ЕКСПЕРТНИЙ ВИСНОВОК

Зареєстровано в Адміністрації
Державної служби спеціального зв’язку
та захисту інформації України

"___"_____р. за №_____

Дійсний до "___"_____ ____р.

Перший заступник Голови Служби

_____ С.О.Фесенко

м. п.

За результатами експертизи встановлено, що

комплекс засобів захисту інформації від несанкціонованого

назва засобу технічного захисту інформації

доступу системи захисту інформації ЛОЗА-2, версія 3.X.Y

який надано на експертизу ТОВ НДІ „Автопром”,

назва та адреса організації

03150, м. Київ, вул. Тверська, 6

відповідає

відповідає, не відповідає

вимогам нормативних документів системи технічного захисту інформації в Україні в обсязі функцій, зазначених у документі “Система захисту інформації ЛОЗА-2, версія 3.X.Y. Технічне завдання”, сукупність яких визначається функціональним профілем:

- КА-3, КО-1, ЦА-1, ДС-1, ДЗ-1, ДВ-1, НР-4, НИ-3, НК-1, НО-2, НЦ-2, НТ-2 для конфігурації “Підвищена безпека”;
- КД-2, КА-2, КО-1, ЦД-1, ЦА-1, ДС-1, ДЗ-1, ДВ-1, НР-4, НИ-2/НИ-3, НК-1, НО-2, НЦ-2, НТ-2 для конфігурації “Стандартна безпека”

з рівнем гарантій Г-4 оцінки коректності їх реалізації згідно з НД ТЗІ 2.5-004-99 та надає можливість виконання вимог НД ТЗІ 2.5-008-2002 щодо захисту інформації від несанкціонованого доступу.

Вимоги до умов експлуатації та сфери використання об’єкта експертизи визначені у відповідному розділі цього експертного висновку.

Генеральний директор
ТОВ НДІАКС „Екотех” Суслов В.Ю.

_____	_____	_____
керівник Організатора експертизи	підпис м.п.	ініціали, прізвище

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА НАЙМЕНУВАНЬ, ЩО ВИКОРИСТАНІ У ДОКУМЕНТІ

В документі використовуються терміни і визначення, що відповідають встановленим нормативним документом ТЗІ 1.1-003-99 “Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу”, та такі скорочення:

АС – автоматизована система;

ІТС – інформаційно-телекомунікаційна система;

КЗЗ – комплекс засобів захисту;

НД – нормативний документ;

НД ТЗІ - нормативний документ системи технічного захисту інформації;

НСД - несанкціонований доступ;

ОЕ – об’єкт експертизи

ОС - операційна система;

ПЗ - програмне забезпечення;

ТЗІ – технічний захист інформації;

ФПЗ – функціональний профіль захищеності.

1 ЗАГАЛЬНІ ВІДОМОСТІ ЩОДО ОБ'ЄКТА ЕСПЕРТИЗИ

1.1 Повна та скорочена назва ОЕ

Повне найменування об’єкта експертизи (надалі – ОЕ) – система захисту інформації ЛОЗА-2, версія 3.X.Y.

Скорочена назва ОЕ – система ЛОЗА-2.

1.2 Розробник ОЕ

Розробник системи захисту інформації ЛОЗА-2 – ТОВ Науково-дослідний інститут «Автопром» (далі – Розробник).

1.3 Замовник та Організатор експертизи

Замовником державної експертизи є власник ОЕ – ТОВ Науково-дослідний інститут «Автопром» (далі – Замовник).

Адреса Замовника: Україна, 03150, м. Київ, вул. Тверська, 6, ТОВ Науково-дослідний інститут “Автопром”.

Організатором державної експертизи є ТОВ “Науково-дослідний інститут автоматизованих комп’ютерних систем (НДІАКС) “Екотех” (далі – Організатор експертизи.

Адреса Організатора експертизи: 03187 м. Київ, пр. Глушкова 40, корп. 5, ТОВ НДІАКС “Екотех”.

