

ЗАТВЕРДЖЕНО
ЄААД.468244.185-ЛУ

Підп. та дата	
Інв. № дубл	
Взам. інв. №	
Підп. та дата	
Інв. № ориг.	

**Центр сертифікації ключів
ринку електричної енергії**

Комплексна система захисту інформації

Програма та методика попередніх випробовувань

ЄААД.468244.185.ПМ.02

2014 р.

ЗМІСТ

1 Загальні відомості	4
2 Об'єкт попередніх випробувань.....	5
3 Мета і задачі попередніх випробувань КСЗІ ЦСК.....	5
4 Загальні положення.....	6
5 Обсяг експертизи КСЗІ ЦСК.....	7
6 Умови і порядок проведення попередніх випробувань КСЗІ ЦСК.....	9
7 Вимоги щодо забезпечення конфіденційності при виконанні робіт	9
8 Матеріально-технічне забезпечення експертних робіт	9
9 Звітність	9
ДОДАТОК А.....	10

ПЕРЕЛІК СКОРОЧЕНЬ

ДСТУ	-	Державний стандарт України
ЕОТ	-	Електронно-обчислювальна техніка
КЗЗ	-	Комплекс засобів захисту
КС	-	Комп'ютерна система
КСЗІ	-	Комплексна система захисту інформації
НД	-	Нормативний документ
НСД	-	Несанкціонований доступ
ОС	-	Операційна система
ПЗ	-	Програмне забезпечення
ПЕОМ	-	Персональна електронно-обчислювальна система
ПЕМВН	-	Побічні електромагнітні випромінювання та навід
ПТК	-	Програмно-технічний комплекс
ТЗ	-	Технічне завдання
ТЗІ	-	Технічний захист інформації
ТУ	-	Технічні умови
ЦСК	-	Центр сертифікації ключів

ТЕРМІНИ ТА ВИЗНАЧЕННЯ

У цьому документі використовуються терміни та визначення згідно з:

- ДСТУ 3396.2-97 "Захист інформації. Технічний захист інформації. Терміни та визначення";
 - НД ТЗІ 1.1-003-99 "Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу";
- Правила посиленої сертифікації. Затверджені наказом ДСТСЗІ СБ України №3 від 13.01.2005 р. Зареєстровані в Міністерстві юстиції України за №104/10384 від 27.01.2005 р.

1 ЗАГАЛЬНІ ВІДОМОСТІ

1.1 Програма попередніх випробувань КСЗІ визначає об'єкти, умови, порядок та об'єм проведення робіт (випробувань) з оцінки захищеності інформації в ЦСК ринку електричної енергії (надалі - використовуються визначення "комп'ютерна система" або "об'єкт ЕОТ" згідно з контекстом викладення положень окремих розділів і пунктів Програми і методики).

1.2 Програма розроблена відповідно до законів України "Про захист інформації в інформаційно-телекомунікаційних системах", нормативних документів, "Положення про технічний захист інформації в Україні", "Концепції технічного захисту інформації в Україні", інших нормативно-правових актів та нормативних документів системи технічного захисту інформації в Україні.

2 ОБ'ЄКТ ПОПЕРЕДНІХ ВИПРОБУВАНЬ

2.1 Попереднім випробуванням підлягає інформаційно-телекомунікаційна система ЦСК ринку електричної енергії. Технічні засоби серверного сегменту програмно-технічного комплексу (ПТК) ЦСК а також робочі станції (далі - РС) персоналу ЦСК об'єднані у локальну обчислювальну мережу (ЛОМ).

2.2 Об'єктом попередніх випробувань згідно даної Програми є комплексна система захисту інформації (далі - КСЗІ) ЦСК ринку електричної енергії.

2.3 Попереднім випробуванням та перевіркам в складі КСЗІ ЦСК підлягає сукупність програмно-апаратних засобів, які утворюють ПТК ЦСК та призначені для:

- виконання функцій ЦСК (структура та склад ПТК та програмного забезпечення наведено у РКД та ЕД);
- реалізації політики безпеки інформації в ЦСК (згідно 3.1.2 ТЗ на КСЗІ, захист інформації, яка обробляється й зберігається в ЦСК, від НСД здійснюється комплексом засобів захисту ПТК ЦСК);
- фізичне середовище у складі:
 - приміщень будівлі ЦСК;
 - інженерних комунікацій і обладнання цих систем, системи енергоживлення об'єкта, системи заземлення об'єкта, допоміжних технічних засобів та систем об'єкта, системи життєзабезпечення об'єкта (водопостачання, теплопостачання та ін.);
 - організаційно-правових та інженерно-технічних заходів захисту, включаючи захист від фізичного НСД до компонентів ПТК ЦСК і захист від витоку інформації технічними каналами.

3 МЕТА І ЗАДАЧІ ПОПЕРЕДНІХ ВИПРОБУВАНЬ КСЗІ ЦСК

3.1 Попередні випробування проводяться з метою оцінки захищеності інформації, яка обробляється або циркулює в ЦСК ринку електричної енергії.

3.2 Оцінка захищеності інформації ЦСК полягає у визначенні відповідності КСЗІ ЦСК вимогам ТЗ та нормативних документів у галузі технічного захисту інформації (далі - НД ТЗІ).

3.3 Завданнями попередніх випробувань КСЗІ ЦСК є перевірка:

- відповідності існуючих умов експлуатації КС та коректності функціонального профілю захищеності від загроз НСД вимогам, що встановлені ТЗ на створення КСЗІ ЦСК та Правилами посиленої сертифікації;
- відповідності заходів забезпечення безпеки і засобів захисту КС (коректність результатів проектування і реалізації КЗЗ);
- реального існування заходів забезпечення безпеки і засобів захисту КС, що реалізують функціональні послуги безпеки, та технічних засобів захисту інформації від витоку технічними каналами;
- виконання рівня гарантій, який визначений ТЗ на КСЗІ ЦСК;
- повноти та достатності технічної документації;
- необхідності внесення змін і доповнень до організаційно-розпорядчих документів, визначення вимог до організаційних, фізичних та інших заходів захисту, що реалізуються у доповнення до комплексу програмно-технічних засобів захисту, тощо.

4 ЗАГАЛЬНІ ПОЛОЖЕННЯ

4.1 Роботи щодо попередніх випробувань КСЗІ ЦСК повинні здійснюватися на підставі наступних нормативно - правових актів та нормативних документів:

- Закон України "Про захист інформації в інформаційно-телекомунікаційних системах";
- Закон України „Про електронний цифровий підпис”;
- Положення про технічний захист інформації в Україні. Затверджене Указом Президента України від 27 вересня 1999 р. N 1229 (зі змінами, внесеними Указом Президента України від 6 жовтня 2000 року N 1120);
- Правила посиленої сертифікації (наказ ДСТСЗІ СБ України від 13 січня 2005 р № 3);
- ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення;
- ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт;
- ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення;
- Тимчасове положення про категоріювання об'єктів (НД ТЗІ 1.6-005-2013). Затверджене наказом Державної служби України з питань технічного захисту інформації від 10 липня 1995 р. №35;
- НД ТЗІ 1.1-003-99 Термінологія в 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;
- НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі (зі змінами затвердженими наказом ДСТСЗІ СБУ №37 від 18.06.2002 р.);
- НД ТЗІ 2.5-008-2002. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2;
- ДБН А.2.2-2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та проектної документації для будівництва. Затверджені наказом Держкоммістобудування України від 02.09.96 р. № 156;
- НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі;
- НД ТЗІ 2.1-001-2001 Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення. Затверджений наказом ДСТЗІ від 09.02.2001 р. № 2;
- НД ТЗІ 3.6-001-2000. Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу. Затверджений наказом ДСТСЗІ СБУ від 20 грудня 2000 року №60;
- НД ТЗІ 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці;
- Тимчасові рекомендації з технічного захисту інформації від витоків каналами побічних електромагнітних випромінювань і наводок (ТР ПЕМВН-95).

4.2 Роботи щодо попередніх випробувань КСЗІ ЦСК здійснюються в робочих приміщеннях об'єкту інформаційної діяльності ЦСК ринку електричної енергії.

