НОРМАТИВНИЙ ДОКУМЕНТ
СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-комунікаційній системі

НД ТЗІ 3.7-003-2023

Адміністрація Державної служби спеціального зв'язку та захисту інформації України

Київ 2023

НОРМАТИВНИЙ ДОКУМЕНТ
СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

ЗАТВЕРДЖЕНО

Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України

____ _____ 2023 року № _____

Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-комунікаційній системі

НД ТЗІ 3.7-003-2023

Адміністрація Державної служби спеціального зв'язку та захисту України

Київ

ПЕРЕДМОВА

1. РОЗРОБЛЕНО і ВНЕСЕНО Департаментом захисту інформації Адміністрації Державної служби спеціального зв'язку та захисту України.
2. УВЕДЕНО НА ЗАМІНУ НД ТЗІ 3.7-003-2005.

Зміст

НД ТЗІ 3.7-003-23

Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-комунікаційній системі

1. Галузь використання

Цей документ визначає основи організації та порядок виконання робіт із захисту інформації в інформаційно-комунікаційних системах (далі – ІКС) – порядок прийняття рішень щодо складу комплексної системи захисту інформації залежно від умов функціонування ІКС і видів оброблюваної інформації, визначення обсягу і змісту робіт, етапності робіт, основних завдань та порядку виконання робіт кожного етапу.

Дія цього нормативного документа системи технічного захисту інформації (далі – НД ТЗІ) поширюється тільки на ІКС, в яких здійснюється обробка інформації автоматизованим способом. Отже, для таких ІКС чинні всі нормативно-правові акти та нормативні документи щодо створення автоматизованих систем (далі – АС) та щодо захисту інформації в АС. НД ТЗІ не встановлює нових норм, а систематизує в одному документі вимоги, норми і правила, які безпосередньо або непрямим чином випливають з положень чинних нормативних документів.

Цей НД ТЗІ побудовано у вигляді керівництва, яке містить перелік робіт і посилання на чинні нормативні документи, відповідно до яких ці роботи необхідно виконувати. Якщо якийсь з етапів чи видів робіт не нормовано, наводиться короткий зміст робіт та якими результатами вони повинні закінчуватися.

НД ТЗІ призначено для суб'єктів інформаційних відносин (власників або розпорядників ІКС, користувачів), діяльність яких пов'язана з обробкою інформації, що підлягає захисту, розробників комплексних систем захисту інформації в ІКС, для постачальників компонентів ІКС, а також для фізичних та юридичних осіб, які здійснюють оцінку захищеності оброблюваної інформації щодо відповідності вимогам технічного захисту інформації (далі – ТЗІ).

Встановлений цим НД ТЗІ порядок є обов'язковим для всіх суб'єктів системи ТЗІ в Україні незалежно від їхньої організаційно-правової форми та форми власності, в ІКС яких обробляється інформація, яка є власністю держави, належить до державної чи іншої таємниці або окремих видів інформації, необхідність захисту якої визначено законодавством. Якщо в ІКС обробляються інші види інформації, то вимоги цього нормативного документа суб'єкти системи ТЗІ можуть використовувати як рекомендації.

2. Нормативні посилання

У цьому НД ТЗІ наведено посилання на такі нормативні документи:

ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення;

ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт;

ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення;

ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення;

ДБН 2.2-3-2012 Склад, порядок розроблення, погодження та затвердження проектної документації для будівництва;

РД 50-34.698-90 Автоматизовані системи. Вимоги до змісту документів;

НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 28.04.1999 № 22;

НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 28.04.1999 № 22;

НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі, затверджений наказом ДСТСЗІ СБ України від 04.12.2000 № 53;

НД ТЗІ 1.6-003-2004 Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації, затверджений наказом ДСТСЗІ СБ України від 10.03.2004 № 04;

НД ТЗІ 2.3-025-21 Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, затверджений наказом Адміністрації Держспецзв'язку від 01.02.2022 року № 53;

НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 28.04.1999 № 22;

НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 28.04.1999 № 22;

НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 20.12.2000 № 60;

НД ТЗІ 3.6-003-2016 Порядок проведення робіт зі створення та атестації комплексів технічного захисту інформації, затверджений наказом Адміністрації Держспецзв'язку від 07.04.2016 № 41дск;

НД ТЗІ 3.6-004-21 Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці, затверджений наказом Адміністрації Держспецзв'язку від 01.02.2022 року № 53;

НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі, затверджений наказом ДСТСЗІ СБ України від 28.04.1999 № 22;

Положення про державну експертизу у сфері технічного захисту інформації, затверджене наказом Адміністрації Держспецзв'язку від 16.05.2007 № 93, зареєстроване в Міністерстві юстиції України 16.07.2007 за № 820/14087;

Порядок оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації, затверджений наказом Адміністрації Держспецзв'язку від 26.03.2007 № 45, зареєстрований в Міністерстві юстиції України 10.04.2007 за № 320/13587;

Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб, затверджене наказом ДСТСЗІ СБ України від 23.02.2002 № 9 і зареєстроване в Міністерстві юстиції України 13.03.2002 за № 245/6533;

ISO 7498-2-89 Information proceeding systems. Open Systems Interconnection. Basic Reference Model. Part 2: Security Architecture.

3. Визначення

У цьому НД ТЗІ подано терміни та визначення згідно із ДСТУ 3396.2-97 ДСТУ 2226-93, НД ТЗІ 1.1-003-99.