1.4 Вид, мета експертизи та підстави її проведення

Дана експертиза являється первинною державною експертизою комплексу засобів захисту інформації від несанкціонованого доступу (згідно із класифікацією, наведеною в [10]).

Метою даної державної експертизи є оцінювання реалізованих в ОЕ функціональних послуг безпеки (ФПБ) та рівня гарантій коректності їх реалізації на відповідність вимогам НД ТЗІ 2.5-004-99 в обсязі вимог, визначених Технічним завданням [1].

Дана експертиза проводилася на підставі таких документів:

– доручення Державної служби спеціального зв’язку та захисту інформації України (далі – Держспецзв’язку України) на проведення державної експертизи з технічного захисту інформації системи ЛОЗА-2, версія 3.X.Y від 14.04 2011р. № 08/6-899;

– договору від 26.04.2011р. № 222-2011 між Замовником і Організатором.

2 ЗАГАЛЬНА ХАРАКТЕРИСТИКА ОБ'ЄКТА ЕКСПЕРТИЗИ

2.1 Цілі забезпечення безпеки інформації, вирішення яких покладається на ОЕ

Система ЛОЗА-2 – це комплекс засобів захисту від несанкціонованого доступу, призначений для використання в складі комплексної системи захисту інформації в автоматизованих системах класу “2” (згідно із класифікацією, наведеною в документі [8]).

2.2 Вимоги до апаратного середовища функціонування ОЕ

ОЕ може функціонувати у будь-якому апаратному середовищі, в якому використовуються комп’ютери на платформах x86/x64.

2.3 Вимоги до програмного середовища функціонування ОЕ

Програмні засоби системи ЛОЗА-2 можуть працювати в операційній системі (ОС) Microsoft Windows XP/Vista/7/2003/2008/2008 R2 (підтримуються 32- та 64-бітні версії).

2.4 Завдання захисту, вирішення яких забезпечується ОЕ

Система ЛОЗА-2 виконує такі функції щодо захисту інформації:

– захист даних довільних форматів на рівні папок жорсткого диска сервера та робочих станцій;

– захист даних довільних форматів на знімних носіях (захист здійснюється на рівні диска);

– захист текстових документів та електронних таблиць MS Office;

– контроль входу до системи, ідентифікація та автентифікація користувачів;

– контроль доступу до процесів;

– контроль доступу до знімних носіїв, в тому числі можливість дозволити роботу тільки із зареєстрованими носіями USB Flash;

– контроль друку інформації;

– контроль цілісності програмного середовища (перевіряється цілісність файлів та папок, розділів та параметрів реєстру, завантажувальних секторів, а також облікових записів Windows);

– гарантоване видалення інформації;

– стійкість до відмов та відновлення після збоїв програмного чи апаратного забезпечення;

– реєстрація важливих подій та аудит журналів Windows, в тому числі миттєву реакцію на виникнення небезпечних подій;

– формування довільних протоколів роботи користувачів, в тому числі протоколу друку.

Система ЛОЗА-2 підтримує:

– різні рівні повноважень користувачів та різні рівні конфіденційності інформації (цілком таємно, таємно, для службового користування, відкрита інформація);

– різні ролі користувачів: роль звичайного користувача та декілька адміністративних ролей (адміністратор безпеки, системний адміністратор, адміністратор документів).

2.5 Перелік функцій захисту та політик безпеки ФПБ ОЕ

Системиа ЛОЗА-2 може постачатися у двох конфігураціях – «Підвищена безпека» та «Стандартна безпека». Перша з них реалізує більш жорстку політику безпеки інформації.

