



НОРМАТИВНИЙ ДОКУМЕНТ
СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

**Методичні вказівки щодо розробки технічного завдання
на створення комплексної системи захисту інформації в
автоматизованій системі**

Департамент спеціальних телекомунікаційних систем та захисту
інформації Служби безпеки України

Київ 1999

НОРМАТИВНИЙ ДОКУМЕНТ
СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Затверджено
Наказом Департаменту спеціальних
телекомунікаційних систем та захисту інформації
Служби безпеки України
від “ 28 ” квітня 1999 р. № 22

**Методичні вказівки щодо розробки технічного завдання
на створення комплексної системи захисту інформації в
автоматизованій системі**

НД ТЗІ 3.7-001-99

ДСТСЗІ СБ України

Київ

Передмова

1 РОЗРОБЛЕНО товариством з обмеженою відповідальністю «Інститут комп'ютерних технологій»

2 ВНЕСЕНО Головним управлінням технічного захисту інформації Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України

3 ВВЕДЕНО замість нормативного документу системи технічного захисту інформації “Тимчасові рекомендації щодо розроблення розділу із захисту інформації в технічному завданні на створення автоматизованої системи (ТРАС-96)”, який втрачає чинність з 01.07.99р.

Цей документ не може бути повністю або частково відтворений, тиражований і розповсюджений без дозволу Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України

Зміст

1	Галузь використання.....	4
2	Нормативні посилання	4
3	Визначення	5
4	Позначення і скорочення.....	5
5	Загальні вимоги до розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі	5
5.1	Загальні положення.....	6
5.2	Порядок розроблення технічного завдання.....	6
5.3	Зміст технічного завдання.....	7
6	Вимоги до змісту розділів технічного завдання	7
6.1	Загальні відомості	7
6.2	Мета і призначення комплексної системи захисту інформації	8
6.3	Загальна характеристика автоматизованої системи і умов її функціонування.....	8
6.4	Вимоги до комплексної системи захисту інформації.....	9
6.4.1	Вимоги до комплексної системи захисту інформації в АС в частині захисту від несанкціонованого доступу.....	9
6.4.2	Вимоги до комплексної системи захисту інформації в АС в частині захисту від витоку інформації технічними каналами.....	10
6.5	Вимоги до складу проектної та експлуатаційної документації.....	9
6.6	Етапи виконання робіт	12
6.7	Порядок внесення змін і доповнень до технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі	12
6.8	Порядок проведення випробувань комплексної системи захисту інформації.....	12

МЕТОДИЧНІ ВКАЗІВКИ ЩОДО РОЗРОБКИ ТЕХНІЧНОГО ЗАВДАННЯ НА СТВОРЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНІЙ СИСТЕМІ

Чинний с 1999-07-01

1 Галузь використання

Цей нормативний документ встановлює вимоги до порядку розробки, складу і змісту технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі, призначеній для оброблення, зберігання і передачі (далі — оброблення) інформації з обмеженим доступом* або інформації, захист якої гарантується державою.

Положення цього документа розповсюджуються на державні органи, Збройні Сили, інші військові формування, МВС, Раду Міністрів Автономної Республіки Крим і органи місцевого самоврядування, а також підприємства, установи і організації всіх форм власності, які володіють, користуються і розпоряджаються інформацією, що є власністю держави, або інформацією, захист якої гарантується державою.

Власники (користувачі) інформації, яка не є власністю держави або захист якої не гарантується державою, положення цього документа застосовують за своїм розсудом.

Зміни заходів, проведених раніше відповідно до вимог діючих керівних документів, не вимагається.

Нормативний документ розроблено у доповнення до діючих нормативних документів щодо створення об'єктів інформатики.