4.3 Випробування проводяться комісією у складі представників ДП "ЕНЕРГОРИНОК", яка призначається наказом директора ДП "ЕНЕРГОРИНОК".

5 ОБСЯГ ЕКСПЕРТИЗИ КСЗІ ЦСК

5.1 Об'єм попередніх випробувань КСЗІ ЦСК визначається поставленою метою випробувань і включає проведення наступних перевірок :

- виконання вимог ТЗ та НД ТЗІ щодо організації робіт із захисту інформації на об'єкті;
- виконання вимог ТЗ на КСЗІ, Правил посиленої сертифікації (наказ від 13.01.2005 р. № 3) та НД ТЗІ щодо захисту інформації від несанкціонованого доступу;
- виконання вимог ТЗ на КСЗІ, Правил посиленої сертифікації та НД ТЗІ щодо захисту інформації від витоку по каналах ПЕМВН;
- виконання вимог ТЗ на КСЗІ щодо підсистеми антивірусного захисту ЦСК.

5.2 Випробування КСЗІ ЦСК включає перелік етапів перевірок і випробувань, наведений у табл. 1.

Таблиця 1 - Етапи випробувань і видів перевірок.

Найменування перевірки (перевірок)	Документ, що визначає вимоги за даним пунктом випробувань	Розділ методики	Обсяг випроб.
1 Перевірка виконання вимог НД ТЗІ та Правил посиленої сертифікації			
1.1 Перевірка на відповідність організаційно-технічним вимогам по захисту інформації			
1.1.1 Перевірка організаційно-технічних документів Замовника із питань впровадження заходів захисту від НСД та забезпечення режиму безпеки.	п. 5.1.7, розділ 6 ТЗ на КСЗІ ЦСК, НД ТЗІ 2.5-008-2002, НД ТЗІ 1.4-001-2000, розділ 5 Правил посиленої сертифікації, Методика контролю захищеності об'єкту ЕОТ	п. А.4.1	ЦСК згідно п. 5.3.
Найменування перевірки (перевірок)	Документ, що визначає вимоги за даним пунктом випробувань	Розділ методики	Обсяг випроб.
1.2 Перевірка на відповідність вимогам по захисту інформації від загроз НСД			
1.2.1 Перевірка умов експлуатації ЦСК , функціонального профілю захищеності від загроз НСД, впроваджених організаційних заходів	розділ 3, п. 5.2, 6.3 ТЗ на КСЗІ ЦСК, НД ТЗІ 2.5-008-2002, НД ТЗІ 1.4-001-2000, Правила посиленої сертифікації	п. А.4.2.1	ЦСК згідно п. 5.3.
1.2.2 Ідентифікації системного та спеціального ПЗ ПТК, що встановлені у КС	п. 3.3.4 ТЗ на КСЗІ ЦСК, РКД і ЕД на ЦСК	п.А.4.2.2	ЦСК згідно п. 5.3.
1.2.3 Перевірка коректності інсталяції та конфігурування ОС та спеціального ПЗ ПТК ЦСК	п.3.3.4 ТЗ на КСЗІ ЦСК, НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-008-2002, РКД і ЕД на ЦСК , Правила посиленої сертифікації	п.А.4.2.3	ЦСК згідно п. 5.3.
1.2.4. Перевірка реалізації заходів забезпечення безпеки і КЗЗ ПТК ЦСК, механізми яких реалізують вимоги до функцій (послуг) забезпечення конфіденційності, цілісності, доступності, спостережності і керованості.	підрозділ 5.3 ТЗ на КСЗІ ЦСК, НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-008-2002, РКД і ЕД на ЦСК	п.А.4.2.4.	ЦСК згідно п. 5.3.
1.2.5. Перевірка відповідності заходів забезпечення безпеки і КЗЗ ПТК ЦСК (перевірка виконання вимог до функцій (послуг) забезпечення безпеки).	підрозділи 5.3 ТЗ на КСЗІ ЦСК, НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-008-2002, РКД і ЕД на ЦСК	п.А.4.2.5.	ЦСК згідно п. 5.3.
1.2.6 Перевірка реалізації заходів забезпечення безпеки і КЗЗ робочої станції генерації ключів.	підрозділи 5.3-5.5 ТЗ на КСЗІ ЦСК, НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-008-2002, РКД і ЕД на ЦСК	п.А.4.2.5.	ЦСК згідно п. 5.3.
1.2.7 Перевірка відповідності заходів забезпечення безпеки і КЗЗ робочої станції генерації ключів	підрозділи 5.3-5.5 ТЗ на КСЗІ ЦСК, НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-008-2002, РКД і ЕД на ЦСК	п.А.4.2.7.	
1.2.8 Перевірка відповідності заходів забезпечення безпеки і КЗЗ міжмережевого екрану ПТК ЦСК (перевірка виконання вимог до функцій (послуг) забезпечення безпеки)	п 4.3.11ТЗ на КСЗІ ЦСК	п. А.4.2.8	
1.3 Перевірка на відповідність вимогам по захисту інформації від витоку по технічних каналах			

1.3.1 Перевірка на відповідність вимогам по захисту інформації від витоку по каналах ПЕМВН в т.ч.:			
1.3.1.1 Перевірка відповідності фактичних розмірів КЗ наданим документам.	План об'єкту, План розміщення ЕОТ,	п.А.4.3.1	ЦСК згідно п. 5.3.
1.3.1.2. Перевірка вимог до спеціальних приміщень ЦСК.	План об'єкту, План розміщення ЕОТ, додаток 4 до Правил посиленої сертифікації	п.А.4.3.1	ЦСК згідно п. 5.3.
1.3.1.3. Перевірка правильності розміщення технічних засобів ПТК ЦСК.	додаток 4 до Правил посиленої сертифікації, НД ТЗІ 1.6-005-2013,	п.А.4.3.1	ЦСК згідно п. 5.3.
1.3.1.4. Перевірка ефективності екранування спеціальних приміщень ЦСК.	додаток 4 до Правил посиленої сертифікації, протоколи спецвипробувань, Припис на експлуатацію, НД ТЗІ 1.6-005-2013, ТР ТЗІ ПЕМВН-95,	п.А.4.3.1	ЦСК згідно п. 5.3.
1.3.1.5. Перевірка схеми енергопостачання, розміщення і монтажу обладнання і силових кабелів, монтажу і параметрів заземлення і кіл заземлення.	ТР ТЗІ ПЕМВН-95, НД ТЗІ 1.6-005-2013,	п.А.4.3.1	ЦСК згідно п. 5.3.
1.3.1.6. Перевірка засобів захисту, їхніх сертифікатів, виконання правил їхньої експлуатації.	Правила посиленої сертифікації, сертифікати, ТУ і ІЗ на засоби захисту	п.А.4.3.1	ЦСК згідно п. 5.3.
1.3.1.7. Перевірка документів (актів, протоколів) апаратного контролю ефективності захисту інформації на об'єкті ЦСК.	Методика контролю захищеності об'єкту ЕОТ	п.А.4.3.1	ЦСК згідно п. 5.3.
1.3.1.8. Інструментальна перевірка ефективності захисту інформації від витоку по ПЕМВ (при необхідності).	додаток 4 до Правил посиленої сертифікації, Методика контролю захищеності об'єкту ЕОТ і її додатки.	п.А.4.3.1	окрема ПЕОМ (ОТЗ) ЦСК
1.4 Перевірка підсистеми антивірусного захисту КСЗІ ЦСК			
1.4.1 Перевірка виконання вимог до організаційних заходів при впровадженні підсистеми антивірусного захисту	підрозділ. 6.3 ТЗ на КСЗІ ЦСК Інструкція про порядок забезпечення антивірусного захисту	п. А.4.3.2.	ЦСК згідно п. 5.3.
1.4.2 Перевірка виконання вимог до функціонального забезпечення, структури та функціонування системи антивірусного захисту	п. 5.1.14, 6.3 ТЗ на КСЗІ ЦСК	п. А.4.3.2.	
2 Оцінка рівня довіри до коректності реалізованої КСЗІ ЦСК (перевірка виконання вимог до рівня гарантій КС)			
2.1 Перевірка виконання вимог критеріїв гарантій	п. 5.2.2 ТЗ на КСЗІ ЦСК, НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-008-2002, РКД і ЕД на КС	р.5	ЦСК згідно п. 5.3
3 Оформлення звітних матеріалів			

5.3 Перевірки по підрозділам 1.1, 1.3 та розділу 2 таблиці 1 здійснюються для ЦСК в цілому. Випробування по підрозділам 1.2 та 1.4 таблиці 1 здійснюються на кожній ПЕОМ ЦСК.