Система ЛОЗА-2 має забезпечувати надання послуг безпеки, наведених нижче (назви та скорочення відповідають документу [7]):

– для конфігурації “Підвищена безпека” відповідно до наступного профілю ([1], підпункт 2.7, таблиця 2.1);

{КА-3, КО-1, ЦА-1, ДС-1, ДЗ-1, ДВ-1, НР-4, НИ-3, НК-1, НО-2, НЦ-2, НТ-2}

– для конфігурації “Стандартна безпека” відповідно до наступного профілю ([1], підпункт 2.7, таблиця 2.2);

{КД-2, КА-2, КО-1, ЦД-1, ЦА-1, ДС-1, ДЗ-1, ДВ-1, НР-4, НИ-2/НИ-3, НК-1, НО-2, НЦ-2, НТ-2}

Опис послуг функціонального профілю захищеності наведений в таблицях 1.1 та 1.2.

Таблиця 1.1 – Опис послуг функціонального профілю захищеності для конфігурації “Підвищена безпека”.

Назва послуги	Рівень надання послуги	
	Позначення	Назва
Конфіденційність		
Адміністративна конфіденційність	КА-3	Повна адміністративна конфіденційність
Повторне використання об’єктів	КО-1	Повторне використання об’єктів
Цілісність		
Адміністративна цілісність	ЦА-1	Мінімальна адміністративна цілісність
Доступність		
Стійкість до відмов	ДС-1	Стійкість при обмежених відмовах
Гаряча заміна	ДЗ-1	Модернізація
Відновлення після збоїв	ДВ-1	Ручне відновлення

Назва послуги	Рівень надання послуги	
	Позначення	Назва
Спостереженість		
Реєстрація	НР-4	Детальна реєстрація
Ідентифікація та автентифікація	НИ-3	Множинна ідентифікація і автентифікація
Достовірний канал	НК-1	Однонаправлений достовірний канал
Розподіл обов’язків	НО-2	Розподіл обов’язків адміністраторів
Цілісність комплексу засобів захисту	НЦ-2	КЗЗ з гарантованою цілісністю
Самотестування	НТ-2	Самотестування при старті

Таблиця 1.2 – Опис послуг функціонального профілю захищеності для конфігурації “Стандартна безпека”.

Назва послуги	Рівень надання послуги	
	Позначення	Назва
Конфіденційність		
Довірча конфіденційність	КД-2	Базова довірча конфіденційність
Адміністративна конфіденційність	КА-2	Базова адміністративна конфіденційність
Повторне використання об’єктів	КО-1	Повторне використання об’єктів
Цілісність		
Довірча цілісність	ЦД-1	Мінімальна довірча цілісність
Адміністративна цілісність	ЦА-1	Мінімальна адміністративна цілісність
Доступність		
Стійкість до відмов	ДС-1	Стійкість при обмежених відмовах
Гаряча заміна	ДЗ-1	Модернізація
Відновлення після збоїв	ДВ-1	Ручне відновлення
Спостереженість		
Реєстрація	НР-4	Детальна реєстрація
Ідентифікація та автентифікація	НИ-2/НИ-3*	Одиночна ідентифікація і автентифікація/ Множинна ідентифікація і автентифікація
Достовірний канал	НК-1	Однонаправлений достовірний канал
Розподіл обов’язків	НО-2	Розподіл обов’язків адміністраторів

Назва послуги	Рівень надання послуги	
	Позначення	Назва
Цілісність комплексу засобів захисту	НЦ-2	КЗЗ з гарантованою цілісністю
Самотестування	НТ-2	Самотестування при старті

*в залежності від значення параметра конфігурації «Перевіряти ключовий диск під час входу до Windows».

2.6 Ідентифікація ОЕ

Версії ОЕ нумеруються за шаблоном 3.X.Y, де X та Y можуть приймати значення 0,1,2 і т.д. X позначає номер редакції, Y – номер модифікації.

Початкова версія ОЕ має номер 3.2.0

Випуск нової редакції (збільшення X) залишає незмінними такі характеристики ОЕ:

– вимоги, сформульовані в Технічному завданні на створення ОЕ[1];

– рішення ескізного проекту ОЕ (склад ОЕ (підсистеми і основні модулі та зв’язки між ними), порядок роботи системи, політика безпеки, підходи до забезпечення цілісності);

Випуск нової модифікації (збільшення Y) додатково залишає незмінними рішення технічного проекту ОЕ.