2 Нормативні посилання

В цьому документі використані посилання на такі нормативно-правові акти та нормативні документи:

* Згідно з законом України "Про інформацію", вся інформація поділяється на відкриту та інформацію з обмеженим доступом. Такий поділ за режимами доступу здійснюється виключно на підставі ступеня конфіденційності інформації. Поряд з конфіденційністю істотними характеристиками інформації є її цілісність і доступність, проте на сьогоднішній день іншої класифікації інформації, крім наведеної, не запроваджено. З метою збереження загальності викладу далі в тексті замість терміну "інформація з обмеженим доступом" використовується термін "інформація", який має на увазі будь-яку інформацію, щодо якої регламентовані певні вимоги до забезпечення її конфіденційності, цілісності та доступності.

Закон України "Про інформацію".

Положення про технічний захист інформації в Україні.

НД ТЗІ 1.1-003-99. Термінологія у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

ТР ЕОТ-95. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок.

ТР ПЕМВН-95. Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок.

3 Визначення

В цьому НД ТЗІ застосовуються терміни і визначення, встановлені ДСТУ 3396.2-97 "Захист інформації. Технічний захист інформації. Терміни і визначення" і НД ТЗІ 1.1-003-99 "Термінологія у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу".

4 Позначення і скорочення

В цьому НД ТЗІ використовуються такі позначення і скорочення:

АС — автоматизована система;

ЕОТ — електронна обчислювальна техніка;

ЕМВ — електромагнітне випромінювання.

ЗОТ — засіб обчислювальної техніки;

ІзОД — інформація з обмеженим доступом;

КЗЗ — комплекс засобів захисту;

КС — комп'ютерна система;

КСЗІ — комплексна система захисту інформації;

НД — нормативний документ;

НСД — несанкціонований доступ;

ОС — обчислювальна система;

ПЗ — програмне забезпечення;

ПЕМВН — побічні електромагнітні випромінювання і наводки;

ТЗ — технічне завдання;

ТЗІ — технічний захист інформації.

5 Загальні вимоги до розробки технічного завдання на створення комплексної системи захисту інформації в

автоматизованій системі

5.1 Загальні положення

Технічне завдання на створення КСЗІ в АС (ТЗ на КСЗІ) є засадничим організаційно-технічним документом для виконання робіт щодо забезпечення захисту інформації в системі.

Технічне завдання на КСЗІ розробляється у разі необхідності розробки або модернізації КСЗІ існуючої (що функціонує) АС. В разі розробки КСЗІ в процесі проектування АС допускається оформлення вимог з захисту інформації в АС у вигляді окремого (часткового) ТЗ, доповнення до загального ТЗ на АС або розділу загального ТЗ на АС.

Технічне завдання на КСЗІ повинно розроблятися з урахуванням комплексного підходу до побудови КСЗІ, який передбачає об'єднання в єдину систему всіх необхідних заходів і засобів захисту від різноманітних загроз безпеці інформації на всіх етапах життєвого циклу АС.

В технічному завданні на КСЗІ викладаються вимоги до функціонального складу і порядку розробки і впровадження технічних засобів, що забезпечують безпеку інформації в процесі її оброблення в обчислювальній системі АС. Додатково треба викласти вимоги до організаційних, фізичних та інших заходів захисту, що реалізуються поза обчислювальною системою АС у доповнення до комплексу програмно-технічних засобів захисту інформації.

Перелік вимог з захисту інформації, які включаються в ТЗ на КСЗІ, може бути для кожної конкретної АС як розширений, так і скорочений відносно рекомендованого в даному документі переліку в рамках діючих законодавчих і нормативних документів.

Вимоги повинні передбачати розроблення та використання сучасних ефективних засобів і методів захисту, які дають можливість забезпечити виконання цих вимог з найменшими матеріальними затратами.

Технічне завдання на КСЗІ є одним із обов'язкових засадничих документів під час проведення експертизи АС на відповідність вимогам захищеності інформації.

5.2 Порядок розроблення технічного завдання

Вихідними даними для розроблення ТЗ на КСЗІ є функціональний профіль захищеності КС від НСД і вимоги до захищеності інформації від витоку технічними каналами.

Функціональний профіль захищеності інформації в конкретній АС може бути визначений в результаті проведення аналізу загроз та оцінки ризиків або обраний на підставі класу АС відповідно до НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні класи захищеності оброблюваної інформації від несанкціонованого доступу".

