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

Зі Зміною №1, затвердженою наказом Департаменту СТСЗІ СБ України від 18.06.02 №37

із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806

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.

Зміст

1 Галузь використання 5
2 Нормативні посилання 5
3 Визначення 6
4 Позначення і скорочення 6
5 Загальні вимоги до розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі 6
5.1 Загальні положення 6
5.2 Порядок розроблення технічного завдання 7
5.3 Зміст технічного завдання 8
6 Вимоги до змісту розділів технічного завдання 8
6.1 Загальні відомості 8
6.2 Мета і призначення комплексної системи захисту інформації 9
6.3 Загальна характеристика автоматизованої системи і умов її функціонування 9
6.4 Вимоги до комплексної системи захисту інформації 10
6.4.1 Вимоги до комплексної системи захисту інформації в АС в частині захисту від несанкціонованого доступу 10
6.4.2 Вимоги до комплексної системи захисту інформації в АС в частині захисту від витоку інформації технічними каналами 11
6.5 Вимоги до складу проектної та експлуатаційної документації 13
6.6 Етапи виконання робіт 13
6.7 Порядок внесення змін і доповнень до технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі 13
6.8 Порядок проведення випробувань комплексної системи захисту інформації 13
7 Приклад побудови технічного завдання на створення комплексної системи захисту інформації 14

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

Чинний з 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, яка належить до державних інформаційних ресурсів, або інформацією, вимога щодо захисту якої встановлена законом. Власники (користувачі) іншої інформації, положення цього документа застосовують на свій розсуд.

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:

Закон України "Про інформацію ".

Положення про технічний захист інформації в Україні.

НД ТЗІ1.1-003-99. Термінологія у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

---

* 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.

НД ТЗІ2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

НД ТЗІ2.5-005-99. 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.

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 розроблятись 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.

Приклад побудови технічного завдання на створення комплексної системи захисту інформації в АС, який спрямований на надання методичної допомоги власникам АС, наведено в доповненні.

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 захисту інформації від витоку технічними каналами визначаються на підставі нормативних документів з технічного захисту інформації, якими встановлено норми захищеності інформації від витоку технічними каналами та порядок виконання відповідних робіт.

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 спец перевірок і спец досліджень 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. У випадках, передбачених Положенням про технічний захист інформації в Україні, ТЗ на КСЗІ погоджується Адміністрацією Державної служби спеціального зв'язку та захисту інформації.

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 категорованих 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 Адміністрацією Державної служби спеціального зв'язку та захисту інформації 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 завадову 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 (виміряних) 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.

7 Приклад побудови технічного завдання на створення комплексної системи захисту інформації

Доповнення
до НД ТЗІ 3.7-001-99
Зміна № 1

Доповнення до НД ТЗІ 3.7-001-99 являє собою зразок технічного завдання на створення КСЗІ в теоретичній автоматизованій системі. Розділи технічного завдання містять певну множину вимог, характерних для більшості КСЗІ реальних автоматизованих систем і, в той же час, мають відкриту форму. Відкрита форма розділів ТЗ найбільш сприяє досягненню мети Доповнення – не базуючись на конкретній архітектурі АС, надати наочний приклад ТЗ на створення КСЗІ в АС, розробленого з використанням методичних вказівок основної частини НД ТЗІ.

Власникам АС рекомендуємо утримуватися від використання змісту Доповнення як "трафарету" під час розробки технічних завдань на створення КСЗІ в АС, що мають чітко визначені архітектуру, функціональне призначення, фізичне середовище експлуатації, персонал, технологію обробки інформації, мережу передачі даних і т.п.

УЗГОДЖЕНО	ЗАТВЕРДЖУЮ
…….	…….
…….	…….
М.П.	М.П.
"____"_____ 200_ р.	"____"_____ 200 _ р.

АВТОМАТИЗОВАНА СИСТЕМА

.....

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ

Технічне завдання

(Часткове технічне завдання)

……. – 200_ р.

З М І С Т

Стор.