Для документації, що є незмінною при новій модифікації, номер версії позначається як 3.2.Y, 3.3.Y і т.д.

Для іншої документації номер версії позначається звичайним чином, наприклад, 3.4.5.

3 НОРМАТИВНІ ДОКУМЕНТИ, НА ВІДПОВІДНІСТЬ ВИМОГАМ ЯКИХ ЗДІЙСНЮВАЛАСЬ ОЦІНКА ОБ'ЄКТА ЕКСПЕРТИЗИ

Експертне оцінювання ОЕ проводилося на відповідність вимогам таких нормативних документів системи ТЗІ:

1. НД ТЗІ 2.5-008-2002 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу “2”;

2. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від НСД;

3. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації у комп’ютерних системах від НСД;

4. Наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 16.05.2007 № 93 „Про затвердження положення про державну експертизу в сфері технічного захисту інформації”;

5. НД ТЗІ 2.7-009-09 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу;

6. НД ТЗІ 2.7-010-09 Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.

Функціональний профіль захищеності та рівень гарантій коректності реалізації функціональних послуг безпеки об’єкта експертизи перевірявся на відповідність вимогам, визначеним в документі:

Система захисту інформації ЛОЗА-2, версія 3.X.Y. Технічне завдання.

4 МЕТОДИКА ПРОВЕДЕННЯ ЕКСПЕРТНИХ РОБІТ

Експертні роботи проводилися згідно з документом:

“Державна експертиза з технічного захисту інформації системи захисту інформації ЛОЗА-2, версія 3.X.Y на відповідність вимогам нормативних документів у сфері технічного захисту інформації. Програма експертних випробувань функціональних послуг безпеки та гарантій коректності їх реалізації”.

Обсяг та методи оцінювання ОЕ визначені методиками:

1) Методика експертних випробувань функціональних послуг безпеки [3];
2) Методика експертних випробувань щодо гарантій коректності реалізації функціональних послуг безпеки [4].

Програма експертних випробувань та Методики розроблені Організатором експертизи і погоджені Держспецзв’язку України (лист № 08/3 – 2137 від 19.08.2011).

5 ПЕРЕЛІК ДОКУМЕНТІВ, СКЛАД ПРОГРАМНИХ ЗАСОБІВ, ЯКІ НАДАНО НА ЕКСПЕРТИЗУ

5.1 Перелік документів, що надані на експертизу

Для проведення випробування Розробником надана наступна документація:

1. Документи на систему захисту:

Система захисту інформації ЛОЗА-2 версія 3.X.Y. Технічне завдання.;

ЛОЗА-2-3.П1.01.1 Система захисту інформації ЛОЗА-2, версія 3.X.Y. Пояснювальна записка до ескізного проекту;

ЛОЗА-2-3.П2.01.1 Система захисту інформації ЛОЗА-2, версія 3.2.Y. Пояснювальна записка до технічного проекту;

ЛОЗА-2-3.ПД.01.1 Система захисту інформації ЛОЗА-2, версія 3.2.Y. Загальний опис системи;

ЛОЗА-2-3.ПА.01.1 Система захисту інформації ЛОЗА-2, версія 3.2.Y. Опис програмного забезпечення;

ЛОЗА-2-3.ПА.02.1 Система захисту інформації ЛОЗА-2, версія 3.2.Y. Опис інтерфейсу ядра системи;

ЛОЗА-2-3.І3.01.1 Система захисту інформації ЛОЗА-2, версія 3.2.0. Інструкція адміністратора безпеки;

ЛОЗА-2-3.І3.02.1 Система захисту інформації ЛОЗА-2, версія 3.2.0. Інструкція користувача системи;

ЛОЗА-2-3.І3.03.1 Система захисту інформації ЛОЗА-2, версія 3.2.0. Інструкція системного адміністратора;