Вимоги до захищеності інформації від витоку технічними каналами визначаються на підставі НД ТЗІ ТР ЕОТ-95 "Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок" і ТР ПЕМВН-95 "Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок".

В технічному завданні повинно бути наведено обґрунтування вибору функціонального профілю захищеності і вимог до показників захищеності інформації від витоку технічними каналами.

Перелік основних робіт етапу формування ТЗ такий:

класифікація та опис ресурсів АС (ОС, засобів зв'язку і комунікацій, інформації, її категорій, виду подання, місця зберігання, технології обробки тощо, обслуговуючого персоналу і користувачів, території і приміщень і т. ін.);

розробка інформаційної моделі для існуючої АС, тобто опис (формальний або неформальний) інформаційних потоків АС, інтерфейсів між користувачем і АС і т. ін.;

визначення переліку загроз і можливих каналів витоку інформації;

експертна оцінка очікуваних втрат у разі здійснення загроз;

визначення послуг безпеки, які треба реалізувати;

обґрунтування необхідності проведення спецперевірок і спецдосліджень ЗОТ та інших технічних засобів, а також спеціального обладнання приміщень;

визначення вимог до організаційних, фізичних та інших заходів захисту, що реалізуються у доповнення до комплексу програмно-технічних засобів захисту;

визначення вимог до метрологічного забезпечення робіт;

визначення переліку макетів, що розробляються, і технологічних стендів;

оцінка вартості і ефективності обраних засобів;

прийняття остаточного рішення про склад КСЗІ.

Вимоги з захисту інформації визначаються замовником, погоджуються з розробником АС і виконавцем робіт по створенню КСЗІ в АС. Виконавець повинен мати відповідну ліцензію Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України (Департамент). У випадках, передбачених Положенням про технічний захист інформації в Україні, ТЗ на КСЗІ погоджується з Департаментом.

5.3 Зміст технічного завдання

Технічне завдання на КСЗІ оформлюється відповідно до того ж самого ДСТУ, що і основне ТЗ на АС, і в загальному випадку повинно містити такі основні підрозділи:

загальні відомості;

мета і призначення комплексної системи захисту інформації;

загальна характеристика автоматизованої системи та умов її функціонування;

вимоги до комплексної системи захисту інформації;

вимоги до складу проектної та експлуатаційної документації;

етапи виконання робіт;

порядок внесення змін і доповнень до ТЗ;

порядок проведення випробувань комплексної системи захисту інформації.

6 Вимоги до змісту розділів технічного завдання

6.1 Загальні відомості

В підрозділі зазначають:

повне найменування КСЗІ та її умовне позначення;

шифр теми і реквізити договору;

найменування підприємств-розробників і замовника (користувача) КСЗІ та їх реквізити;

перелік документів, на підставі яких створюється КСЗІ, ким і коли затверджені ці документи;

планові терміни початку і закінчення роботи із створення КСЗІ;

відомості про джерела і порядок фінансування робіт;

порядок оформлення і подання замовнику результатів робіт із створення КСЗІ, з виготовлення і налагодження окремих засобів (технічних, програмних, інформаційних) і програмно-технічних (програмно-методичних) комплексів системи.

6.2 Мета і призначення комплексної системи захисту інформації

Вказується мета розробки КСЗІ в АС, функціональне призначення і особливості застосування. Необхідно зазначати, на підставі яких нормативно-правових актів, інших нормативних документів регламентується порядок захисту інформації в АС.

6.3 Загальна характеристика автоматизованої системи і умов її функціонування

В підрозділі рекомендується зазначити такі моменти, які впливають на безпеку інформації під час її оброблення в АС та на загальні вимоги до реалізації СЗІ:

загальну структурну схему і склад ОС АС (перелік і склад устаткування, технічних і програмних засобів, їх зв'язки, особливості конфігурації і архітектури, особливості підключення до локальних або глобальних мереж тощо);

технічні характеристики каналів зв'язку (пропускна спроможність, типи кабельних ліній, види зв'язку з віддаленими сегментами АС і користувачами і т. ін.);

