



АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

Н А К А З
20.07.2007 N 141

Зареєстровано в Міністерстві
юстиції України
30 липня 2007 р.
за N 862/14129

Про затвердження Положення про порядок
розроблення, виробництва та експлуатації засобів
криптографічного захисту конфіденційної інформації
та відкритої інформації з використанням
електронного цифрового підпису

На виконання Положення про порядок здійснення криптографічного захисту інформації в Україні, затвердженого Указом Президента України від 22 травня 1998 року N 505 ([505/98](#)), відповідно до Законів України "Про Державну службу спеціального зв'язку та захисту інформації України" ([3475-15](#)), "Про інформацію" ([2657-12](#)), "Про електронний цифровий підпис" ([852-15](#)), "Про стандарти, технічні регламенти та процедури оцінки відповідності" ([3164-15](#)), з метою встановлення порядку розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної інформації та засобів електронного цифрового підпису **Н А К А З У Ю:**

1. Затвердити Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної інформації та відкритої інформації з використанням електронного цифрового підпису (додається).

2. Визнати таким, що втратив чинність, наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від [30.11.99](#) N 53 ([z0868-99](#)) "Про затвердження Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту конфіденційної інформації", зареєстрований у Міністерстві юстиції України [15.12.99](#) за N 868/4161.

3. Начальнику Департаменту стратегії розвитку спеціальних інформаційно-телекомунікаційних систем Адміністрації Державної служби спеціального зв'язку та захисту інформації України забезпечити подання в установленому порядку наказу на державну реєстрацію до Міністерства юстиції України.

4. Контроль за виконанням наказу покласти на першого заступника Голови Державної служби спеціального зв'язку та захисту інформації України.

Т.в.о. Голови Служби О.І.Сиров

ЗАТВЕРДЖЕНО
Наказ Адміністрації
Державної служби
спеціального зв'язку
та захисту інформації
України
20.07.2007 N 141

Зареєстровано в Міністерстві
юстиції України
30 липня 2007 р.
за N 862/14129

ПОЛОЖЕННЯ
про порядок розроблення, виробництва
та експлуатації засобів криптографічного захисту
конфіденційної інформації та відкритої інформації
з використанням електронного цифрового підпису

Це Положення розроблено відповідно до Законів України "Про Державну службу спеціального зв'язку та захисту інформації України" ([3475-15](#)), "Про інформацію" ([2657-12](#)), "Про електронний цифровий підпис" ([852-15](#)), "Про захист інформації в інформаційно-телекомунікаційних системах" ([80/94-ВР](#)), "Про стандарти, технічні регламенти та процедури оцінки відповідності" ([3164-15](#)) та Положення про порядок здійснення криптографічного захисту інформації в Україні, затвердженого Указом Президента України від 22 травня 1998 року N 505 ([505/98](#)).

1. Загальні положення

1.1. Це Положення визначає вимоги до порядку розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної інформації та відкритої інформації з використанням електронного цифрового підпису.

Розроблення, виготовлення, уведення в експлуатацію та експлуатація засобів криптографічного захисту інформації, що становить державну таємницю, та конфіденційної інформації, що є власністю держави, здійснюються в порядку, визначеному іншими нормативно-правовими актами.

1.2. Вимоги цього Положення обов'язкові для виконання державними органами, підприємствами, установами і організаціями незалежно від форм власності, діяльність яких пов'язана з розробленням, виробництвом, сертифікаційними випробуваннями (експертними роботами) та експлуатацією засобів криптографічного захисту конфіденційної інформації, а також відкритої інформації з використанням електронного цифрового підпису.

1.3. На підставі цього Положення, відповідно до Закону України "Про Національний банк України" ([679-14](#)) Національним банком України визначаються вимоги щодо захисту електронних банківських документів та організації управління інформаційною безпекою в банківській системі України, особливості розроблення, виробництва, випробувань, уведення та експлуатації засобів криптографічного захисту інформації (далі - КЗІ), які розробляються, виробляються та випробовуються безпосередньо

Національним банком України для власних потреб та потреб банківської системи України, а також особливості експлуатації засобів КЗІ Національного банку України в небанківських установах, що їх використовують.

