Прим. № __
ПРОЕКТ

ЗАТВЕРДЖЕНО
Наказ Державної служби спеціального зв’язку та захисту інформації України від 200 №

ІНСТРУКЦІЯ
про порядок постачання і використання ключів до засобів криптографічного захисту інформації, що реалізують криптографічний алгоритм, визначений ГОСТ 28147-89

1. Загальні положення

1.1. Інструкція "Про порядок постачання і використання ключів до засобів криптографічного захисту інформації, що реалізують криптографічний алгоритм, визначений ГОСТ 28147-89" (далі – Інструкція) встановлює порядок постачання та використання ключів, що передбачений п. 1.7 ГОСТ 28147-89 "Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования".

1.2. Інструкція розроблена відповідно законів України "Про Державну службу спеціального зв’язку та захисту інформації України", "Про електронний цифровий підпис", "Про захист інформації в інформаційно-телекомунікаційних системах" та з урахуванням вимог Законів України "Про інформацію", "Про ліцензування певних видів господарської діяльності".

1.3. Вимоги цієї Інструкції обов`язкові для виконання державними органами, підприємствами, установами та організаціями всіх форм власності, які здійснюють розроблення, виробництво, використання, експлуатацію, сертифікаційні випробування, тематичні дослідження, експертизу, ввезення, вивезення криптосистем і засобів криптографічного захисту інформації (далі – КЗІ), що реалізують криптографічний алгоритм, визначений ГОСТ 28147-89, надають послуги в галузі КЗІ із використанням зазначених засобів КЗІ (в тому числі послуги електронного цифрового підпису), їх постачання або торгівлю ними.

Дія цієї Інструкції не розповсюджується на криптосистеми та засоби КЗІ, які призначені для захисту інформації, яка становить державну таємницю.

1.4. Використані у цій Інструкції терміни відповідають нормативно-правовим актам щодо порядку розроблення, виготовлення та експлуатації засобів КЗІ, а також ГОСТ 28147-89.

Крім того, в Інструкції використовуються такі терміни:

довгостроковий ключовий елемент (далі – ДКЕ) – ключ, що визначає заповнення таблиць блоку підстановок алгоритму криптографічного перетворення, визначеного ГОСТ 28147-89;

замовник – юридична особа будь-якої форми власності, яка замовляє встановленим порядком ключі до засобів КЗІ, в тому числі засобів електронного цифрового підпису, в яких реалізується криптографічний алгоритм, визначений ГОСТ 28147-89. В якості замовників можуть виступати розробники, виробники, постачальники та користувачі засобами КЗІ;

засіб електронного цифрового підпису – програмний засіб, програмно-апаратний або апаратний пристрій, призначені для генерації ключів, накладення та/або перевірки електронного цифрового підпису;

методика генерації ключових даних – опис послідовності операцій (алгоритму), що виконуються у процесі генерації ключових даних;

методика розподілу ключових даних – опис послідовності операцій (алгоритму), що виконуються у мережі захищеного інформаційного обміну з метою формування (отримання) необхідних ключів;

носій ключової інформації (далі – НКІ) – матеріальний носій інформації, що призначений для запису та збереження ключових даних;

постачальник – підрозділ Державної служби спеціального зв’язку та захисту інформації України (далі – ДССЗІ України), що здійснює постачання ключів до засобів КЗІ;

разовий (сеансовий) ключ (далі – РК) – ключ, що визначає порядок заповнення ключового запам'ятовуючого пристрою алгоритму криптографічного перетворення, який визначено ГОСТ 28147-89.

2. Порядок використання ключових даних

2.1. РК можуть бути отримані від постачальника або генерують замовником із застосуванням засобу КЗІ, який отримав позитивний висновок ДССЗЗІ України чи сертифікат відповідності.

2.2. ДКЕ можуть бути отримані від постачальника або обираються із додатку 1 до цієї Інструкції.

2.3. ДКЕ може обираються із додатку 1 до цієї Інструкції у наступних випадках їх застосування:

- використання у генераторах випадкових послідовностей згідно додатку А ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння";

- обчислення гешфункції згідно ГОСТ 34.311-95 "Система обработки информации. Защита криптографическая. Функция хеширования";

- криптографічного захисту конфіденційної інформації (крім інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом), з метою забезпечення її конфіденційності та імітозахисту при зберіганні та (або) обміну інформацією каналами (лініями) зв’язку.

2.4. Для використання у засобах КЗІ, зазначених у пункті 2.3 цієї Інструкції, ДКЕ можуть також обиратись з посилених сертифікатів відкритого ключа електронного цифрового підпису.

2.5. В якості ДКЕ, що призначені для криптографічного захисту інформації з обмеженим доступом, вимога щодо захисту якої встановлена

законом, з метою забезпечення її конфіденційності та імітозахисту, використовуються ДКЕ, отримані від постачальника.

2.6. Генерація РК у засобах КЗІ повинна здійснюватися відповідно до державних стандартів або за методикою генерації ключових даних, яка погоджується встановленим порядком на підставі результатів її державної експертизи у сфері КЗІ.

2.7. Генерація ДКЕ, вказаних в пункті 2.5, та їх запис на НКІ здійснюється постачальником.

2.8. Ключові дані можуть розподілятися між засобами КЗІ каналами (лініями) зв'язку у захищеному вигляді. Розподіл ключових даних повинен здійснюватися відповідно до державних стандартів або за методикою розподілу ключових даних, погодженою встановленим порядком на підставі результатів її державної експертизи у сфері КЗІ.

2.8. За необхідністю методика генерації ключових даних та методика розподілу ключових даних можуть бути викладені в одному документі – методика генерації та розподілу ключових даних.

