НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ
КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

Терміни та визначення

ДСТУ _____

(Проект)

Видання офіційне

Київ

ДЕРЖСПОЖИВСТАНДАРТ УКРАЇНИ

200_

ПЕРЕДМОВА

1 РОЗРОБЛЕНО: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби Безпеки України (ДСТСЗІ СБ України), Національна академія наук України (НАН України), ЗАТ "Інститут інформаційних технологій"
РОЗРОБНИКИ: І. Коваленко, д-р фіз.-мат. наук, д-р техн. наук, академік НАН України; І. Горбенко, д-р техн. наук; Г. Гулак; О. Потій, канд. техн. наук; Ю. Горбенко
2 ПРИЙНЯТО ТА НАДАНО ЧИННОСТІ: _____
3 ВВЕДЕНО ВПЕРШЕ

ЗМІСТ

ВСТУП

Даний стандарт складений ДСТСЗІ СБ України та містить 67 українських термінів і визначень до них із теорії та практики криптографічного захисту інформації. Метою його розробки було узагальнення та встановлення єдиного тлумачення термінології, яка використовується в галузі криптографічного захисту інформації.

При розробленні стандарту відбиралися тільки ті терміни, що набули порівняно широкого практичного застосування.

ДСТУ _____

НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ
КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ
Терміни та визначення

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ
Термины и определения

INFORMATION TECHNOLOGY
CRYPTOGRAPHIC PROTECTION OF INFORMATION
Terms and definitions

Чинний від _____

1 СФЕРА ЗАСТОСУВАННЯ

Цей стандарт встановлює терміни та визначення понять у сфері криптографічного захисту інформації.

Терміни, подані в цьому стандарті, рекомендовано для вживання в технічній та експлуатаційній документації, а також у довідковій та навчально-методичній літературі, що належить до сфери криптографічного захисту інформації.

Терміни стандарту рекомендовано для використання організаціями, установами усіх форм власності та іншими суб’єктами, які проводять діяльність у сфері криптографічного захисту інформації.

2 ЗАГАЛЬНІ ПОЯСНЕННЯ

2.1 Для кожного поняття встановлено один, а в окремих випадках – два застандартизовані терміни. Проте, використовуючи застандартизовані терміни, у межах одного документу слід вживати лише один із термінів-синонімів.

2.2 Наявність квадратних дужок у терміні і визначенні певної термінологічної статті означає, що в ній суміщено дві терміностатті, у яких переважає однаковий текст. Першу статтю треба читати, беручи до уваги текст поза дужками разом з текстом у першій парі квадратних дужок, пропускаючи текст у інших парах дужок. Другу статтю читають, замінюючи текст першої пари квадратних дужок текстом другої пари квадратних дужок і т. д. Наприклад, в термінологічній статті

блок [відкритого тексту] [шифртексту]

Частина [відкритого тексту] [шифртексту], що подана певним числом символів відповідного алфавіту, та розмір якої визначається певним алгоритмом криптографічного перетворення

суміщено дві терміностатті

блок відкритого тексту

Частина відкритого тексту, що подана певним числом символів відповідного алфавіту, та розмір якої визначається певним алгоритмом криптографічного перетворення

та

блок шифртексту

Частина шифртексту, що подана певним числом символів відповідного алфавіту, та розмір якої визначається певним алгоритмом криптографічного перетворення

В абетковому покажчику суміщені терміни подано окремо без дужок, з посиланням на той самий номер терміностатті.

2.3 Наявність квадратних дужок лише у терміні певної термінологічної статті означає, що в ньому суміщено два або більше термінів-синонімів.

2.4 У інших документах визначення понять, встановлені цим стандартом, можна змінювати, вводячи до них похідні ознаки, розкриваючи зміст поняття,

зазначаючи об'єкти, що належать обсягові виозначуваного поняття. Зміни не повинні порушувати обсягу і змісту понять, визначених у стандарті.

2.5 Терміни встановлені цим стандартом та вжиті у визначеннях, виділено підкресленням.

2.6 У стандарті, як довідкові, подано англійські (en) та російські (ru) терміни-еквіваленти застандартизованих термінів, узяті з міжнародних та національних стандартів, словників та науково-технічної літератури.

2.7 У терміностаттях поряд із кожним іменником на позначення конкретної події, що відбулася, або має відбутися, подано дієслова в фігурних дужках.