1 Перелік скорочень 18

2 Терміни та визначення 19

3 Загальні відомості 20

4 Мета і призначення комплексної системи захисту інформації 20

5 Загальна характеристика АС та умови функціонування 21

6 Вимоги до комплексної системи захисту інформації 23

6.1 Загальні вимоги. 23

6.2 Вимоги до КСЗІ в частині захисту від несанкціонованого доступу 25

6.2.1 Вимоги до функціональних послуг 26

6.3 Вимоги до гарантій 28

6.3.1 Вимоги до гарантій архітектури КЗЗ 28

6.3.2 Вимоги до гарантій середовища опрацювання 29

6.3.3 Вимоги до гарантій проектування 29

6.3.4 Вимоги до гарантій середовища функціонування 29

6.3.5 Вимоги до гарантій експлуатаційної документації 30

6.3.6 Вимоги до гарантій випробувань комплексу засобів захисту 30

6.4 Вимоги до криптографічної підсистеми 31

6.5 Вимоги до КСЗІ в частині захисту від витоку технічними каналами 31

6.5.2 Вимоги до кіл заземлення АС 32

6.5.3 Вимоги до структурованої кабельної мережі АС 32

7 Вимоги до складу проектної та експлуатаційної документації КСЗІ 32

8 Етапи виконання робіт 33

9 Порядок внесення змін і доповнень до ТЗ 33
10 Порядок проведення випробувань комплексної системи захисту 34
інформації 34

1 Перелік скорочень

АРМ - автоматизоване робоче місце;
АС - автоматизована система;
ЕОТ - електронно-обчислювальна техніка;
ІзОД - інформація з обмеженим доступом;
КЗЗ - комплекс засобів захисту;
КЗІ - криптографічний захист інформації;
КСЗІ - комплексна система захисту інформації;
ЛОМ - локальна обчислювальна мережа;
НД ТЗІ - нормативний документ системи технічного захисту інформації;
НСД - несанкціонований доступ;
ОС - операційна система;
ПЗ - програмне забезпечення;
ТЗ - технічне завдання;
….. - ……
….. - ……

2 Терміни та визначення

У цьому ТЗ використовуються терміни та визначення згідно з ДСТУ 3396.2-97, ДСТУ….., НД ТЗІ 1.1-003-99 "Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу", а також такі терміни та визначення:

….. -……;

….. -……;

….. -…… .

3 Загальні відомості

Це технічне завдання визначає вимоги до комплексу організаційних та технічних заходів щодо забезпечення захисту інформації в автоматизованій системі (АС) ……

Умовне позначення АС:……

Шифр: …… Договір: ……

Замовник - **……**

Виконавець - **……**

Початок робіт: ……Закінчення: ……

Підстава для розробки: ……

Фінансування роботи здійснюється за рахунок ……

Технічне завдання на комплексну систему захисту інформації оформлено відповідно до ДСТУ……, НД ТЗІ ……. .

4 Мета і призначення комплексної системи захисту інформації

Метою створення комплексної системи захисту інформації є забезпечення безпеки критичної інформації в процесі оброблення її засобами АС …… . Захист інформації повинен забезпечуватися на всіх технологічних етапах обробки критичної інформації і в усіх режимах функціонування.

Процес оброблення інформації складається з таких технологічних етапів:

формалізації первинної інформації, одержаної від …….., а також …… та зберігання її в локальних базах даних у вигляді блоків даних;

використання формалізованої, накопиченої ..…… інформації процедурами ……, …….. прикладного програмного забезпечення ……. для вирішення функціональних завдань АС щодо **…….;**

обміну блоками даних між окремими автоматизованими робочими місцями та локальними …… АС каналами структурованої кабельної системи передачі даних під час ……;

обміну блоками даних (зашифрованих даних) між …….. та віддаленими автоматизованими робочими місцями і локальними …… АС каналами зв'язку загального користування;

…….. .

Для забезпечення безпеки інформації на всіх стадіях життєвого циклу АС комплексна система захисту інформації передбачає застосування таких заходів та засобів захисту інформації:

організаційні заходи, що реалізуються поза обчислювальною системою АС;

програмно-апаратні засоби захисту від несанкціонованого доступу;

запобігання витоку інформації технічними каналами;

захисту інформації під час передавання/приймання її каналами зв'язку;

…….. .

КСЗІ в АС призначена для:

захисту інформації з обмеженим доступом від витоку її технічними каналами;

керування доступом користувачів до інформаційних ресурсів АС;

розмежування доступу користувачів АС до інформації різних категорій конфіденційності;

блокування несанкціонованих дій з критичною інформацією;

створення багаторівневого захисту інформаційних ресурсів АС від атак;

контролю та захисту внутрішніх і зовнішніх потоків інформації, яка обробляється розподіленою обчислювальною системою АС;

реєстрації спроб реалізації загроз інформації та оперативного сповіщення адміністраторів безпеки про факти несанкціонованих дій з інформацією обмеженого доступу;

…….. .

…… ….. .

Нормативно-правовою базою щодо захисту інформації та створення КСЗІ АС …… є Закони України "Про інформацію", "Про державну таємницю", "Про захист інформації в інформаційно-телекомунікаційних системах", ……., державні стандарти …… та нормативні документи системи ТЗІ в Україні, а також …… .

5 Загальна характеристика АС та умови функціонування

Згідно з НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу" АС …… відноситься до …. класу, як …… .