2.9. Термін дії ДКЕ, що визначені у пункті 2.3 цієї Інструкції, а також термін дії РК, що використовується у генераторах випадкових послідовностей, реалізованих відповідно до додатку А ДСТУ 4145-2002, визначається замовником.

У інших випадках термін дії РК та ДКЕ визначається за результатами сертифікації або державної експертизи у сфері КЗІ конкретного засобу КЗІ, до якого вони призначені.

2.10. Необхідність обмеження доступу до ДКЕ, що призначені для використання у випадках, які передбачені пунктом 2.3 цієї Інструкції та отримані від постачальника, визначається Замовником.

У інших випадках ступінь обмеження доступу до ДКЕ, а також ступінь обмеження доступу до РК, повинен відповідати ступеню обмеження доступу встановленому для інформації, криптографічні перетворення якої здійснюється із застосуванням цих ключових даних.

2.11. Умови зберігання, використання, формування та обміну ключовими даними повинні унеможливлювати їх несанкціоновану модифікацію або підміну.

Для ключових даних, по відношенню до яких встановлена необхідність обмеження доступу, умови зберігання, використання та обміну ключами даними додатково повинні унеможливлювати ознайомлення з їх змістом сторонніх осіб.

2.12. Конкретний порядок використання ключових даних та поводження з НКІ, термін дії та ступінь обмеження доступу вказується у правилах користування засобом КЗІ (для засобів криптографічного захисту конфіденційної інформації, що є власністю держави) або в інструкції із забезпечення безпеки експлуатації засобу КЗІ (для засобів криптографічного захисту конфіденційної інформації та засобів електронного цифрового підпису).

3. Порядок постачання ключових даних

3.1. Постачання ключових даних здійснюється на договірних засадах.

3.2. Ключові дані постачаються на НКІ у вигляді ключових документів. Ключовий документ містить один НКІ, який вміщено у спеціальну захисну упаковку, на яку нанесено відповідне маркування.

Типи рекомендованих НКІ та форматів ключових даних, що розміщуються на них, наведено у додатку 2 цієї Інструкції.

3.3. Постачання ключових даних включає в себе такі етапи:

- подачу замовником заявки;
- розгляд постачальником заявки та прийняття відповідного рішення щодо неї;
- укладання договору про постачання ключових даних;
- здійснення постачання ключових даних замовнику;
- контроль за дотриманням порядку постачання та використання ключових даних;

3.4. Подача замовником заявки.

3.4.1 У разі необхідності одержання замовником ключових даних він направляє постачальнику заявку, в якій вказується:

- юридична адреса і банківські реквізити Замовника;
- відомості щодо ліцензії на право впровадження господарської діяльності (серія, номер ліцензії, термін дії, види робіт тощо);
- призначення ключових даних (у тому числі, у яких засобах КЗІ будуть використовуватися ключові дані, наявність сертифікату відповідності або експертного висновку на зазначені засоби КЗІ, криптосистеми, тощо);
- тип, необхідна кількість комплектів (серій) НКІ та кількість примірників у кожному комплекті (серії);
- ступінь обмеження доступу до НКІ;
- гарантії оплати робіт з постачання НКІ.

3.4.2. У разі, коли тип НКІ, структура та формат даних, що міститься на ньому, не відповідає додатку 2 цієї Інструкції, до заявки додатково додаються матеріали в яких викладено:

- опис зовнішнього вигляду НКІ (тип носія, зміст та порядок маркування НКІ, порядок розташування даних на НКІ тощо);
- повний та однозначний опис структури даних, що повинні міститися на НКІ, у тому числі опис усіх елементів даних та порядку їх розташування, спосіб нанесення інформації, порядок застосування вільних ділянок, опис алгоритму або порядку формування службової інформації, яка міститься на НКІ, особливості розташування та змісту даних в залежності від серії та номеру примірника у серії тощо).

3.5. Розгляд постачальником заявки та прийняття відповідного рішення

3.5.1. Постачальник розглядає заявку для визначення юридичного статусу замовника, оцінювання достатнього обсягу наданих відомостей, юридичної чинності наданих документів та технологічної можливості виготовлення НКІ.

3.5.2. За результатами розгляду заявки постачальник приймає рішення про можливість постачання чи відмову у здійсненні постачання ключових даних.

3.5.3. Про прийняте рішення постачальник повідомляє замовника у письмовому вигляді протягом 28 робочих днів з дня отримання заявки.

3.5.4. За умов позитивного рішення щодо постачання ключових даних постачальник разом з рішенням надсилає замовнику проект відповідного договору.

3.5.6. У разі негативних результатів розгляду заявки постачальник інформує замовника про причини відмови у постачанні ключових даних.

3.6. Укладання договору на постачання ключових даних.

3.6.1. Договір на постачання ключових даних укладається із домовленості між постачальником та замовником.

3.6.2. У договорі про постачання вказуються:

- обов'язки сторін;
- порядок оплати, умови та терміни постачання НКІ;
- порядок звітності та здійснення контролю за використанням НКІ;
- порядок використання та постачання НКІ іншим учасникам захищеного інформаційного обміну або підрозділам (філіям) замовника (за необхідності);
- відповідальність сторін;
- юридичні адреси сторін та інші реквізити.

3.7. Здійснення постачання ключових даних.

3.7.1. Постачання ключових даних здійснюється відповідно до договору про постачання, який укладено між постачальником та замовником.

3.8. Постачання ключових даних підрозділам замовника.

3.8.1. Замовник має право здійснювати постачання ключових даних отриманих від постачальника своїм структурним підрозділам та взаємодіючим з ним організаціям у порядку передбаченому договором, який укладається відповідно до пункту 3.6 цієї Інструкції.

