Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі

НД ТЗІ 3.7-003-05

Затверджено

наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України

“ 08 ” листопада 2005 р. №125

ПЕРЕДМОВА

1 Галузь використання

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

Дія цього НД ТЗІ поширюється тільки на ІТС, в яких здійснюється обробка інформації автоматизованим способом. Відповідно, для таких ІТС чинні всі нормативно-правові акти та нормативні документи щодо створення 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 витікають з положень діючих нормативних документів.

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

НД ТЗІ призначений для суб’єктів інформаційних відносин (власників або розпорядників ІТС, користувачів), діяльність яких пов’язана з обробкою інформації, що підлягає захисту, розробників комплексних систем захисту інформації в ІТС, для постачальників компонентів ІТС, а також для фізичних та юридичних осіб, які здійснюють оцінку захищеності оброблюваної інформації на відповідність вимогам 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 ІТС яких обробляється інформація, яка є власністю держави, належить до державної чи іншої таємниці або окремих видів інформації, необхідність захисту якої визначено

законодавством. Якщо в ІТС 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 А.2.2-2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та проектної документації для будівництва.

ДБН 2.2-3-2004 Склад, порядок розроблення, погодження та затвердження проектної документації для будівництва.

ГОСТ 34.201 - 89 Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем.

ГОСТ 34.601 - 90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания.

ГОСТ 34.602 - 89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.

РД 50 - 34.698 - 90 Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Требования к содержанию документов.

Комплекс стандартов Единая система программной документации (ЕСПД)

Комплекс стандартов Единая система конструкторской документации (ЕСКД)

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

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

НД ТЗІ 1.6-003-2004

НД ТЗІ 2.1-001-2001 Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення. Затверджено наказом ДСТСЗІ СБ України від 09.02.2001 № 2.

НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено 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. Затверджено 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. Затверджено наказом ДСТСЗІ СБ України від 20.12.2000 № 60.

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

НД ТЗІ 2.5-007-2001

НД ТЗІ 2.5-008-2002 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2. Затверджено наказом ДСТСЗІ СБ України від 13.12.2002 № 84.

НД ТЗІ 2.5-010-2003 Вимоги до захисту інформації WEB - сторінки від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 02.04.2003 № 33.

Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ЕОТ-95). Затверджені наказом ДСТЗІ від 09.06.1995 № 25.

СТР-3

СТР-2

СВТР-78

Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ТЗІ-ПЕМВН-95). Затверджені наказом Державної служби України з питань технічного захисту інформації від 09.06.95 № 25.

Положення про державну експертизу в сфері технічного захисту інформації. Затверджене наказом ДСТСЗІ СБ України від 29.12.1999 №62 і зареєстроване в Міністерстві юстиції України 24.01.2000 за №40/4261.

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.

3 Визначення

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

Інші терміни вживаються у такому значенні:

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

телекомунікаційна 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) телекомунікаційних 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-телекомунікаційною системою в цьому НД ТЗІ розуміється будь-яка система, 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

ГОСТ - регіональний (міждержавний) стандарт

ДСТУ - державний стандарт України

ДТЗ - допоміжні технічні засоби

ЕСКД – єдина система конструкторської документації

ЕСПД - єдина система програмної документації

ІТС - 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

ТЗІ - технічний захист інформації

5 Загальні положення

5.1 Цей НД ТЗІ встановлює у доповнення до ГОСТ серії 34 "Информационная технология. Комплекс стандартов на автоматизированные системы" вимоги в частині організації робіт із захисту інформації та порядку створення КСЗІ в ІТС, а також розвиває основні положення ДСТУ 3396.0, ДСТУ 3396.1, НД ТЗІ 1.1-002, інших НД із захисту інформації.

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

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

5.4 Порядок створення КСЗІ в ІТС розглядається цим НД як сукупність впорядкованих у часі, взаємопов'язаних, об'єднаних в окремі етапи робіт, виконання яких необхідне й достатньє 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 ІТС, визначеними ГОСТ 34.601, і викладені у розділі 6 цього НД.

