1. **Загальні положення та вимоги щодо організації робіт із захисту інформації та порядку створення комплексної системи захисту 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 захисту інформації.

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.

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.

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.

1. **Основні засоби та заходи, що входять до складу КСЗІ.**

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.

1. **Порядок створення, завдання, функції, структура та повноваження служби захисту інформації щодо організації робіт зі створення КСЗІ в ІКС.**

Служба захисту інформації утворюється згідно з рішенням керівника організації, що є власником (розпорядником) системи.

Згідно з НД ТЗІ 1.4-001 основними **завданнями СЗІ є:**

* Організація заходів із створення і використання комплексної системи захисту інформації (КСЗІ) на всіх етапах життєвого циклу автоматизованої системи (АС).
* Захист законних прав щодо безпеки інформації в організації, окремих її структурних підрозділах, персоналу під час обміну інформацією між собою та із зовнішніми вітчизняними та закордонними організаціями.
* Організація та координація заходів, пов'язаних із захистом інформації в АС та підтримка належного рівня захищеності інформації, ресурсів і технологій.
* Дослідження технології оброблення інформації в АС задля виявлення ймовірних каналів її витоку та інших загроз безпеці інформації, формування моделі загроз, розроблення політики безпеки інформації, визначення заходів, спрямованих на її реалізацію.
* Розроблення проектів нормативних і розпорядчих документів, чинних у межах організації, згідно з якими має підтримуватися певний рівень захисту інформації в АС.
* Робота з персоналом.
* Виконання відповідних функцій під час експлуатації КСЗІ.
* Виконання певних функцій під час створення КСЗІ.

СЗІ має виконувати такі функції:

* забезпечувати якісне виконання організаційно-технічних заходів із захисту інформації в АС;
* перевіряти відповідність прийнятих в організації правил, інструкцій щодо оброблення інформації, здійснювати контроль за виконанням цих вимог;
* здійснювати контрольні перевірки стану захищеності інформації в АС;
* забезпечувати конфіденційність заходів із монтажу, експлуатації та технічного обслуговування засобів захисту інформації, встановлених в АС (організації);
* сприяти (технічними та організаційними заходами) створенню і дотриманню умов зберігання інформації, отриманої організацією на договірних, контрактних **або** інших основах від організацій-партнерів, постачальників, клієнтів та приватних осіб;
* періодично надавати керівництву організації звіт про стан захищеності інформації в АС і про дотримання користувачами та персоналом АС встановленого порядку і правил захисту інформації;
* негайно повідомляти керівництво АС (організації) про виявлені атаки та викритих порушників.

**Структуру СЗІ**, її склад і чисельність визначають на підставі фактичних потреб АС із забезпечення вимог політики безпеки інформації. Чисельність і склад СЗІ мають бути достатніми для виконання всіх завдань із захисту інформації в АС. Умовно співробітників СЗІ за функціональними обов'язками можна розділити на:

* Співробітник групи безпеки
* Адміністратор безпеки системи
* Адміністратор безпеки даних
* Керівник групи

**Повноваження та відповідальність служби захисту інформації**

**Права. С**ЗІ має право:

- здійснювати контроль за діяльністю будь-якого структурного підрозділу організації (АС) щодо виконання ним вимог нормативно-правових актів і нормативних документів з захисту інформації;