1.4. Використані в цьому Положенні терміни відповідають термінам, визначеним у нормативно-правових актах у сфері криптографічного захисту інформації та у сфері електронного цифрового підпису. Крім того, використовуються такі терміни:

засіб КЗІ - програмний, апаратно-програмний та апаратний засіб, призначений для криптографічного захисту інформації;

ключові дані (ключ) - конкретний стан деяких параметрів криптографічного алгоритму, які забезпечують вибір одного криптографічного перетворення із сукупності усіх можливих для цього криптографічного алгоритму;

ключовий документ - матеріальний носій із зафіксованими відповідним чином ключовими даними;

компрометація - будь-який випадок (втрата, розголошення, крадіжка, несанкціоноване копіювання тощо) з ключовими документами (ключовими даними) та засобами КЗІ, який призвів (може призвести) до розголошення (витоку) інформації про них, а також інформації, яка обробляється та передається;

криптографічне перетворення інформації - перетворення інформації з використанням ключових даних з метою приховування (відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства, дати створення тощо;

режим безпеки - система правових норм, організаційних та організаційно-технічних заходів, яка створена в державних органах, на підприємствах, в установах та організаціях під час розроблення, дослідження, виробництва та експлуатації засобів КЗІ з метою обмеження доступу до інформації;

сертифікаційні випробування - випробування засобів КЗІ, що проводяться з метою встановлення відповідності їх характеристик та властивостей вимогам нормативних документів в сфері КЗІ;

вимоги до засобів КЗІ - вимоги до принципів побудови засобів КЗІ та технічної реалізації криптографічних алгоритмів у засобах КЗІ, вимоги до криптографічних якостей, а також вимоги і норми щодо захисту засобів КЗІ від витоку інформативних сигналів каналами побічних електромагнітних випромінювань та наведень (далі - ПЕМВН);

порушник - юридична або фізична особа, яка навмисно чи ненавмисно здійснює несанкціоновані дії щодо інформації в системі;

технічний засіб оброблення інформації - технічний засіб, призначений для приймання, накопичення, зберігання, перетворення, відображення та передавання інформації;

управління ключовими даними - дії, пов'язані з генерацією, розподіленням, доставлянням, уведенням у дію, зміненням, зберіганням, обліком та знищенням ключових даних, а також носіїв ключових даних;

шифрування - перетворення відкритого тексту в шифротекст (зашифрування) та відновлення відкритого тексту із шифротексту (розшифрування) при відомих ключових даних.

1.5. Залежно від способу реалізації розрізняють такі типи засобів КЗІ:

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 (у тому числі криптографічні функції) яких реалізовується в оптичних, механічних, мікроелектронних або інших спеціалізованих пристроях.

Користувач апаратних засобів КЗІ не має доступу до змісту запам'ятовувальних елементів, що зберігають мікропрограми керування пристроєм. Алгоритм функціонування пристрою змінюється тільки його розробником або виробником.

Залежно від виконання встановлюються такі види засобів КЗІ:

вид А - засоби, які на конструктивному, алгоритмічному та програмному рівнях є єдиними виробами, що функціонують (експлуатуються) відокремлено від будь-яких інших технічних засобів;

вид Б - засоби, які на конструктивному, алгоритмічному та програмному рівнях є єдиними виробами та призначені для використання у складі комплексів оброблення та передавання інформації;

вид В - вироби, що є окремими вузлами (модулями, блоками, платами, програмними компонентами тощо), які самостійно не експлуатуються та призначені для застосування як складові частини при побудові засобів видів А та Б.