Примітка:

Під час створення КСЗІ в програмно-керованих АТС загального користування можна керуватися, крім цього НД ТЗІ, положеннями НД ТЗІ 2.7-001-99.

Етапи робіт, які виконуються під час створення КСЗІ в конкретній ІТС, 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 включати нові етапи робіт. За необхідністю дозволяється змінювати послідовність виконання окремих етапів - виконувати одночасно декілька етапів робіт, окремі етапи

виконувати до завершення попередніх і т.п., якщо це не призводить до зниження якості робіт і не суперечить цілям їх виконання.

Примітка:

Під словами “не призводить до зниження якості робіт і не суперечить цілям їх виконання” розуміється, що зміст етапів передбачає виконання всіх основних робіт, встановлених ДСТУ 3396.1 - визначення й оцінка загроз для інформації, формування вимог, розроблення й реалізація проекту КСЗІ, проведення випробувань КСЗІ та введення її в експлуатацію в складі ІТС.

5.5 Виконання окремих видів робіт під час створення КСЗІ здійснюється у відповідності до вимог міжвідомчих та відомчих НД ТЗІ. Цей НД у розділі 6 містить посилання тільки на НД ТЗІ міжвідомчого рівня.

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

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

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

- витоку технічними каналами, до яких відносяться 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 ін;

- спеціального впливу на інформацію, який може здійснюватися шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту.

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

5.7 У випадках, визначених законодавством, роботи з проектування, розроблення, виготовлення, випробування, експлуатації ІТС мають виконуватись у комплексі із заходами, щодо забезпечення режиму секретності, протидії технічним розвідкам, а також з організаційними заходами щодо охорони інформації з обмеженим доступом, яка не є державною таємницею.

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

Створення КЗЗ здійснюється в усіх ІТС, 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 ІТС, де така необхідність визначена власником інформації.

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

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

Примітка:

У залежності від складу КСЗІ може виявитись, що для її створення необхідно виконувати декілька різних видів робіт, які підлягають ліцензуванню в межах господарської діяльності з технічного захисту інформації. У цьому випадку розробник КСЗІ повинен мати право на провадження хоча б одного з таких видів робіт. Для виконання робіт, на провадження яких розробник КСЗІ не має ліцензії, залучаються співвиконавці, які відповідні ліцензії мають.

5.10 Для організації робіт зі створення КСЗІ в ІТС 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).

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

Примітка:

Інтегрована ІТС за своїм складом та структурою, функціональними завданнями, можливими суттєвими відмінностями середовищ функціонування кожної складової ІТС та ін. може бути неоднорідною системою. Для кожної окремої системи у складі такої ІТС 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. А, отже, і вимоги до політики безпеки інформації, вимоги до функціонального профілю захищеності інформації, вимоги до реалізації послуг безпеки тощо в різних складових ІТС на різних об’єктах, де будуть розгортатися її компоненти, мають бути різними.

У цьому випадку КСЗІ інтегрованої ІТС рекомендується будувати за модульним принципом (коли кожна достатньо незалежна складова частина ІТС має свій власний модуль КСЗІ, а КСЗІ інтегрованої ІТС є сукупністю всіх модулів, взаємодія яких

забезпечується окремою підсистемою взаємодії та обміну інформації, яка є єдиною для всієї КСЗІ ІТС). Вибір заходів і механізмів захисту кожного модуля здійснюється відповідно до політики безпеки інформації в ІТС і концепції побудови КСЗІ ІТС, 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 оптимізація матеріальних витрат на проектування КСЗІ; ця процедура зводиться до проектування 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) ІТС.

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

5.12 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 ІТС

6.1.1 Обґрунтування необхідності створення КСЗІ

6.1.1.1 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.

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

- аналізу нормативно-правових актів (державних, відомчих та таких, що діють в 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 і т.п.) експлуатації ІТС у разі створення КСЗІ.