3.8.2. При цьому забороняється тиражувати отримані від постачальника ключові документи та копіювати ключові дані на інші НКІ, якщо це не визначено правилами користування або інструкцією із забезпечення безпеки експлуатації конкретного засобу КЗІ.

3.9. Контроль за дотриманням норм і рекомендацій, встановлених цією Інструкцією, при постачанні та використанні ключових даних, здійснюється відповідно до нормативно-правових актів в сфері КЗІ та зобов’язань, взятих на себе замовником та постачальником при укладанні договору про постачання ключів.

Начальник підрозділу Служби

Додаток 1
до Інструкції про порядок постачання і використання ключів до засобів криптогра-фічного захисту інформації, що реалізують криптографічний алгоритм, визначений ГОСТ 28147-89

Перелік ДКЕ,
які рекомендуються до застосування у засобах КЗІ

ДКЕ № 1

	0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*
K1	**A**	**9**	**D**	**6**	**E**	**B**	**4**	**5**	**F**	**1**	**3**	**C**	**7**	**0**	**8**	**2**
K2	**8**	**0**	**C**	**4**	**9**	**6**	**7**	**B**	**2**	**3**	**1**	**F**	**5**	**E**	**A**	**D**
K3	**F**	**6**	**5**	**8**	**E**	**B**	**A**	**4**	**C**	**0**	**3**	**7**	**2**	**9**	**1**	**D**
K4	**3**	**8**	**D**	**9**	**6**	**B**	**F**	**0**	**2**	**5**	**C**	**A**	**4**	**E**	**1**	**7**
K5	**F**	**8**	**E**	**9**	**7**	**2**	**0**	**D**	**C**	**6**	**1**	**5**	**B**	**4**	**3**	**A**
K6	**2**	**8**	**9**	**7**	**5**	**F**	**0**	**B**	**C**	**1**	**D**	**E**	**A**	**3**	**6**	**4**
K7	**3**	**8**	**B**	**5**	**6**	**4**	**E**	**A**	**2**	**C**	**1**	**7**	**9**	**F**	**D**	**0**
K8	**1**	**2**	**3**	**E**	**6**	**D**	**B**	**8**	**F**	**A**	**C**	**5**	**7**	**9**	**0**	**4**

ДКЕ № 2

	0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*
K1	**E**	**9**	**3**	**7**	**F**	**4**	**C**	**B**	**6**	**A**	**D**	**1**	**0**	**5**	**8**	**2**
K2	**A**	**D**	**C**	**7**	**6**	**E**	**8**	**1**	**F**	**3**	**B**	**4**	**0**	**9**	**5**	**2**
K3	**4**	**B**	**1**	**F**	**9**	**2**	**E**	**C**	**6**	**A**	**8**	**7**	**3**	**5**	**0**	**D**
K4	**4**	**5**	**1**	**C**	**7**	**E**	**9**	**2**	**A**	**F**	**B**	**D**	**0**	**8**	**6**	**3**
K5	**C**	**B**	**3**	**9**	**F**	**0**	**4**	**5**	**7**	**2**	**E**	**D**	**1**	**A**	**8**	**6**
K6	**8**	**7**	**3**	**A**	**9**	**6**	**E**	**5**	**D**	**0**	**4**	**C**	**1**	**2**	**F**	**B**
K7	**F**	**0**	**E**	**6**	**8**	**D**	**5**	**9**	**A**	**3**	**1**	**C**	**4**	**B**	**7**	**2**
K8	**4**	**3**	**E**	**D**	**5**	**0**	**2**	**B**	**1**	**A**	**7**	**6**	**9**	**F**	**8**	**C**

ДКЕ № 3

	0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*
K1	**D**	**9**	**1**	**E**	**7**	**2**	**C**	**5**	**4**	**B**	**6**	**F**	**3**	**8**	**A**	**0**
K2	**7**	**8**	**6**	**B**	**0**	**3**	**4**	**D**	**9**	**5**	**F**	**E**	**A**	**C**	**2**	**1**
K3	**A**	**5**	**3**	**C**	**9**	**8**	**D**	**6**	**4**	**F**	**E**	**0**	**2**	**B**	**1**	**7**
K4	**B**	**A**	**C**	**1**	**5**	**6**	**9**	**E**	**2**	**D**	**F**	**7**	**0**	**4**	**3**	**8**
K5	**5**	**B**	**3**	**0**	**F**	**9**	**E**	**4**	**1**	**C**	**8**	**6**	**2**	**A**	**7**	**D**
K6	**4**	**3**	**B**	**D**	**1**	**F**	**8**	**2**	**7**	**E**	**C**	**9**	**A**	**0**	**6**	**5**
K7	**3**	**7**	**8**	**B**	**1**	**E**	**5**	**0**	**D**	**4**	**C**	**A**	**2**	**9**	**F**	**6**
K8	**6**	**D**	**C**	**A**	**B**	**7**	**9**	**3**	**F**	**E**	**1**	**2**	**0**	**8**	**4**	**5**

ДКЕ № 4

	0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*
K1	**9**	**C**	**3**	**D**	**7**	**6**	**E**	**1**	**A**	**2**	**0**	**4**	**8**	**F**	**5**	**B**
K2	**A**	**5**	**B**	**E**	**7**	**6**	**0**	**C**	**2**	**8**	**F**	**4**	**D**	**3**	**9**	**1**
K3	**4**	**C**	**3**	**0**	**D**	**2**	**E**	**B**	**7**	**F**	**5**	**9**	**1**	**8**	**A**	**6**
K4	**3**	**9**	**4**	**5**	**E**	**7**	**8**	**6**	**D**	**0**	**2**	**F**	**B**	**C**	**A**	**1**
K5	**2**	**9**	**C**	**F**	**D**	**B**	**4**	**1**	**7**	**5**	**3**	**E**	**6**	**8**	**A**	**0**
K6	**E**	**5**	**D**	**B**	**1**	**9**	**4**	**2**	**F**	**8**	**7**	**0**	**3**	**C**	**A**	**6**
K7	**E**	**6**	**5**	**A**	**9**	**D**	**4**	**8**	**B**	**C**	**0**	**3**	**7**	**1**	**F**	**2**
K8	**1**	**9**	**C**	**B**	**7**	**6**	**8**	**3**	**2**	**F**	**E**	**0**	**5**	**A**	**4**	**D**