5.4 Послідовність проведення перевірок і кількісні та якісні характеристики, що підлягають оцінюванню, визначаються "Методикою попередніх випробувань КСЗІ ЦСК" (див. Додаток А).

6 УМОВИ І ПОРЯДОК ПРОВЕДЕННЯ ПОПЕРЕДНІХ ВИПРОБУВАНЬ КСЗІ ЦСК

6.1 Попередні випробування КСЗІ ЦСК здійснюються в робочих експлуатаційних режимах за умови наявності всієї сукупності апаратних та програмних засобів захисту інформації, а також технічної і програмної документації на комплексну систему захисту інформації, що розробляється згідно з вимогами технічного завдання на КСЗІ ЦСК.

7 ВИМОГИ ЩОДО ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ПРИ ВИКОНАННІ РОБІТ

7.1 Перелік осіб, які можуть бути ознайомлені з матеріалами проектної та експлуатаційної документації, що підлягають захисту, визначається Замовником. Порядок доступу цих осіб до матеріалів встановлюється згідно з діючими нормативними документами України.

8 МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ЕКСПЕРТНИХ РОБІТ

8.1 Роботи з перевірки працездатності засобів та механізмів захисту інформації здійснюються з використанням штатних засобів ОС і КЗЗ та додаткових програмних засобів.

9 ЗВІТНІСТЬ

9.1 Результати попередніх випробувань КСЗІ ЦСК в цілому оцінюються за результатами окремих видів перевірок, виконаних відповідно до розділу 5 даної Програми. Результати випробувань не можуть вважатися позитивними, якщо не виконуються вимоги ТЗ.

9.2 Результати попередніх випробувань оформлюються протоколами, що складаються за результатами окремих видів перевірок, які підписуються і прикладаються до Акту попередніх випробувань.

ДОДАТОК А

МЕТОДИКА ПОПЕРЕДНІХ ВИПРОБУВАНЬ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ЦЕНТРУ СЕРТИФІКАЦІЇ КЛЮЧІВ РИНКУ ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ

А.1 ОБ'ЄКТ ПОПЕРЕДНІХ ВИПРОБУВАНЬ

А.1.1 Об'єкт попередніх випробувань визначений у розділі 2 програми попередніх випробувань комплексної системи захисту інформації відомчого центру сертифікації ключів ринку електричної енергії.

А.2 МЕТА І ЗАДАЧІ ПОПЕРЕДНІХ ВИПРОБУВАНЬ КСЗІ ЦСК

А.2.1 Мета і задачі попередніх випробувань КСЗІ ЦСК визначені у розділі 3 програми попередніх випробувань комплексної системи захисту інформації відомчого центру сертифікації ключів ринку електричної енергії.

А.3 МЕТОДИ ВИПРОБУВАНЬ

А.3.1 Застосовуються наступні методи перевірок і випробувань:

- експертно-документальний метод;
- метод функціональної перевірки;
- спроби “злому” систем захисту інформації від НСД (тестування на проникнення);
- виміри й оцінка захищеності інформації в ЦСК за прийнятими критеріями для окремих каналів витоку (при необхідності).

А.3.2 Експертно-документальний метод передбачає оцінку відповідності ЦСК (об'єкта ЕОТ) вимогам по безпеці інформації на підставі представлених робочої конструкторської й експлуатаційної документації, матеріалів, документів, актів, сертифікатів, ліцензій, розпоряджень на експлуатацію та інших підтверджень про виконання необхідних заходів із захисту інформації.

А.3.3 Метод функціональної перевірки полягає у визначенні відповідності вимогам ТЗ складу функціональних послуг КЗЗ ПТК ЦСК і переліку, що задаються параметрами їхнього виконання, шляхом демонстрації роботи окремих штатних служб, засобів і механізмів захисту КС. Перевірка й випробування окремих функцій захисту інформації або комплексу цих функцій проводиться за допомогою ручного тестування шляхом пробного запуску штатних служб, засобів і механізмів захисту і спостереження за їхнім виконанням.

А.4 МЕТОДИКА ОЦІНКИ КОРЕКТНОСТІ СТВОРЕНОЇ КСЗІ ЦСК (ПЕРЕВІРКА ВИКОНАННЯ ВИМОГ НД ТЗІ)

А.4.1 Методика випробувань на відповідність організаційно-технічним вимогам по захисту інформації

Види й обсяг випробувань на відповідність організаційно-технічним вимогам по захисту інформації проводяться в обсязі, зазначеному в таблиці 1 Програми.

А.4.1.1 Перевірка організаційно-технічних документів Замовника із питань впровадження заходів захисту від НСД та забезпечення режиму безпеки

А.4.1.1.1 Метою перевірки є встановлення факту, чи дійсно склад і зміст цих документів відповідає вимогам розділу 6 ТЗ на КСЗІ ЦСК, розділу 5 Правил посиленої сертифікації, НД ТЗІ 2.5-008-2002, НД ТЗІ 1.4-001-2000.

А.4.1.1.2 Перевірка організаційно-технічних документів Замовника здійснюється експертно-документальним методом.

А.4.1.1.3 Результати перевірки вважаються позитивними, якщо організаційно-технічні документи відповідають вимогам п. 6 ТЗ на КСЗІ ЦСК, розділу 5 Правил посиленої сертифікації НД ТЗІ 2.5-008-2002, НД ТЗІ 1.4-001-2000.

А.4.1.1.4 Результати перевірки вважаються негативними, якщо організаційно-технічні документи не відповідають вимогам ТЗ на КСЗІ ЦСК, розділу 5 Правил посиленої сертифікації НД ТЗІ 2.5-008-2002, НД ТЗІ 1.4-001-2000.

А.4.2 Методика перевірки на відповідність вимогам по захисту інформації від загроз НСД

Випробування проводяться в обсязі, зазначеному в таблиці 1 “Програми...”.

А.4.2.1 Перевірка умов експлуатації ЦСК, функціонального профілю захищеності від загроз НСД, впроваджених організаційних заходів

А.4.2.1.1 Метою оцінки є встановлення відповідності існуючих умов експлуатації ЦСК функціонального профілю захищеності від загроз НСД та впроваджених організаційних заходів вимогам п.п. 3.3 – 3.5, 5.1 – 5.5 ТЗ на КСЗІ ЦСК, розділу 5 Правил посиленої сертифікації.

А.4.2.1.2 Перевірка здійснюється експертно-документальним методом.

А.4.2.1.3 Послідовність дій:

- перегляд та аналіз реальних умов експлуатації ЦСК;
- перегляд визначеного функціонального профілю захищеності від загроз НСД;
- перегляд та аналіз складу впроваджених організаційних заходів.

А.4.2.1.4 Результати перевірки вважаються позитивними, якщо надані матеріали відповідають вимогам п.п. 3.3 – 3.5, 5.1 – 5.5 ТЗ на КСЗІ ЦСК, розділу 5 Правил посиленої сертифікації, НД ТЗІ 2.5-008-2002 .

А.4.2.1.5 Результати перевірки вважаються негативними, якщо надані матеріали не відповідають вимогам вказаних в ТЗ та НД ТЗІ.

А.4.2.2 Ідентифікації системного та спеціального ПЗ ПТК, що встановлені у КС

А.4.2.2.1 Метою ідентифікації є встановлення відповідності системного та спеціального ПЗ ПТК, що встановлені у КС, вимогам п.п. 3.3.4 ТЗ на КСЗІ ЦСК, Правил посиленої сертифікації .