1. подавати керівництву організації пропозиції щодо призупинення процесу обробки інформації, заборони обробки, зміни режимів обробки, тощо у випадку виявлення порушень політики безпеки або у випадку виникнення реальної загрози порушення безпеки;
2. складати і подавати керівництву організації акти щодо виявлених порушень політики безпеки, готувати рекомендації щодо їхнього усунення;
3. проводити службові розслідування у випадках виявлення порушень;
4. отримувати доступ до робіт та документів структурних підрозділів організації (АС), необхідних для оцінки вжитих заходів з захисту інформації та підготовки пропозицій щодо їхнього подальшого удосконалення;
5. готувати пропозиції щодо залучення на договірній основі до виконання робіт з захисту інформації інших організацій, які мають ліцензії на відповідний вид діяльності;
6. готувати пропозиції щодо забезпечення АС (КСЗІ) необхідними технічними і програмними засобами захисту інформації та іншою спеціальною технікою, які дозволені для використання в Україні з метою забезпечення захисту інформації;
7. виходити до керівництва організації з пропозиціями щодо подання заяв до відповідних державних органів на проведення державної експертизи КСЗІ або сертифікації окремих засобів захисту інформації;
8. узгоджувати умови включення до складу АС нових компонентів та подавати керівництву пропозиції щодо заборони їхнього включення, якщо вони порушують прийняту політику безпеки або рівень захищеності ресурсів АС;
9. надавати висновки з питань, що належать до компетенції СЗІ, які необхідні для здійснення виробничої діяльності організації, особливо технологій, доступ до яких обмежено, інших проектів, що потребують технічної підтримки з боку співробітників СЗІ;
10. виходити до керівництва організації з пропозиціями щодо узгодження планів і регламенту відвідування АС сторонніми особами;
11. інші права, які надані СЗІ у відповідності з специфікою та особливостями діяльності організації (АС).

**Обов’язки.** СЗІ зобов’язана:

1. організовувати забезпечення повноти та якісного виконання організаційно-технічних заходів з захисту інформації в АС;
2. вчасно і в повному обсязі доводити до користувачів і персоналу АС інформацію про зміни в галузі захисту інформації, які їх стосуються;
3. перевіряти відповідність прийнятих в АС (організації) правил, інструкцій щодо обробки інформації, здійснювати контроль за виконанням цих вимог;
4. здійснювати контрольні перевірки стану захищеності інформації в АС;
5. забезпечувати конфіденційність робіт з монтажу, експлуатації та технічного обслуговування засобів захисту інформації, встановлених в АС (організації);
6. сприяти і, у разі необхідності, брати безпосередню участь у проведенні вищими органами перевірок стану захищеності інформації в АС;
7. сприяти (технічними та організаційними заходами) створенню і дотриманню умов збереження інформації, отриманої організацією на договірних, контрактних або інших підставах від організацій-партнерів, постачальників, клієнтів та приватних осіб;
8. періодично, не рідше одного разу на місяць (інший термін), подавати керівництву організації звіт про стан захищеності інформації в АС і дотримання користувачами та персоналом АС встановленого порядку і правил захисту інформації;
9. негайно повідомляти керівництво АС (організації) про виявлені атаки та викритих порушників;
10. Інші обов’язки, покладені на керівника та співробітників СЗІ у відповідності з специфікою та особливостями діяльності АС (організації).

**Відповідальність.** Керівництво та співробітники СЗІ за невиконання або неналежне виконання службових обов’язків, допущені ними порушення встановленого порядку захисту інформації в АС несуть дисциплінарну, адміністративну, цивільно-правову, кримінальну відповідальність згідно з законодавством України.

Персональна відповідальність керівника та співробітників СЗІ визначається посадовими (функціональними) інструкціями.

Відповідальність за діяльність СЗІ покладається на її керівника.

Керівник СЗІ відповідає за:

1. організацію робіт з захисту інформації в АС, ефективність захисту інформації відповідно до діючих нормативно-правових актів;
2. своєчасне розроблення і виконання “Плану захисту інформації в автоматизованій системі”;
3. якісне виконання співробітниками СЗІ завдань, функцій та обов'язків, зазначених у цьому Положенні, посадових інструкціях, а також планових заходів з захисту інформації, затверджених керівником організації;
4. координацію планів діяльності підрозділів та служб АС (організації) з питань захисту інформації;
5. створення системи навчання співробітників, користувачів, персоналу АС з питань захисту інформації;
6. виконання особисто та співробітниками СЗІ розпоряджень керівника організації, правил внутрішнього трудового розпорядку, встановленого режиму, правил охорони праці та протипожежної охорони.