ДКЕ № 5

	0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*
K1	**3**	**4**	**D**	**8**	**C**	**7**	**A**	**2**	**0**	**E**	**9**	**F**	**B**	**1**	**5**	**6**
K2	**C**	**7**	**6**	**9**	**3**	**8**	**B**	**5**	**F**	**A**	**0**	**D**	**4**	**2**	**1**	**E**
K3	**E**	**4**	**8**	**7**	**B**	**3**	**A**	**C**	**1**	**2**	**6**	**9**	**D**	**F**	**0**	**5**
K4	**3**	**9**	**6**	**D**	**8**	**F**	**A**	**2**	**7**	**E**	**C**	**0**	**B**	**4**	**1**	**5**
K5	**5**	**C**	**A**	**7**	**2**	**1**	**F**	**D**	**E**	**3**	**B**	**4**	**0**	**8**	**9**	**6**
K6	**1**	**8**	**B**	**E**	**7**	**4**	**A**	**0**	**C**	**3**	**5**	**D**	**9**	**F**	**6**	**2**
K7	**9**	**B**	**A**	**D**	**5**	**E**	**2**	**3**	**0**	**6**	**4**	**C**	**F**	**1**	**7**	**8**
K8	**E**	**9**	**1**	**8**	**5**	**F**	**B**	**0**	**6**	**2**	**C**	**7**	**A**	**4**	**D**	**3**

ДКЕ № 6

	0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*
K1	**F**	**C**	**9**	**6**	**E**	**2**	**1**	**B**	**0**	**D**	**4**	**A**	**7**	**8**	**3**	**5**
K2	**E**	**C**	**5**	**0**	**7**	**4**	**A**	**3**	**2**	**6**	**1**	**D**	**9**	**B**	**F**	**8**
K3	**5**	**6**	**D**	**9**	**B**	**E**	**A**	**3**	**F**	**2**	**8**	**1**	**4**	**0**	**7**	**C**
K4	**1**	**F**	**7**	**4**	**2**	**E**	**C**	**3**	**6**	**B**	**9**	**8**	**0**	**5**	**A**	**D**
K5	**F**	**9**	**E**	**6**	**D**	**1**	**5**	**8**	**4**	**2**	**3**	**C**	**A**	**B**	**0**	**7**
K6	**B**	**0**	**D**	**7**	**C**	**E**	**1**	**4**	**2**	**3**	**6**	**8**	**A**	**5**	**F**	**9**
K7	**7**	**E**	**F**	**8**	**D**	**0**	**B**	**3**	**A**	**1**	**4**	**2**	**9**	**C**	**6**	**5**
K8	**1**	**5**	**E**	**B**	**2**	**C**	**3**	**8**	**A**	**0**	**9**	**7**	**F**	**6**	**4**	**D**

ДКЕ № 7

	0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*
K1	**F**	**D**	**A**	**5**	**C**	**0**	**1**	**6**	**9**	**2**	**E**	**7**	**3**	**B**	**4**	**8**
K2	**2**	**5**	**A**	**0**	**6**	**9**	**1**	**F**	**D**	**4**	**7**	**E**	**B**	**3**	**8**	**C**
K3	**3**	**E**	**4**	**B**	**5**	**9**	**1**	**2**	**F**	**6**	**8**	**D**	**7**	**0**	**A**	**C**
K4	**4**	**A**	**B**	**9**	**F**	**2**	**E**	**5**	**D**	**1**	**3**	**6**	**0**	**7**	**C**	**8**
K5	**F**	**6**	**5**	**8**	**9**	**7**	**C**	**B**	**0**	**A**	**3**	**1**	**2**	**4**	**D**	**E**
K6	**C**	**B**	**F**	**4**	**5**	**1**	**E**	**9**	**0**	**8**	**D**	**2**	**A**	**7**	**3**	**6**
K7	**D**	**2**	**4**	**8**	**B**	**C**	**1**	**3**	**A**	**5**	**9**	**E**	**7**	**F**	**0**	**6**
K8	**1**	**5**	**0**	**F**	**6**	**A**	**3**	**E**	**7**	**2**	**C**	**D**	**B**	**8**	**9**	**4**

ДКЕ № 8

	0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*
K1	**E**	**4**	**B**	**2**	**8**	**7**	**5**	**C**	**9**	**D**	**0**	**3**	**1**	**F**	**6**	**A**
K2	**3**	**E**	**C**	**A**	**6**	**2**	**D**	**1**	**9**	**8**	**7**	**4**	**0**	**F**	**5**	**B**
K3	**5**	**2**	**8**	**7**	**1**	**F**	**E**	**6**	**4**	**D**	**B**	**0**	**A**	**3**	**C**	**9**
K4	**C**	**A**	**7**	**D**	**E**	**3**	**0**	**2**	**9**	**5**	**1**	**6**	**B**	**4**	**F**	**8**
K5	**6**	**3**	**F**	**7**	**0**	**9**	**A**	**8**	**B**	**C**	**4**	**1**	**5**	**2**	**D**	**E**
K6	**6**	**D**	**F**	**1**	**5**	**3**	**8**	**0**	**B**	**A**	**E**	**4**	**9**	**C**	**2**	**7**
K7	**2**	**F**	**C**	**5**	**B**	**1**	**3**	**E**	**0**	**6**	**D**	**A**	**7**	**9**	**4**	**8**
K8	**3**	**0**	**5**	**C**	**8**	**F**	**D**	**E**	**B**	**6**	**2**	**9**	**7**	**1**	**4**	**A**