Залежно від призначення встановлюються такі категорії засобів КЗІ:

засоби шифрування інформації (далі - засоби категорії "Ш");

засоби, призначені для виготовлення ключових даних або ключових документів (незалежно від виду носія ключової інформації) та управління ключовими даними, що використовуються в засобах КЗІ (далі - засоби категорії "К");

засоби захисту від нав'язування неправдивої інформації або захисту від несанкціонованої модифікації, що реалізують алгоритми криптографічного перетворення інформації (далі - криптоалгоритми), у тому числі засоби імітозахисту та електронного цифрового підпису (далі - засоби категорії "П");

засоби захисту інформації від несанкціонованого доступу (у тому числі засоби розмежування доступу до ресурсів електронно-обчислювальної техніки), у яких реалізовані криптоалгоритми (далі - засоби категорії "Р").

1.6. У процесі розроблення, виробництва та експлуатації засобів КЗІ беруть участь і взаємодіють між собою:

замовники;

розробники;

виробники;

організації, що експлуатують засоби КЗІ;

організації, що проводять сертифікаційні випробування (експертні роботи);

Державна служба спеціального зв'язку та захисту інформації України (далі - Держспецзв'язку).

1.7. Замовниками виступають органи державної влади та місцевого самоврядування, а також суб'єкти господарювання, які здійснюють фінансування робіт з розроблення засобів КЗІ, або ті, що уклали з виробниками договір про виготовлення та (або) постачання цих засобів.

1.8. Ліцензування господарської діяльності в галузі криптографічного захисту інформації здійснюється відповідно до чинного законодавства.

1.9. Суб'єкти, які здійснюють розроблення, виробництво та експлуатацію засобів КЗІ, визначають режим доступу до інформації про ці засоби, встановлюють і підтримують відповідний режим безпеки з урахуванням вимог замовника та відповідно до нормативно-правових актів у сфері КЗІ.

1.10. Розробники та виробники реалізують вимоги до засобів КЗІ шляхом вибору і розробки необхідних алгоритмічних, програмних, схемно-технічних, конструкторських та технологічних рішень, які забезпечують виконання встановлених вимог.

1.11. Поширення інформації з питань КЗІ, яка надається Держспецзв'язку суб'єктам господарювання, здійснюється за погодженням з Держспецзв'язку.

Держспецзв'язку забезпечує конфіденційність інформації та дотримання авторських прав щодо наданих їй матеріалів.

2. Розроблення засобів КЗІ

2.1. Розроблення засобів КЗІ здійснюється відповідно до вимог нормативно-правових актів і національних стандартів у сфері КЗІ, а також нормативних документів з питань розроблення та поставлення продукції на виробництво.

2.2. Розроблення засобів КЗІ здійснюється шляхом виконання відповідних науково-дослідних робіт (далі - НДР) з розроблення нових принципів побудови і функціонування засобів КЗІ та дослідно-конструкторських робіт (далі - ДКР) зі створення нових або модернізації існуючих зразків засобів КЗІ.

Залежно від організаційної форми робіт з розроблення засобів КЗІ розробники засобів КЗІ в цьому Положенні йменуються як виконавці НДР (ДКР).

2.3. НДР з розроблення нових принципів побудови і функціонування засобів КЗІ виконується згідно з технічним завданням (далі - ТЗ), яке погоджується виконавцем НДР.

2.4. Погоджене виконавцем ТЗ на НДР надсилається до Держспецзв'язку, яка протягом одного місяця його погоджує або надає вмотивовану відмову. Після затвердження ТЗ замовником один його примірник надсилається до Держспецзв'язку.

2.5. За результатами НДР готується ТЗ на ДКР з розроблення нового або модернізації існуючого зразка засобу КЗІ з підготовкою, за необхідності, техніко-економічного обґрунтування ДКР.

2.6. За наявності необхідного досвіду з проведення відповідних робіт допускається розроблення ТЗ на ДКР без попереднього виконання НДР.