2.8 Пояснення, подані в круглих дужках світлим шрифтом після термінів, що зазначають сферу вживання багатозначних термінів, не є частинами термінів.

2.9 У вузькоспеціалізованих документах узяту в круглі дужки (набрану жирним шрифтом частину терміна) можна не вживати, а використовувати його коротку форму.

3 ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ

3.1 **[абсолютна] [досконала] стійкість**

Властивість шифру, що полягає в неможливості отримання будь-якої інформації про відкритий текст або ключ при застосуванні даного шифру

en [perfect] [unconditional] secrecy
ru [абсолютная] [совершенная] стойкость

3.2 **автентифікація {автентифікувати}**

Встановлення {встановити} справжності {-ість} твердження, що [об'єкт] [суб'єкт] має очікувані властивості

en authentification
ru аутентификация

Примітка. Автентифікація включає в себе дві процедури: ідентифікацію та верифікацію

3.3 **алфавіт [відкритого тексту] [шифртексту]**

Алфавіт, яким подано [відкритий текст] [шифртекст]

en [plaintext] [chiphertext] alphabet
ru алфавит [открытого текста] [шифртекста]

Примітка 1. Алфавітом є довільна скінченна непорожня множина деяких символів. Розрізняють літерний, цифровий (двійковий, десятковий), літерно-цифровий (змішаний) та ін. алфавіти.

Примітка 2. Відкритий текст і шифртекст можуть подаватися як в однакових, так і в різних алфавітах.

3.4 **блок [відкритого тексту] [шифртексту]**

Частина [відкритого тексту] [шифртексту], що подана певним числом символів відповідного

en [plaintext] [ciphertext] block
ru блок [открытого

алфавіту, та розмір якої визначається певним алгоритмом криптографічного перетворення

текста] [шифртекста]

3.5 **блоковий шифр**

Шифр, в якому криптографічне перетворення задається на блоках [відкритого тексту] [шифртексту]

en block cipher
ru блочный шифр

3.6 **верифікація {верифікувати}**

Перевірка {перевірити} ідентифікатора {ідентифікатор} або правильності {-ість} реалізації алгоритму криптографічного перетворення

en verification
ru верификация

3.7 **відкритий текст**
відкрите повідомлення

Будь-яке повідомлення над яким ще не здійснено чергову операцію шифрування

en plaintext, plaintext message
ru открытый текст, открытое сообщение

Примітка. Відкрите повідомлення може також бути попередньо зашифроване.

3.8 **відстань єдиності шифру**

Мінімально необхідне число символів шифртексту, яке дозволяє без знання ключа однозначно знайти відкритий текст

en cipher unicity distance
ru расстояние единственности шифра

3.9 **гама**

Послідовність [величин] [символів], що належать [скінченній множині] [алфавіту]

en gamma
ru гамма

3.10 **генератор [випадкової] [псевдовипадкової] послідовності**

Засіб формування послідовності символів, яка за певними статистичними властивостями близька до випадкової послідовності

en random [bit] [number] generator

ru генератор случайной последовательности

Примітка. Якщо засіб формування послідовності символів заснований на використанні реальних процесів випадкової природи (наприклад, шумових процесів радіоелементів) маємо генератор випадкової послідовності; якщо послідовність символів генерується програмним методом, маємо генератор псевдовипадкової послідовності.

3.11 **генератор ключів**

Генератор [випадкової] [псевдовипадкової] послідовності, об’єднаний з засобом формування та тестування ключів певного криптографічного алгоритму

en key generator

ru генератор ключей

3.12 **дешифрування {дешифрувати}**

Застосування {застосувати} криптоаналітичної {-у} атаки {-у}, спрямованої на перетворення шифртексту у відкритий текст без знання ключа або розкриття ключів криптографічного перетворення з використанням наявних науково-технічних засобів та методів

en attack on a cipher

ru дешифрование

3.13 **досконалий шифр**

Шифр, що має [досконалу] [абсолютну] стійкість

en perfect cipher

ru совершенный шифр

3.14 **зашифрування {зашифрувати}**

Перетворення {перетворити} відкритого {-ий} тексту {текст} у шифртекст

en encryption

ru зашифрование

3.15 **розшифрування {розшифрувати}**

Відновлення {відновити} відкритого {-ий} тексту {текст} з шифртексту за відомими ключами