Інші терміни вживаються в такому значенні:

інформаційна система – організаційно-технічна система, що реалізує технологію обробки інформації за допомогою засобів обчислювальної техніки та програмного забезпечення;

комунікаційна система – організаційно-технічна система, що реалізує технологію інформаційного обміну за допомогою технічних і програмних засобів шляхом передавання та приймання інформації у вигляді сигналів, знаків, звуків, зображень чи іншим чином;

інтегрована система – сукупність двох або кількох взаємопов'язаних інформаційних та (або) комунікаційних систем, в якій функціонування однієї (кількох) з них залежить від результатів функціонування іншої (інших) таким чином, що цю сукупність у процесі взаємодії можна розглядати як єдину систему.

Під інформаційно-комунікаційною системою в цьому НД ТЗІ слід розуміти будь-яка систему, яка відповідає одному з трьох наведених вище видів автоматизованих систем.

4. Позначення та скорочення

У цьому НД використано такі позначення та скорочення:
АС – автоматизована система;
ДСТУ – державний стандарт України;
ДТЗ – допоміжні технічні засоби;
ІКС – інформаційно-телекомунікаційна система;
КЗЗ – комплекс засобів захисту від несанкціонованого доступу;
КС – комп'ютерна система;
КСЗІ – комплексна система захисту інформації;
НД – нормативний документ;
НД ТЗІ – нормативний документ системи технічного захисту інформації;
НДР – науково-дослідна робота;
НСД – несанкціонований доступ;
ОТЗ – основні технічні засоби;
ПЕМВН – побічні електромагнітні випромінювання та наведення;
СЗІ – служба захисту інформації;
ТЗ – технічне завдання.

5. Загальні положення

5.1. Цей НД ТЗІ встановлює вимоги в частині організації робіт із захисту інформації та порядку створення КСЗІ в ІКС, а також розвиває основні положення ДСТУ 3396.0-96, ДСТУ 3396.1-96, НД ТЗІ 1.1-002-99, інших НД із захисту інформації.

5.2. Порядок створення КСЗІ в ІКС є єдиним незалежно від того, створюється КСЗІ в ІКС, яка проєктується, чи в діючій ІКС, якщо виникла необхідність забезпечення захисту інформації або модернізації вже створеної КСЗІ.

5.3. Процес створення КСЗІ полягає у виконанні комплексу взаємоузгоджених заходів, спрямованих на розроблення і впровадження інформаційної технології, яка забезпечує обробку інформації в ІКС згідно з вимогами, встановленими нормативно-правовими актами та НД у сфері захисту інформації.

5.4. Порядок створення КСЗІ в ІКС розглядається цим НД як сукупність впорядкованих у часі, взаємопов'язаних, об'єднаних в окремі етапи робіт, виконання яких необхідне й достатнє для КСЗІ, що створюється.

Послідовність виконання та типовий зміст робіт кожного з етапів створення КСЗІ повинні узгоджуватися з відповідними стадіями і етапами робіт зі створення ІКС, викладеними у розділі 6 цього НД.

Етапи робіт, які виконуються під час створення КСЗІ в конкретній ІКС, їх зміст та результати, терміни виконання визначаються ТЗ на створення КСЗІ на підставі цього НД.

Дозволяється виключати окремі етапи робіт або поєднувати декілька етапів, а також вводити нові етапи робіт. У разі потреби дозволяється змінювати послідовність виконання окремих етапів – виконувати одночасно декілька етапів робіт, окремі етапи виконувати до завершення попередніх тощо, якщо це не призводить до зниження якості робіт і не суперечить цілям їх виконання. При цьому зміст етапів має передбачати виконання всіх основних робіт, встановлених ДСТУ 3396.1-96 – визначення й оцінка загроз для інформації, формування вимог, розроблення й реалізація проєкту КСЗІ, проведення випробувань КСЗІ та введення її в експлуатацію в складі ІКС.

Якщо у галузі впроваджені в установленому порядку і діють НД ТЗІ відомчого рівня або існують відповідні нормативні документи, чинність яких поширюється на організацію-власника ІКС або саму ІКС, то вони мають вищу силу і в першу чергу необхідно керуватися ними.

Якщо певний вид робіт не нормовано національною нормативною базою з ТЗІ будь-якого з наведених рівнів, то допускається використання рекомендацій міжнародних стандартів в частині, що не суперечить нормативно-правовим актам та нормативним документам України.

5.5. До складу КСЗІ входять заходи та засоби, які реалізують способи, методи, механізми захисту інформації від:

- витоку технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, акустоелектричні та інші канали;
- несанкціонованих дій та несанкціонованого доступу до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм, використання комп'ютерних вірусів та інше;
- спеціального впливу на інформацію, який може здійснюватися шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту.

Для кожної конкретної ІКС склад, структура та вимоги до КСЗІ визначаються властивостями оброблюваної інформації, класом автоматизованої системи та умовами експлуатації ІКС.

5.6. У випадках, визначених законодавством, роботи з проєктування, розроблення, виготовлення, випробування, експлуатації ІКС мають виконуватися у комплексі із заходами щодо забезпечення режиму секретності, протидії технічним розвідкам, а також з режимними заходами щодо охорони інформації з обмеженим доступом, яка не є державною таємницею.

5.7. Створення комплексів технічного захисту інформації від витоку технічними каналами здійснюється, якщо в ІКС обробляється інформація, що становить державну таємницю, або коли необхідність цього визначено власником інформації.

Створення КЗЗ здійснюється в усіх ІКС, де обробляється інформація, що є власністю держави, належить до державної чи іншої таємниці або до окремих видів інформації, необхідність захисту якої визначено законодавством, а також в ІКС, де така необхідність визначена власником інформації.

Рішення щодо необхідності вжиття заходів захисту від спеціальних впливів на інформацію приймається власником інформації в кожному випадку окремо.