ЛОЗА-2-3.І3.04.1 Система захисту інформації ЛОЗА-2, версія 3.2.0. Інструкція адміністратора документів;

ЛОЗА-2-3.І3.05.1 Система захисту інформації ЛОЗА-2, версія 3.2.0. Програма “Захищені документи”. Інструкція користувача;

ЛОЗА-2-3.І3.06.1 Система захисту інформації ЛОЗА-2, версія 3.2.0. Програмні засоби адміністрування системи. Інструкція користувача.;

ЛОЗА-2-3.І3.07.1 Система захисту інформації ЛОЗА-2, версія 3.2.0. Інструкція з інсталяції системи;

ЛОЗА-2-3.ПД.01.1 Система захисту інформації ЛОЗА-2, версія 3.2.0. Паспорт (проект);

ЛОЗА-2-3.ПМ.01.1 Система захисту інформації ЛОЗА-2, версія 3.X.Y. Програма та методика випробувань.

2. Документація з випробувань системи захисту інформації ЛОЗА-2, версія 3.2.0, проведених Розробником:

– Система захисту інформації ЛОЗА-2, версія 3.2.0. Журнал випробувань;

– Система захисту інформації ЛОЗА-2, версія 3.2.0. Звіт про випробування програмного засобу;

– Протокол №1 випробувань програмного засобу.

3. Документація з процедури розробки системи ЛОЗА-2, версія 3.X.Y

Система захисту інформації ЛОЗА-2, версія 3.X.Y. Інструкція розробника.

Система захисту інформації ЛОЗА-2, версія 3.X.Y. Методика забезпечення фізичної, технічної, організаційної та кадрової безпеки у процесі розробки

Документи «Система захисту інформації ЛОЗА -2 версія 3.X.Y. Технічне завдання» та «ЛОЗА-2-3.ПМ.01.1 Система захисту інформації ЛОЗА-2, версія 3.X.Y. Програма та методика випробувань» погоджені з Держспецзв’язку України.

5.2 Склад програмних засобів, що надані на експертизу

Розробником на експертизу надано комплект поставки ОЕ, що складається з наступних функціональних модулів та компонентів:

1. Ядро системи:

Сервер безпеки (файл - LOZASec.exe);

Сервер документів (файл - LOZADocSrv.exe);

Starter (файл - LOZAStarter.exe);

Бібліотека входу до системи для Windows XP/2003 (файл - LOZAGina.dll);

Бібліотека входу до системи для Windows Vista/7/2008 (файл - LOZACred.dll);

Драйвер файлової системи (файл - LOZAFilt.sys).

LOZAGuard (файл LOZAGuard.exe - тільки для робочих станцій)

2. Адміністративні утиліти:

Аудитор (файл - Auditor.exe);

Керування захистом (файл - Safety.exe);

Монітор захисту (файл - Secmon.exe.).

3. Програма для роботи з документами:

Захищені документи (файл - Prodoc.exe).

4. Програма для відновлення системи

Відновлення системи (файл - LozaRecover.exe);

5. Утиліта *WFolders.exe* для вилучення файлів.

6. Утиліта режиму користувача *UserAgent.exe*.

7. Програма для ініціалізації ключових CD/DVD-дисків *LOZAKeygen.exe*.

8. Шаблон безпеки *LOZA-inf***,** призначений для виконання налаштувань політики безпеки операційної системи.

6 РЕЗУЛЬТАТИ ЕКСПЕРТНИХ РОБІТ

6.1 Результати оцінювання ФПБ

Відповідно до Методики [3] випробування функцій захисту ФПБ ОЕ проводились шляхом:

– аналізу документації, перелік якої наведено вище в розділі 5.1;

– виконання незалежного тестування відповідно до переліку тестів [5], розробленого Організатором.

