**Тема № 3**
**Заняття № 1**
Застело Г.І.

# Порядок проведення робіт із створення КТЗІ в ІТС. НД ТЗІ 3.7-003-05.

## Питання:

*1. Загальні положення відносно створення КСЗІ.*

*2. Обґрунтування необхідності створення КСЗІ.*

*3. Характеристика етапів створення КСЗІ.*

## Питання:

*1. Загальні положення відносно створення КСЗІ.*

*2. Обґрунтування необхідності створення КСЗІ.*

*3. Характеристика етапів створення КСЗІ.*

# НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення КСЗІ в ІТС»

Цей документ ***визначає*** основи організації та порядок виконання робіт із захисту інформації в ІТС - порядок прийняття рішень щодо складу КСЗІ 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.**

**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.

**Комплексна система захисту інформації** (КСЗІ) (рос. - комплексная система защиты информации) – це сукупність організаційних, інженерних і програмно-апаратних засобів, що забезпечують захист інформації в ІКС.

***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.

***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 ЗІ.

***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 достатньо 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.

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.

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 КСЗ
- введення її в експлуатацію в складі ІТС.

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 ТЗІ будь-якого з наведених рівнів, то ***допускається використання рекомендацій міжнародних стандартів*** в частині, що не суперечить нормативно – правовим актам та нормативним документам України.

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

- ***витоку технічними каналами***, до яких відносяться канали ПЕВіН, 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.

## Вопросы:

*1. Загальні положення відносно створення КСЗІ.*

*2. Обґрунтування необхідності створення КСЗІ.*

*3. Характеристика етапів 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 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.

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

Після прийняття рішення про необхідність створення КСЗІ в ІТС для організації цих робіт створюється ***Служба захисту інформації*** (далі - СЗІ) в ІТС. Як виняток СЗІ може створюватися на більш пізніх етапах робіт, але не пізніше етапу підготовки КСЗІ до введення в дію.

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

***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
- технології обробки інформації,
- канали обміну інформацією,
- перелік конкретних загроз тощо.

*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;
- 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***.
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.

***Суб'єкти КСЗІ***

В процес створення КСЗІ беруть участь таки ***сторони*:**

- організація, для якої здійснюється створення КСЗІ (Замовник);
- організація, яка здійснює заходи зі створення КСЗІ (Виконавець);
- Державна служба спеціального зв'язку і захисту інформації України (ДССЗЗІУ) (Контролюючий орган);
- організація, яка здійснює державну експертизу КСЗІ (Організатор експертизи);
- організація, яка за необхідністю притягується Замовником або Виконавцем для виконання деяких робіт зі створення КСЗІ (Підрядчик).

***Об'єкти захисту КСЗІ***

Об'єктами захисту КСЗІ є ***інформація, у любому її вигляді і формі представлення.***
В залежності від виду і форми представлення інформаційних сигналів, що циркулюють і інформаційно-телекомунікаційної системі (ИТС), у тому числі і у автоматизованих системах (АС), при створенні КСЗІ можуть використовувати різні засоби захисту.

## Вопросы:

*1. Загальні положення відносно створення КСЗІ.*

*2. Обґрунтування необхідності створення КСЗІ.*

*3. Характеристика етапів створення КСЗІ.*

*НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення КСЗІ в ІТС»* визначає ***6 етапів створення КСЗІ*** та її документації:

**1. Формування вимог до КСЗІ в ІТС**

1.1. Обґрунтування необхідності створення КСЗІ і призначення СЗІ:
- наказ про порядок проведення робіт зі створення КСЗІ
- наказ про створення СЗІ
- положення про СЗІ
- перелік інформації, що підлягає обробленню в ІТС та потребує захисту

1.2. Категоріювання ІТС:
- наказ про призначення комісії з категоріювання
- акт категоріювання

1.3. Обстеження середовищ функціонування ІТС:
- наказ про призначення комісії з обстеження
- акт обстеження
- формуляр ІТС

1.4. Опис моделі порушника політики безпеки інформації: модель порушника

1.5. Опис моделі загроз для інформації: модель загроз

1.6. Формування завдання на створення КСЗІ: звіт за результатами проведення аналізу ризиків та формування завдань на створення КСЗІ

**2. Розробка політики безпеки інформації в ІТС**

2.1. Вибір варіанту КСЗІ

2.2. Складання політики безпеки

2.3. Складання плану захисту

2.4. Складання календарного плану робіт із захисту інформації

**3. Розробка Технічного завдання на створення КСЗІ:**

- складання технічного завдання та погодження його з органами Держспецзв'язку

**4. Розробка проекту КСЗІ:**

- складання документів ескізного проекту КСЗІ
- складання документів технічного проекту КСЗІ
- складання документів робочого проекту КСЗІ

**5. Введення КСЗІ в дію та оцінка захищеності інформації в ІТС**

5.1. Підготовка КСЗІ до введення в дію:

- інструкція про порядок введення в експлуатацію КСЗІ

5.2. Навчання користувачів:

- інструкція адміністратора безпеки в ІТС
- інструкція системного адміністратора ІТС
- інструкція користувача ІТС
- правила управління паролями в ІТС
- правила видачі, вилучення та обміну персональних ідентифікаторів, інших атрибутів розмежування доступу в ІТС

5.3. Комплектування КСЗІ

5.4. Будівельно-монтажні роботи:

- наказ про призначення комісії з приймання робіт
- акт приймання робіт

5.5. Пусконалагоджувальні роботи:

- акт інсталяції та налагоджування АВПЗ і КЗЗ від НСД
- акт завершення пусконалагоджувальних робіт

5.6. Попередні випробування КСЗІ:

- наказ про створення комісії з проведення випробувань
- програма та методика попередніх випробувань
- протокол про проведення попередніх випробувань
- акт завершення попередніх випробувань

5.7. Дослідна експлуатація КСЗІ:

- наказ про введення ІТС в дослідну експлуатацію
- акт завершення дослідної експлуатації
- акт завершення робіт зі створення КСЗІ

5.8. Державна експертиза КСЗІ:

- заявка на проведення державної експертиза КСЗІ
- експертний висновок щодо відповідності КСЗІ вимогам НД ТЗІ
- атестат відповідності КСЗІ вимогам НД ТЗІ
- наказ про дозвіл на обробку в ІТС інформації, яка підлягає захисту

**6. Супровід КСЗІ:**

- наказ про порядок забезпечення захисту інформації в ІТС
- інструкція щодо забезпечення правил обробки ІзОД в ІТС
- інструкція з антивірусного захисту інформації в ІТС
- інструкція про порядок використання засобів КЗІ в ІТС
- інструкція про порядок обліку та використання машинних носіїв інформації
- інструкція з правил управління паролями в ІТС
- інструкція про порядок створення і зберігання резервних копій інформаційних ресурсів ІТС
- інструкція про порядок проведення контролю режиму обробки та захисту інформації в ІТС
- інструкція про порядок супроводу та модернізації КСЗІ в ІТС
- інструкція про порядок відновлювальних та ремонтних робіт ІТС
- інші інструкції.