6.1.1.3 На підставі проведеного аналізу приймається рішення про необхідність створення КСЗІ.

6.1.2 Обстеження середовищ функціонування ІТС

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

6.1.2.2 Метою обстеження є підготовка засадничих даних для формування вимог до КСЗІ у вигляді опису кожного середовища функціонування ІТС 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.

Примітка:

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 розглядатись обчислювальною системою як об’єкт-процес, а в інформаційному середовищі – як пасивний об’єкт КС.

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

6.1.2.4 При обстеженні обчислювальної системи ІТС 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 та ін.

Мають бути виявлені компоненти обчислювальної системи, які містять і які не містять засобів і механізмів захисту інформації, потенційні можливості цих засобів і механізмів,

їхні властивості і характеристики, в тому числі ті, що встановлюються за умовчанням та ін.

Метою такого аналізу є надання загального уявлення про наявність потенційних можливостей щодо забезпечення захисту інформації, виявлення компонентів ІТС, які вимагають підвищених вимог до захисту інформації і впровадження додаткових заходів захисту.

6.1.2.5 При обстеженні інформаційного середовища аналізу підлягає вся інформація, що обробляється, а також зберігається в ІТС (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 представлення в ІТС.

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

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 ІТС.

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

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

Порядок проведення обстеження повинен відповідати ДСТУ 3396.1.

Аналізу підлягають такі характеристики фізичного середовища:

- територіальне розміщення компонентів ІТС (генеральний план, ситуаційний план);

- наявність охорони території та перепускний режим;

- наявність категорійованих приміщень, в яких мають розміщуватися компоненти ІТС;

- режим доступу до компонентів фізичного середовища ІТС;

- 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 та технічні характеристики систем заземлення;

- умови зберігання магнітних, оптико-магнітних, паперових та інших носіїв інформації;

- наявність проектної та експлуатаційної документації на компоненти фізичного середовища.

6.1.2.7 При обстеженні середовища користувачів здійснюється аналіз:

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

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

- повноважень користувачів щодо управління КСЗІ;

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

- наявності СЗІ в ІТС.

6.1.2.8 Результати обстеження середовищ функціонування ІТС оформлюються у вигляді акту і включаються, у разі необхідності, до відповідних розділів плану захисту інформації в ІТС (далі - План захисту), який розробляється згідно з НД ТЗІ 1.4-001.

6.1.2.9 За результатами обстеження середовищ функціонування ІТС затверджується перелік об'єктів захисту (з урахуванням рекомендацій НД ТЗІ 1.4-001, НД ТЗІ 2.5-007, НД ТЗІ 2.5-008, НД ТЗІ 2.5-010 щодо класифікації об'єктів), а також визначаються потенційні загрози для інформації і розробляються модель загроз та модель порушника. Побудова моделей здійснюється відповідно до положень НД ТЗІ 1.1-002, НД ТЗІ 1.4-001 та НД ТЗІ 1.6-003. Модель загроз для інформації та модель порушника рекомендується оформляти у вигляді окремих документів (або поєднаних в один документ) Плану захисту.

3.Визначення загальної структури та складу КСЗІ, вимоги до можливих заходів, методів та засобів захисту інформації.

6.2 Розробка політики безпеки інформації в ІТС

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 необхідності 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 варіанту КСЗІ

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

6.2.3 Оформлення політики безпеки

6.2.3.1 На цьому етапі здійснюється:

- вибір основних рішень з протидії всім суттєвим загрозам, формування загальних вимог, правил, обмежень, рекомендацій і т.п., які регламентують використання захищених технологій обробки інформації в ІТС, окремих заходів і засобів захисту інформації, діяльність користувачів всіх категорій;

- документальне оформлення політики безпеки інформації.

6.2.3.2 Політика безпеки може розроблятись для ІТС в цілому або, якщо мають місце особливості функціонування окремих компонентів КСЗІ, для окремої компоненти, для окремої функціональної задачі, для окремої технології обробки інформації тощо.