А.4.2.2.2 Перевірка здійснюється експертно-документальним методом.

А.4.2.2.3 Ідентифікації ОС Windows здійснюється за документацією розробника. Ідентифікація ОС здійснюється з використанням процедур, які ініціюються шляхом запуску на виконання з командного рядка наступних системних команд:

- визначення списку файлів та підкаталогів каталогу - команда dir;
- визначення версії файлу - команда filever;
- ідентифікація конфігурації комп'ютера і операційної системи - команда systeminfo.

А.4.2.2.4 Результати перевірки вважаються позитивними, якщо надані матеріали відповідають вимогам документації розробника.

А.4.2.2.5 Результати перевірки вважаються негативними, якщо надані матеріали не відповідають вимогам розділів 1,2 зазначеного документу.

А.4.2.2.6 Ідентифікації спеціального ПЗ ПТК здійснюється згідно експлуатаційних документів підприємства-розробника ПТК ЦСК:

- ЄААД.468244.185.ПА.01 Опис програмного забезпечення;
- ЄААД.00021-11 01-1 Програмний комплекс ЦСК. Програмна експлуатаційна документація;
- ЄААД.00021-11 03-1 Програмний комплекс користувача ЦСК. Програмна експлуатаційна документація;
- ЄААД.00049 Мережевий криптомодуль “Гряда-301”. Програмна експлуатаційна документація;
- ЄААД.00044 Криптографічний модуль “Гряда-61”. Програмна експлуатаційна документація.

Результати перевірки вважаються позитивними, якщо надані матеріали відповідають вимогам зазначених документів.

Результати перевірки вважаються негативними, якщо надані матеріали не відповідають вимогам зазначених документів.

А.4.2.3 Перевірка коректності інсталяції та конфігурування ОС та спеціального ПЗ ПТК ЦСК

А.4.2.3.1 Метою перевірки є встановлення факту, що інсталяція та конфігурування параметрів безпеки КЗЗ системного та спеціального ПЗ ПТК, що встановлені у КС, виконані відповідно до вимог п. 3.2.7 ТЗ на КСЗІ ЦСК.

А.4.2.3.2 Перевірка здійснюється експертно-документальним методом.

А.4.2.3.3 Перевірка інсталяції та конфігурування ОС Windows 8.1 здійснюється згідно з документацією розробника.

Перевірка конфігурування параметрів безпеки ОС виконується на функціональному рівні шляхом виклику штатних компонент програмних засобів захисту для перевірки, аналізу і перегляду поточних настройок безпеки для розгорнутої конфігурації ПЕОМ (локальних параметрів безпеки, політик облікових записів, локальних політик та ін.), опис роботи з якими наведений в настанові адміністратора щодо послуг безпеки та технічній документації на КЗЗ.

Результати перевірки вважаються позитивними, якщо надані матеріали Замовника відповідають вимогам розділів 2,3 зазначеного документу.

Результати перевірки вважаються негативними, якщо надані матеріали не відповідають вимогам розділів 2,3 зазначеного документу.

А.4.2.3.4 Перевірка інсталяції та конфігурування спеціального ПЗ ПТК здійснюється згідно експлуатаційних документів підприємства-розробника ПТК ЦСК:

- ЄААД.468244.185.ІЭ.01 Центральні сервери. Інструкція з експлуатації КТЗ;
- ЄААД.468244.185.ІЭ.02 Сервери взаємодії. Інструкція з експлуатації КТЗ;
- ЄААД.468244.185.ІЭ.03 Комунікаційне обладнання. Інструкція з експлуатації КТЗ;
- ЄААД.468244.185.ІЭ.04 РС адміністратора сертифікації та системного адміністратора. Інструкція з експлуатації КТЗ;
- ЄААД.468244.185.ІЭ.05 РС адміністратора безпеки. Інструкція з експлуатації КТЗ;
- ЄААД.468244.185.ІЭ.06 РС адміністратора реєстрації. Інструкція з експлуатації КТЗ;
- ЄААД.468244.185.ІЭ.08 РС. Інструкція з експлуатації КТЗ;
- ЄААД.468244.185.ІЭ.09 КСЗІ. Засоби антивірусного захисту. Інструкція з експлуатації КТЗ;
- ЄААД.468244.185.ІЭ.10 КСЗІ. Засоби резервного копіювання. Інструкція з експлуатації КТЗ;
- ЄААД.468244.185.ІЭ.11 КСЗІ. КЗЗ серверів. Інструкція з експлуатації;
- ЄААД.468244.185.ІЭ.12 КСЗІ. КЗЗ робочих станцій. Інструкція з експлуатації;
- ЄААД.468244.185.ІЭ.13 Сервер моніторингу та синхронізації часу. Інструкція з експлуатації КТЗ.

Результати перевірки вважаються позитивними, якщо надані матеріали відповідають вимогам зазначених документів.

Результати перевірки вважаються негативними, якщо надані матеріали не відповідають вимогам зазначених документів.

А.4.2.4 Перевірка реалізації заходів забезпечення безпеки і КЗЗ ПТК ЦСК, механізми яких реалізують вимоги до функцій (послуг) забезпечення конфіденційності, цілісності, доступності, спостережності і керованості

А.4.2.4.1 Метою перевірки є установлення факту, чи дійсно наявні у складі ПТК ЦСК заходи забезпечення безпеки і КЗЗ ПТК ЦСК у визначених умовах експлуатації реально існують і функціонують відповідно до вимог 4.2- 4.3, 5.1- 5.5 ТЗ на КСЗІ ЦСК.

А.4.2.4.2. Перевірка здійснюється експертно-документальним методом.

А.4.2.4.3 Перевірка полягає в перевірці наявності у складі системи компонентів, як внутрішніх засобів і механізмів безпеки, так і зовнішніх (фізичних і організаційних заходів захисту), що забезпечують виконання вимог 4.2- 4.3, 5.1- 5.5 ТЗ на КСЗІ до КЗЗ ПТК ЦСК.

А.4.2.4.4 Перевірка реальності існування заходів забезпечення безпеки і КЗЗ ПТК ЦСК здійснюється шляхом аналізу техноробочого проекту на КСЗІ ЦСК із виконання вимог до:

- основних функцій КЗЗ ПТК ЦСК (розділ 4 ТЗ на КСЗІ);
- об'єктів захисту (5.1 ТЗ на КСЗІ);
- суб'єктів доступу (5.1 ТЗ на КСЗІ);
- взаємодія суб'єктів і об'єктів (5.1 ТЗ на КСЗІ);

Встановлення факту існування більшості правових, організаційних, фізичних і технічних заходів забезпечення безпеки і засобів захисту КС здійснюється простою візуальною перевіркою і перевіркою наявності відповідної організаційно-розпорядничої та нормативної документації.

А.4.2.4.5 Перевірка основних функцій КЗЗ ПТК ЦСК здійснюється шляхом аналізу виконання вимог до функцій:

- керування доступом;
- забезпечення керованості ПТК ЦСК;
- реєстрації подій, що мають відношення до безпеки;
- забезпечення контролю цілісності.

Результати перевірки основних функцій КЗЗ ПТК ЦСК вважаються позитивними, якщо надані матеріали відповідають вимогам 5.1 - 5.5 ТЗ на КСЗІ ЦСК. Результати перевірки основних функцій КЗЗ ПТК ЦСК вважаються негативними, якщо надані матеріали не відповідають вимогам 5.1 - 5.5 ТЗ на КСЗІ ЦСК.

А.4.2.4.6 Перевірка об'єктів захисту КЗЗ ПТК ЦСК здійснюється шляхом встановлення відповідності програмно-інформаційних ресурсів ПТК ЦСК, що підлягають захисту, вимогам, що наведені у 5.1 ТЗ на КСЗІ ЦСК.

Результати перевірки об'єктів захисту КЗЗ ПТК ЦСК вважаються позитивними, якщо надані матеріали відповідають вимогам 5.1 - 5.5 ТЗ на КСЗІ ЦСК. Результати перевірки об'єктів захисту КЗЗ ПТК ЦСК вважаються негативними, якщо надані матеріали не відповідають вимогам 5.1 - 5.5 ТЗ на КСЗІ ЦСК.