характеристики інформації, що обробляється (категорії інформації, вищий гриф секретності і т. ін.);

характеристики персоналу (кількість користувачів і категорій користувачів, форми допуску тощо);

характеристики фізичного середовища (наявність категоризованих приміщень, територіальне розміщення компонентів АС, їх фізичні параметри, вплив на них чинників навколишнього середовища, захищеність від засобів технічної розвідки і т.п.);

загальну технічну характеристику АС (обсяги основних інформаційних масивів і потоків, швидкість обміну інформацією і продуктивність системи під час розв'язання функціональних завдань, тривалість процедури підготовки АС до роботи після подачі живлення на її компоненти, тривалість процедури відновлення працездатності після збоїв, наявність засобів підвищення надійності і живучості і т. ін.);

особливості функціонування АС (надання машинного часу або устаткування в оренду стороннім організаціям, цілодобовий режим роботи без відключення живлення тощо);

особливості реалізованих або припустимих заходів організаційних, фізичних та інших заходів захисту (режимні заходи в приміщеннях і на території, охорона, сигналізація, протипожежна охорона і т. ін.);

інші чинники, що впливають на безпеку оброблюваної інформації;

потенційні загрози інформації (способи здійснення НСД, можливі технічні канали

витоку інформації і умови їх формування, стихійні лиха і т. ін.), а також можливі наслідки їх реалізації;

клас АС згідно з НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні класи захищеності оброблюваної інформації від несанкціонованого доступу".

Крім того, треба описати функціонуючі в складі АС (для існуючої АС) засоби захисту, а також засоби захисту, реалізовані в компонентах, які планується використовувати для побудови АС. При цьому треба враховувати, що функції захисту, які реалізуються засобами імпортного виробництва, не мають зв'язаного з ними рівня гарантій. Використання таких засобів у складі КСЗІ можливе тільки за наявності експертного висновку, зареєстрованого Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України.

В підрозділі не вказуються ті характеристики і умови функціонування АС, опис яких є в ТЗ на АС або в інших документах. Даються тільки посилання на розділи цих документів.

6.4 Вимоги до комплексної системи захисту інформації

6.4.1 Вимоги до комплексної системи захисту інформації в АС в частині захисту від несанкціонованого доступу

Вимоги до комплексної системи захисту інформації в АС в частині захисту від НСД мають бути викладені відповідно до НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності комп'ютерних систем від несанкціонованого доступу" (далі - Критерії). Згідно з цим документом в процесі оцінки захищеності КС розглядаються вимоги двох видів: вимоги до функцій (послуг) забезпечення безпеки і вимоги до рівня гарантій. Відповідно, в ТЗ на КСЗІ повинні бути зазначені вимоги обох видів.

Має бути вказаний функціональний профіль захищеності, який передбачається реалізувати. Профіль може бути або вибраний із профілів, описаних в НД ТЗІ 2.5-005-99, або визначений як упорядкована сукупність рівнів послуг згідно з вимогами зазначеного документа. Повинен бути вказаний рівень гарантій, що передбачається досягти.

Опису послуг має передувати опис політики безпеки інформації, яку повинен реалізувати комплекс засобів захисту ОС АС. Опис політики безпеки має включати в себе опис:

об'єктів (елементів ресурсів) ОС;

принципів керування доступом користувачів до інформації (довірче і/або адміністративне керування доступом);

правил розмежування інформаційних потоків;

правил маркірування носіїв інформації;

основних атрибутів доступу користувачів, процесів і пасивних об'єктів;

правил розмежування доступу користувачів і процесів до пасивних об'єктів;

правил адміністрування КЗЗ і реєстрації дій користувачів;

інші загальні моменти політики безпеки, які вважає за потрібне описати розробник ТЗ.

Вимоги до послуг безпеки мають бути викладені і згруповані в тому порядку і стилі, в якому вони подані в Критеріях. В розділі мають бути викладені вимоги до реалізації послуг забезпечення:

конфіденційності;
цілісності;
доступності;
спостереженості.