Призначення АС:

автоматизація обробки ……інформації……в галузі……;

моделювання процесів утворення ……в залежності від……;

організація та наповнення інтегрованої бази даних ……;

прогноз розвитку ……, а також оцінка …….;

……;

…… .

Найвищий гриф інформації, що буде оброблятися засобами АС та передаватися каналами зв'язку, - …….

Режим обробки інформації з найвищим грифом:

при ..... - постійний;

при .....- одноразовий, нерегулярний.

До складу АС входять:

головний інформаційно-аналітичний підрозділ.....;

інформаційно-аналітичні підрозділи.....;

регіональні інформаційно-аналітичні підрозділи.....;

…… .

Інформаційний ресурс АС являє собою …… При цьому …… необхідні і достатні для вирішення завдань щодо забезпечення …… . У складі АС …… виконують функції збору, формалізації, накопичення, обробки та передачі інформації.

Засоби АС повинні забезпечувати такі види інформаційних зв'язків:

обмін інформацією між ……;

обмін інформацією згідно ……;

……;

…… .

Принципи організації інформаційних зв'язків ……:

……сприймає на себе і контролює всі вихідні інформаційні потоки від ……, які організаційно і функціонально залежать від даного рівня управління;

…… - є джерелом інформації для ……;

……, що є постачальником інформації у ……, самостійно формує відповідні інформаційні повідомлення;

……, ……та ……мають доступ до …… безпосередньо підпорядкованих їм АРМ для обробки і поповнення власних ……. необхідними відомостями;

перевірка повноважень зовнішніх стосовно …… користувачів за правом доступу до …… здійснюється в рамках …… .

Базовими елементами …… є автоматизовані робочі місця, що повинні забезпечувати постачання частково формалізованої та структурно упорядкованої (уніфікованої) первинної інформації для …… .Технологічною основою для розгортання …… є …… IBM-PC - сумісні ПЕОМ.

За необхідністю окремі …… можуть оснащуватися спеціалізованими автоматизованими засобами обробки (передачі) інформації (у тому числі мобільними). Такі спеціалізовані засоби можуть тимчасово та/або постійно встановлюватися в ……. Крім того, ці засоби можуть використовуватися для тимчасового або постійного підключення до …… . …… можуть мати постійний або тимчасовиий зв'язок із ……, які вже функціонують або будуть розроблятися в майбутному .

Головним елементом АС є ……, розгорнутий на базі …… . Решта елементів АС будуть знаходитись в …… .

…… АС повинні мати виходи на …… .

Комунікаційні засоби функціональних вузлів працюють цілодобово без вимкнення живлення (….. годин на добу з подальшим вимкненням живлення). Технічні засоби АРМ функціональних вузлів допускають їх цілодобову роботу без вимкнення живлення (….. годин на добу з подальшим вимкненням живлення).

Базове програмне забезпечення АРМ складається з:

мережевої операційної системи …… ;
системи керування базами даних …….. ;
спеціального програмного забезпечення ……. ;
……

6 Вимоги до комплексної системи захисту інформації

6.1 Загальні вимоги.

Архітектура АС повинна дозволяти розв'язання функціональних завдань у замкненому середовищі. Структура мережі, розподіл потоків даних повинні забезпечувати мінімально можливий час передачі критичної інформації між локальними сегментами мережі.

Робота АС у штатних режимах повинна бути можливою лише за умови функціонування системи захисту інформації.

Розташування, монтаж та прокладку інженерно-технічних комунікацій АС, в тому числі систем заземлення та електроживлення технічних засобів, які приймають участь у обробці інформації, необхідно виконувати з дотриманням вимог відповідних стандартів та нормативних документів системи ТЗІ.

Організаційні та підготовчі заходи щодо технічного захисту інформації повинні проводитися одночасно і складати перший етап робіт зі створення КСЗІ, на якому повинні бути виявлені потенційні загрози безпеці інформації.

Під час проведення обстеження приміщень, технічних засобів та систем забезпечення інформаційної діяльності АС ……необхідно, по-перше, виконати роботи з дослідження можливостей витоку інформації внаслідок роботи основних технічних засобів перетворення (обробки, зберігання, відображення) інформації, …… (ТЗПІ) та допоміжних технічних засобів та систем (ДТЗС). (Конкретний перелік ТЗПІ та ДТЗС надається Замовником).

По-друге, як джерела витоку ІзОД також повинні бути розглянуті ланки передачі інформації, ланки електроживлення, заземлення, керування та сигналізації, а також ланки, створені паразитними зв'язками, конструктивними елементами будівель, споруд, устаткування та інше.