en decryption

ru расшифрование

3.16 **шифрування**

Процеси зашифрування та розшифрування

en encryption

ru шифрование

3.17 **попереднє шифрування**

Шифрування повідомлення за деякий час до його пересилання лініями зв'язку, або перед застосуванням основного криптографічного алгоритму в повному обсязі

en primary encryption

ru предварительное шифрование

3.18 **[лінійне] [познакове] шифрування**

Шифрування повідомлення, яке здійснюється одночасно з його пересиланням лініями зв'язку

en linear encryption

ru [линейное] [поточное] шифрование

3.19 **[наскрізне] [абонентське] шифрування**

Шифрування повідомлення на ключі абонента, яке залишається зашифрованим цим ключем до отримання, незалежно від каналу пересилання

en end-to-end encryption

ru [сквозное] [абонентское] шифрование

3.20 **канальне шифрування**

Шифрування повідомлення, яке передається на відрізку міжстанційного з'єднання

en channel encryption

ru канальное шифрование

3.21 **еквівалентні ключі**

Різні ключі, на яких результати зашифрування однакових відкритих текстів і розшифрування однакових шифртекстів збігаються, для будь-якого відкритого тексту або шифртексту

en equivalent keys

ru эквивалентные ключи

3.22 **ідентифікація {ідентифікувати}**

Присвоєння {присвоїти} [суб'єктом] [об'єктом] та пред'явлення {пред'явити} [суб'єкту] [об'єкту] ідентифікатора {ідентифікатор}

en identification

ru идентификация

3.23 **імітовставка**

код автентифікації повідомлення

Відрізок даних фіксованої довжини, отриманий за певним правилом з відкритого тексту і ключа та доданий до [відкритого тексту] [шифртексту] для забезпечення імітозахисту

en imitation insertion

ru имитационная вставка

3.24 **імітозахист**

Захист повідомлення від його модифікації

en imitation security,
imitation defence

ru имитозащита

3.25 **імітостійкість (криптографічної системи)**

Здатність криптографічної системи протистояти нав'язуванню неправдивої інформації будь-якими відомими способами

en imitation resistance

ru имитостойкость

Примітка. Імітостійкість криптографічної системи є чисельною характеристикою складності здійснення спроби імітації

3.26 **управління ключами**

Сукупність функцій (дій), що пов’язані з генеруванням, реєструванням, сертифікацією, розподіленням (розповсюдженням), уведенням в дію (інсталюванням), розгортанням, зберіганням, архівуванням, скасуванням (видаленням), зняттям з реєстрації та знищенням ключів

en key management
ru управление ключами

3.27 **ключ**
ключові дані

Конкретний секретний стан деяких параметрів криптографічного алгоритму перетворень даних, які забезпечують вибір одного криптографічного перетворення із сукупності усіх можливих для даного криптографічного алгоритму

en key
ru ключ, ключевые данные

3.28 **відкритий ключ**

Ключ, який не приховується на кожному із етапів його життєвого циклу

en public key
ru открытый ключ

3.29 [**таємний] [особистий] ключ**

Ключ, який не повинен бути доступним стороннім на кожному із етапів його життєвого циклу

Примітка. Під сторонніми розуміється об’єкти [суб’єкти] [процеси] [особи] тощо, що не мають певного права на доступ

en [secret] [privat] key
ru [секретный] [личный] ключ

3.30 **разовий ключ**

Ключ, який застосовується для зашифрування

en session key
ru разовый ключ

тільки одного повідомлення

3.31 **сеансовий ключ**

Ключ, який застосовують для зашифрування лише впродовж одного сеансу зв'язку або визначеного обмеженого часу

en short-term key

ru сеансовый ключ

3.32 **[довгостроковий] [довготривалий] ключ**

Ключ, який можна вживати впродовж визначеного довготривалого часу

en long-term key

ru долгосрочный ключ

3.33 **ключ для зашифрування**

Ключ, який визначає криптографічне перетворення відкритого тексту у шифртекст

en encryption key

ru ключ для зашифрования

3.34 **ключ для розшифрування**

Ключ, який визначає криптографічне перетворення шифртексту у відкритий текст

en decryption key

ru ключ для расшифрования

3.35 **[головний] [майстер] [базовий] ключ**

(при багаторівневій архітектурі управління ключами)