2.7. ТЗ на ДКР розробляється спільно замовником і виконавцем або виконавцем на підставі вихідних даних замовника, у яких указуються перелік можливих загроз криптографічній системі (перехоплення повідомлень, крадіжка ключових документів та іншої критичної інформації тощо), прогнозовані характеристики технічних можливостей потенційного порушника та можливі заходи протидії (фізико-хімічні методи знищення критичної інформації тощо). Особлива увага при цьому приділяється забезпеченню безпеки системи управління ключовими даними (ключами).

За необхідності, до розроблення ТЗ залучаються організації, які мають ліцензію Адміністрації Держспецзв'язку та здійснюють сертифікаційні випробування (експертні роботи) криптосистем та засобів КЗІ.

2.8. Залежно від вірогідних умов експлуатації засобів КЗІ та відповідно до цінності інформації, що захищається, визначаються чотири рівні можливостей порушника:

нульовий рівень - ненавмисне порушення конфіденційності, цілісності та підтвердження авторства інформації;

перший рівень - порушник має обмежені кошти та самостійно створює засоби, розробляє методи атак на засоби КЗІ, а також інформаційно-телекомунікаційні системи із застосуванням широко розповсюджених програмних засобів та електронно-обчислювальної техніки;

другий рівень - порушник корпоративного типу має змогу створення спеціальних технічних засобів, вартість яких співвідноситься з можливими фінансовими збитками, що виникатимуть від порушення конфіденційності, цілісності та підтвердження авторства інформації, зокрема при втраті, спотворенні та знищенні інформації, що захищається. У цьому разі для розподілу обчислень при проведенні атак можуть застосовуватися локальні обчислювальні мережі;

третій рівень - порушник має науково-технічний ресурс, який прирівнюється до науково-технічного ресурсу спеціальної служби економічно розвинутої держави.

2.9. З урахуванням встановленого рівня можливостей порушника обирається необхідний клас засобів КЗІ:

клас А1 - відповідає вимогам забезпечення стійкості криптоперетворення в умовах, коли можливості порушника обмежені лише сучасним станом науки і техніки (захист від порушника третього рівня);

клас Б1 - відповідає вимогам забезпечення стійкості криптоперетворення в умовах недокументованих можливостей у прикладному програмному забезпеченні (захист від порушника другого рівня);

клас Б2 - відповідає вимогам забезпечення стійкості криптоперетворення в умовах здійснення порушником навмисного зовнішнього впливу (захист від порушника другого рівня);

клас В1 - відповідає вимогам забезпечення стійкості криптоперетворення в умовах несанкціонованих дій з боку легального користувача системи (захист від порушника першого рівня);

клас В2 - відповідає вимогам забезпечення стійкості криптоперетворення в умовах помилкових дій обслуговувального персоналу та відмов технічних засобів (захист від порушника першого та нульового рівнів);

клас В3 - відповідає вимогам забезпечення стійкості криптоперетворення за рахунок стійкості криптоалгоритму та правильної його реалізації в засобі КЗІ (захист від порушника нульового рівня).

Класи засобів КЗІ наведено в порядку зменшення вимог таким чином, що рівень, наведений вище, передбачає виконання вимог усіх наведених нижче класів.

2.10. У ТЗ на ДКР з розроблення нового типу або модернізації існуючого зразка засобу КЗІ вносяться:

відомості про замовника та виконавця ДКР;

відомості про категорію, тип, вид і клас засобу та відомості про його застосування (у тому числі типова схема організації зв'язку із зазначенням способу застосування засобу КЗІ, максимальна кількість абонентів у мережі, вид інформації, що підлягає обробці, швидкість обробки, необхідний рівень захисту інформації, тип виконання і конструктивні особливості реалізації виробу);

вимоги до криптоалгоритму та його реалізації (у тому числі вимоги щодо завадостійкості і криптостійкості алгоритму, вимоги до імітозахисту повідомлень, порядок моделювання і верифікації моделей, порядок реалізації і тестування програмного забезпечення засобу);

вимоги до ключової системи та її організації (у тому числі вид та кількість ключів, періодичність їх зміни, вимоги до носіїв ключової інформації);

