

АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

НАКАЗ

12.06.2007 N 114

**Про затвердження Інструкції
про порядок постачання і використання ключів
до засобів криптографічного захисту інформації**

Відповідно до Законів України "Про інформацію" ([2657-12](#)), "Про Державну службу спеціального зв'язку та захисту інформації України" ([3475-15](#)), "Про електронний цифровий підпис" ([852-15](#)), "Про захист інформації в інформаційно-телекомунікаційних системах" ([80/94-ВР](#)), Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації, затвердженого постановою Кабінету Міністрів України від 24.06.2006 N 868 ([868-2006-п](#)), **НАКАЗ** У Ю:

1. Затвердити Інструкцію про порядок постачання і використання ключів до засобів криптографічного захисту інформації, що додається.
2. Начальнику Департаменту регулювання діяльності у сфері криптографічного захисту інформації Адміністрації Державної служби спеціального зв'язку та захисту інформації України забезпечити подання цього наказу в установленому порядку на державну реєстрацію до Міністерства юстиції України.
3. Контроль за виконанням цього наказу покласти на першого заступника Голови Державної служби спеціального зв'язку та захисту інформації України.

Голова Служби Ю.Б.Чеботаренко

Зареєстровано в Міністерстві

юстиції України

25 червня 2007 р.

за N 729/13996

ІНСТРУКЦІЯ

про порядок постачання і використання ключів

до засобів криптографічного захисту інформації

1. Загальні положення

1.1. Інструкція про порядок постачання і використання ключів до засобів криптографічного захисту інформації (далі - Інструкція) розроблена відповідно до Законів України "Про інформацію" ([2657-12](#)), "Про Державну службу спеціального зв'язку та захисту інформації України" ([3475-15](#)), "Про електронний цифровий підпис" ([852-15](#)), "Про захист інформації в інформаційно-телекомунікаційних системах" ([80/94-ВР](#)), Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації, затвердженого постановою Кабінету Міністрів України від 24.06.2006 N 868 ([868-2006-п](#)).

1.2. Інструкція встановлює порядок постачання та використання ключів до засобів криптографічного захисту інформації (далі - КЗІ), які реалізують криптографічний алгоритм, визначений ГОСТ 2814789 "Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования" (далі - ГОСТ 2814789).

1.3. Вимоги цієї Інструкції обов'язкові для виконання органами державної влади та органами місцевого самоврядування, підприємствами, установами та організаціями всіх форм власності, які здійснюють розроблення, виробництво, використання, експлуатацію, сертифікаційні випробування, тематичні дослідження, експертизу, увезення, вивезення криптосистем і засобів КЗІ, що реалізують криптографічний алгоритм, визначений ГОСТ 28147-89, надають послуги в галузі КЗІ з використанням зазначених засобів КЗІ (у тому

числі послуги електронного цифрового підпису), здійснюють їх постачання або торгівлю ними.

1.4. Дія цієї Інструкції не розповсюджується на діяльність, пов'язану з постачанням і використанням ключів до засобів КЗІ, що становить державну таємницю.

1.5. Використані в цій Інструкції терміни мають такі значення:

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

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

методика генерації ключів - опис послідовності операцій (алгоритму), що виконуються у процесі генерації ключів;

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

носіє ключової інформації (далі - НКІ) - матеріальний носій інформації, що призначений для запису та збереження ключів;

постачальник - підприємство, установа, організація або підрозділ Державної служби спеціального зв'язку та захисту інформації України (далі - Держспецзв'язку), які визначаються Держспецзв'язку для здійснення постачання ключових документів до засобів КЗІ;

разовий (сеансовий) ключ (далі - РК) - ключ, який визначає порядок заповнення ключового запам'ятовувального пристрою засобу КЗІ, що реалізує алгоритм криптографічного перетворення, визначений ГОСТ 28147-89.