5.8. Роботи зі створення КСЗІ виконуються організацією-власником (розпорядником) ІКС з дотриманням вимог нормативно-правових актів щодо провадження діяльності у сфері захисту інформації.

Якщо для створення КСЗІ необхідно виконувати декілька різних видів робіт, які підлягають ліцензуванню в межах господарської діяльності (отримання дозволу) з ТЗІ, то розробник КСЗІ повинен мати право на провадження хоча б одного з таких видів робіт. До виконання робіт, на провадження яких розробник КСЗІ не має ліцензії (дозволу), залучаються співвиконавці, які мають відповідні ліцензії.

5.9. Для організації робіт зі створення КСЗІ в ІКС створюється служба захисту інформації, порядок створення, завдання, функції, структура та повноваження якої визначено в НД 1.4-001-2000.

СЗІ створюється після прийняття рішення про необхідність створення КСЗІ (п. 6.1.1). Як виняток, СЗІ може створюватися на більш пізніх етапах робіт, але не пізніше етапу підготовки КСЗІ до введення в дію (п. 6.5).

5.10. Встановлений цим НД порядок створення КСЗІ поширюється і на складові частини (або їх сукупність) КСЗІ інтегрованих ІКС.

Інтегрована ІКС за своїм складом та структурою, функціональними завданнями, можливими суттєвими відмінностями середовищ функціонування кожної складової ІКС та іншим може бути неоднорідною системою. Для кожної окремої системи у складі такої ІКС існують тільки їй властиві критичні інформаційні ресурси, програмно-апаратні засоби обробки даних, архітектура обчислювальної системи, характеристики середовища користувачів та технології обробки інформації, канали обміну інформацією, перелік конкретних загроз тощо. Отже, вимоги до політики безпеки інформації, вимоги до функціонального профілю захищеності інформації, вимоги до реалізації послуг безпеки тощо в різних складових ІКС на різних об’єктах, де будуть розгортатися її компоненти, мають бути різними.

У цьому випадку КСЗІ інтегрованої ІКС рекомендується будувати за модульним принципом (коли кожна достатньо незалежна складова частина ІКС

має свій власний модуль КСЗІ, а КСЗІ інтегрованої ІКС є сукупністю всіх модулів, взаємодія яких забезпечується окремою підсистемою взаємодії та обміну інформації, яка є єдиною для всієї КСЗІ ІКС). Вибір заходів і механізмів захисту кожного модуля здійснюється відповідно до політики безпеки інформації в ІКС і концепції побудови КСЗІ ІКС, чим забезпечується їх узгодження між собою.

Такий підхід має на меті забезпечити:

- реалізацію відкритої архітектури безпеки, зміст концепції якої надано в ISO 7498-2-89 Information proceeding systems. Open Systems Interconnection. Basic Reference Model. Part 2: Security Architecture;
- можливість незалежної розробки, впровадження, проведення випробувань, експлуатації окремо кожної складової частини КСЗІ;
- уніфікацію і здешевлення проєктування КСЗІ. Ця процедура зводиться до проєктування певної кількості типових компонентів, кожен з яких має тільки свої власні дані (для формування бази даних захисту), а не механізми захисту;
- можливість оцінювання кожної складової частини КСЗІ окремо (для будь-якого виду випробувань).

Рішення щодо доцільності застосування цього порядку окремо для кожної частини КСЗІ приймається власником (розпорядником) ІКС.

Якщо інтегрована ІКС має багатьох власників, право кожного з яких поширюється на певну частину ІКС, власник складової частини ІКС у питаннях створення КСЗІ самостійно діє відповідно до цього НД ТЗІ.

5.11. Порядок розроблення, впровадження, використання у складі КСЗІ засобів і систем криптографічного захисту інформації регламентується нормативно-правовими актами і НД з криптографічного захисту інформації і в цьому документі не розглядається.

6. Етапи створення КСЗІ

6.1. Формування загальних вимог до КСЗІ в ІКС

6.1.1. Обґрунтування необхідності створення КСЗІ

Підставою для визначення необхідності створення КСЗІ є норми та вимоги чинного законодавства, які встановлюють обов'язковість обмеження доступу до певних видів інформації або забезпечення її цілісності чи доступності, або прийняте власником інформації рішення щодо цього, якщо нормативно-правові акти надають йому право діяти на власний розсуд.

Вихідні дані для обґрунтування необхідності створення КСЗІ у загальному випадку одержуються за результатами:

- аналізу нормативно-правових актів (державних, відомчих та таких, що діють у межах установи, організації, підприємства), на підставі яких може встановлюватися обмеження доступу до певних видів інформації чи заборона такого обмеження або визначатися необхідність забезпечення захисту інформації згідно з іншими критеріями;

- визначення наявності у складі інформації, яка підлягає автоматизованій обробці, таких її видів, що потребують обмеження доступу до неї або забезпечення цілісності чи доступності відповідно до вимог нормативно-правових актів;

- оцінки можливих переваг (фінансово-економічних, соціальних тощо) експлуатації ІКС у разі створення КСЗІ.

На підставі проведеного аналізу приймається рішення про необхідність створення КСЗІ.

6.1.2. Обстеження середовищ функціонування ІКС

Під час виконання цих робіт ІКС розглядається як організаційно-технічна система, яка поєднує обчислювальну систему, фізичне середовище, середовище користувачів, оброблювану інформацію і технологію її обробки (далі – середовища функціонування ІКС).

Метою обстеження є підготовка засадничих даних для формування вимог до КСЗІ у вигляді опису кожного середовища функціонування ІКС та виявлення в ньому елементів, які безпосередньо чи опосередковано можуть впливати на безпеку інформації, виявлення взаємного впливу елементів різних середовищ, документування результатів обстеження для використання на наступних етапах робіт.