Для кожної включеної до розділу послуги відповідно до Критеріїв має бути визначений рівень послуги, який передбачається реалізувати. Має бути описана політика даної послуги: визначення об'єктів, до яких застосовується дана послуга, і правил (в тому числі, що застосовуються за умовчуванням), відповідно до яких повинні функціонувати механізми, що реалізують послугу. Відповідно до особливостей розроблюваної АС мають бути конкретизовані всі вимоги, що викладені в Критеріях для відповідного рівня кожної послуги.

У разі, якщо передбачається реалізувати послуги безпеки, які не зазначені в Критеріях, їх також необхідно описати, дотримуючись, по можливості, стилю, прийнятого для опису інших послуг.

Вимоги до гарантій також мають бути викладені і згруповані в тому порядку і стилі, як вони подані в Критеріях. Це передбачає включення вимог:

до архітектури КЗЗ (додатково до загальних вимог до архітектури на даному етапі бажано визначити основні модулі (підсистеми), з яких повинен складатися КЗЗ);

до середовища розробки (організації процесу розробки і системи керування конфігурацією);

до гарантій проектування (етапності розробки і проектної документації);

до середовища функціонування;

до експлуатаційної документації;

до випробувань комплексу засобів захисту.

Всі вимоги повинні відповідати належному рівню гарантій.

Оскільки деякі з вимог гарантій стосуються розроблюваної системи в цілому, а не тільки КЗЗ, то в даному розділі допускається дати посилання на інші підрозділи ТЗ. Зокрема, вимоги до етапності розробки і складу документації мають бути визначені в розділах "Вимоги до складу проектної та експлуатаційної документації" та "Етапи виконання робіт". Крім того, допускаються посилання на інші документи, що розробляються на більш пізніх етапах.

6.4.2 Вимоги до комплексної системи захисту інформації в АС в частині захисту від витоку інформації технічними каналами

Мають бути сформульовані загальні вимоги до об'єктів (компонентів АС), що захищаються, визначені засоби захисту і засоби їх використання (наприклад, реалізація вимог до захищеності повинна досягатись без застосування екранування приміщень, активні засоби мають застосовуватись тільки для захисту інформації головного сервера АС і т. ін.).

Наводиться перелік нормативних і методичних документів, відповідно до яких повинні проводитись роботи щодо захисту інформації від витоку технічними каналами.

Мають бути вказані вимоги до розмірів зони безпеки інформації.

Мають бути вказані необхідні величини показників захищеності, що враховують реальну заводську обстановку на об'єкті електронної обчислювальної техніки. Основними показниками є:

відношення величин електричної і магнітної складових напруженості поля побічних електромагнітних випромінювань до рівня завад на об'єкті ЕОТ;

відношення величини напруженості інформативного сигналу в провідних комунікаціях на межі зони безпеки інформації до рівня завад на об'єкті ЕОТ;

величина нерівномірності струму, який споживається по мережі електроживлення;

коефіцієнт екранування засобів обчислювальної техніки, в тому числі від впливу зовнішніх ЕМВ.

Гранично допустимі значення основних показників є нормованими величинами і визначаються за відповідними методиками.

Відношення розрахованих (вимірних) значень основних показників до гранично допустимих (нормованих) значень визначають необхідні умови захисту інформації.

Мають бути вказані вимоги щодо застосування способів, методів і засобів досягнення необхідних показників захищеності. Рекомендується застосування таких способів, методів і засобів:

а) системо- і схемотехнічних методів:

обмеження використання інтерфейсів з передачею сигналів у вигляді послідовного коду і в режимі багатократних повторень;

використання мультиплексних режимів обробки інформації, а також ЗОТ і системного забезпечення, що базуються на багаторозрядних платформах, інтерфейсів з передачею сигналів у вигляді багаторозрядного паралельного коду;

використання раціональних способів монтажу, за яких забезпечується мінімальна довжина електричних зв'язків і комунікацій;

використання ЗОТ і технічних засобів, до складу яких входять стійкі до самозбудження схеми, розв'язувальні і фільтрувальні елементи, комплектуючі з низькими рівнями ЕМВ;

використання мережевих фільтрів для блокування витоку ІзОД мережами електроживлення, а також лінійних (високочастотних) фільтрів для блокування витоку ІзОД лініями зв'язку;

використання ЗОТ і технічних засобів у захисному виконанні;

б) засобів просторового і лінійного "зашумлення";

в) засобів локального або загального екранування;

г) засобів оптимального розміщення ЗОТ і технічних засобів з метою мінімізації зони, в межах якої граничне відношення сигнал/шум не перевищує встановлених норм.