Інші терміни застосовуються у значеннях, наведених у нормативно-правових актах з питань криптографічного захисту інформації, електронного цифрового підпису, а також ГОСТ 28147-89.

2. Порядок використання ключів

2.1. РК можуть бути отримані від постачальника або генеруватися замовником із застосуванням засобу КЗІ, який має сертифікат відповідності або позитивний експертний висновок Адміністрації Держспецзв'язку.

2.2. ДКЕ можуть бути отримані від постачальника або обираються з переліку ДКЕ, які рекомендуються до застосування у засобах КЗІ, який наведений в додатку 1 до цієї Інструкції.

2.3. ДКЕ можуть обиратися з переліку, наведеного в додатку 1 до цієї Інструкції, у разі:

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

обчислення гешфункції згідно з ГОСТ 34.311-95 "Информационная технология. Криптографическая защита информации. 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) обміні інформацією каналами (лініями) зв'язку;

використання у засобах КЗІ категорії "Р" (крім засобів, призначених для криптографічного захисту конфіденційної інформації, що є власністю держави).

2.4. У випадках, передбачених пунктом 2.3 цієї Інструкції, ДКЕ можуть також обиратися з посилених сертифікатів відкритого ключа електронного цифрового підпису.

2.5. ДКЕ для криптографічного захисту конфіденційної інформації, що є власністю держави, постачаються встановленим порядком.

При цьому генерація ДКЕ та їх запис на НКІ здійснюються постачальником.

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

2.7. Ключі можуть розподілятися між засобами КЗІ каналами (лініями) зв'язку в захищеному вигляді. Розподіл ключів повинен здійснюватися відповідно до національних стандартів або за методикою розподілу ключів, погодженою встановленим порядком на підставі результатів державної експертизи у сфері КЗІ.

2.8. Дозволяється методику генерації ключів та методику розподілу ключів викладати в одному документі - методиці генерації та розподілу ключів.

2.9. Термін дії ДКЕ, наведених у додатку 1 до цієї Інструкції, а також термін дії РК, генерація яких здійснена відповідно до національних стандартів, визначається замовником.

В інших випадках термін дії ДКЕ та РК 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, у тому числі отриманих від постачальника, визначається замовником.

В інших випадках ступінь обмеження доступу до ДКЕ, а також ступінь обмеження доступу до РК повинен відповідати ступеню обмеження доступу, установленому для інформації, криптографічні перетворення якої здійснюються із застосуванням цих ключів.

2.11. Умови зберігання, використання, формування та обміну ключами повинні унеможлилювати їх несанкціоновану модифікацію або підміну.

Для ключів, щодо яких установлена необхідність обмеження доступу, умови зберігання, використання та обміну ключами додатково повинні унеможлилювати ознайомлення з їх змістом сторонніх осіб.

2.12. Порядок використання ключів та поводження з НКІ, термін дії та ступінь обмеження доступу вказуються в експлуатаційній документації на засоби КЗІ, для яких призначені НКІ.

3. Порядок постачання ключів

3.1. Постачання ключів здійснюється на підставі укладених договорів між постачальником та замовником.

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

Типи рекомендованих НКІ та форматів ключів, що розміщуються на них, наведені в додатку 2 до цієї Інструкції.

3.3. Постачання ключів здійснюється у такому порядку:

подача замовником заявки;

розгляд заявки та прийняття відповідного рішення щодо постачання ключів;

укладання договору постачання ключових документів з постачальником;

здійснення постачання ключових документів замовнику;

контроль за дотриманням порядку постачання та використання ключів.

3.4. Подача замовником заявки

3.4.1. У разі необхідності одержання замовником ключів він направляє до Адміністрації Держспецзв'язку заявку, у якій вказуються:

місцезнаходження та інші реквізити замовника;

відомості щодо наявності ліцензії на право провадження господарської діяльності у сфері КЗІ (серія, номер ліцензії, термін дії, види робіт, особливі умови);

призначення ключів (у тому числі, у яких засобах КЗІ будуть використовуватися ключі, наявність сертифіката 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 ключів;

гарантії оплати робіт за договором постачання ключових документів.