вимоги до управління ключовими даними (у тому числі їх генерації);

вимоги до показників надійності засобів КЗІ (обов'язково - для засобів категорій "Ш" і "К");

вимоги до електромагнітної сумісності та завадозахищеності (обов'язково для засобів категорії "К");

відомості про типи технічних засобів оброблення інформації, які передбачаються для спільної роботи із засобами КЗІ, у тому числі вимоги до інтерфейсів;

вимоги до каналів зв'язку із зазначенням допустимих відхилень параметрів каналу, при яких повинно забезпечуватися стійке функціонування засобу;

вимоги до протоколу входження у зв'язок;

перелік нормативно-правових, нормативних та інших документів, які містять вимоги та положення щодо розроблення або модернізації існуючого зразка засобу КЗІ;

вимоги до дослідної ділянки для випробувань засобів КЗІ;

вимоги щодо сертифікаційних випробувань (експертних робіт).

2.11. Погоджене виконавцем ТЗ на ДКР надсилається до Держспецзв'язку, яка протягом одного місяця його погоджує або надає вмотивовану відмову. Після затвердження ТЗ замовником один його примірник надсилається до Держспецзв'язку.

2.12. Вимоги до засобів КЗІ та вимоги до ключової системи можуть бути викладені в частковому (спеціальному) ТЗ, порядок оформлення, погодження та затвердження якого відповідає порядку, установленому для основного ТЗ.

2.13. У засобах КЗІ використовуються криптоалгоритми та криптопротоколи, які є національними стандартами або рекомендовані Адміністрацією Держспецзв'язку, або погоджені Адміністрацією Держспецзв'язку для використання в банківській системі України за відповідним зверненням та обґрунтуванням Національного банку України.

Методики генерації випадкових (псевдовипадкових) послідовностей для управління ключами повинні бути погоджені з Адміністрацією Держспецзв'язку.

2.14. Засоби КЗІ розробляються з урахуванням можливих загроз у вірогідних умовах їх експлуатації.

2.15. У засобах КЗІ повинні бути реалізовані методи захисту, що відповідають установленим вимогам, залежно від виду, типу, категорії, класу засобу КЗІ.

Зокрема в засобах КЗІ видів А та Б категорій "Ш" та "П" повинні бути реалізовані:

для класу В3 - механізми контролю цілісності криптографічних перетворень та захисту ключових даних (для програмних засобів КЗІ - контролю цілісності програмного забезпечення), надійного тестування засобу на правильність функціонування та блокування його роботи в разі виявлення порушень; механізми гарантованого знищення (неможливості відновлення будь-яким способом) ключових даних після закінчення терміну їх дії;

для класу В2 - механізми захисту від порушення конфіденційності інформації внаслідок помилкових дій оператора або в разі відхилень у роботі складових елементів засобу КЗІ;

для класу В1 - механізми розподілу повноважень щодо використання функцій засобу КЗІ;

для класу Б2 - механізми захисту засобу КЗІ від здійснення порушником навмисного зовнішнього впливу; механізми захисту від порушення конфіденційності та цілісності ключових даних на ключових документах;

для класу Б1 - механізми захисту критичної інформації (ключових даних, відкритої інформації) від недокументованих можливостей прикладного програмного забезпечення;

для класу А1 - механізми гарантованого знищення ключових даних після закінчення терміну їх дії або в разі несанкціонованого доступу до криптографічної схеми (або за командою оператора); механізми захисту ключових даних на їх носіях від несанкціонованого зчитування.

Вимоги до засобів КЗІ наведено в порядку збільшення вимог таким чином, що клас, наведений нижче, передбачає виконання вимог усіх наведених вище класів засобів КЗІ.

Вимоги для засобів КЗІ категорії "К" визначаються з урахуванням їх призначення, умов розташування та експлуатації.

Вимоги для засобів КЗІ категорії "Р" визначаються з урахуванням вимог нормативних документів системи технічного захисту інформації.