А.4.2.4.7 Перевірка суб'єктів доступу КЗЗ ПТК ЦСК здійснюється шляхом встановлення відповідності складу користувачів ЦСК вимогам, що наведені у 5.1.4.2 ТЗ на КСЗІ ЦСК.

Результати перевірки суб'єктів доступу КЗЗ ПТК ЦСК вважаються позитивними, якщо надані матеріали відповідають вимогам 5.1.4.2 ТЗ на КСЗІ ЦСК. Результати перевірки суб'єктів доступу КЗЗ ПТК ЦСК вважаються негативними, якщо надані матеріали не відповідають вимогам 5.1.4.2 ТЗ на КСЗІ ЦСК.

А.4.2.4.8 Перевірка взаємодії суб'єктів і об'єктів здійснюється шляхом аналізу виконання вимог до:

- атрибутів доступу, що їм належать;
- загальних правил розмежування доступу користувачів до ресурсів КС ЦСК;
- одержання прав по типу доступу суб'єктів стосовно об'єктів.

Результати перевірки атрибутів доступу суб'єктів і об'єктів вважаються позитивними, якщо надані матеріали відповідають вимогам 5.1 ТЗ на КСЗІ ЦСК. Результати перевірки атрибутів доступу суб'єктів і об'єктів вважаються негативними, якщо надані матеріали не відповідають вимогам 5.1 ТЗ на КСЗІ ЦСК.

Результати перевірки загальних правил розмежування доступу користувачів до ресурсів КС ЦСК вважаються позитивними, якщо надані матеріали відповідають вимогам 5.1 ТЗ на КСЗІ ЦСК. Результати перевірки вважаються негативними, якщо надані матеріали не відповідають вимогам 5.1 ТЗ на КСЗІ ЦСК.

Результати перевірки одержання прав по типу доступу суб'єктів стосовно об'єктів КС ЦСК вважаються позитивними, якщо надані матеріали відповідають вимогам 5.1.5 - 5.1.16 ТЗ на КСЗІ ЦСК. Результати перевірки вважаються негативними, якщо надані матеріали не відповідають вимогам 5.1.5 - 5.1.16 ТЗ на КСЗІ ЦСК.

А.4.2.5 Перевірка відповідності заходів забезпечення безпеки і КЗЗ ЛОМ ПТК ЦСК (перевірка виконання вимог до функцій (послуг) забезпечення безпеки)

А.4.2.5.1 Метою перевірки відповідності заходів забезпечення безпеки і КЗЗ КС вимогам розділу 4 та розділу 5 ТЗ на КСЗІ ЦСК.

А.4.2.5.2 Перевірка здійснюється відповідно до технічної і експлуатаційної документації Постачальника цих засобів.

А.4.2.5.3 Перевірка специфікацій вимог, які визначають правила взаємодії об'єктів автоматизованої системи, для кожної послуги здійснюється на відповідність вимогам НД ТЗІ 2.5-004-1999 з урахуванням, що взаємодія суб'єктів доступу і об'єктів захисту ЦСК здійснюється згідно з загальними правилами розмежування доступу і атрибутами доступу, визначеними у розділі 5.1 та вимогами до функцій програмних засобів захисту, зазначених у пп. 5.2 - 5.3 ТЗ на КСЗІ ЦСК.

В цьому розділі для кожної послуги наведено перевірки специфікацій щодо визначеної ТЗ на КСЗІ ЦСК множини об'єктів, яких ця послуга стосується.

А.4.2.5.6 Перевірка виконання вимог до функцій (послуг) забезпечення конфіденційності.

Перевірці підлягають функції (послуги) забезпечення конфіденційності: КА (адміністративна конфіденційність КА-2), КД (довірча конфіденційність КД-2) та КВ (конфіденційність при обміні КВ-1), які

згідно п.п. 5.2 ТЗ на КСЗІ ЦСК реалізуються механізмами безпеки КЗЗ ЛОМ ПТК ЦСК відповідно до пп. 5.3.1 – 5.3.3 ТЗ на КСЗІ ЦСК.

Всі перевірки здійснюються шляхом виклику штатних компонент програмних або програмно-апаратних засобів захисту для перевірки, аналізу і перегляду поточних налаштувань безпеки для розгорнутої конфігурації ЛОМ ПТК ЦСК (локальних параметрів безпеки, політик облікових записів, локальних політик та ін.), опис роботи з якими наведений в настанові адміністратору щодо послуг безпеки та технічній документації на КЗЗ.

Перевірка виконання вимог до функцій (послуг) забезпечення конфіденційності вважається виконаною, якщо склад функціональних служб і механізмів захисту, а також номенклатура і діапазон значень їх настановних параметрів відповідає вимогам 5.2.3 ТЗ на КСЗІ ЦСК.

А.4.2.5.7 Перевірка виконання вимог до функцій (послуг) забезпечення цілісності.

Перевірці підлягають такі функції (послуги) забезпечення цілісності: адміністративна цілісність (ЦА-1), цілісність при обміні (ЦВ-1) які реалізується механізмами безпеки КЗЗ ЛОМ ПТК ЦСК згідно з 5.3.4 – 5.3.5 ТЗ на КСЗІ ЦСК.

Всі перевірки здійснюються шляхом виклику штатних компонент програмних або програмно-апаратних засобів захисту для перевірки, аналізу і перегляду поточних налаштувань безпеки для розгорнутої конфігурації ЛОМ ПТК ЦСК (локальних параметрів безпеки, політик облікових записів, локальних політик та ін.), опис роботи з якими наведений в настанові адміністратору щодо послуг безпеки та технічній документації на КЗЗ.

Перевірка виконання вимог до функцій (послуг) забезпечення цілісності вважається виконаною, якщо склад функціональних служб і механізмів захисту, а також номенклатура і діапазон значень їхніх настановних параметрів відповідає вимогам 5.2.3 ТЗ на КСЗІ ЦСК.

А.4.2.5.8 Перевірка виконання вимог до функцій (послуг) забезпечення доступності.

Перевірці підлягають такі функції (послуги) забезпечення доступності: використання ресурсів (ДР-1), відновлення після збоїв (ДВ-1), які реалізовуються організаційно-технічними заходами захисту та механізмами безпеки КЗЗ ЛОМ ПТК ЦСК відповідно до вимог 5.3.8 – 5.3.9 ТЗ на КСЗІ ЦСК.

Всі перевірки здійснюються шляхом виклику штатних компонент програмних або програмно-апаратних засобів захисту для перевірки, аналізу і перегляду поточних налаштувань безпеки для розгорнутої конфігурації ЛОМ ПТК ЦСК (локальних параметрів безпеки, політик облікових записів, локальних політик та ін.), опис роботи з якими наведений в настанові адміністратору щодо послуг безпеки та технічній документації на КЗЗ.

Перевірка виконання вимог до функцій (послуг) забезпечення доступності вважається виконаною, якщо склад функціональних служб і механізмів захисту, а також номенклатура і діапазон значень їхніх настановних параметрів відповідає вимогам 5.2.3 ТЗ на КСЗІ ЦСК.

А.4.2.5.9 Перевірка виконання вимог до функцій (послуг) забезпечення спостережності і керованості.

Перевірці підлягають такі функції (послуги) забезпечення спостережливості і керованості: реєстрація (НР-2), ідентифікація і автентифікація (НІ-2), ідентифікація і автентифікація (НІ-3), достовірний канал (НК-1), розподіл обов'язків (НО-3), цілісність комплексу засобів захисту (НЦ-1), цілісність комплексу засобів захисту (НЦ-2), самотестування (НТ-2), ідентифікація і автентифікація при обміні (НВ-1), які реалізуються механізмами безпеки КЗЗ ЛОМ ПТК ЦСК відповідно до вимог 5.3.10 – 5.3.18 ТЗ на КСЗІ ЦСК.

Всі перевірки здійснюються шляхом виклику штатних компонент програмних або програмно-апаратних засобів захисту для перевірки, аналізу і перегляду поточних налаштувань безпеки для розгорнутої конфігурації ПЕОМ (локальних параметрів безпеки, локальних політик та ін.), опис роботи з якими наведений в настанові адміністратору щодо послуг безпеки та в технічній документації на КЗЗ.