Ключ найвищого рівня у ієрархії ключів при їх зашифруванні, який, як правило, не шифрується і розміщується в захищеній частині засобу криптографічного захисту інформації

en master key

ru [главный] [базовый] ключ

3.36 **системний ключ**

Ключ, який є постійним для певної криптографічної системи

en system key

ru системный ключ

3.37 **слабкий ключ**

Ключ, застосування якого призводить або може призвести до зниження стійкості криптографічного перетворення

en weak key

ru слабый ключ

3.38 **узгодження ключів**

Формування для двох або кількох абонентів спільних таємних даних (ключів) для здійснення захищеного інформаційного обміну

en key agreement

ru согласование ключей

3.39 **криптографічний захист інформації**

Вид захисту, що реалізується за допомогою криптографічного перетворення інформації

en cryptographic protection of information

ru криптографическая защита информации

3.40 **засіб криптографічного захисту інформації**

Програмний, апаратно-програмний або апаратний засіб, призначений для криптографічного захисту інформації

en facility for cryptographic protection of information

ru средство криптографической защиты информации

Примітка 1. Залежно від способу реалізації розрізняють такі типи засобів криптографічного захисту інформації:

програмні засоби, що функціонують у середовищі операційних систем електронно-обчислювальної техніки та взаємодіють із загальним прикладним програмним забезпеченням;

апаратно-програмні засоби, у яких частину криптографічних функцій реалізовано в спеціальному апаратному пристрої до електронно-обчислювальної техніки, керування яким здійснюється за допомогою спеціального програмного забезпечення;

апаратні засоби, алгоритм функціонування (включаючи криптографічні функції) яких реалізується в оптичних, механічних, мікроелектронних або інших спеціалізованих пристроях.

Примітка 2. До засобів криптографічного захисту інформації належать:

засоби шифрування інформації;

засоби, призначені для виготовлення ключових даних або документів (незалежно від виду носія ключової інформації) та управління ключовими даними, що використовуються в засобах криптографічного захисту інформації;

засоби захисту від нав'язування неправдивої інформації або захисту від несанкціонованої модифікації, що реалізують алгоритми криптографічного перетворення інформації (криптоалгоритми), включаючи засоби імітозахисту та електронного цифрового підпису;

засоби захисту інформації від несанкціонованого доступу (у тому числі засоби розмежування доступу до ресурсів електронно-обчислювальної техніки), у яких реалізовано криптоалгоритми.

3.41 **(криптографічний) комутатор**

en switchboard

ru коммутатор криптографический

Елемент засобу криптографічного захисту інформації, що реалізує [перестановку] [підстановку] символів блоку, які подаються на його вхід

3.42 **криптограма**

en cryptogram

ru криптограмма

Повідомлення, яке містить шифртекст та, у разі необхідності, іншу додаткову інформацію

Примітка. Під додатковою інформацією розуміється

адреса, відкритий ключ, дата, цифровий підпис, номер та інше.

3.43 (**криптоаналітична) атака**
криптоатака
Спроба реалізації загрози інформації з використанням методів криптографічного аналізу

en attack on a cipher, cryptanalytic attack
ru криптографическая атака

Примітка. Під загрозою інформації розуміється витік, можливість блокування, чи порушення цілісності інформації.

3.44 (**криптографічна) зв'язність**
криптозв'язність
Можливість для абонентів певної мережі встановити між собою захищений зв'язок з використанням засобів криптографічного захисту інформації та ключових даних

en cryptographyc connectivity
ru криптографическая связность

3.45 (**криптографічна) система**
криптосистема
Сукупність засобів криптографічного захисту інформації, необхідних ключових даних, документації, використання яких забезпечує належний рівень захищеності інформації

en cryptographyc system, cryptosystem
ru криптографическая система

3.46 (**криптографічна) стійкість**
криптостійкість
Здатність криптографічної системи протистояти дешифруванню методами криптографічного

en cryptographyc strength
ru криптографическая стойкость

аналізу

Примітка. Криптографічна стійкість чисельно характеризується складністю дешифрування (наприклад, в одиницях часу або кількості операцій засобу обчислювальної техніки) з урахуванням наявних засобів та методів криптографічного аналізу

3.47 **(криптографічне) перетворення**
криптоперетворення

en cryptographyc transformation
ru криптографическое преобразование

Перетворення інформації з метою приховування або відновлення її змісту, підтвердження справжності, цілісності, авторства, захисту від несанкціонованого доступу тощо, що здійснюється з використанням спеціальних (ключових) даних.