Слід враховувати, що середовища функціонування є множинами, що перетинаються, окремі їхні елементи можуть входити одночасно до різних середовищ і мати в них різні якості. Наприклад, програмне забезпечення може розглядатися обчислювальною системою як об’єкт-процес, а в інформаційному середовищі – як пасивний об’єкт КС.

Обстеження виконується, коли розроблена концепція ІКС (основні принципи і підходи побудови), визначені основні завдання і характеристики ІКС, функціональних комплексів ІКС та існує варіант(и) їх реалізації.

При обстеженні обчислювальної системи ІКС повинні бути проаналізовані й описані:

- загальна структурна схема і склад (перелік і склад обладнання, технічних і програмних засобів, їхні зв’язки, особливості конфігурації, архітектури й топології, програмні і програмно-апаратні засоби захисту інформації, взаємне розміщення засобів тощо);

- види і характеристики каналів зв’язку;

- особливості взаємодії окремих компонентів, їх взаємний вплив один на одного;

- можливі обмеження щодо використання засобів тощо.

Мають бути виявлені компоненти обчислювальної системи, які містять і які не містять засобів і механізмів захисту інформації, потенційних можливостей цих засобів і механізмів, їхніх властивостей і характеристик, у тому числі тих, що встановлюються за умовчанням, тощо.

Метою такого аналізу є надання загального уявлення про наявність потенційних можливостей щодо забезпечення захисту інформації, виявлення

компонентів ІКС, які вимагають підвищених вимог до захисту інформації і впровадження додаткових заходів захисту.

При обстеженні інформаційного середовища аналізу підлягає вся інформація, що обробляється, а також зберігається в ІКС (дані і програмне забезпечення). Під час аналізу інформація повинна бути класифікована за режимом доступу, за правовим режимом, визначені й описані види (в термінах об'єктів КС) її подання в ІКС.

Для кожного виду інформації і типу об'єкта, в якому вона міститься, приводяться у відповідність властивості захищеності інформації (конфіденційність, цілісність, доступність) чи КС (спостережність), яким вони повинні відповідати.

Аналіз технології обробки інформації повинен виявити особливості обігу електронних документів, мають бути визначені й описані інформаційні потоки і середовища, через які вони передаються, джерела утворення потоків та місця їх призначення, принципи та методи керування інформаційними потоками, складені структурні схеми потоків. Фіксуються види носіїв інформації та порядок їх використання під час функціонування ІКС.

Для кожного структурного елемента схеми інформаційних потоків фіксуються склад інформаційних об'єктів, режим доступу до них, можливий вплив на нього (елемента) елементів середовища користувачів, фізичного середовища з точки зору збереження властивостей інформації.

При обстеженні фізичного середовища проводиться аналіз взаємного розміщення засобів обробки інформації ІКС на об'єктах інформаційної діяльності, комунікацій, систем життєзабезпечення і зв'язку, а також визначається режим функціонування цих об'єктів.

Порядок проведення обстеження повинен відповідати ДСТУ 3396.1-96.

Аналізу підлягають такі характеристики фізичного середовища:

- територіальне розміщення компонентів ІКС (генеральний план, ситуаційний план);
- наявність охорони території та перепускний режим;
- наявність категорійованих приміщень, у яких мають розміщуватися компоненти ІКС;
- режим доступу до компонентів фізичного середовища ІКС;
- вплив чинників навколишнього середовища, захищеність від засобів технічної розвідки;
- наявність елементів комунікацій, систем життєзабезпечення і зв'язку, що мають вихід за межі контрольованої зони;
- наявність і технічні характеристики систем заземлення;
- умови зберігання магнітних, оптико-магнітних, паперових та інших носіїв інформації;
- наявність проєктної та експлуатаційної документації на компоненти фізичного середовища.

При обстеженні середовища користувачів проводиться аналіз:

- функціонального та кількісного складу користувачів, їхніх функціональних обов'язків та рівня кваліфікації;

- повноважень користувачів щодо допуску до відомостей, які обробляються в ІКС, доступу до ІКС та її окремих компонентів;

- повноважень користувачів щодо управління КСЗІ;

- рівня можливостей різних категорій користувачів, що надаються (можуть бути доступними) їм засобами ІКС;

- наявності СЗІ в ІКС.

Результати обстеження середовищ функціонування ІКС оформлюються у вигляді акта і вносяться у разі потреби до відповідних розділів плану захисту інформації в ІКС (далі – План захисту), який розробляється згідно з НД ТЗІ 1.4-001-2000.

За результатами обстеження середовищ функціонування ІКС затверджується перелік об'єктів захисту, а також визначаються потенційні загрози для інформації і розробляються модель загроз і модель порушника. Моделі загроз будуються відповідно до положень НД ТЗІ 1.1-002-99 та НД ТЗІ 1.4-001-2000. Модель загроз для інформації та модель порушника рекомендується оформляти у вигляді окремих документів (або поєднаних в один документ) Плану захисту.

6.1.3. Формування завдання на створення КСЗІ

На цьому етапі:

- визначаються завдання захисту інформації в ІКС, мета створення КСЗІ, варіант вирішення завдань захисту (відповідно до ДСТУ 3396.1-96), основні напрями забезпечення захисту (відповідно до п. 5.8);

- проводиться аналіз ризиків (вивчення моделі загроз і моделі порушника, можливих наслідків від реалізації потенційних загроз, величини можливих збитків тощо) і визначається перелік суттєвих загроз;

- визначаються загальна структура та склад КСЗІ, вимоги до можливих заходів, методів та засобів захисту інформації, допустимі обмеження щодо застосування певних заходів і засобів захисту (наприклад, обмеження щодо використання засобів активного захисту від витоку інформації каналами ПЕМВН за рахунок використання засобів ЕОТ в захищеному виконанні тощо), інші обмеження щодо середовищ функціонування ІКС, обмеження щодо використання ресурсів ІКС для реалізації завдань захисту, припустимі витрати на створення КСЗІ, умови створення, введення в дію і функціонування КСЗІ (окремих її підсистем, компонентів), загальні вимоги до співвідношення та меж застосування в ІКС (окремих її підсистемах, компонентах) організаційних, інженерно-технічних, технічних, криптографічних та інших заходів захисту інформації, що ввійдуть до складу КСЗІ.