По-третє, необхідно провести дослідження засобів обчислювальної техніки, які формують, передають, приймають, перетворюють, відображають та зберігають ІзОД, щодо наявності технічних каналів витоку інформації шляхом побічних електромагнітних випромінювань та наводок (ПЕМВН).

Неформалізована модель загроз для інформації (додається), яка розроблена із врахуванням результатів обстеження приміщень, технічних засобів та систем забезпечення інформаційної діяльності АС, включає:

ситуаційний план розташування структурних елементів АС із зазначенням місць розташування технічних засобів та систем обробки інформації і життєзабезпечення, джерел електроживлення, контурів заземлення, енергетичних мереж, а також інженерних комунікацій, що виходять за межі зони безпеки інформації;

опис можливих технічних каналів витоку інформації та впливу на неї;

опис можливих способів реалізації несанкціонованого доступу до інформації;

оцінку обсягів можливих збитків від реалізації загроз безпеці інформації;

……..

……..

Для реалізації частини політики безпеки інформації, яка покладається на технічні заходи і відповідає реальній моделі загроз, КЗЗ повинен мати такі функціональні можливості:

забезпечення входу в систему та завантаження операційної системи на робочій станції за умови пред'явлення електронного ідентифікатора і/або введення особистого паролю;

контроль за вводом інформації в АС та інсталяцією програмного забезпечення;

контроль за виведенням інформації на носії, що вилучаються;

підтримка функцій адміністратора захисту інформації в АС;

реєстрація дій користувачів по відношенню до ресурсів системи;

забезпечення цілісності інформаційних ресурсів (у тому числі і антивірусний захист);

перевірка цілісності та роботоздатності КСЗІ;

надання користувачам прав доступу до ресурсів АС згідно прийнятої політики безпеки, та їх ліквідація по закінченню строку дії;

багаторівневе розмежування повноважень персоналу АС по відношенню до ресурсів АС;

контроль за запуском процесів та іх виконанням;

автоматичне блокування екрану робочої станції на час відсутності користувача;

заборона роботи зареєстрованим користувачам у невідведений час;

шифрування інформації, автентифікація повідомлень і підтвердження їх походження при передачі каналами зв'язку;

……;

…….

Виконання завдань повинне здійснюватися зареєстрованими користувачами у функціонально замкненому середовищі із забезпеченням доступу до ресурсів, що обмежені рамками завдань.

Програмне забезпечення АРМ користувачів повинне містити програмні модулі захисту, що забезпечують взаємодію із сервером захисту для реалізації функціональних послуг безпеки.

……
……

Для керування КСЗІ у складі АС повинно бути передбачено АРМ адміністратора безпеки. Аналогічні АРМ повинні включатися до складу віддалених сегментів АС. Вказані АРМ (а також сервери захисту та інші мережні сервери) повинні розташовуватися у виділених приміщеннях із дотриманням необхідних організаційних заходів.

Введення інформації з магнітних носіїв, де це технологічно необхідно, має здійснюватися на виділених робочіх місцях, із вжиттям відповідних організаційних заходів.

……
……

КСЗІ повинна забезпечувати підтримку:

не менше ……. категорій таємності інформації;

не менше …… рівнів повноважень користувачів;

роботи не менше …… користувачів та …….груп користувачів.

……
……
…

Комплексна система захисту інформації повинна реалізовуватися як сукупність узгоджених за часом та місцем застосування організаційних, підготовчих технічних і технічних заходів.

Організаційні заходи повинні включати:

визначення та встановлення обов'язків із захисту інформації підрозділів та осіб, що приймають участь в обробці інформації;

визначення технологічних процесів обробки інформації з урахуванням вимог із захисту інформації;

встановлення порядку впровадження та модернізації засобів обробки інформації, програмних та технічних засобів захисту інформації;

організацію фізичного та протипожежного захисту АС;

розробку правил та порядку контролю функціонування КСЗІ;

……
……

Під час створення КЗЗ для забезпечення вимог щодо захисту інформації повинні використовуватися засоби технічного захисту інформаціїї з "Переліку засобів технічного захисту інформації загального призначення", затвердженого ДСТСЗІ СБ України або розроблятися та реалізовуватися спеціальні засоби ТЗІ, як невід'ємна частина АС .

6.2 Вимоги до КСЗІ в частині захисту від несанкціонованого доступу

Нейтралізація загроз несанкціонованого доступу до інформації в АС ……. повинна забезпечуватися реалізацією КЗЗ політики функціональних послуг, які визначаються профілем захищеності АС від НСД.