3.4.2. У разі, коли тип НКІ, структура та формат даних, що міститься на ньому, не відповідають вимогам, зазначеним у додатку 2 до цієї Інструкції, до заявки додаються матеріали, у яких викладаються:

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 у залежності від серії та номера примірника у серії тощо).

3.5. Розгляд заявки та прийняття відповідного рішення

3.5.1. Адміністрація Держспецзв'язку розглядає заявку та приймає рішення про можливість постачання чи відмову в постачанні ключових документів.

3.5.2. Про прийняте рішення Адміністрація Держспецзв'язку повідомляє замовника в письмовому вигляді протягом 30 днів з дня отримання заявки.

3.5.3. За умови позитивного рішення щодо постачання ключових документів Адміністрація Держспецзв'язку повідомляє замовника та передає матеріали постачальнику, який надсилає замовнику проект відповідного договору.

3.5.4. У разі негативних результатів розгляду заявки Адміністрація Держспецзв'язку інформує замовника про причини відмови в постачанні ключових документів.

3.6. Укладання договору постачання ключових документів

3.6.1. Договір постачання ключових документів укладається за домовленістю між постачальником та замовником.

3.6.2. Зміст договору постачання ключових документів повинен відповідати вимогам законодавства України.

Крім того, у договорі постачання ключових документів обов'язково вказуються:

порядок оплати, умови та терміни постачання ключових документів;

порядок звітності та здійснення контролю за використанням ключових документів;

порядок використання та постачання ключових документів іншим учасникам захищеного інформаційного обміну або підрозділам (філіям) замовника (за потреби у разі такого використання чи постачання).

3.7. Здійснення постачання ключових документів

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

3.7.2. Про виконання договору постачання ключових документів постачальник повідомляє Адміністрацію Держспецзв'язку.

3.8. Замовник має право здійснювати постачання ключових документів, отриманих від постачальника, своїм структурним підрозділам та взаємодіючим з ним юридичним та фізичним особам у порядку, передбаченому договором, який укладається відповідно до пункту 3.6 цієї Інструкції.

При цьому забороняється тиражувати отримані від постачальника ключові документи та копіювати ключі на інші НКІ, якщо це не визначено експлуатаційною документацією на конкретний засіб КЗІ.

Начальник Департаменту

регулювання діяльності

у сфері криптографічного

захисту інформації

Адміністрації Держспецзв'язку

В.П.Гребнев

ДКЕ N 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 N 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

ТИПИ

рекомендованих НКІ та форматів ключів,
що розміщуються на них

1. Загальні положення

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

1.2. Найменування НКІ, що однозначно визначає його тип, складається з трьох частин:

частина 1, визначає тип ключів, що містяться на НКІ (РК або ДКЕ);

частина 2, визначає тип фізичного носія (А, Б, В, Г, Д);

частина 3, визначає кількість ключів, які розміщуються на НКІ.

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

1.3. Тип фізичного носія визначається, виходячи з такого:

"А" - ключі представлені у вигляді таблиці, яка надрукована на аркуші папера;

"Б" - ключі представлені у вигляді файла відповідного формату, який розміщується на стандартному накопичувачі на гнучкому магнітному диску (1,44 Мб, 3,5");

"В" - ключі представлені у вигляді файла відповідного формату, який розміщується на стандартному компакт-диску типу CD-R, діаметром 12 см;

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

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

Найменування ключового

документа															Ступінь														
															обмеження														
Конфіденційно																													
															доступу														
ДКЕ-А-001																													
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															Ключові														
															> дані ДКЕ														
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																													
123456															001														
Номер серії															Номер примірника														

Примітка. Використовувані умовні позначення мають відповідати позначенням, наведеним у ГОСТ 28147-89.