Перевірка виконання вимог до функцій (послуг) забезпечення спостережливості і керованості вважається виконаною, якщо склад функціональних служб і механізмів захисту, а також номенклатура і діапазон значень їхніх настановних параметрів відповідає встановленому 5.2.3 ТЗ на КСЗІ ЦСК.

А.4.2.6 Перевірка реалізації заходів забезпечення безпеки і КЗЗ робочої станції (РС) генерації ключів.

А.4.2.6.1 Метою перевірки є установлення факту, чи дійсно наявні у складі РС генерації ключів ЦСК заходи забезпечення безпеки і КЗЗ ПТК ЦСК у визначених умовах експлуатації реально існують і функціонують відповідно до вимог 4.3.21 та 5.1 ТЗ на КСЗІ ЦСК.

4.2.6.2. Перевірка здійснюється експертно-документальним методом.

4.2.6.3 Перевірка реальності існування заходів забезпечення безпеки і КЗЗ ПТК ЦСК здійснюється шляхом аналізу виконання вимог до:

- основних функцій КЗЗ РС генерації ключів ЦСК (4.3.21 ТЗ на КСЗІ ЦСК);
- об'єктів захисту (5.1.2 ТЗ на КСЗІ ЦСК);
- суб'єктів доступу в т.ч. взаємодії суб'єктів і об'єктів (5.1.3 ТЗ на КСЗІ ЦСК);
- правил розмежування інформаційних потоків (5.1.4 ТЗ на КСЗІ ЦСК).

Встановлення факту існування більшості правових, організаційних, фізичних і технічних заходів забезпечення безпеки і засобів захисту КС здійснюється простою візуальною перевіркою і перевіркою наявності відповідної організаційно-розпорядницької та нормативної документації.

А.4.2.6.4 Результати перевірки основних функцій КЗЗ РС генерації ключів ЦСК вважаються позитивними, якщо надані матеріали відповідають вимогам 4.3.21 ТЗ на КСЗІ ЦСК. Результати перевірки основних функцій КЗЗ вважаються негативними, якщо надані матеріали не відповідають вимогам 4.3.21 ТЗ на КСЗІ ЦСК.

А.4.2.6.5 Перевірка об'єктів захисту КЗЗ РС генерації ключів ЦСК здійснюється шляхом встановлення відповідності програмно-інформаційних ресурсів ПТК ЦСК, що підлягають захисту, вимогам, що наведені у 5.1.2 ТЗ на КСЗІ ЦСК:

Результати перевірки об'єктів захисту КЗЗ РС генерації ключів ЦСК вважаються позитивними, якщо надані матеріали відповідають вимогам 5.1.2 ТЗ на КСЗІ ЦСК. Результати перевірки об'єктів захисту КЗЗ вважаються негативними, якщо надані матеріали не відповідають вимогам 5.1.2 ТЗ на КСЗІ ЦСК.

А.4.2.6.6 Перевірка суб'єктів доступу КЗЗ РС генерації ключів ЦСК здійснюється шляхом встановлення відповідності складу користувачів ЦСК вимогам, що наведені у 5.1.3 ТЗ на КСЗІ ЦСК.

Результати перевірки вважаються позитивними, якщо надані матеріали відповідають вимогам 5.1.3 ТЗ на КСЗІ ЦСК. Результати перевірки вважаються негативними, якщо надані матеріали не відповідають вимогам 5.1.3 ТЗ на КСЗІ ЦСК.

А.4.2.6.7 Перевірка взаємодії суб'єктів і об'єктів здійснюється шляхом аналізу виконання вимог до:

- атрибутів доступу, що їм належать;
- правил розмежування доступу користувачів до ресурсів КС ЦСК;
- одержання прав по типу доступу суб'єктів стосовно об'єктів.

Результати перевірки атрибутів доступу суб'єктів і об'єктів вважаються позитивними, якщо надані матеріали відповідають вимогам 5.1.4 ТЗ на КСЗІ ЦСК. Результати перевірки вважаються негативними, якщо надані матеріали не відповідають вимогам 5.1.4 ТЗ на КСЗІ ЦСК.

А.4.2.6.8 Перевірка правил розмежування інформаційних потоків здійснюється шляхом аналізу виконання вимог до:

- правил розмежування доступу користувачів до ресурсів КС ЦСК;
- одержання прав по типу доступу суб'єктів стосовно об'єктів.

Результати перевірки загальних правил розмежування доступу користувачів до ресурсів РС генерації ключів ЦСК вважаються позитивними, якщо надані матеріали відповідають вимогам 5.1.2 - 5.1.4 та 4.3.21 ТЗ на КСЗІ ЦСК. Результати перевірки вважаються негативними, якщо надані матеріали не відповідають вимогам 5.1.2 - 5.1.4 та 4.3.21 ТЗ на КСЗІ ЦСК.

Результати перевірки одержання прав по типу доступу суб'єктів стосовно об'єктів РС генерації ключів ЦСК вважаються позитивними, якщо надані матеріали відповідають вимогам 5.1.5 - 5.1.18 ТЗ на КСЗІ ЦСК. Результати перевірки вважаються негативними, якщо надані матеріали Замовника не відповідають вимогам 5.1.5 - 5.1.18 ТЗ на КСЗІ ЦСК.

А.4.2.7 Перевірка відповідності заходів забезпечення безпеки і КЗЗ міжмережевого екрану ЛОМ ПТК ЦСК (перевірка виконання вимог до функцій (послуг) забезпечення безпеки)

Перевірці підлягають функції (послуги), щодо керування потоками інформації із зовнішньої телекомунікаційної мережі у ЛОМ ЦСК.

Перевірка повинна включати:

- підключення комп'ютеру з встановленим сканером безпеки до інтерфейсу комутатора, призначення комп'ютеру IP-адреси із внутрішньої мережі;

- сканування адрес локальної мережі (спроба підключитися до серверів та робочих станцій, доступ до яких не передбачений адміністратором безпеки);
- сканування робочих станцій і серверів, до яких комутатор надає доступ для отримання списку відкритих портів і версій сервісів, що використовуються (сканування виконується як із випадкових номерів портів, так і з портів із діапазону 1-1024);
- пошук вразливостей серед програмного забезпечення на віддалених системах, до яких комутатором наданий доступ;
- зміна MAC-адреси мережевої карти комп'ютера із встановленим сканером безпеки і повтор тестування;
- встановлення випадкової IP-адреси (при поверненні до попередньої MAC-адреси) комп'ютера із встановленим сканером безпеки і повтор тестування;
- зміна IP-адреси комп'ютера із встановленим сканером безпеки на зарезервовані IP-адреси (10.x.x.x і т.ін.) і повтор тестування;
- сканування діапазону IP-адрес і здійснення спроб підключення до адміністративного інтерфейсу комутатора;
- аналіз конфігурації комутатора, що задана адміністратором (заборона підключення адміністратора з несанкціонованих портів комутатора, наявність перенаправлення мережевого трафіку і т.ін.);
- перевірка наявності необхідних оновлень безпеки для програмного забезпечення комутатора.

Перевірка виконання вимог до функцій (послуг) вважається виконаною, якщо склад функціональних служб і механізмів захисту, а також номенклатура і діапазон значень їхніх настановних параметрів відповідає зазначеним функціям щодо керування потоками інформації із зовнішньої телекомунікаційної мережі у ЛОМ ЦСК відповідно до вимог 4.3.11 ТЗ на КСЗІ ЦСК.

А.4.3 Перевірка на відповідність вимогам по захисту інформації від витоку по технічних каналах, а також від порушення цілісності інформації в ЕОТ внаслідок деструктивного впливу зовнішніх електромагнітних полів

А.4.3.1 Перевірка на відповідність вимогам по захисту інформації від витоку по каналах ПЕМВН

А.4.3.1.1 Перевірка відповідності об'єкту ЕОТ вимогам по захисту інформації здійснюється експертно-документальним методом.