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

Примітка:

1. Положення політики безпеки, які пов’язані з рішеннями, що приймаються на наступних етапах робіт (стосовно проектних рішень, організації робіт, встановлення відповідальності, порядку впровадження і експлуатації КСЗІ та ін.), вносяться до документу після прийняття цих рішень на відповідних етапах.

2. Як виняток виконання робіт, передбачених пп. 6.2, 6.1.3, 6.1.2.9, може включатися до вимог технічного завдання на створення КСЗІ, а самі роботи виконуватись відповідно до етапів, визначених в ТЗ.

6.3 Розробка технічного завдання на створення КСЗІ

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

6.3.2 ТЗ на створення КСЗІ розробляється на відповідній стадії робіт зі створення ІТС 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 ІТС.

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

6.3.3 Для оформлення ТЗ на КСЗІ можуть бути використані такі варіанти:

- у вигляді окремого розділу ТЗ на створення ІТС;

- у вигляді окремого (часткового) ТЗ;

- у вигляді доповнення до ТЗ на створення ІТС.

Обмежень щодо вибору варіанту не встановлюється.

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

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

Примітка:

Як однотипні складові частини можуть розглядатися КСЗІ ІТС, які забезпечують функціонування вузлів комутації однієї й тієї ж мережі передачі даних, КСЗІ локальних обчислювальних мереж з однаковими функціональними задачами інтегрованої ІТС і т.п., якщо умови їх функціонування не мають суттєвих відмінностей.

При цьому до ТЗ включаються вимоги, які є загальними для окремих складових ІТС та для ІТС 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 ІТС є дотримання в них єдиної системи понять, позначень, ідентифікації об’єктів тощо, які застосовуються в ТЗ на створення ІТС.

6.3.7 Для будь-якого з наведених варіантів розроблення та оформлення ТЗ на КСЗІ його зміст, порядок погодження та затвердження повинен відповідати НД ТЗІ 3.7-001 та ГОСТ 34.602.

6.4 Розробка проекту КСЗІ

6.4.1 Порядок розробки проекту КСЗІ

6.4.1.1 Проект КСЗІ розробляється на підставі та у відповідності до ТЗ на створення ІТС (доповнення до нього, окремого ТЗ на створення КСЗІ).

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

6.4.1.3 Проект КСЗІ виконується на таких стадіях створення ІТС: ескізний проект, технічний проект, робочий проект.

Примітка:

Дозволяється вилучати етап “Ескізний проект КСЗІ”, а також поєднувати етапи “Технічний проект КСЗІ” і “Робочий проект КСЗІ” в один етап “Техноробочий проект КСЗІ”.

6.4.1.4 Для всіх стадій розробки проекту КСЗІ склад документації визначається ТЗ на КСЗІ, види та зміст - ГОСТ 34.201, НД ТЗІ 2.5-004. Документація на програмні засоби виконується згідно з комплексом стандартів ЄСПД, на технічні засоби – згідно з комплексом стандартів ЄСКД.

6.4.2 Ескізний проект КСЗІ

6.4.2.1 На цьому етапі здійснюється розробка попередніх проектних рішень КСЗІ та, у разі необхідності, її окремих складових частин, а також розроблення, оформлення, узгодження та затвердження документації на КСЗІ. Зміст та стиль документації повинні бути достатніми для повного опису проектних рішень рівня ескізного проекту.

6.4.2.2 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.

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

6.4.3 Технічний проект КСЗІ

6.4.3.1 Розробка проектних рішень КСЗІ

Виконується розробка: загальних проектних 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.

Здійснюються організаційно-технічні заходи щодо забезпечення послідовності розробки КЗЗ, архітектури, середовища розробки, випробувань, середовища функціонування та експлуатаційної документації КЗЗ у відповідності до заданих рівнем гарантій реалізації послуг безпеки згідно із специфікаціями НД ТЗІ 2.5-004, НД ТЗІ 2.5-007, НД ТЗІ 2.5-008, НД ТЗІ 2.5-010.