Оформлюється звіт про виконання робіт цієї стадії та оформлення заявки на розробку КСЗІ (тактико-технічного завдання на створення КСЗІ або іншого документа аналогічного змісту, що його замінює).

6.2. Розробка політики безпеки інформації в ІКС

6.2.1. Вивчення об'єкта, на якому створюється КСЗІ, проведення науково-дослідних робіт

На цьому етапі розробник КСЗІ проводить детальне вивчення об'єкта, на якому створюється КСЗІ, уточнює моделі загроз, потенційного порушника та результати аналізу можливості керування ризиками, які виконані на попередніх етапах, а також виконує у разі потреби додаткові науково-дослідні роботи, пов'язані з пошуком шляхів реалізації завдання на створення КСЗІ, оформлює і затверджує звіти з НДР, що виконувалися.

6.2.2. Вибір варіанта КСЗІ

У загальному випадку за результатами робіт попереднього етапу готуються альтернативні варіанти концепції створення КСЗІ і планів їх реалізації, проводиться оцінка переваг і недоліків кожного варіанта, вибір найбільш оптимального варіанта. Концепція оформлюється у вигляді звіта.

6.2.3. Оформлення політики безпеки

На цьому етапі проводиться:

- вибір основних рішень з протидії всім суттєвим загрозам, формування загальних вимог, правил, обмежень, рекомендацій тощо, які регламентують використання захищених технологій обробки інформації в ІКС, окремих заходів і засобів захисту інформації, діяльність користувачів усіх категорій;
- документальне оформлення політики безпеки інформації.

Політика безпеки може розроблятися для ІКС в цілому або якщо мають місце особливості функціонування окремих компонентів КСЗІ, для окремої компоненти, для окремого функціонального завдання, для окремої технології обробки інформації тощо.

Політика безпеки розробляється згідно з положеннями НД ТЗІ 1.1-002-99 та рекомендаціями НД ТЗІ 1.4-001-2000. Політику безпеки рекомендується оформляти у вигляді окремого документа Плану захисту.

Положення політики безпеки, пов'язані з рішеннями, що приймаються на наступних етапах робіт (стосовно проєктних рішень, організації робіт, встановлення відповідальності, порядку впровадження і експлуатації КСЗІ та інше), вносяться до документа після прийняття цих рішень на відповідних етапах. Як виняток, виконання робіт, передбачених пп. 6.1.2, 6.1.3, 6.2, може включатися до вимог технічного завдання на створення КСЗІ, а самі роботи можуть виконуватися відповідно до етапів, визначених у ТЗ.

6.3. Розробка технічного завдання на створення КСЗІ

6.3.1. ТЗ на створення КСЗІ в ІКС є засадним організаційно-технічним документом, який визначає вимоги із захисту оброблюваної в ІКС інформації, порядок створення КСЗІ, порядок проведення всіх видів випробувань КСЗІ та введення її в експлуатацію в складі ІКС.

6.3.2. ТЗ на створення КСЗІ розробляється на відповідній стадії робіт зі створення ІКС з урахуванням комплексного підходу до побудови КСЗІ, який передбачає об'єднання в єдину систему усіх необхідних заходів і засобів захисту від різноманітних загроз безпеці інформації на всіх етапах життєвого циклу ІКС.

ТЗ на створення КСЗІ може розроблятися для вперше створюваних ІКС, а також під час модернізації вже існуючих ІКС.

6.3.3. Для оформлення ТЗ на КСЗІ можуть бути використані такі варіанти:
- у вигляді окремого розділу ТЗ на створення ІКС;
- у вигляді окремого (часткового) ТЗ;
- у вигляді доповнення до ТЗ на створення ІКС.

Обмежень щодо вибору варіанта не встановлюється.

6.3.4. Перший варіант рекомендується застосовувати для вперше створюваних ІКС. Другий або третій варіанти рекомендується застосовувати у випадку модернізації КСЗІ, модернізації діючих ІКС, а також для ІКС, які вже мають затверджене ТЗ на створення, в якому не міститься окремого розділу із захисту інформації.

6.3.5. Для інтегрованих ІКС, які будуються за модульним принципом (п. 5.11), вимоги до КСЗІ кожної зі складових частин ІКС рекомендується оформляти окремим документом. Дозволяється готувати один документ (доповнення до ТЗ на створення ІКС, окреме ТЗ) на декілька однотипних складових частин КСЗІ, вказавши існуючі між ними відмінності чи особливості.

Як однотипні складові частини КСЗІ ІКС можуть розглядатися частини КСЗІ, які забезпечують функціонування вузлів комутації однієї й тієї самої мережі передачі даних, КСЗІ локальних обчислювальних мереж з однаковими функціональними завданнями інтегрованої ІКС тощо, якщо умови їх функціонування не мають суттєвих відмінностей.

При цьому до ТЗ включаються вимоги, які є загальними для окремих складових ІКС та для ІКС в цілому, а також вимоги до забезпечення безпечної взаємодії цих складових частин.