ДКЕ № 9

	0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*
K1	**9**	**0**	**B**	**C**	**2**	**4**	**3**	**F**	**D**	**6**	**E**	**1**	**A**	**7**	**5**	**8**
K2	**3**	**5**	**0**	**F**	**8**	**7**	**E**	**C**	**D**	**A**	**1**	**6**	**B**	**2**	**4**	**9**
K3	**8**	**4**	**5**	**A**	**E**	**B**	**D**	**6**	**C**	**F**	**7**	**9**	**3**	**1**	**2**	**0**
K4	**5**	**4**	**F**	**0**	**C**	**B**	**A**	**9**	**1**	**E**	**8**	**6**	**3**	**2**	**D**	**7**
K5	**7**	**C**	**3**	**0**	**6**	**8**	**E**	**B**	**1**	**F**	**D**	**A**	**9**	**5**	**2**	**4**
K6	**7**	**4**	**3**	**B**	**6**	**A**	**8**	**1**	**9**	**C**	**E**	**D**	**0**	**F**	**2**	**5**
K7	**7**	**E**	**9**	**F**	**1**	**4**	**8**	**3**	**B**	**D**	**0**	**2**	**6**	**A**	**5**	**C**
K8	**E**	**2**	**8**	**F**	**3**	**0**	**7**	**C**	**B**	**D**	**1**	**5**	**6**	**4**	**9**	**A**

ДКЕ № 10

	0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*
K1	**8**	**4**	**6**	**9**	**B**	**C**	**1**	**2**	**3**	**7**	**E**	**0**	**D**	**A**	**F**	**5**
K2	**7**	**D**	**1**	**8**	**A**	**E**	**4**	**F**	**9**	**0**	**6**	**3**	**2**	**C**	**B**	**5**
K3	**C**	**8**	**D**	**1**	**A**	**2**	**9**	**6**	**3**	**4**	**E**	**7**	**5**	**F**	**0**	**B**
K4	**2**	**B**	**3**	**4**	**C**	**7**	**9**	**D**	**F**	**8**	**5**	**0**	**1**	**E**	**A**	**6**
K5	**8**	**3**	**D**	**A**	**E**	**F**	**5**	**1**	**4**	**7**	**B**	**C**	**2**	**0**	**6**	**9**
K6	**4**	**C**	**9**	**B**	**E**	**A**	**7**	**6**	**3**	**5**	**0**	**F**	**1**	**2**	**8**	**D**
K7	**5**	**8**	**E**	**7**	**3**	**0**	**1**	**D**	**A**	**6**	**9**	**2**	**F**	**B**	**C**	**4**
K8	**A**	**3**	**5**	**9**	**0**	**D**	**7**	**8**	**C**	**4**	**1**	**6**	**B**	**F**	**2**	**E**

Додаток 2
до Інструкції про порядок постачання і використання ключів до засобів криптогра-фічного захисту інформації, що реалізують криптографічний алгоритм, визначений ГОСТ 28147-89

Типи рекомендованих носіїв ключової інформації

1. Загальні положення

1.1. Залежно від типу та кількості ключових даних, що містяться на НКІ, а також типу носія постачальником можуть постачатися різні типи НКІ.

1.2. У загальному випадку найменування НКІ, що однозначно визначає його тип, складається з трьох частин:

- частина 1, визначає тип ключових даних, що містяться на НКІ (РК або ДКЕ);
- частина 2, визначає тип фізичного носія (А, Б, В, Г або Д);
- частина 3, визначає кількість ключів, що розміщуються на НКІ.

Наприклад: РК-А-001, ДКЕ-Б-005, РК-Г-366 тощо.

1.3. Тип фізичного носія визначається виходячи з наступного:

«А» – ключові дані представлено у вигляді таблиці, яка надрукована на аркуші паперу;

«Б» – ключові дані представлено у вигляді файлу відповідного формату, що розміщується на стандартному накопичувачу на гнучкому магнітному диску (1.44Мб, 3.5”);

«В» – ключові дані представлено у вигляді файлу відповідного формату, що розміщується на стандартному компакт-диск типу CD-R, діаметром 12 см.

«Г» – ключові дані представлено у вигляді файлу відповідного формату, що розміщується на стандартному компакт-диск типу CD-R, діаметром 8 см.

«Д» - ключові дані представлено у вигляді файлу відповідного формату, що розміщується на запам’ятовуючому пристрої типу USB-флеш, виконаному у вигляді брелока.

1.4. Кількість ключів, що можуть розміщуватися на електронних носіях (носії типу «Б», «В», «Г» та «Д»), визначається замовником, але не більше ніж 999. На носіях типу «А» розміщується лише по одному ключу.

1.5. НКІ виготовляються серіями у визначеній замовником кількості примірників.