Мають бути вказані вимоги до проведення спецдосліджень ЗОТ і технічних засобів, мета яких — пряме вимірювання показників ЕМВ.

Мають бути вказані вимоги до проведення спецперевірки ЗОТ, мета якої — виявлення та вилучення (блокування) спеціальних електронних (закладних) пристроїв.

6.5 Вимоги до складу проектної та експлуатаційної документації

В цьому розділі слід навести перелік проектної та експлуатаційної документації, що розробляється в процесі створення КСЗІ в АС.

Склад обов'язкової проектної і експлуатаційної документації визначається вимогами нормативних документів, відповідно до яких проводиться розробка (зокрема, вимогами Критеріїв для відповідного рівня гарантій). Повний перелік необхідної документації визначається розробником КСЗІ і погоджується із замовником.

6.6 Етапи виконання робіт

Процес створення КСЗІ доцільно поділяти на три основні етапи: попередній, проектування і розробки КСЗІ, проведення випробувань і передачі в експлуатацію КСЗІ. Кожний з етапів допускається поділяти на окремі підетапи.

Приблизний перелік основних робіт, що проводяться на попередньому етапі, наведено в підрозділі 5.

До переліку робіт етапу проектування і розробки КСЗІ включаються роботи з вибору і модернізації штатних засобів захисту ПЗ і апаратури, що використовуються, архітектури ЗОТ, стандартних інтерфейсів і протоколів обміну, а також з розробки додаткового ПЗ і апаратної частини засобів захисту.

Етап випробувань і передачі в експлуатацію КСЗІ містить роботи, пов'язані з забезпеченням організації та проведення випробувань, включаючи, в разі необхідності, розробку спеціальної апаратури, ПЗ і відповідної документації.

Всі основні роботи кожного етапу відображаються в календарному плані, де зазначаються терміни проведення робіт за окремими етапами, види звітності і форми подання результатів замовнику.

6.7 Порядок внесення змін і доповнень до технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі

Зміни затвердженого ТЗ на створення КСЗІ в АС, необхідність внесення яких виявлена в процесі виконання робіт, оформляються окремим доповненням, яке погоджується і затверджується в тому ж порядку і на тому ж рівні, що і основний документ.

Доповнення до ТЗ на створення КСЗІ в АС складається з вступної частини і змінюваних підрозділів. У вступній частині зазначається причина випуску доповнення. В змінюваних підрозділах наводяться номери та зміст змінюваних, нових або пунктів, що скасовуються.

6.8 Порядок проведення випробувань комплексної системи захисту інформації

Для кожного виду випробувань (попередніх, державних, сертифікаційних та ін.) комплексної системи (підсистеми, компонента) захисту виконавець розробляє "Програму і методику випробувань комплексної системи (підсистеми, компонента) захисту інформації в АС", яка затверджується в установленому порядку. Терміни подання проекту Програми, його розгляду і затвердження погоджуються з замовником.

Для проведення випробувань замовником призначається комісія, склад якої погоджується з розробником КСЗІ.

Випробування проводяться з використанням умовної інформації (що не є ІЗОД).

Наводиться необхідне для проведення випробувань забезпечення (необхідна нормативна, методична та інша документація, програмні та технічні засоби, метрологічне, спеціальне та інше обладнання, створення інших умов для проведення випробувань), сторона, що його надає, порядок усунення зауважень і т.ін.

Наводиться перелік документів, якими завершуються випробування (етапи випробувань): акт приймання, сертифікат (атестат, експертний висновок) відповідності встановленим критеріям, наказ про введення в експлуатацію тощо.