6.3.6. Єдиним обмеженням при розробці окремого ТЗ на створення КСЗІ або доповнення до ТЗ на створення ІКС є дотримання в них єдиної системи понять, позначень, ідентифікації об'єктів тощо, які застосовуються в ТЗ на створення ІКС.

6.3.7. Для будь-якого з наведених варіантів розроблення та оформлення ТЗ на КСЗІ його зміст, порядок погодження та затвердження повинні відповідати НД ТЗІ 3.7-001-99.

6.4. Розробка проєкту КСЗІ

6.4.1. Порядок розробки проєкту КСЗІ

Проєкт КСЗІ розробляється на підставі та відповідно до ТЗ на створення ІКС (доповнення до нього, окремого ТЗ на створення КСЗІ).

Під час розробки проєкту КСЗІ обґрунтовуються і приймаються проєктні рішення, які дають змогу реалізувати вимоги ТЗ, забезпечити сумісність і взаємодію різних компонентів КСЗІ, а також різних заходів і способів захисту інформації.

Проєкт КСЗІ виконується на таких стадіях створення ІКС: ескізний проєкт, технічний проєкт, робочий проєкт.

Дозволяється вилучати етап ескізний проєкт, а також поєднувати етапи технічного і робочого проєктів в один етап технороботчий проєкт.

Для всіх стадій розробки проєкту КСЗІ склад документації визначається ТЗ на КСЗІ та НД ТЗІ 2.5-004-99. Додатково розробляється документація на програмні та технічні засоби.

6.4.2. Ескізний проєкт КСЗІ

На цьому етапі проводиться розробка попередніх проєктних рішень КСЗІ та у разі потреби її окремих складових частин, а також розроблення, оформлення, узгодження та затвердження документації на КСЗІ. Зміст та стиль документації повинні бути достатніми для повного опису проєктних рішень рівня ескізного проєкту.

Визначаються: функції КСЗІ в цілому та функції її окремих складових частин; склад комплексів технічного захисту інформації від витоку технічними каналами та від спеціальних впливів; склад заходів протидії технічним розвідкам, організаційних, правових та інших заходів захисту; склад КЗЗ; узагальнена структура КСЗІ та схема взаємодії складових частин.

Пропонуються попередні технічні рішення, за допомогою яких передбачається реалізація завдань і функцій КСЗІ.

6.4.3. Технічний проєкт КСЗІ

Розробка проєктних рішень КСЗІ:

- виконується розробка: загальних проєктних рішень, необхідних для реалізації вимог ТЗ на КСЗІ; рішень щодо структури КСЗІ (організаційної структури, структури технічних і програмних засобів), алгоритмів функціонування та умов використання засобів захисту; рішень щодо архітектури КЗЗ та механізмів реалізації, визначених функціональним профілем послуг безпеки інформації;
- проводяться організаційно-технічні заходи щодо забезпечення послідовності розробки КЗЗ, архітектури, середовища розробки, випробувань, середовища функціонування та експлуатаційної документації КЗЗ відповідно до заданих рівнем гарантій реалізації послуг безпеки згідно зі специфікаціями НД ТЗІ 2.5-004-99.

Розробка документації на КСЗІ:

- виконується розроблення, оформлення, узгодження та затвердження документації в обсязі, передбаченому ТЗ на КСЗІ. Зміст і стиль документації повинні бути достатніми для повного опису проєктних рішень рівня технічного проєкту;

- готується та оформляється документація на постачання засобів захисту або продукції, що містить їх у своєму складі, для комплектації КСЗІ. Якщо необхідної продукції немає на ринку засобів захисту, то визначаються технічні вимоги (складаються технічні завдання) на розроблення відповідних засобів;

- здійснюється розроблення, оформлення і затвердження завдань на проєктування і суміжних питань, які пов'язані зі створенням КСЗІ або впливають на умови її функціонування (будівельні, електротехнічні, санітарно-технічні та інші підготовчі роботи).

6.4.4. Робочий проєкт КСЗІ

На цьому етапі здійснюється розроблення, оформлення та затвердження робочої та експлуатаційної документації КСЗІ та у разі потреби її окремих складових частин.

Робоча документація містить детальні рішення щодо реалізації технічного проєкту КСЗІ, щодо забезпечення управління КСЗІ і взаємодії її компонентів, а також документацію, необхідну для тестування, проведення пусконалагоджувальних робіт, проведення випробувань КСЗІ.

Проводиться розробка засобів захисту інформації, передбачених п. 6.4.3, або адаптація готової продукції до умов функціонування КСЗІ. Розробка засобів захисту інформації від НСД проводиться згідно з НД ТЗІ 3.6-001-2000.

До складу робочої документації на КЗЗ повинні входити описи процедур інсталяції та ініціалізації комплексу, налагодження всіх механізмів розмежування доступу користувачів до інформації та апаратних ресурсів ІКС, контролю за діями користувачів, формування та актуалізації баз даних захисту, а також контролю цілісності програмного забезпечення та баз даних захисту.

Документація робочого проєкту повинна містити вихідні дані для внесення їх до баз даних захисту.

Експлуатаційна документація містить опис порядку функціонування КСЗІ та настанови (інструкції) щодо забезпечення цього порядку обслуговуючим персоналом і користувачами, порядку супроводження КСЗІ впродовж життєвого циклу ІКС.

6.5. Введення КСЗІ в дію та оцінка захищеності інформації в ІКС

Про проведення робіт, передбачених п.п. 6.5.3 – 6.5.8 цього етапу, робиться відповідний запис у паспорті (формулярі) ІКС.