За потреби, можуть визначатися спеціальні вимоги щодо захисту засобів КЗІ будь-якого класу від витоку інформації каналами ПЕМВН.

2.16. На етапі ескізно-технічного проектування здійснюються опрацювання та практична реалізація функцій захисту згідно з вимогами до засобів КЗІ. При цьому основна увага при проектуванні засобу КЗІ приділяється вузлам, які обробляють критичну інформацію, у тому числі:

- уведення та оброблення ключових даних;
- оброблення вхідної та вихідної інформації;
- шифрування інформації;

- генератори випадкових (псевдовипадкових) послідовностей, які використовуються для формування ключів, векторів ініціалізації тощо;

- самотестування;

- системи сигналізації при несанкціонованому доступі до засобу КЗІ, зміні параметрів навколишнього середовища, електроживлення тощо.

2.17. Розроблення засобів КЗІ здійснюється з використанням тільки ліцензійного програмного забезпечення або, за погодженням із замовником, комп'ютерних програм вільного використання, які повинні бути забезпечені документацією, що підтверджує правомірність їх використання згідно з ліцензією або належність до комп'ютерних програм вільного використання.

2.18. Розробник розробляє робочу конструкторську документацію на засіб КЗІ, до складу якої обов'язково входять проект технічних умов (для апаратних та апаратно-програмних засобів КЗІ), експлуатаційні документи, інструкція із забезпечення безпеки експлуатації засобу КЗІ та інструкція щодо порядку генерації ключових даних і поводження (обліку, зберігання, знищення) з ключовими документами.

2.19. Проект технічних умов (далі - ТУ) погоджується з Держспецзв'язку.

За потреби, розробником у ТУ вноситься перелік допустимих змін, які без погодження з Держспецзв'язку можуть уноситися під час виробництва засобу КЗІ до його конструкції, схемотехнічних рішень, програмного забезпечення та переліку комплектувальних виробів тощо. У цьому разі до проекту ТУ, що подається на погодження, додається пояснювальна записка з обґрунтуванням можливості внесення відповідних змін без впливу на криптографічні та спеціальні якості засобів КЗІ.

У разі визначення в технічному завданні вимог щодо захисту засобу КЗІ від витоку інформації каналами ПЕМВН у ТУ наводяться посилання на методику контролю спеціальних показників в умовах серійного виробництва засобів КЗІ, яка має бути узгоджена з організацією, що здійснює сертифікаційні випробування (експертні роботи), та Держспецзв'язку.

2.20. У конструкторській документації на засіб КЗІ обов'язково наводяться:

склад апаратних і програмних (мікропрограмних) компонентів засобу КЗІ та технічних засобів, які передбачаються до спільної роботи із засобами КЗІ, а також вимоги до інтерфейсів;

специфікація розроблення апаратного та загального програмного забезпечення, вузлів засобів КЗІ (документування розроблення рекомендується здійснювати з використанням мов програмування високого рівня для загального програмного забезпечення та вузлів, що програмуються, а також функціональних і принципів електричних схем для апаратної частини);

схеми апаратної та програмної компоненти засобу КЗІ, їх взаємозв'язок, у тому числі всі мікроконтролери, логічні інтегральні мікросхеми, буферні регістри введення/виведення даних тощо;

технічні характеристики (за необхідності - спеціальні характеристики) інтерфейсів сполучення засобів КЗІ, у тому числі фізичні та логічні порти, зовнішні пристрої введення/виведення інформації, засобів дистанційного керування, зовнішніх засобів механічного захисту (кришки, замки тощо);

криптографічні алгоритми, які реалізовано в засобі КЗІ;

алгоритми тестування та методи ручної перевірки засобу КЗІ, у тому числі індикація (відображення) припустимих і неприпустимих його станів.