Рис. 2. Зовнішній вигляд носія "ДКЕ-А-001"

(приклад)

3.2. Ключові дані ДКЕ визначають заповнення таблиць блока підстановки К. Кожний вузол заміни (K1, K2, ..., K8) визначає таблицю з шістнадцяти рядків (від 0 до 15), кожен з яких містить по 4 біти (представлені в шістнадцятьковому вигляді). При цьому за молодшою адресою розташовується молодший біт (див. рис. 4).

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

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

4. Електронні НКІ

4.1. До електронних НКІ належать носії типів "Б", "В", "Г" та "Д", які дають змогу записувати та зчитувати дані стандартними засобами електронної обчислювальної техніки, які обладнані відповідними пристроями зчитування (запису).

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

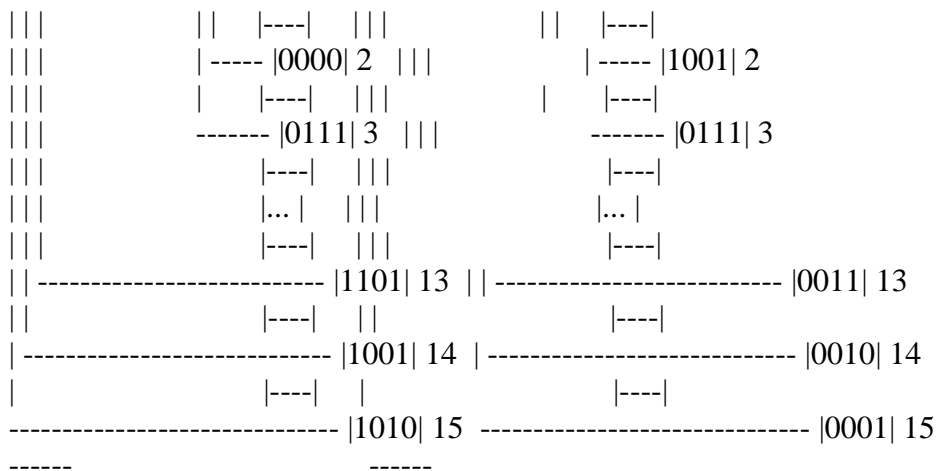
4.3. Ключові файли розміщуються на електронних НКІ в каталозі "KEY". Структура НКІ не повинна містити будь-яких інших файлів та каталогів.

4.4. Найменування ключових файлів, які містять ключові дані РК - "RKXXXXXX.YYY", де РК - ознака ключового файла, що визначає тип ключа, XXXXXX - номер серії НКІ (однаковий для всіх ключових файлів, що містяться на НКІ, YYY - номер ключового файла (001, 002, ..., 999). Довжина ключового файла - 256 біт (32 байти).

4.5. Найменування ключових файлів, які містять ключові дані ДКЕ - "DKXXXXXX.YYY", де ДК - ознака ключового файла, що визначає тип ключа, XXXXXX - номер серії НКІ (однаковий для всіх ключових файлів, що містяться на НКІ, YYY - номер ключового файла (001, 002, ..., 999). Довжина ключового файла - 512 біт (64 байти).

4.6. Структура ключового файла, який містить ключові дані РК, представлена на рис. 3.

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



Таблиця (16x4)
вузла заміни К1

Таблиця (16x4)
вузла заміни К8

Примітки.

1. Використовувані умовні позначення мають відповідати позначенням, наведеним у ГОСТ 28147-89.
2. Як ключ представлено ДКЕ, наведений як приклад НКІ "ДКЕ-А-001".

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

4.10. ДКЕ довжиною 512 біт (64 байти) містить (умовно) 8 вузлів заміни (К1, К2, ..., К8) по 64 біти (8 байт) у 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 біти в кожному. При цьому молодша тетрада відповідає молодшому номеру рядка в таблиці.

Начальник Департаменту

регулювання діяльності

у сфері криптографічного

захисту інформації

Адміністрації Держспецзв'язку

В.П.Гребнев