Примітка. Розрізняють такі види криптографічних перетворень: зашифрування, розшифрування, формування та/або перевіряння цифрового підпису, вироблення імітовставки тощо

3.48 **асиметричне криптографічне перетворення**

en asymmetric cryptographic technique
ru асимметрическое криптографическое преобразование

Пряме та однозначно визначене обернене криптографічні перетворення інформації, які здійснюються за допомогою пов’язаних між собою різних відкритого та [таємного] [особистого] ключів

3.49 **симетричне криптографічне перетворення**

Пряме та однозначно визначене обернене криптографічні перетворення інформації, які здійснюються з використанням одного і того ж [таємного] [особистого] ключа

en symmetric cryptographic technique

ru симметрическое криптографическое преобразование

3.50 (**криптографічний) алгоритм криптоалгоритм**

Набір математичних правил та процедур, за допомогою яких здійснюється криптографічне перетворення

en cryptographyc algorithm, transformation

ru криптографический алгоритм

3.51 (**криптографічний) аналіз криптоаналіз**

Напрям криптології, що вивчає методи аналізу криптографічних систем з метою оцінки їх криптографічної стійкості до дешифрування, знаходження способів несанкціонованого доступу до системи, підробки даних, повідомлень та підписів, порушення інформаційних процесів тощо

en cryptanalysis

ru криптографический анализ

3.52 (**криптографічний) протокол криптопротокол**

Визначена послідовність дій (взаємодії) [суб'єків] [об'єктів] обміну інформацією, в якій хоча б одна дія є криптографічним перетворенням повідомлень

en cryptographyc protocol

ru криптографический протокол

3.53 **криптологія**

Наукова дисципліна, що вивчає проблеми криптографічного захисту інформації та криптографічного аналізу

en cryptology
ru криптология

3.54 **криптографія**

Напрям криптології, що вивчає принципи побудови та властивості криптографічних перетворень

en cryptography
ru криптография

3.55 **метод дешифрування**

Метод, який спеціально розроблений та призначений для відновлення алгоритму шифрування, ключів та відкритого тексту, при відомій криптограмі, та, можливо, деякій додатковій інформації, але при невідомому ключі

Примітка. Під додатковою інформацією мається на увазі інформація про криптографічну систему, принципи генерації або використання ключів, відкритий текст тощо

en cryptanalysis method
ru метод дешифрования

3.56 **[однобічна] [односпрямована] функція**

Функція, у якої для всіх значень аргументів існує поліноміальний алгоритм обчислення значення функції, але майже для всіх значень функції не існує поліноміального алгоритму обернення функції

en one-way function
ru однонаправленная функция

3.57 [**повний] [тотальний] перебір ключів**

Метод дешифрування, що полягає у відновленні

en exhaustive key search
ru [полный] [тотальный]

відкритого тексту шляхом перебору всієї множини ключів (можливо – до першого успіху), та визначення ключа, для якого цей відкритий текст є семантично вірогідний або відповідає іншому об'єктивному критерію

перебор ключей

3.58 **потоковий шифр**

Шифр, в якому шифруванню послідовно підлягають усі символи відкритого тексту

en stream cipher
ru поточный шифр

3.59 **простір ключів**

Множина усіх припустимих ключів даної криптосистеми

en key space
ru пространство ключей

Примітка. Головними характеристиками простору ключів є максимальна кількість нееквівалентних ключів, відсутність слабких ключів