Функціональний профіль захищеності -….КЦД…. = { КД-.., КА-.., КО-…, КК-…, КВ-…, ЦД-…, ЦА-…, ЦВ-…, ДР-…, ДС-…, ДЗ-…, ДВ-…, НР-…, НК-…, НО-…, НЦ-…, НТ-…, НВ-…, НА-…, НП-…}, для АС …-го класу з підвищеними вимогами до забезпечення конфіденційності, цілісності і доступності оброблюваної інформації визначено згідно з НД ТЗІ 2.5-005-99 "Класифікація…….".

Реалізація політики функціональних послуг та виконання основних функцій АС здійснюється за участтю активних та пасивних об'єктів.

До активних об'єктів відносяться користувачі АС. Користувачі АС поділяються за функціональними обов'язками на:

користувачів;

користувачів із повноваженнями ……;

адміністраторів безпеки;

адміністраторів баз даних;

……. .

До пасивних об'єктів відносяться:

процеси;

файлова система;

програмне забезпечення ;

пристрої введення/виведення (НГМД, CD ROM, …..);

……. .

Основними атрибутами доступу користувачів є:

ім′я користувача (групи користувачів);

пароль;

……. .

6.2.1 Вимоги до функціональних послуг

Важливим етапом розробки ТЗ на створення КСЗІ є викладення вимог до функціональних послуг, які визначено профілем захищеності АС на попередніх етапах. Специфікація вимог до функціональних послуг в залежності від їх рівня надається у НД ТЗІ 2.5-004-99 "Критерії…" і є переліком саме тих вимог, що конкретизуються шляхом визначення об'єктів, атрибутів доступу, інформаційних потоків, інформації та подій для журналу реєстрації, …….. .

Як зразок наводиться опис політики функціональних послуг **КА-2.**, **НР-2.**, **НТ-2.** та **ДВ-1**.

КА-2. Базова адміністративна конфіденційність.

Політика реалізації послуги, яка реалізується КЗЗ, повинна розповсюджуватися на наступні об’єкти захисту: файли даних різних форматів, бази даних, що зберігаються на магнітних носіях великої ємності (жорсткі диски, з’ємні магнітні, магніто-оптичні диски тощо) та містять дані різних категорій обмеження доступу, а також на файли бази даних системи захисту, файли ведення захищеного журналу реєстрації подій, функціональні програми обробки даних з обмеженим доступом, порти введення-виведення інформації з/на ГМД та периферійні пристрої АРМ, що входять до АС.

Розмежування доступу користувачів до об’єктів захисту повинне здійснюватися на підставі атрибутів об’єктів, що характеризують категорію обмеження доступу даних, які в них зберігаються, та атрибутів користувачів,

що характеризують їх права доступу (рівень допуску та повноваження стосовно доступу).

Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів, яким надані відповідні повноваження.

КЗЗ повинен надавати можливість адміністратору безпеки для кожного процесу, який використовується для обробки даних з обмеженим доступом, визначити конкретних користувачів і/або групи користувачів, які мають право його ініціювати. Права доступу для кожного об’єкту захисту повинні встановлюватися в момент його створення.

КЗЗ повинен при виведенні даних з обмеженим доступом на паперовий носій забезпечувати можливість друку на кожній сторінці (аркуші) реквізитів паперового документу, до складу яких повинні входити гриф обмеження доступу, номер сторінки, ідентифікатор АС, ідентифікатор файлу, бази даних тощо, звідки здійснюється друк документу. На останньому аркуші документу додатково зазначається загальна кількість сторінок у документі, дата друкування.

НР-2. Захищений журнал.

КЗЗ повинен бути здатним здійснювати реєстрацію таких подій, що мають безпосереднє відношення до безпеки:

вхід/вихід користувача в систему (ім'я користувача, дата, час);

реєстрація та видалення з системи користувачів (ім'я користувача, дата, час);

зміна паролю (ім'я користувача, дата, час);

зміна прав та повноважень доступу до файлів, ресурсів БД: полів, записів, форм, запитів, звітів тощо (ім'я користувача, дата, час, значення атрибутів доступу);

виведення документу на принтер (ім'я користувача, ідентифікатор файлу, дата, час);

створення, доступ та знищення файлів, БД (ім'я користувача, ідентифікатор файлу, звіт, запит, форма БД, дата, час);

запуск прикладних програм (процесів) (ім'я користувача, ім’я програми, дата, час);

виявлення фактів порушення цілісності КЗЗ (код порушення, ім'я користувача, дата, час).

КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого ознайомлення, модифікації або знищення.

Адміністратори, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації.

НТ-2. Самотестування при старті.

Політика самотестування, що реалізується КЗЗ, повинна описувати властивості АС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ.

З метою оцінки правильності функціонування АС КЗЗ повинен бути спроможним виконувати тести:

апаратної частини сервера та АРМ;

програмної частини сервера та АРМ;

кабельної мережі;

комплексної системи захисту.