6.5.1. Підготовка КСЗІ до введення в дію:

- проводяться роботи з підготовки організаційної структури та розробки розпорядчих документів, що регламентують діяльність із забезпечення захисту інформації в ІКС;

- здійснюється створення СЗІ (призначаються відповідальні особи за захист інформації), якщо цього не було зроблено на попередніх етапах;

- в основному має бути завершена розробка і затверджені документи, що входять до Плану захисту (за виключенням тих, для розробки яких необхідні результати наступних етапів робіт).

Створення СЗІ та розробка Плану захисту здійснюються згідно з НД ТЗІ 1.4-001-2000.

6.5.2. Навчання користувачів

Проводиться навчання користувачів ІКС всіх категорій (технічного обслуговуючого персоналу, звичайних користувачів та користувачів, які мають повноваження щодо управління засобами КСЗІ, тощо) в частині, що їх стосується, основним положенням документів Плану захисту, які необхідні їм для дотримання правил політики безпеки інформації, експлуатації засобів захисту інформації тощо, проводиться перевірка їх уміння користуватися впровадженими технологіями захисту інформації і реєстрація результатів навчання.

6.5.3. Комплектування КСЗІ

Забезпечується отримання продукції (засобів захисту інформації, матеріалів, обладнання та іншого) від постачальників та співвиконавців робіт. Приймається рішення щодо підготовки до проведення оцінки на відповідність вимогам НД ТЗІ засобів захисту, які на момент проєктування КСЗІ не мали відповідного сертифіката або експертного висновку, а також щодо порядку проведення такої оцінки під час державної експертизи КСЗІ.

6.5.4. Будівельно-монтажні роботи

Роботи цього етапу виконуються під час переобладнання існуючих або при будівництві нових спеціалізованих споруд (приміщень), призначених для розміщення технічних засобів ІКС та персоналу, сховищ матеріальних носіїв інформації.

При проведенні будівельно-монтажних робіт враховуються вимоги технічного завдання на створення КСЗІ в ІКС.

Будівельні роботи проводяться силами організації-власника ІКС або будівельно-монтажних організацій згідно з проєктною документацією на будівництво, яка розробляється проєктною організацією відповідно до вимог ДБН 2.2-3-2012.

Після завершення будівельних робіт створюється комісія з прийняття робіт, до складу якої входять представники організації-замовника будівельних робіт, проєктної та будівельно-монтажної організацій. За результатами роботи

комісії складається за довільною формою акт приймання робіт з оцінкою їх відповідності вимогам ТЗІ, який затверджується керівником організації-замовника будівництва.

6.5.5. Пусконалагоджувальні роботи

Метою пусконалагоджувальних робіт є:

- монтаж обладнання і атестація комплексу технічного захисту інформації від витоку технічними каналами;
- встановлення і налагодження КЗЗ;
- перевірка працездатності засобів захисту інформації в автономному режимі та при їх комплексній взаємодії.

Монтаж ОТЗ ІКС, кабельного обладнання, мереж живлення та заземлення здійснюється згідно з конструкторською документацією робочого проєкту.

Якщо до складу КСЗІ входять ОТЗ, які не мають сертифіката або експертного висновку про відповідність вимогам з ТЗІ, визначаються мінімально допустимі відстані між цими засобами та ДТЗ за результатами їх спеціальних досліджень.

У разі неможливості дотримання вимог з розміщення ОТЗ або наявності підстав щодо можливого порушення умов їх постачання оцінка монтажних робіт ОТЗ має бути підтверджена результатами контрольних інструментальних вимірювань рівня ПЕМВН.

Спеціальні дослідження та інструментальні вимірювання рівня ПЕМВН виконуються підрозділом ТЗІ організації-власника ІКС або іншими суб'єктами господарювання за умови наявності ліцензії чи дозволу на проведення відповідного виду робіт.

За результатами робіт складається акт, де зазначаються: категорії приміщень, де розташоване обладнання ІКС, межі контрольованих зон для приміщень, перелік ОТЗ, ДТЗ і комунікацій (із зазначенням найменування, типу, заводського номера), що знаходяться у цих приміщеннях, оцінка відповідності проведення монтажних робіт вимогам експлуатаційних документів на засоби та НД ТЗІ 3.6-003-2016, пропозиції щодо застосування додаткових заходів захисту, впровадження яких є необхідним у разі неможливості під час виконання монтажних робіт дотримання окремих вимог із розміщення ОТЗ. Акт затверджується керівником організації – власника ІКС.

Упроваджуються додаткові заходи захисту, необхідність впровадження яких зафіксована в акті, відповідно до порядку проведення робіт етапу та відповідне коригування проєктної, робочої, експлуатаційної документації.

Оцінка повноти та якості виконання робіт з ТЗІ в приміщеннях проводиться шляхом атестації впровадженого комплексу ТЗІ від витоку технічними каналами, за результатами якої реєструється Акт атестації комплексу технічного захисту інформації.

Проводяться інсталяція, ініціалізація та перевірка працездатності КЗЗ згідно з документацією робочого проєкту.

Інсталяція та ініціалізація КЗЗ, який має експертний висновок про відповідність вимогам НД ТЗІ, здійснюються в порядку, визначеному в експлуатаційній документації на цей комплекс.

Під час інсталяції мають бути задіяні всі механізми розмежування доступу користувачів до інформації та апаратних ресурсів ІКС, контролю за діями користувачів, а також контролю цілісності програмного забезпечення та бази даних захисту КЗЗ.

До бази даних захисту вносяться відомості про користувачів ІКС, встановлюються їх повноваження щодо доступу до захищених об'єктів КС, їх створення, модифікації, архівування, знищення, експорту/імпорту із системи та інші дані.

6.5.6. Попередні випробування

Метою попередніх випробувань є перевірка працездатності КСЗІ та визначення можливості прийняття її у дослідну експлуатацію.

Під час випробувань перевіряються працездатність КСЗІ та відповідність її вимогам ТЗ.

