



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	С. IV
1 Сфера застосування.....	1
2 Загальні пояснення.....	2
3 Терміни та визначення понять.....	4
Додаток А Абетковий покажчик українських термінів.....	20
Додаток Б Абетковий покажчик англійських термінів	23
Додаток В Абетковий покажчик російських термінів.....	26
Бібліографія	29

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.

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 терміноstatтях 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 узяті в круглі дужки (набрані 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 authentication
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

en block cipher

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

ru блочный шифр

3.6 верифікація {верифікувати}

en verification

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

ru верификация

3.7 відкритий текст

en plaintext, plaintext

відкрите повідомлення

message

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

ru открытый текст,
открытое сообщение

Примітка. Відкрите повідомлення може також бути попередньо зашифроване.

3.8 відстань єдиності шифру

en cipher unicity distance

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

ru расстояние
единственности шифра

3.9 гама

en gamma

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

ru гамма

ДСТУ _____

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}

en encryption

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

ru зашифрование

3.15 розшифрування {розшифрувати}

en decryption

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

ru расшифрование

3.16 шифрування

en encryption

Процеси зашифрування та розшифрування

ru шифрование

3.17 попереднє шифрування

en primary encryption

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

ru предварительное
шифрование

3.18 [лінійне] [познакове] шифрування

en linear encryption

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

ru [линейное] [поточное]
шифрование

3.19 [наскрізне] [абонентське] шифрування

en end-to-end encryption

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

ru [сквозное]
[абонентское]
шифрование

3.20 каналне шифрування

en channel encryption

Шифрування повідомлення, яке передається на відрізок міжстанційного з'єднання

ru каналное шифрование

ДСТУ _____

3.21 еквівалентні ключі

en equivalent keys

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

ги эквивалентные ключи

3.22 ідентифікація {ідентифікувати}

en identification

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

ги идентификация

3.23 імітовставка

en imitation insertion

код автентифікації повідомлення

ги имитационная вставка

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

3.24 імітозахист

en imitation security,
imitation defence

Захист повідомлення від його модифікації

ги имитозащита

3.25 імітостійкість (криптографічної системи)

en imitation resistance

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

ги имитостойкость

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

3.26 управління ключами

en key management

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

ru управление ключами

3.27 ключ

en key

ключові дані

ru ключ, ключевые

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

данные

3.28 відкритий ключ

en public key

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

ru открытый ключ

3.29 [таємний] [особистий] ключ

en [secret] [privat] key

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

ru [секретный] [личный] ключ

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

3.30 разовий ключ

en session key

Ключ, який застосовується для зашифрування

ru разовый ключ

ДСТУ _____

тільки одного повідомлення

3.31 сеансовий ключ

en short-term key

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

ru сеансовый ключ

3.32 [довгостроковий] [довготривалий] ключ

en long-term key

Ключ, який можна вживати впродовж визначеного довготривалого часу

ru долгосрочный ключ

3.33 ключ для зашифрування

en encryption key

Ключ, який визначає криптографічне перетворення відкритого тексту у шифртекст

ru ключ для зашифрования

3.34 ключ для розшифрування

en decryption key

Ключ, який визначає криптографічне перетворення шифртексту у відкритий текст

ru ключ для расшифрования

3.35 [головний] [майстер] [базовий] ключ
(при багаторівневій архітектурі управління ключами)

en master key

ru [главный] [базовый] ключ

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

3.36 системний ключ

en system key

Ключ, який є постійним для певної криптографічної системи

ru системный ключ

3.37 слабкий ключ

en weak key

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

ru слабый ключ

3.38 узгодження ключів

en key agreement

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

ru согласование ключей

3.39 криптографічний захист інформаціїen cryptographic protection
of information

Вид захисту, що реалізується за допомогою криптографічного перетворення інформації

ru криптографическая
защита информации**3.40 засіб криптографічного захисту інформації**en facility for cryptographic
protection of information

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

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;