Тести апаратної та програмної частин сервера, АРМ та кабельної мережі повинні виконуватися також за запитами адміністратора мережі.

Тести комплексної системи захисту повинні виконуватися також за запитом адміністратора комплексної системи захисту.

ДВ-1. Ручне відновлення.

До переліку подій, після здійснення яких КЗЗ має переводити АС у стан блокування подальшої роботи, повинні бути включені відмови або переривання процесів завантаження АС, ініціації та перевірки цілісності КЗЗ, процедур автентифікації користувачів, процедур ведення журналу реєстрації подій.

Повернення АС до нормального функціонування може бути здійснено тільки після втручання адміністратора безпеки або користувачів, яким надані відповідні повноваження.

Повторна інсталяція КЗЗ можлива після копіювання адміністратором безпеки журналу подій на ГМД для проведення аналізу можливих фактів порушень політики безпеки. Інсталяція КЗЗ здійснюється адміністратором АС за участю адміністратора безпеки. За результатами робіт складається відповідний акт.

…-… ……

…….

…… .

6.3 Вимоги до гарантій

Вимоги до гарантій повинні формуватися на основі критерію Г…, визначеного власником АС у відповідності до НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу".

Ці вимоги спрямовані на забезпечення структурованості комплексу засобів захисту у відповідності до принципів модульності, ……. і приховування даних.

6.3.1 Вимоги до гарантій архітектури КЗЗ

Архітектурна КЗЗ повинна бути у змозі повністю реалізувати частину обраної політики безпеки і складатися із достатньо визначених і максимально

незалежних програмних і/або програмно-апаратних компонентів (модулів), які ідентифікуються.

Під час створення КЗЗ необхідно мінімізувати набір модулів та врахування особливостей взаємодії всіх елементів АС, які мають відношення до обробки критичної інформації.

У складі КЗЗ виділити ядро захисту та зовнішній інтерфейс доступу до функціональних послуг.

Структура модулів повинна дозволяти тестування КЗЗ на рівні функціонально-завершених вузлів.

……...……
……
… .

6.3.2 Вимоги до гарантій середовища опрацювання

Всі стадії життєвого циклу системи захисту інформації повинні бути документовані.

Програмні засоби КЗЗ повинні розроблятися в ліцензійно забезпеченому середовищі.

Всі залежні від реалізації параметри мов програмування та компіляторів повинні бути документованими.

……
…….

6.3.3 Вимоги до гарантій проектування

На стадії виконання технічного проекту Розробник повинен розробити проект архітектури КЗЗ. Представлений проект повинен містити перелік і опис компонентів КЗЗ і функцій, що реалізуються ними.

Документально оформити методики діяльності на кожному етапі життєвого циклу та умови переходу від одного етапу до наступного. Необхідно визначити процедури внесення змін та фіксувати всі зміни на кожному етапі.

Розробник повинен мати систему керування якістю, яка включає документовані методики керування розробкою програмного, апаратного, програмно-апаратного забезпечення.

……
…….

6.3.4 Вимоги до гарантій середовища функціонування

Розробник повинен представити засоби інсталяції, генерації і запуску АС, які гарантують, що експлуатація АС починається з безпечного стану. Розробник повинен представити перелік усіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації і запуску.

Повинна існувати система технічних, організаційних і фізичних заходів безпеки, яка гарантує, що програмне і програмно-апаратне забезпечення КЗЗ, що поставляється Замовнику, точно відповідає еталонній копії.

……
…….

6.3.5 Вимоги до гарантій експлуатаційної документації

У вигляді окремих документів або розділів (підрозділів) інших документів Розробник повинен надати опис послуг безпеки, що реалізуються КЗЗ, настанови адміністратора щодо послуг безпеки, настанови користувача щодо послуг безпеки.

В опису функцій безпеки повинні бути викладені основні, необхідні для правильного використання послуг безпеки, принципи політики безпеки, що реалізується КЗЗ, а також самі послуги.

Настанови адміністратора щодо послуг безпеки мають містити опис засобів інсталяції, генерації і запуску АС, опис усіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації і запуску АС, опис властивостей АС, які можуть бути використані для періодичної оцінки правильності функціонування КЗЗ, а також інструкції щодо використання адміністратором послуг безпеки для підтримки політики безпеки, прийнятої в організації, що експлуатує АС.

Настанови користувача щодо послуг безпеки мають містити інструкції стосовно використання функцій безпеки звичайним користувачем (не адміністратором).

Настанови адміністратора і настанови користувача можуть бути об'єднані в настанови з установлення та експлуатації.

……
…….