А.4.3.1.2 Необхідними даними для оцінки відповідності об'єкту ЕОТ вимогам по захисту інформації від витоку по каналах ПЕМВН є:

- додаток 4 до Правил посиленої сертифікації;
- ТЗ на створення КСЗІ ЦСК;
- розділ політики безпеки, у якому висвітлюються питання захисту інформації від витоку технічними каналами;
- акт обстеження об'єкту ЕОТ, включаючи ситуаційний план об'єкту ЕОТ (особливості і схема розташування об'єкту з вказівкою меж контрольованої зони), поэтажні планування розташування та плани приміщень об'єкту ЕОТ, склад і схеми розміщення основних технічних засобів ЕОТ і допоміжних технічних засобів і обладнання; план контрольованих зон об'єкту ЕОТ; схеми розміщення кабелів та кіл ДТЗС; схеми і характеристики систем енергоживлення і заземлення об'єкту; склад і розміщення засобів захисту інформації;
- документи проектної, будівельно-монтажної організації по створенню спеціальних приміщень;
- протоколи із результатами проведення спеціальних досліджень та спеціальних перевірок об'єкту ЕОТ;
- акт атестації екранованої серверної шафи.

А.4.3.1.3 Комісія повинна переконатися, що надані матеріали відповідають реальним характеристикам експлуатаційного середовища, загальним характеристикам, особливостям та реальним умовам технологій обробки інформації у КС, що мають відношення до проявів суттєвих загроз для інформації з боку каналів ПЕМВН.

А.4.3.1.4 Перевірка відповідності фактичних розмірів КЗ наданим документам

Перевірка відповідності фактичних розмірів КЗ наданим документам виконується шляхом:

- аналізу вихідних даних щодо обстеження об'єкту ЕОТ (ситуаційного плану, умов експлуатації, плану розташування приміщення, схеми розташування ОТЗ, наказів керівництва Замовника щодо встановлення межі КЗ, план контрольованих зон об'єкту ЕОТ);

- візуального огляду об'єкту ЕОТ з оцінкою реальних відстаней до межі КЗ.

Перевірка вважається виконаною, якщо фактичні розміри КЗ відповідають представленим документам.

А.4.3.1.5 Перевірка вимог до спеціальних приміщень ЦСК

Метою перевірки є визначення відповідності приміщень вимогам режиму безпеки та додатка 4 до Правил посиленої сертифікації.

Перевірка приміщень виконується у такому порядку:

- аналіз даних щодо об'єкту інформаційної діяльності (ОІД) ЦСК (наказів керівництва щодо переліку спеціальних приміщень та інших організаційно-розпорядчих документів щодо забезпечення режиму безпеки та ТЗІ, акти атестації спеціальних приміщень, акт приймання будівельних робіт (за наявності таких робіт) з оцінкою їх відповідності вимогам ТЗІ, умов експлуатації, плану розташування приміщення, план контрольованих зон ОІД ЦСК);
- візуальний огляд спеціальних приміщень ОІД ЦСК і оцінка додержання вимог щодо забезпечення режиму безпеки та ТЗІ;
- порівняння вихідних даних з даними, що отримані за результатами обстеження.

Перевірка вважається виконаною, якщо спеціальні приміщення ОІД ЦСК відповідають вимогам щодо забезпечення режиму безпеки та додатка 4 до Правил посиленої сертифікації і наданим документам.

А.4.3.1.6 Перевірка правильності розміщення технічних засобів ПТК ЦСК

Метою перевірки є визначення розміщення серверу ЦСК та РС генерації ключів ЦСК (далі — технічних засобів) відповідно до вимог з забезпечення режиму безпеки та додатка 4 до Правил посиленої сертифікації.

Перевірка розміщення технічних засобів ПТК ЦСК виконується у такому порядку:

- візуальний огляд спеціальних приміщень ОІД ЦСК з оцінкою додержання вимог щодо забезпечення режиму безпеки та ТЗІ;
- порівняння вихідних даних з даними, що отримані за результатами обстеження.

Перевірка вважається виконаною, якщо розміщення серверу ЦСК та РС генерації ключів ЦСК відповідають вимогам щодо забезпечення режиму безпеки та додатка 4 до Правил посиленої сертифікації і наданим документам.

А.4.3.1.7 Перевірка ефективності екранування серверної шафи

Метою перевірки ефективності екранування серверної шафи є визначення заданої у п. 8 додатку 4 Правил посиленої сертифікації ефективності екранування спеціальних приміщень щодо захисту від впливів зовнішніх електромагнітних полів.

Перевірка виконується у такому порядку:

- перевіряється конструкторська документація щодо забезпечення заданої ефективності екранування на етапі проектування та монтажу екранів серверної шафи. У якості критерію перевірки використовуються «Рекомендации по применению, устройству и монтажу экранированных помещений и кабин.», М., Связь 1972.;
- візуально перевіряється відповідність реального стану елементів серверної шафи конструкторським рішенням проекту;
- оцінюються результати спеціальних досліджень по даним протоколів забезпеченню реальної ефективності екранування в т.ч.:
- аналіз вихідних даних (протоколів із результатами проведення спеціальних досліджень та спеціальних перевірок ОІД ЦСК, відомостей щодо використаних методичних і нормативних документів та контрольно-виміральної апаратури, порядку проведення спеціальних досліджень об'єкту ЕОТ, протоколів із результатами апаратного контролю ефективності захисту інформації від витоків каналами ПЕМВН, наявності відповідних ліцензій Адміністрації Держспецзв'язку України у осіб, які виконували спеціальні дослідження та спеціальні перевірки об'єкту ЕОТ);
- оцінка відповідності вимогам НД ТЗІ виконаних спеціальних досліджень та спеціальних перевірок ОТЗ об'єкту ЕОТ і коректності отриманих результатів;
- Перевірка вважається виконаною, якщо:
- проектні рішення відповідають вимогам по створенню екранованого приміщення (екранованої шафи) із заданою ефективністю екранування;

- підтверджується документально (є відповідні акти на виробництво) та візуально проектні рішення реалізовані у натурі;
- особи (підприємства), які виконували спеціальні дослідження та спеціальні перевірки об'єкту ЕОТ, мають відповідні ліцензії Адміністрації Держспецзв'язку України на проведення подібних робіт;
- спеціальні дослідження та спеціальні перевірки ОТЗ об'єкту ЕОТ виконані згідно з методичними і нормативними документами ТЗІ з використанням відповідної контрольно-вимірювальної апаратури;
- ефективність екранування серверної шафи відповідає вимогам п. 8 додатку Правил посилення сертифікації.
- Перевірка вважається невиконаною, і випробування можуть бути припинені через наступні порушення вимог по безпеці інформації:
- ефективність екранування серверної шафи не відповідає вимогам п. 8 додатку Правил посилення сертифікації;
- цілком або частково відсутні результати апаратурного контролю ефективності екранування серверної шафи.

А.4.3.1.8 Перевірка схеми енергопостачання ОТЗ, розміщення і монтажу обладнання і силових кабелів, монтажу і параметрам заземлення і кіл заземлення

Метою перевірки є визначення виконання вимог щодо схеми енергопостачання ПТК ЦСК, розміщенню і монтажу обладнання і силових кабелів, розміщення, монтажу і параметрів заземлення і кіл заземлення технічних засобів на ОІД ЦСК вимогам ТР ЕОТ - 95, ТР ПЕМВН-95.

Перевірка вважається виконаною, якщо об'єкт ЕОТ відповідає вимогам зазначених документів. Для об'єкту ЕОТ перевірка вважається невиконаною, і випробування можуть бути припинені через порушення вимог зазначених документів.

А.4.3.1.9 Перевірка сертифікатів і виконання правил експлуатації засобів захисту від ПЕМВН

Метою перевірки є визначення наявності сертифікатів і виконання правил експлуатації засобів захисту.

Комісія розглядає сертифікати, експертні висновки, узгоджені з відповідними державними органами технічні умови тощо, які засвідчують можливість використання програмно-технічні компонентів КСЗІ для захисту інформації. У процесі перевірки комісія повинна переконатися в відповідності цих документів вимогам НД ТЗІ.