6.4.3.2 Розробка документації на КСЗІ

Виконується розроблення, оформлення, узгодження та затвердження документації в обсязі, передбаченому ТЗ на КСЗІ. Зміст та стиль документації повинні бути достатніми для повного опису проектних рішень рівня технічного проекту.

6.4.3.3 Розробка документації на постачання засобів захисту інформації та/або технічних вимог (технічних завдань) на їх розробку.

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.

6.4.3.4 Розробка завдань на проектування в суміжних частинах

Здійснюється розроблення, оформлення і затвердження завдань на проектування з 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 проект КСЗІ

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

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

6.4.4.2 Проводиться розробка засобів захисту інформації, передбачених п.6.4.3.3, або адаптація готової продукції до умов функціонування КСЗІ. Розробка засобів захисту інформації від НСД здійснюється згідно з НД ТЗІ 3.6-001.

6.4.4.3 До складу робочої документації на комплекси технічного захисту інформації від витоку технічними каналами повинні входити схеми розміщення ОТЗ ІТС, кабельного обладнання, мереж живлення та систем заземлення, які виконуються у відповідності до вимог нормативних документів ТР ЕОТ – 95, ТР ТЗІ-ПЕМВН-95, СТР-2, СТР-3, СВТР-78. При цьому враховуються умови їх розміщення і мінімально допустимі відстані між цими засобами та ДТЗ (засоби зв’язку, системи та засоби кондиціювання, сигналізації, електроосвітлення, радіомовлення, часофікації тощо), що знаходяться у приміщенні, де розташоване обладнання ІТС, та у суміжних приміщеннях. Зазначені умови розміщення та мінімально допустимі відстані беруться з експлуатаційної документації, яка супроводжує сертифіковані ОТЗ.

У разі відсутності для ОТЗ, що використовуються в складі КСЗІ, сертифікатів відповідності вимогам з технічного захисту інформації, мінімально допустимі відстані та інші умови розміщення цих засобів мають бути визначені за результатами їх спеціальних досліджень на етапі проведення пусконалагоджувальних робіт.

6.4.4.4 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 ІТС, контролю за діями користувачів, формування та актуалізації баз даних захисту, а також контролю цілісності програмного забезпечення та баз даних захисту.

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

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

6.5 Введення КСЗІ в дію та оцінка захищеності інформації в ІТС

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

6.5.1 Підготовка КСЗІ до введення в дію

6.5.1.1 Проводяться роботи з підготовки організаційної структури та розробки розпорядчих документів, що регламентують діяльність із забезпечення захисту інформації в ІТС.

6.5.1.2 Здійснюється створення СЗІ (призначаються відповідальні особи за захист інформації), якщо цього не було зроблено на попередніх етапах.

6.5.1.3 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).

6.5.1.4 Створення СЗІ та розробка Плану захисту здійснюється згідно з НД ТЗІ 1.4-001.

6.5.2 Навчання користувачів

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

6.5.3 Комплектування КСЗІ

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

6.5.4 Будівельно-монтажні роботи

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

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

6.5.4.2 Будівельні роботи здійснюються силами організації-власника ІТС або будівельно-монтажними організаціями згідно з проектною документацією на будівництво, яка розробляється проектною організацією у відповідності до вимог нормативних документів ДБН А.2.2-2, ДБН 2.2-3-2004.

6.5.4.3 Після завершення будівельних робіт створюється комісія з прийняття робіт, до складу якої входять представники організації-замовника будівельних робіт, проектної 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

6.5.5.1 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.

6.5.5.2 Монтаж ОТЗ ІТС, кабельного обладнання, мереж живлення та заземлення здійснюється згідно з конструкторською документацією робочого проекту.

Якщо до складу КСЗІ входять ОТЗ, які не мають сертифікатів відповідності вимогам з ТЗІ, визначаються мінімально допустимі відстані між цими засобами та ДТЗ за результатами їх спеціальних досліджень.