Співробітники СЗІ відповідають за:

1. додержання вимог нормативних документів, що визначають порядок організації робіт з захисту інформації, інформаційних ресурсів та технологій;
2. повноту та якість розроблення і впровадження організаційно-технічних заходів з захисту інформації в АС, точність та достовірність отриманих результатів і висновків з питань, що належать до компетенції СЗІ;
3. дотримання термінів проведення контрольних, інспекційних, перевірочних та інших заходів з оцінки стану захищеності інформації в АС, які включені до плану робіт СЗІ;
4. якість та правомірність документального оформлення результатів робіт окремих етапів створення КСЗІ, документального оформлення результатів перевірок;
5. інші питання персональної відповідальності, які покладені на керівника та співробітників СЗІ у відповідності з специфікою та особливостями діяльності АС (організації).
6. **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 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.

1. **Обстеження середовищ функціонування ІКС.**

Під час виконання обстеження, ІТС розглядається як організаційно-технічна система, яка поєднує обчислювальну систему, фізичне середовище, середовище користувачів, оброблювану інформацію і технологію її обробки Все це називається середовищем функціонування ІТС.

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.

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.

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.

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.

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. [[5](#L5)].

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.

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.

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.

1. **Формування завдання на створення КСЗІ.**

На цьому етапі:

* визначаються завдання захисту інформації в ІТС, мета створення КСЗІ, варіант вирішення задач захисту (відповідно до ДСТУ 3396.1), основні напрями забезпечення захисту (відповідно до п. 5.8);
* здійснюється аналіз ризиків (вивчення моделі загроз і моделі порушника, можливих наслідків від реалізації потенційних загроз, величини можливих збитків та ін.) 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 ІТС, обмеження щодо використання ресурсів ІТС для реалізації задач 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 ІТС (окремих її підсистемах, компонентах) організаційних, інженерно-технічних, технічних, криптографічних та інших заходів захисту інформації, що ввійдуть до складу КСЗІ.

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

1. **Розробка політики безпеки інформації в ІКС.**

**Вивчення об’єкта, на якому створюється КСЗІ, проведення науково-дослідних робіт (НДР)**

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.

**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.

**Оформлення політики безпеки**

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.

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.

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.

Слід враховувати наступне:

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. Результати обстеження середовища функціонування ІТС, завдання на створення КСЗІ, результати розроблення політики безпеки, можуть включатися до вимог технічного завдання на створення КСЗІ, а самі роботи виконуватись відповідно до етапів, визначених в ТЗ.

1. **Розробка технічного завдання на створення КСЗІ.**

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.

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.

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.

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.

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.

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 34.601.

1. **Розробка проекту КСЗІ.**

**Порядок розробки проекту КСЗІ**

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

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.

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

**Ескізний проект КСЗІ**

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.

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.

**Технічний проект КСЗІ**

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.

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.

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.

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).

**Робочий проект КСЗІ**

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.

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.

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.

1. **Введення КСЗІ в дію та оцінка захищеності інформації в ІКС.**

**Підготовка КСЗІ до введення в дію**

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

**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.

**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.

**Будівельно-монтажні роботи**

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.

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

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.

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.

**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 ІТС.

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.

**Дослідна експлуатація**

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.

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

**Державна експертиза КСЗІ**

Державна експертиза КСЗІ є окремим етапом приймальних випробувань ІТС.

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.

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.

1. **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.

Необхідною умовою супроводження КСЗІ є проведення інспекційних перевірок щодо дотримання вимог встановленої політики інформаційної безпеки. У разі виявлення порушень вживаються додаткові заходи щодо їх усунення.

З появою нових вимог стосовно захисту інформації, закріплених в нормативно-правових актах України, комплексна система захисту інформації коригується відповідно до цих вимог. 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.