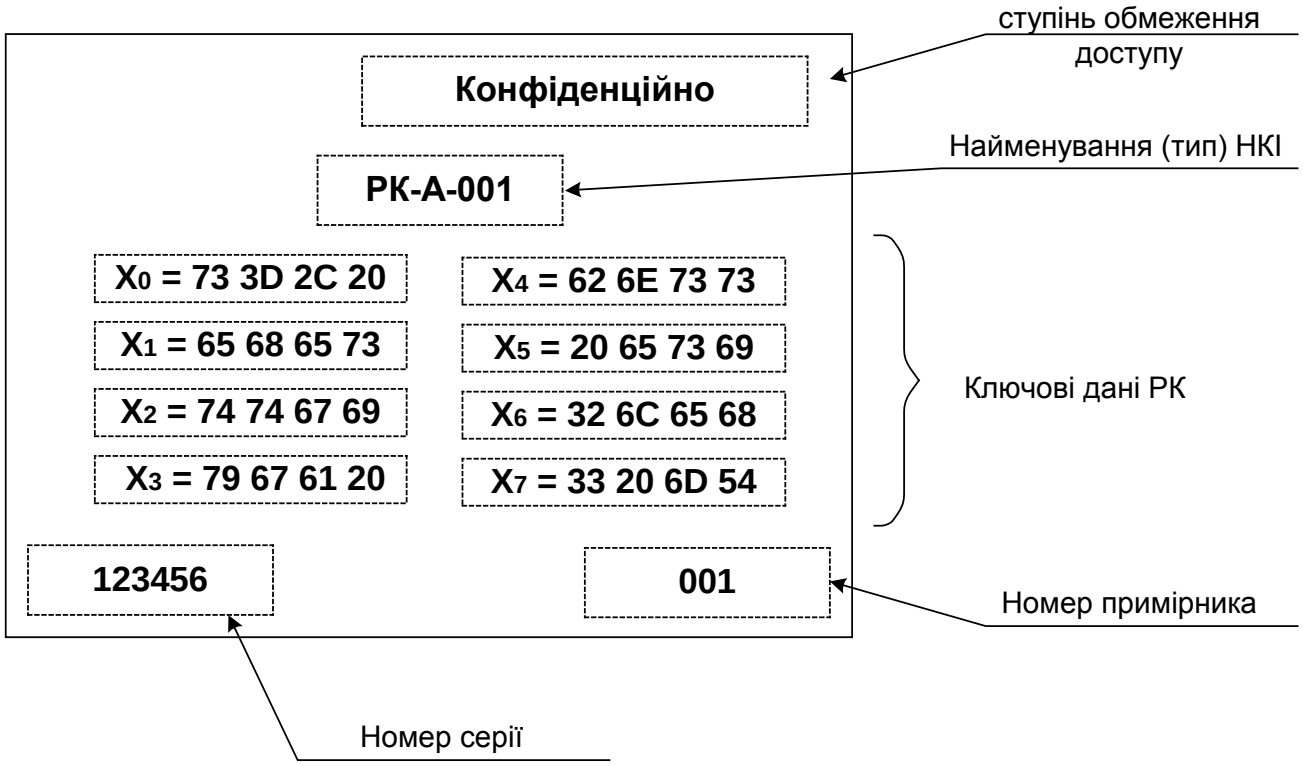
1.6. Кожний носій постачається замовнику у відповідній захисній упаковці, яка забезпечує захист НКІ від впливу зовнішнього середовища та унеможливлює безконтрольне вилучення НКІ та ознайомлення з його вмістом.

1.7. Зовнішній вигляд упаковки, розташування елементів маркування та порядок розкриття упаковок визначаються Правилами розкриття НКІ в упаковках відповідного типу, що постачаються замовнику разом з НКІ.

2. Носії ключової інформації типу РК-А-001

2.1. НКІ типу «РК-А-001» (рис. 1) являє собою аркуш паперу формату А5, на якому друкарським способом нанесено:

- ступінь обмеження доступу;
- найменування;
- ключові дані РК;
- номер серії;
- номер примірника.



Примітка: Використані умовні позначення відповідають позначенням, прийнятим у ГОСТ 28147-89.

Рис. 1. Зовнішній вигляд НКІ типу «РК-А-001» (приклад).

2.2. Ключові дані РК визначають заповнення відповідних 32-розрядних накопичувачів ключового запам'ятовуючого пристрою (відповідно до позначень ГОСТ 28147-89).

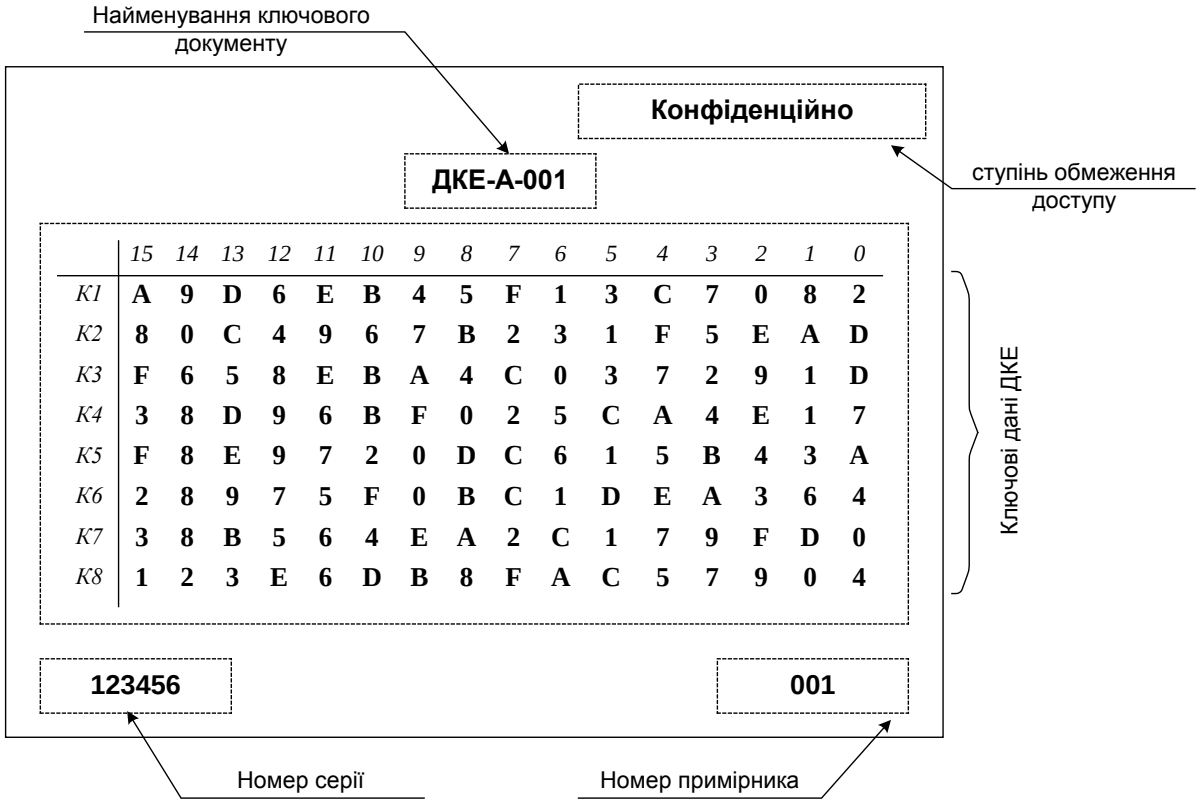
2.3. Заповнення накопичувачів ключового запам'ятовуючого пристрою (відповідно до позначень ГОСТ 28147-89) представлено шістнадцятирічним 32 розрядним словом, при цьому молодший біт відповідає молодшому розряду відповідного накопичувача (див. рис. 3).

