналізу перетворень зі спарюванням точок еліптичних кривих і перетворень в зрізаних кільцях поліномів на алгебраїчних решітках. Розглядаються проблемні питання теорії та практики криптоаналізу асиметричних криптоперетворень.

У Розділі 10 ми наводимо результати досліджень і розробок, що досягнені в останні роки як авторами, так і на світовому рівні. Особлива увага приділена проблемним питанням оцінки стійкості криптографічних перетворень і безпеці криптографічних протоколів. Обговорюються тенденції розвитку криптології та робляться деякі прогнози. Ми враховуємо велику динаміку розвитку та вдосконалення в криптології, закритість досліджень, особливо в частині криптоаналізу. Тому викладення ведеться з урахуванням вказаної специфіки.

Монографія адресована в першу чергу розробникам криптографічних систем, спеціалістам, що пов'язані з експлуатацією та застосуванням криптографічних систем, комплексів і засобів інформації в інформаційних та інформаційно-телекомунікаційних системах, для підготовки докторантів та аспірантів, магістрів і бакалаврів у галузі «Інформаційна безпека». Ми сподіваємося, що монографія послугує подальшому розвитку національної системи криптографічного захисту інформації, системи електронного цифрового підпису, її трансформації в ІВК, що є традиційною в технологічно розвинених державах, вирішенню завдань взаємодії на міжнародному та міждержавному рівнях.

Ми з розумінням ставимося до того, що в монографії не враховано багато поглядів інших авторів, у ній проглядається недостатній рівень деталізації. Але необхідно зізнатися, що монографія є першим кроком підручника, який планується написати на її основі. З урахуванням вищевказаного і здійснювався відбір матеріалу.

Виражаємо вдячність ректору Харківського національного університету радіоелектроніки, члену-кореспонденту Національної академії наук України професору Бондаренко М.Ф за спонукання та підтримку в написанні монографії, генеральному директору ЗАТ «Інститут інформаційних технологій» Сінаюку С.Ю. за підтримку та фінансове забезпечення видання. Ряд поданих у монографії результатів, на які є посилання в тексті, отримані разом зі співробітниками кафедри й аспірантами, а також співробітниками ЗАТ «Інститут інформаційних технологій» під час спільної роботи.

Безумовно, як завжди, велика подяка Горбенко Ганні Миколаївні та Горбенко Ользі Миколаївні, які терпіли та підтримували нашу роботу над монографією в останні роки.

Дуже вдячні рецензентам монографії:

доктору технічних наук, професору, заслуженому діячу науки і техніки, Лауреату державної премії, начальнику спеціальної кафедри інституту державної служби спеціального зв'язку та захисту інформації НТТУ КПІ, Скрипнику Леоніду Васильовичу;

доктору технічних наук, професору, завідувачу кафедри Національного авіаційного університету, м. Київ, Корченко О.Г.;

доктору технічних наук, професору, Лауреату державної премії, заступнику начальника Харківського університету Повітряних Сил ім. І. Кожедуба, Стасєву Юрію Володимировичу.

Також попередньо вибачаємось за можливі похибки та неспівпадання наших поглядів з поглядами інших спеціалістів. Будемо вдячні всім за висловлені зауваження та побажання щодо матеріалу та результатів, наведених у монографії. Відповідальність за всі погрішності й можливі помилки автори залишають за собою. Але більшість результатів впроваджені на практиці і, на наш погляд, пройшли добру апробацію. Останнє дає нам наснагу та сили для подальшої роботи – сподіваємось, що основний матеріал цієї монографії ми використаємо при підготовці підручника «Прикладна криптологія».

Автори вдячні робочій групі видавництва «Форт», яка взяла участь у виданні книги. Зокрема Едуарду Миколайовичу Олійнику за інтерес, що був виявлений до цієї книги, й активне співробітництво; Кліменко Світлані Олександрівні, яка читала й редагувала рукопис; Бондаренко Олені Сергіївні, яка правила верстаний матеріал і готувала рукопис до друку. Ми щиро вдячні їм за критичні зауваження та пропозиції, окремо за увагу й терпіння. Якщо, незважаючи на наші зусилля, похибки чи помилки в тексті все ж таки залишилися, то відповідальність за них автори залишають за собою.