3.60 **сертифікат відкритого ключа**

Електронний документ, що засвідчує належність відкритого ключа конкретній особі, а також його чинність

en public-key certificat
ru сертификат открытого ключа

3.61 **сертифікація {сертифікувати} відкритих {відкриті} ключів {ключі}**

Формування {формувати} даних {-і}, що дозволяють в подальшому здійснювати автентифікацію та контроль цілісності ключів, зокрема, перевірку того, що поданий ключ дійсно належить учаснику інформаційного обміну, який

en public-key certification
ru сертификация открытых ключей

3.62 **геш-функція**

Функція, що перетворює послідовність елементів даних довільної довжини (прообраз) у послідовність елементів даних фіксованої довжини (образ)

en hash function
ru хеш-функция

3.63 **гешування {гешувати}**

Процес застосування геш-функції до відповідних даних

en hashing
ru хеширование

3.64 **(електронний) цифровий підпис**

Сукупність даних, отриманих за результатом певного криптографічного перетворення деякого набору даних, яка додається до цього набору даних або логічно поєднується з ним і дає змогу підтвердити його цілісність та автентичність та перевірити автентичність підписувача

en digital signature
ru (электронная) цифровая подпись

Примітка 1. Як правило, до процесу накладання цифрового підпису повідомлення підлягає гешуванню.

Примітка 2. Цифровий підпис забезпечує як захист від підробки даних, у тому числі отримувачем, так і можливість перевірки цілісності даних і автентичності джерела повідомлення.

3.65 **шифр**

Сукупність оборотних відображень множини відкритих текстів у множину шифртекстів, які здійснюються за певними правилами із застосуванням ключів

en cipher

ru шифр

3.66 **шифратор**

Пристрій, що апаратно або програмно-апаратно реалізує функції введення і перетворення ключів, зашифрування та розшифрування даних

en encryptor, cipher machine, enciphering unit

ru шифратор

3.67 **шифртекст**

зашифроване повідомлення

Результат перетворення відкритого тексту криптографічною системою, яке визначається ключем

Примітка. При аналізі стійкості криптосистеми вважають, що шифртекст відомий криптоаналітикові.

en ciphertext

ru шифртекст, зашифрованное сообщение

ДОДАТОК А

(довідковий)

АБЕТКОВИЙ ПОКАЖЧИК УКРАЇНСЬКИХ ТЕРМІНІВ

імітостійкість	3.25
імітостійкість системи криптографічної	3.25
ключ	3.27
ключ базовий	3.35
ключ відкритий	3.28
ключ головний	3.35
ключ для зашифрування	3.33
ключ для розшифрування	3.34
ключ довгостроковий	3.32
ключ довготривалий	3.32
ключ майстер	3.35
ключ особистий	3.29
ключ разовий	3.30
ключ сеансовий	3.31
ключ системний	3.36
ключ слабкий	3.37
ключ таємний	3.29
ключі еквівалентні	3.21
код автентифікації повідомлення	3.23
комутатор криптографічний	3.41
криптограма	3.42
криптографія	3.54
криптологія	3.53
метод дешифрування	3.55
перебір ключів повний	3.57
перебір ключів тотальний	3.57
перетворення криптографічне	3.47
перетворення криптографічне асиметричне	3.48
перетворення криптографічне симетричне	3.49
підпис електронний цифровий	3.64

підпис цифровий	3.64
повідомлення відкрите	3.7
повідомлення зашифроване	3.67
простір ключів	3.59
протокол криптографічний	3.52
розшифрування	3.15
сертифікат ключа відкритого	3.60
сертифікація ключів відкритих	3.61
система криптографічна	3.45
стійкість абсолютна	3.1
стійкість досконала	3.1
стійкість криптографічна	3.46
текст відкритий	3.7
узгодження ключів	3.38
управління ключами	3.26
функція однобічна	3.56
функція односпрямована	3.56
шифр	3.65
шифр блоковий	3.5
шифр досконалий	3.13
шифр потоковий	3.58
шифратор	3.66
шифртекст	3.67
шифрування	3.16
шифрування абонентське	3.19
шифрування канальне	3.20
шифрування лінійне	3.18
шифрування наскрізне	3.19
шифрування попереднє	3.17
шифрування потокове	3.18

ДОДАТОК Б

(довідковий)