2.4. Постачальником можуть вноситися незначні зміни у зовнішній вигляд НКІ, порядок взаємного розташування інформації на ньому, розміри та шрифт літер, а також наноситися інша додаткова інформації.

3. Носії ключової інформації типу ДКЕ-А-001

3.1. НКІ типу «ДКЕ-А-001» (рис. 2) являє собою аркуш паперу формату А5, на якому друкарським способом нанесено:

- ступінь обмеження доступу;
- найменування;
- ключові дані ДКЕ;
- номер серії;
- номер примірника.



	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
K1	**A**	**9**	**D**	**6**	**E**	**B**	**4**	**5**	**F**	**1**	**3**	**C**	**7**	**0**	**8**	**2**
K2	**8**	**0**	**C**	**4**	**9**	**6**	**7**	**B**	**2**	**3**	**1**	**F**	**5**	**E**	**A**	**D**
K3	**F**	**6**	**5**	**8**	**E**	**B**	**A**	**4**	**C**	**0**	**3**	**7**	**2**	**9**	**1**	**D**
K4	**3**	**8**	**D**	**9**	**6**	**B**	**F**	**0**	**2**	**5**	**C**	**A**	**4**	**E**	**1**	**7**
K5	**F**	**8**	**E**	**9**	**7**	**2**	**0**	**D**	**C**	**6**	**1**	**5**	**B**	**4**	**3**	**A**
K6	**2**	**8**	**9**	**7**	**5**	**F**	**0**	**B**	**C**	**1**	**D**	**E**	**A**	**3**	**6**	**4**
K7	**3**	**8**	**B**	**5**	**6**	**4**	**E**	**A**	**2**	**C**	**1**	**7**	**9**	**F**	**D**	**0**
K8	**1**	**2**	**3**	**E**	**6**	**D**	**B**	**8**	**F**	**A**	**C**	**5**	**7**	**9**	**0**	**4**

Примітка: Використані умовні позначення відповідають позначенням, прийнятим у ГОСТ 28147-89.

Рис. 2. Зовнішній вигляд носія «ДКЕ-А-1» (приклад).

3.2. Ключові дані ДКЕ таблиць блоку підстановок К криптографічного алгоритму ГОСТ 28147-89 (у позначеннях ГОСТ 28147-89). Кожний вузол заміни (К1, К2, …, К8) визначає таблицю з шістнадцяти рядків (від 0 до 15), кожен з яких містить по 4 біта (представлені у шістнадцятковому вигляді). При цьому, за молодшим адресом розташовується молодший біт (див. рис. 4).

Кожний вузол заміни є підстановкою на множині чисел {0,1,2 … F}.

3.3. Постачальником можуть вноситися незначні зміни у зовнішній вигляд НКІ, порядок взаємного розташування інформації на ньому, розміри та шрифт літер, а також наноситися інша додаткова інформації.

4. Електронні носії ключової інформації

4.1. До електронних НКІ відносяться носії типів «Б», «В», «Г» та «Д», які дозволяють запис та зчитування даних стандартними засобами електронної обчислювальної техніки, що обладнані відповідними пристроями зчитування (запису).

4.2. Ключові дані РК та ДКЕ на електронних НКІ розміщуються у відповідних ключових файлах, кількість яких визначається замовником.

4.3. Ключові файли розміщуються на електронних НКІ у каталозі «KEY». Структура НКІ не містить будь-яких інших файлів та каталогів.