Попередні випробування проводяться згідно з програмою та методиками випробувань. Програму й методики випробувань готує розробник КСЗІ, а узгоджує замовник ІКС. Програма та методики випробувань, протоколи випробувань розробляються та оформлюються згідно з вимогами РД 50-34.698-90.

Попередні випробування організовує замовник ІКС, а проводить розробник КСЗІ спільно із замовником. Для проведення попередніх випробувань замовником ІКС створюється комісія. Головою комісії призначається представник замовника.

Результати попередніх випробувань оформлюються протоколом випробувань, де міститься висновок щодо можливості прийняття КСЗІ у дослідну експлуатацію, а також перелік виявлених недоліків, необхідних заходів з їх усунення, і рекомендовані терміни виконання цих робіт.

Після усунення недоліків у випадку їх наявності та коригування проєктної, робочої, експлуатаційної документації КСЗІ оформлюється акт про приймання КСЗІ у дослідну експлуатацію.

6.5.7. Дослідна експлуатація

Під час дослідної експлуатації КСЗІ:

- відпрацьовуються технології оброблення інформації, обігу машинних носіїв інформації, керування засобами захисту, розмежування доступу користувачів до ресурсів ІКС та автоматизованого контролю за діями користувачів;
- співробітники СЗІ та користувачі ІКС набувають практичних навичок з використання технічних та програмно-апаратних засобів захисту інформації, засвоюють вимоги організаційних та розпорядчих документів з питань розмежування доступу до технічних засобів та інформаційних ресурсів;

- здійснюється (у разі потреби) доопрацювання програмного забезпечення, додаткове налагоджування та конфігурування КЗЗ;

- здійснюється (у разі потреби) коригування робочої та експлуатаційної документації.

За результатами робіт за довільною формою складається акт про завершення дослідної експлуатації, який містить висновок щодо можливості (неможливості) подання КСЗІ на державну експертизу.

6.5.8. Державна експертиза КСЗІ

Державна експертиза КСЗІ є окремим етапом приймальних випробувань ІКС і проводиться з метою визначення відповідності КСЗІ технічному завданню, вимогам НД із захисту інформації та визначення можливості введення КСЗІ в складі ІКС в експлуатацію.

Державна експертиза КСЗІ в ІКС проводиться згідно з Положенням про державну експертизу у сфері технічного захисту інформації, затвердженим наказом Адміністрації Держспецзв'язку від 16.05.2007 № 93, зареєстрованим в Міністерстві юстиції України 16.07.2007 за № 820/14087.

Виявлені під час державної експертизи недоліки усуваються до її завершення, порядок усунення такий самий, як і для попередніх випробувань. Якщо через якісь причини усунути недоліки в ході експертизи неможливо, це оформлюється актом, до якого вноситься перелік необхідних доробок та рекомендації щодо їх виконання. Після завершення передбачених актом робіт проводиться повторна експертиза.

Для інтегрованих ІКС може проводитися державна експертиза кожної складової частини (модуля) КСЗІ окремо.

Державна експертиза КСЗІ інтегрованої ІКС полягає у перевірці взаємодії (адміністрування, обміну даними бази даних захисту тощо) вже оцінених модулів.

Документи, що містять результати робіт кожного з етапів (протоколи, акти, атестати відповідності) для КСЗІ ІКС в цілому, оформлюються з урахуванням відповідних документів на складові частини КСЗІ.

Якщо інтегрована КСЗІ має у своєму складі типові модулі, які створювалися за єдиним ТЗ, то експертиза таких модулів КСЗІ виконується в два етапи: на першому проводиться в повному обсязі експертиза одного обраного типового модуля, а на другому – проводиться перевірка відповідності умов експлуатації типовим на кожному конкретному об'єкті для всіх модулів КСЗІ цього типу.

Введення до складу діючої КСЗІ нового (оціненого) модуля здійснюється без проведення повторної експертизи всієї КСЗІ. Проводиться оцінювання взаємодії нового модуля зі складовими частинами КСЗІ, які вже знаходяться в експлуатації.

Допускається розпочинати і проводити державну експертизу КСЗІ паралельно з роботами етапів проєктування.

У першу чергу такий порядок рекомендується застосовувати для складних з точки зору архітектури, складу та обсягів робіт КСЗІ. При цьому експертами послідовно проводиться оцінка технічних та організаційних рішень на всіх етапах робіт. Це дає змогу оперативно усувати недоліки проєктування та скоротити час проведення державної експертизи, яка може бути в основному завершена до етапу приймальних випробувань ІКС.

Приймальні випробування ІКС проводяться при функціонуючій в її складі КСЗІ. Роботи, вказані в п. 6.5.8, а також пп. 6.5.6, 6.5.7, виконуються з використанням тестових даних, які не містять інформації з обмеженим доступом.

6.6. Супроводження КСЗІ

Виконуються роботи з організаційного забезпечення функціонування КСЗІ та управління засобами захисту інформації відповідно до Плану захисту та експлуатаційної документації на компоненти КСЗІ, гарантійного і післягарантійного технічного обслуговування засобів захисту інформації.

7. Особливості побудови КСЗІ з використанням базових профілів безпеки

Роботи з побудови КСЗІ можуть проводитися з використанням базових профілів безпеки, затверджених Адміністрацією Держспецзв'язку, для відповідного виду інформації, що обробляється в ІКС.

Побудова КСЗІ ІКС з використанням базових профілів проводиться відповідно до НД ТЗІ 3.6-004-21.

Оцінка КСЗІ ІКС, яка побудована з використанням базових профілів безпеки, здійснюється під час проведення державної експертизи відповідно до НД ТЗІ 2.3-025-21.