6.3.6 Вимоги до гарантій випробувань комплексу засобів захисту

Розробник повинен надати для перевірки програму і методику випробувань, процедури випробувань усіх механізмів, що реалізують послуги безпеки. Мають бути представлені аргументи для підтвердження достатності тестового покриття.

Розробник повинен надати докази тестування у вигляді детального переліку результатів тестів і відповідних процедур тестування із тим, щоб отримані результати могли бути перевірені через повторення тестування.

Розробник повинен усунути або нейтралізувати всі знайдені "слабкі місця" і виконати повторне тестування КЗЗ для підтвердження того, що знайдені недоліки були усунені і не з'явилися нові " слабкі місця".

……
……

……
……

6.4 Вимоги до криптографічної підсистеми

Для криптографічного захисту інформації, яка передається каналами зв'язку загального користування та службової інформації, використовувати алгорітми та криптографічні протоколи, які є державними стандартами України або рекомендовані ДСТСЗІ СБ України.

Тип криптографічного алгорітму для шифруваннння/дешифрування інформації і вимоги до його реалізації повинні відповідати ДСТУ……. (ГОСТ……..).

Тип криптографічного алгорітму для формування електронного підпису електронних документів і вимоги до його реалізації повинні відповідати ДСТУ……. (ГОСТ……..).

…… ……. …….. .

Криптографічна підсистема реалізується з обов'язковим дотриманням вимог "Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту конфіденційної інформації", затвердженого наказом № 53 ДСТСЗІ СБ України від 30.11.99 (оформлюється окремим частковим ТЗ).

6.5 Вимоги до КСЗІ в частині захисту від витоку технічними каналами

Для забезпечення захисту інформації від витоку технічними каналами провести аналіз технології оброблення інформації в АС, архітектури та розташування елементів АС; за його результатами визначити зони безпеки інформації та провести у відповідності з вимогами НД ТЗІ категоріювання приміщень АС і засобів обчислювальної техніки.

У відповідності до вимог чинних нормативних документів системи ТЗІ провести заходи щодо блокування витоку інформації та впливу на неї технічними каналами.

6.5.1 Вимоги до системи електроживлення АС …….

Електроживлення основних та допоміжних засобів ЕОТ локального сегменту АС здіснювати від трансформаторної підстанції низької напруги із заземлювальним пристроєм, розміщеної у межах контрольованої території.

Електроживлення окремих АРМ здійснювати через мережеві фільтри типу …….. .

Кола електроживлення прокладати екранованим кабелем окремо від проводів та кабелів, які виходять за межі контрольованої території.

…… …… .

6.5.2 Вимоги до кіл заземлення АС …….

Заземлювальні проводи від основних та допоміжних засобів ЕОТ до системи заземлення прокладати мідним дротом діаметром …найкоротшим шляхом.

Опір кола заземлення від засобу ЕОТ до вузла системи заземлення не повинен перевищувати ……. .

Система заземлення не повинна виходити за межі контрольованої території.

……

…… .

6.5.3 Вимоги до структурованої кабельної мережі АС …….

Комунікаційні елементи структурованої кабельної мережі (кросові панелі, розетки користувачів, кросові шафи, …….) розміщувати на контрольованій території. Монтажні шафи із активною апаратурою (концентратори, маршрутизатори, ……) повинні мати захист від несанкціонованого доступу до апаратури.

Для прокладання горизонтальної підсистеми використати мідні проводи, неекрановану звиту пару типу UTP cat 3.

Для прокладання вертикальної підсистеми використати одномодовий волоконно-оптичний кабель.

За межами контрольованої території волоконно-оптичний кабель прокладати у металевих трубах. Металеві труби не повинні мати гальванічний зв'язок із системою заземлення АС.

……

…… .

7 Вимоги до складу проектної та експлуатаційної документації КСЗІ

Проектна документація на комплексну систему (підсистеми) захисту інформації повинна включати:

- опис концепції захисту інформації;
- опис моделі захисту (неформальної);
- опис інтерфейсу КСЗІ і користувача та інтерфейсу між окремими модулями КСЗІ;
- опис застосованих технічних засобів захисту;
- опис реалізації механізмів, що забезпечують виконання вимог кожного з показників захищеності;
- ……

……..

Керівництво користувача - повине включати короткий опис механізмів захисту та інструкції із роботи з ними в процесі взаємодії користувача з АС.