А.4.3.1.10 Перевірка документів (актів, протоколів) апаратурного контролю ефективності захисту інформації по каналах ПЕМВН на об'єкті ЕОТ

Перевірка документів (актів, протоколів) апаратурного контролю ефективності засобів захисту здійснюється експертно-документальним методом.

Метою оцінки є встановлення факту, чи дійсно склад і зміст цих документів може забезпечити очікуваний рівень захищеності об'єкту ЕОТ від витоку інформації по каналах ПЕМВН.

Перевірка документів (актів, протоколів) апаратурного контролю ефективності захисту інформації на об'єкті ЕОТ робиться за наступними ознаками:

- використані методики контролю;
- використані тестові засоби;
- повнота проведених вимірів по обсягу і видам вимірів (частотний спектр, режими роботи ОТЗ, обмірювані складові електромагнітного поля, напрямки поширення небезпечних сигналів у просторі);
- використана контрольно-вимірювальна апаратура;
- схема вимірів;
- достовірність результатів вимірів.

Для об'єкту ЕОТ перевірка вважається виконаною, якщо документи (акти, протоколи) апаратурного контролю ефективності захисту інформації на об'єкті ЕОТ відповідають вимогам НД ТЗІ.

Для об'єкту ЕОТ перевірка вважається невиконаною і випробування можуть бути припинені, якщо документи (акти, протоколи) апаратурного контролю ефективності захисту інформації від витоку на об'єкті ЕОТ не відповідають вимогам НД ТЗІ.

А.4.3.1.16 Інструментальна перевірка ефективності захисту інформації від витоку по каналах ПЕМВ, також від порушення цілісності внаслідок деструктивного впливу на ЕОТ зовнішніх електромагнітних полів (при необхідності)

Інструментальна перевірка ефективності захисту інформації ЕОТ від витоку по каналах ПЕМВ, а також від порушення цілісності інформації в ЕОТ внаслідок деструктивного впливу зовнішніх електромагнітних полів виконується при необхідності згідно із відповідною методикою.

А.4.3.2 Перевірка підсистеми антивірусного захисту КСЗІ ЦСК

А.4.3.2.1 Мета випробувань - перевірка роботоспроможності та коректності функціонування засобів антивірусного захисту на відповідність вимогам розділу 4.3.10 ТЗ на КСЗІ ЦСК.

4.3.2.3 Об'єкти випробувань - системи антивірусного захисту засобів ЕОТ ЦСК:

- сканери файлової системи;
- активні монітори файлової системи;
- активні монітори поштового сервера;
- активні монітори поштового клієнта.

А.4.3.3.4 Засоби ЕОТ на яких проводиться тестування

Тестування проводиться на всіх засобах ЕОТ із складу ПТК ЦСК, а саме:

1) на РС адміністраторів проводиться тестування:

- сканерів файлової системи;
- активних моніторів файлової системи;
- активних моніторів поштового клієнта.

2) на РС генерації ключів користувачів проводиться тестування:

- сканерів файлової системи;
- активних моніторів файлової системи.

3) на центральних серверах ЦСК проводиться тестування:

- сканерів файлової системи;
- активних моніторів файлової системи;
- активних моніторів поштового клієнта.

4) на серверах взаємодії проводиться тестування:

- сканерів файлової системи;
- активних моніторів файлової системи;
- активних моніторів поштового сервера.

4.3.3.5 Порядок проведення тестування

1) Сканерів файлової системи:

- для тестування використовуються сигнатури (штами) відомих вірусів;
- сигнатури ін'єктуються у файли різних типів та формату;
- виконується завантаження сканера на перевірку файлової системи;
- за результатами перевірки (протоколу перевірки) робиться висновок щодо роботоспроможності та коректності функціонування засобів антивірусного захисту даного типу.

2) Активних моніторів файлової системи:

- для тестування використовуються сигнатури (штами) відомих вірусів;
- сигнатури ін'єктуються у файли різних типів та формату;
- виконується доступ до інфікованих файлів (завантаження на виконання, зчитування для редагування тощо);
- аналізуються технологічні повідомлення оператору щодо виявлення вірусів, які видає активний монітор, та аналізується реакція на виявлення;
- за результатами перевірки робиться висновок щодо роботоспроможності та коректності функціонування засобів антивірусного захисту даного типу.

3) Активних моніторів поштового клієнта:

- для тестування використовуються сигнатури (штами) відомих вірусів;
- сигнатури ін'єктуються у файли різних типів та формату;
- з окремої РС виконується відправка поштових повідомлень з вкладеними інфікованими файлами;
- аналізуються технологічні повідомлення оператора щодо виявлення вірусів, які видає активний монітор, та аналізується реакція на виявлення;
- за результатами перевірки робиться висновок щодо роботоспроможності та коректності функціонування засобів антивірусного захисту даного типу.

4) Активних моніторів поштового сервера:

- для тестування використовуються сигнатури (штами) відомих вірусів;
- сигнатури ін'єктуються у файли різних типів та формату;
- з окремої РС виконується відправка поштових повідомлень з вкладеними інфікованими файлами;
- аналізуються технологічні повідомлення у журналах реєстрації, які веде активний монітор, та аналізується реакція на виявлення;
- за результатами перевірки робиться висновок щодо роботоспроможності та коректності функціонування засобів антивірусного захисту даного типу.

Перевірка вважається виконаною, якщо склад функцій, номенклатура і діапазон значень параметрів програми антивірусного захисту інформації відповідає вимогам розділу 4.3.10 ТЗ на КСЗІ ЦСК.

А.5 МЕТОДИКА ОЦІНКИ РІВНЯ ДОВІРИ ДО КОРЕКТНОСТІ РЕАЛІЗОВАНОЇ КСЗІ ЦСК (ПЕРЕВІРКА ВИКОНАННЯ ВИМОГ ДО РІВНЯ ГАРАНТІЙ)

А.5.1 Перевірка виконання вимог до рівня гарантій КС здійснюється експертно-документальним методом.

А.5.2 Процес випробувань КС полягає у послідовному перегляді та перевірці результатів і умов виконання наданих у НД ТЗІ 2.5-004-99 критеріїв гарантій щодо вимог до архітектури КЗЗ, середовища розробки, послідовності розробки, середовища функціонування, документації і випробувань КЗЗ.

А.5.3 Необхідними даними для перевірки КС є пояснювальна записка техноробочого проекту КСЗІ, який дає уявлення щодо основних компонентів КЗЗ ОС, їх зв'язку з архітектурними компонентами ОС та ролі у реалізації політики безпеки.

А.5.4 КЗЗ вважається у змозі повністю реалізувати політику безпеки, якщо надані матеріали відповідають вимогам розділів 4, 5 та 6 ТЗ на КСЗІ ЦСК, НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-008-2002.

А.5.5 КЗЗ вважається не спроможною повністю реалізувати політику безпеки, якщо надані матеріали не відповідають вимогам розділів 4, 5 та 6 ТЗ на КСЗІ ЦСК, НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-008-2002.

А.6 УМОВИ І ПОРЯДОК ПРОВЕДЕННЯ ПОПЕРЕДНІХ ВИПРОБУВАНЬ

А.6.1 Попередні випробування КСЗІ ЦСК здійснюються в робочих експлуатаційних режимах за умови наявності усієї сукупності апаратних та програмних засобів захисту інформації, а також технічної і програмної документації на комплексну систему захисту інформації, що розробляється згідно з вимогами технічного завдання на КСЗІ ЦСК.

А.7 ПОРЯДОК ПОДАННЯ РЕЗУЛЬТАТІВ ПОПЕРЕДНІХ ВИПРОБУВАНЬ

А.7.1 Результати попередніх випробувань КСЗІ ЦСК в цілому оцінюються за результатами окремих видів перевірок, виконаних відповідно до розділів 4, 5 даної методики. Результати випробувань не можуть вважатися позитивними, якщо не виконуються вимоги ТЗ.

А.7.2 Результати попередніх випробувань оформлюються протоколами, що складаються за результатами окремих видів перевірок, які підписуються і додаються до Акту попередніх випробувань.