6.5.5.3 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.

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

6.5.5.5 За результатами робіт складається акт, де зазначаються: категорії приміщень, де розташоване обладнання ІТС, межі контрольованих зон для приміщень, перелік ОТЗ, ДТЗ і комунікацій (із вказівкою найменування, типу, заводського номеру), що знаходяться у цих приміщеннях, оцінка відповідності проведення монтажних робіт вимогам експлуатаційних документів на засоби та нормативних документів, зазначених у п. 6.4.4.3, 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 ІТС.

6.5.5.6 Здійснюється впровадження додаткових заходів захисту, необхідність впровадження яких зафіксована в акті, відповідно до порядку проведення робіт етапу та відповідне коригування проектної, робочої, експлуатаційної документації.

6.5.5.7 Оцінка повноти та якості виконання робіт з ТЗІ в приміщеннях проводиться шляхом атестації впровадженого комплексу технічного захисту інформації від витоку технічними каналами, за результатами якої надається документ встановленого зразка – "Акт атестації комплексу технічного захисту інформації". Порядок здійснення атестації, зміст та форма "Акту ..." визначається НД ТЗІ 2.1-001.

6.5.5.8 Здійснюється згідно з документацією робочого проекту інсталяція, ініціалізація та перевірка працездатності КЗЗ.

Інсталяція та ініціалізація КЗЗ, який має експертний висновок щодо його відповідності вимогам НД ТЗІ, здійснюється у порядку, визначеному в експлуатаційній документації на цей комплекс.

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

До бази даних захисту вносяться відомості про користувачів ІТС, 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

6.5.6.1 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.

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

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

6.5.6.4 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.

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

6.5.7 Дослідна експлуатація

6.5.7.1 Під час дослідної експлуатації КСЗІ:

відпрацьовуються технології оброблення інформації, обігу машинних носіїв інформації, керування засобами захисту, розмежування доступу користувачів до ресурсів ІТС та автоматизованого контролю за діями користувачів;

співробітники СЗІ та користувачі ІТС 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 (за необхідністю) доопрацювання програмного забезпечення, додаткове налагоджування та конфігурування КЗЗ;

здійснюється (за необхідністю) коригування робочої та експлуатаційної документації.

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

6.5.8 Державна експертиза КСЗІ

6.5.8.1 Державна експертиза КСЗІ є окремим етапом приймальних випробувань ІТС.

6.5.8.2 Державна експертиза проводиться з метою визначення відповідності КСЗІ технічному завданню, вимогам НД із захисту інформації та визначення можливості введення КСЗІ в складі ІТС в експлуатацію.

Державна експертиза КСЗІ в ІТС проводиться згідно з Положенням про державну експертизу в сфері технічного захисту інформації.

6.5.8.3 Виявлені під час державної експертизи недоліки усуваються до її завершення, порядок усунення такий самий, як і для попередніх випробувань. Якщо в силу якихось причин 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.

6.5.8.4 Для інтегрованих ІТС може проводитись державна експертиза кожної складової частини (модуля) КСЗІ окремо.

Державна експертиза КСЗІ інтегрованої ІТС 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 ІТС в цілому, оформлюються з урахуванням відповідних документів на складові частини КСЗІ.

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

6.5.8.6 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.

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

Примітка:

У першу чергу такий порядок рекомендується застосовувати для складних з точки зору архітектури, складу та обсягів робіт КСЗІ. При цьому експертами послідовно здійснюється оцінка технічних та організаційних рішень на всіх етапах робіт. Це дає змогу оперативно усувати недоліки проектування та скоротити час проведення державної

експертизи, яка може бути в основному завершена до етапу приймальних випробувань ІТС.

6.5.8.8 Приймальні випробування ІТС проводяться при функціонуючій в її складі КСЗІ.

Примітка:

Роботи п.6.5.8, а також пп. 6.5.6 і 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, гарантійному і післягарантійному технічному обслуговуванню засобів захисту інформації.