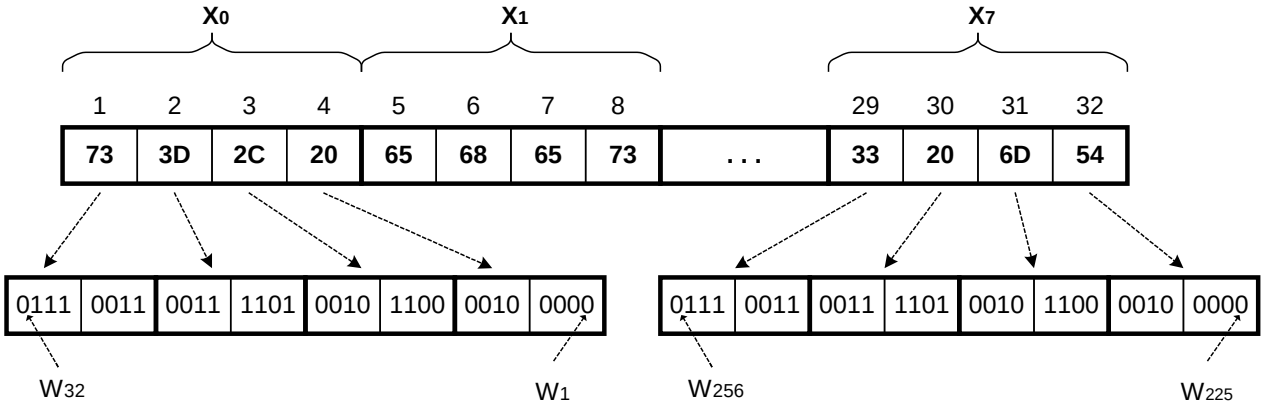
4.4. Найменування ключових файлів, що містить ключові дані РК - «RKXXXXXX.YYY», де RK – ознака ключового файлу, що визначає тип ключових даних, XXXXXX – номер серії НКІ (однаковий для всіх ключових файлів, що містяться на НКІ, YYY – номер ключового файлу (001, 002, … 999). Довжина ключового файлу – 256 біт (32 байти).

4.5. Найменування ключових файлів, що містить ключові дані ДКЕ - «DKXXXXXX.YYY», де DK – ознака ключового файлу, що визначає тип ключових даних, XXXXXX – номер серії НКІ (однаковий для всіх ключових файлів, що містяться на НКІ, YYY – номер ключового файлу (001, 002, … 999). Довжина ключового файлу – 512 біт (64 байти).

4.6. Структура ключового файлу, що містить ключові дані РК, представлена на рис. 3.

4.7. Ключ РК довжиною 256 біт (32 байти) містить (умовно) 8 блоків (X0, X1, …, X7) по 32 біти (4 байта) в кожному. Блоки розміщуються один за одним, в порядку зростання їх номерів.

4.8. Кожний блок (32 розрядне слово – 4 байти) визначає заповнення відповідного накопичувача ключового запам’ятовуючого пристрою, при цьому молодший біт відповідає молодшому розряду накопичувача.

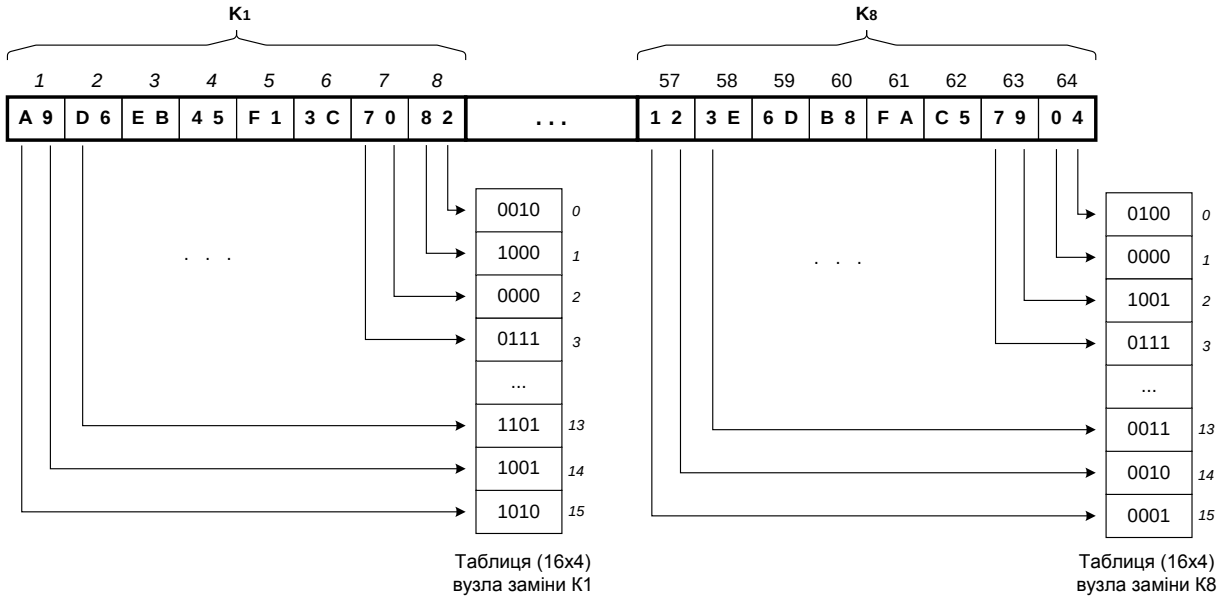


Примітки: 1. *Використані умовні позначення відповідають позначенням, прийнятим у ГОСТ 28147-89.*

2. *В якості ключових даних наведено РК, що наведений в якості прикладу НКІ «РК-А-1».*

Рис. 3. Структура ключового файлу, що містить ключові дані РК (приклад).

4.9. Структура ключового файлу, що містить ключові дані ДКЕ, представлена на рис. 4.



Примітки: 1. *Використані умовні позначення відповідають позначенням, прийнятим у ГОСТ 28147-89.*

2. *В якості ключових даних наведено ДКЕ, що наведений в якості прикладу НКІ «ДКЕ-А-1».*

Рис. 4. Структура ключового файлу, що містить ключові дані ДКЕ (приклад).

4.10. Ключ ДКЕ довжиною 512 біт (64 байти) містить (умовно) 8 вузлів заміни (К1, К2, …, К8) по 64 біти (8 байт) в кожному. Вузли розміщуються один за одним в порядку зростання їх номерів.

4.11. Кожний вузол заміни (64 розрядне слово – 8 байт) визначає таблицю з 16 рядків по 4 біта в кожному. При цьому молодша тетрада відповідає молодшому номеру рядка у таблиці.