АБЕТКОВИЙ ПОКАЖЧИК АНГЛІЙСЬКИХ ТЕРМІНІВ

asymmetric cryptographic technique	3.48
attack on a cipher	3.12
attack on a cipher, cryptanalytic attack	3.43
authentification	3.2
block cipher	3.5
channel encryption	3.20
cipher	3.65
ciphertext	3.67
cipher unicity distance	3.8
cryptanalysis method	3.55
cryptanalysis	3.51
cryptogram	3.42
cryptographyc algorithm, transformation	3.50
cryptographyc connectivity	3.44
cryptographyc strength	3.46
cryptographyc transformation	3.47
cryptography	3.54
cryptographic protection of information	3.39
cryptographyc protocol	3.52
cryptographyc scheme, cryptosystem	3.45
cryptology	3.53
decryption	3.15
decryption key	3.34
digital signature	3.64

encryption	3.14
encryption	3.16
encryption key	3.33
encryptor, cipher machine, enciphering unit	3.66
end-to-end encryption	3.19
exhaustive key search	3.57
facility for cryptographic protection of information	3.40
gamma	3.9
hash function	3.62
hashing	3.63
identification	3.22
imitation insertion	3.23
imitation resistance	3.25
imitation security, imitation defence	3.24
key	3.27
key agreement	3.38
key generator	3.11
key management	3.26
key space	3.59
linear encryption	3.18
long-term key	3.32
master key	3.35
one-way function	3.56
perfect cipher	3.13
perfect secrecy, unconditional secrecy	3.1
plaintext, plaintext message	3.7
plaintext alphabet, ciphertext alphabet	3.3
plaintext block, ciphertext block	3.4
primary encryption	3.17
public-key	3.28

public-key certificat	3.60
public-key certification	3.61
random bit generator, random number generator	3.10
secret key, privat key	3.29
session key	3.30
short-term key	3.31
stream cipher	3.58
switchboard	3.41
symmetric cryptographic technique	3.49
system key	3.36
verification	3.6
weak key	3.37

ДОДАТОК В

(довідковий)

АБЕТКОВИЙ ПОКАЖЧИК РОСІЙСЬКИХ ТЕРМІНІВ

ключ для расшифрования	3.34
ключ долгосрочный	3.32
ключ личный	3.29
ключ открытый	3.28
ключ разовый	3.30
ключ сеансовый	3.31
ключ секретный	3.29
ключ системный	3.36
ключи эквивалентные	3.21
ключ слабый	3.37
код аутентификации сообщения	3.23
коммутатор криптографический	3.41
криптограмма	3.42
криптография	3.54
криптология	3.53
метод дешифрования	3.55
перебор ключей полный	3.57
перебор ключей тотальный	3.57
преобразование криптографическое	3.47
преобразование криптографическое асимметрическое	3.48
преобразование криптографическое симметрическое	3.49
подпись цифровая	3.64
подпись электронная цифровая	3.64
пространство ключей	3.59
протокол криптографический	3.52
расстояние единственности шифра	3.8
расшифрование	3.15
связность криптографическая	3.44
сертификат ключа открытого	3.60
сертификация ключей открытых	3.61

система криптографическая	3.45
согласование ключей	3.38
сообщение открытое	3.7
сообщение зашифрованное	3.67
средство защиты информации криптографической	3.49
стойкость абсолютная	3.1
стойкость криптографическая	3.46
стойкость совершенная	3.1
текст открытый	3.7
управление ключами	3.26
функция однонаправленная	3.56
хеш-функция	3.62
хеширование	3.63
шифр	3.65
шифр блочный	3.5
шифр поточный	3.58
шифр совершенно стойкий	3.13
шифратор	3.66
шифрование	3.16
шифрование абонентское	3.19
шифрование канальное	3.20
шифрование линейное	3.18
шифрование поточное	3.18
шифрование предварительное	3.17
шифрование сквозное	3.19
шифртекст	3.67

БІБЛІОГРАФІЯ

1 ДСТУ 1.5-2003 Національна стандартизація. Правила побудови, викладення, оформлення та вимоги до змісту нормативних документів.

2 ДСТУ 3996-2000 Засади і правила розроблення стандартів на терміни та визначення понять.

3 ДСТУ 4145-2002 Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що грунтується на еліптичних кривих. Формування та перевіряння.

ДСТУ_____

УДК _____

Ключові слова: шифр, шифрування, шифртекст, відкритий текст, ключ, криптографічна стійкість.

_____	_____	_____
Керівник (заст. керівника) організації розробника та її назва	особистий підпис	ім’я прізвище
_____	_____	_____
Керівник розробки (теми), посада	особистий підпис	ім’я прізвище
_____	_____	_____
Відповідальний виконавець, посада	особистий підпис	ім’я прізвище