2.21. В інструкції із забезпечення безпеки експлуатації засобів КЗІ вказуються: права та обов'язки осіб, відповідальних за забезпечення безпеки експлуатації засобу КЗІ;

права та обов'язки користувачів засобів КЗІ;

порядок забезпечення безпеки засобу КЗІ під час його встановлення, експлуатації, виведення з експлуатації, ремонту, а також у разі порушення функціонування інформаційно-телекомунікаційної системи;

питання проведення тестування засобів КЗІ та їх резервування в системі;

дії персоналу в умовах надзвичайних ситуацій, стихійного лиха та підозри компрометації ключів;

порядок проведення контролю за станом забезпечення безпеки засобів КЗІ;

порядок допуску в приміщення, у яких установлені засоби КЗІ.

2.22. У ході виконання ДКР розробником передбачається створення устаткування (допоміжного обладнання) для проведення сертифікаційних випробувань (експертних робіт) засобу КЗІ. Перелік допоміжного обладнання, засобів вимірювальної техніки та кількість дослідних зразків засобу КЗІ, необхідних для проведення таких робіт, визначаються розробником і погоджуються із замовником, випробувальною лабораторією (експертним закладом).

2.23. Технічні та експлуатаційні характеристики дослідних зразків засобу КЗІ, який розробляється у ході виконання ДКР, ефективність та достатність організаційно-технічних заходів щодо забезпечення безпеки інформації перевіряються під час випробувань засобів КЗІ на дослідній ділянці розробника.

За погодженням із замовником випробування дослідних зразків засобу КЗІ можуть здійснюватися у складі інформаційно-телекомунікаційної системи, експлуатацію якої здійснює замовник або послугами якої він користується.

У ході дослідної експлуатації обробку та передавання конфіденційної інформації (для засобів категорій "Ш", "К" та "Р") та (або) реальний інформаційний обмін (для засобів категорії "П") здійснювати не рекомендується.

2.24. Висновки із затвердженого замовником звіту за результатами випробувань дослідних зразків засобу КЗІ надсилаються до Держспецзв'язку.

2.25. За результатами випробувань дослідних зразків засобу КЗІ інструкція із забезпечення безпеки експлуатації засобу КЗІ та інструкція щодо порядку генерації ключових даних і поводження з ключовими документами, за необхідності, доопрацьовуються розробником.

Інструкція із забезпечення безпеки експлуатації засобу КЗІ погоджується із замовником та подається на погодження до Держспецзв'язку на етапі проведення державної експертизи у сфері КЗІ.

Після погодження інструкції із забезпечення безпеки експлуатації засобу КЗІ Держспецзв'язку вона затверджується замовником.

2.26. Якщо ключові документи до засобів КЗІ надаються Держспецзв'язку, то інструкція щодо порядку генерації ключових даних та поводження з ключовими документами надається Держспецзв'язку разом з інструкцією із забезпечення безпеки експлуатації засобу КЗІ.

2.27. Інструкції із забезпечення безпеки експлуатації та щодо порядку генерації ключових даних і поводження з ключовими документами для засобів КЗІ виду В можуть не розроблятися.

Порядок роботи із засобами цього виду та вимоги щодо забезпечення безпеки інформації під час їх використання вказуються відповідно в окремих розділах зазначених інструкцій для засобів КЗІ видів А та Б.

2.28. Порядок забезпечення режиму безпеки під час розроблення засобів КЗІ визначається розробником в окремій інструкції, в якій наводяться вимоги щодо поводження із засобами КЗІ, обладнання приміщень, заходи з запобігання компрометації засобів КЗІ тощо.

3. Виробництво засобів КЗІ

3.1. Виробництво засобів КЗІ здійснюється тільки за наявності сертифіката відповідності (позитивного експертного висновку) на засіб, ТУ та інструкції із забезпечення безпеки експлуатації засобів КЗІ.