Керівництво із системи захисту інформації призначене для забезпечення виконання функціональних обов'язків адміністратора системи захисту (служби захисту інформації в АС) і повинне включати:

- керівництво адміністратора захисту щодо керування захистом, керування та контролю за виконанням привілегійованих процесів під час функціонування АС;
- опис процедур роботи із засобами реєстрації;
- інструкції з розшифрування діагностичних повідомлень КСЗІ та аналізу аудиторських файлів;
- інструкції із супроводу копій програмного забезпечення КСЗІ, із перевірки його працездатності та тестування;
- опис процедур старту КСЗІ;
- опис процедур оперативного відновлення працездатності КСЗІ після збоїв;
- ……

Керівництво з тестування КСЗІ - повинне включати документацію розробника для служби захисту інформації в автоматизованій системі, яка містить опис порядку тестування та повний набір тестових процедур механізмів системи захисту інформації у відповідності до вимог заданого показника захищеності, а також результатів функціонального тестування.

8 Етапи виконання робіт

8.1 Стадія розробки технороботочого проекту КСЗІ АС ……

8.1.1 Проектування та створення КСЗІ.

8.1.2 Розробка (адаптація) програмних і апаратних засобів захисту інформації.

8.1.3 Розробка робочої документації на КСЗІ

8.1.4. Розробка і затвердження "Програми і методики" випробувань КСЗІ.

8.2 Стадія вводу в дію КСЗІ АС ……..

8.2.1. Проведення попередніх випробувань КСЗІ

8.2.2. Відпрацювання КСЗІ в процесі дослідної експлуатації

8.2.3. Проведення приймальних випробовувань КСЗІ

8.2.4. Підготовка персоналу

8.3 Проведення експертизи КСЗІ та отримання «Атестату відповідності».

9 Порядок внесення змін і доповнень до ТЗ

Зміни та доповнення до розділів ТЗ на комплексну систему захисту інформації в АС ……. оформлюються окремим доповненням, яке погоджується та затверджується у порядку погодження та затвердження самого ТЗ.

10 Порядок проведення випробувань комплексної системи захисту інформації

Для кожного виду випробовувань (попередніх, державних, сертифікаційних, атестаційних та інш.) системи захисту Виконавець розробляє "Програму та методику випробовувань комплексної системи захисту в АС", яка затверджується Замовником.

"Програму та методику випробовувань" розробити у відповідності до чинних ДСТУ.

Перевірка роботи КСЗІ АС повинна включати:

- випробовування підсистеми керування доступом;
- випробовування підсистеми реєстрації та обліку;
- випробовування криптографічної підсистеми;
- випробовування підсистеми забеспечення цілісності;
- випробовування підсистеми захисту від витоку інформації технічними каналами;
- випробовування підсистеми керування КСЗІ;
- …….

Для підсистеми керування доступом повинно бути перевірено:

- правильність роботи механізмів ідентифікації та автентифікації користувачів АС;
- правильність роботи механізмів ідентифікації та автентифікації інформаційних ресурсів АС;
- правильність роботи механізмів керування доступом користувачів до інформаційних ресурсів АС;
- правильність роботи механізмів керування потоками інформації згідно категорії її таємності;
- …….

Для підсистеми реєстрації та обліку стану ресурсів АС повинно бути перевірено:

- правильність роботи процедур реєстрації повідомлень щодо зміни стану інформаційних ресурсів АС та компонентів КСЗІ;
- правильність роботи механізмів очищення носіїв інформації, на яких під час роботи АРМ користувачів тимчасово зберігалась ІзОД;
- правильність роботи механізмів сповіщення адміністратора КСЗІ щодо спроб та фактів порушення правил доступу до інформаційних ресурсів АС;
- …….

Для криптографічної підсистеми повинно бути перевірено:

- правильність роботи механізмів генерації криптографічних ключів;
- правильність роботи механізмів шифрування/розшифрування ІзОД;
- правильність роботи механізмів захисту інформації в каналах зв’язку;
- правильність роботи механізмів формування цифрового підпису;
- …….

Для підсистеми забезпечення цілісності інформаційних ресурсів АС повинно бути перевірено:

- правильність роботи механізмів контролю цілісності програмних засобів захисту;
- правильність роботи механізмів контролю цілісності операційного середовища перед створенням процесів;
- правильність роботи механізмів контролю цілісності інформаційних ресурсів АС;
- правильність роботи механізмів тестування засобів захисту інформації;
- правильність роботи механізмів відновлення функцій системи захисту у випадку збою;
- ……...

Для підсистеми захисту від витоку інформації технічними каналами повинно бути перевірено:

- рівень побічного електромагнітного випромінення на межі …….;
- нерівномірність споживання струму у колах електроживлення;
- відсутність паразитної генерації потужних каскадів підсилюючих засобів;
- …… …. .

Для підсистеми керування КСЗІ АС повинно бути перевірено:

- правильність роботи механізмів керування всіма підсистемами КСЗІ;
- правильність роботи механізмів оперативного сповіщення щодо фактів несанкціонованого доступу;
- …….