3.2. Виробники засобів КЗІ повинні:

ужити заходів щодо своєчасної сертифікації або експертизи засобів КЗІ (у тому числі повторної - після закінчення строку дії раніше отриманого сертифіката відповідності або експертного висновку);

погодити зміни, які вносяться у виробу та документацію на них, із замовником та Держспецзв'язку;

забезпечити виконання усіх вимог ТУ;

за наявності вимог у ТУ з усієї партії виробів, що виготовляється, вибрати контрольний еталонний зразок та зберігати його відповідно до встановлених вимог;

забезпечити технічне обслуговування та гарантійний ремонт засобів КЗІ, а також випуск і поставку запасних частин для цих засобів відповідно до Закону України "Про захист прав споживачів" ([1023-12](#)).

3.3. Виробництво засобів КЗІ здійснюється з використанням програмного забезпечення, що відповідає вимогам пункту 2.17 цього Положення.

4. Експлуатація засобів КЗІ

4.1. Для криптографічного захисту інформації використовуються засоби КЗІ, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації.

Сертифікація засобів КЗІ та державна експертиза у сфері криптографічного захисту інформації проводяться в порядку, визначеному іншими нормативно-правовими актами.

4.2. Підставою для початку експлуатації засобів КЗІ в організації (у тому числі її філіях або регіональних представництвах), яка здійснює експлуатацію засобів КЗІ, є відповідний наказ керівника цієї організації.

4.3. З початку експлуатації кожний екземпляр засобу КЗІ береться на облік в організації, яка експлуатує засоби КЗІ.

Одиницею обліку кожного екземпляра засобу КЗІ є:

для апаратних та апаратно-програмних засобів - конструктивно закінчений технічний засіб;

для програмних засобів - інсталяційна дискета, компакт-диск (CDROM) тощо.

4.4. Передача засобів КЗІ здійснюється на підставі відповідних договорів, у яких вказуються порядок установа засобів КЗІ в користувачів та обслуговування цих засобів, забезпечення ключовими документами (ключовими даними), а також ужиття заходів щодо забезпечення режиму безпеки тощо.

4.5. Експлуатація засобів КЗІ здійснюється відповідно до вимог експлуатаційної документації, інструкції із забезпечення безпеки експлуатації засобів КЗІ, а також інструкції щодо порядку генерації ключових даних та поводження з ключовими документами.

4.6. Унесення змін до інструкції щодо порядку генерації ключових даних та поводження з ключовими документами, які отримані від Держспецзв'язку, здійснюється за погодженням з Держспецзв'язку.

4.7. Постачання ключових документів (ключових даних) від Держспецзв'язку організаціям, які експлуатують засоби КЗІ, здійснюється у порядку, установленому Адміністрацією Держспецзв'язку.

4.8. Ключові документи, що постачаються Держспецзв'язку, не можуть тиражуватися або використовуватися для інших засобів КЗІ, якщо це не передбачено договором про постачання ключових документів.

4.9. Користувачі засобів КЗІ повинні бути ознайомлені з інструкцією щодо порядку генерації ключових даних та поводження з ключовими документами в частині, що їх стосується, та дотримуватися вимог цієї інструкції.

У повному обсязі з інструкцією щодо порядку генерації ключових даних та поводження з ключовими документами повинно бути ознайомлено обмежене коло осіб, які мають безпосереднє відношення до проведення відповідних робіт.

4.10. Засоби КЗІ без уведених ключових даних мають гриф обмеження доступу, який відповідає грифу обмеження доступу опису криптосхеми. Гриф обмеження доступу засобів КЗІ з уведеними ключовими даними визначається грифом обмеження доступу ключових документів, але не нижче грифу обмеження доступу опису криптосхеми.

4.11. Гриф обмеження доступу ключових документів, що використовуються для криптографічного захисту інформації, повинен відповідати грифу обмеження доступу інформації, що захищається.

4.12. Застосування засобів КЗІ під час міжнародного обміну інформацією здійснюється відповідно до законодавства та міжнародних угод (договорів) України.

**Начальник Департаменту
стратегії розвитку спеціальних
інформаційно-телекомунікаційних
систем Адміністрації
Держспецзв'язку**

О.А.Муригін