Результати експертних випробувань щодо кожного пункту Методики експертних випробувань [3] викладені у Протоколі експертних випробувань функціональних послуг безпеки [6]. Результати випробувань свідчать, що ОЕ відповідає вимогам нормативних документів системи ТЗІ в обсязі функціонального профілю захищеності, визначеного Технічним завданням ([1], підрозділ 2):

– для конфігурації “Підвищена безпека”:

{КА-3, КО-1, ЦА-1, ДС-1, ДЗ-1, ДВ-1, НР-4, НИ-3, НК-1, НО-2, НЦ-2, НТ-2}

для конфігурації “Стандартна безпека”:

{КД-2, КА-2, КО-1, ЦД-1, ЦА-1, ДС-1, ДЗ-1, ДВ-1, НР-4, НИ-3/НИ-2*, НК-1, НО-2, НЦ-2, НТ-2}

*в залежності від значення параметра конфігурації «Перевіряти ключовий диск під час входу до Windows».

Зміст реалізованих функціональних послуг безпеки та їх рівні відповідають специфікаціям НД ТЗІ 2.5-004 [9] стосовно політики безпеки цих послуг, визначеної в Технічному завданні [1] для об’єктів захисту, вказаних в розділі 2.4 цього експертного висновку.

6.2 Результати оцінювання рівня гарантій коректності реалізації ФПБ

Випробування щодо гарантій безпеки ОЕ здійснювалися за наступними розділами Технічного завдання ([1], розділ 4.3):

– архітектура;

– середовище розробки;

– послідовність розробки;

– середовище функціонування;

– документація;

– випробування КЗЗ.

Результати робіт, проведених за Методикою експертних випробувань щодо гарантій коректності реалізації функціональних послуг безпеки [4], викладено в Протоколі експертних випробувань щодо гарантій коректності реалізації функціональних послуг безпеки [6].

За результатами випробувань щодо рівня гарантій коректності реалізації функціональних послуг безпеки визнано, що:

– реалізація у ОЕ послуг безпеки відповідає з рівнем гарантій Г-4 специфікаціям НД ТЗІ 2.5.004-99 [9] в обсязі функцій, зазначених у Технічному завданні [1];

– впроваджені Розробником архітектура системи, середовище, процедура та послідовність розробки, процедури випробування та розповсюдження системи відповідають специфікаціям рівня гарантій Г-4 згідно з НД ТЗІ 2.5.004-99;

– експлуатаційна документація на ОЕ відповідає специфікаціям рівня гарантій Г-4 згідно з НД ТЗІ 2.5.004-99.

6.3 Результати оцінювання відповідності ОЕ вимогам чинних нормативних документів щодо забезпечення захисту інформації в ІТС

За результатами випробувань щодо можливості використання ОЕ для забезпечення захисту інформації в певних типах ІТС визнано, що ОЕ надає можливість виконання вимог НД ТЗІ 2.5-008-2002 щодо захисту інформації від несанкціонованого доступу в ІТС класу 2.

7 ВИСНОВКИ ЗА РЕЗУЛЬТАТАМИ ЕКСПЕРТИЗИ

7.1 Висновки за результатами оцінювання ФПБ

За результатами випробувань функціональних послуг безпеки визнано наступне:

ОЕ відповідає вимогам НД ТЗІ 2.5-004 [9] в обсязі функціонального профілю захищеності, визначеного Технічним завданням ([1], підрозділ 2):

– для конфігурації “Підвищена безпека”

2.КЦД = {КА-3, КО-1, ЦА-1, ДС-1, ДЗ-1, ДВ-1, НР-4, НИ-3, НК-1, НО-2, НЦ-2, НТ-2}

– для конфігурації “Стандартна безпека”

2.КЦД = {КД-2, КА-2, КО-1, ЦД-1, ЦА-1, ДС-1, ДЗ-1, ДВ-1, НР-4, НИ-3/НИ-2*, НК-1, НО-2, НЦ-2, НТ-2}

*в залежності від значення параметра конфігурації «Перевіряти ключовий диск під час входу до Windows».

Зміст реалізованих функціональних послуг безпеки та їх рівні відповідають вимогам НД ТЗІ 2.5-004 [9] стосовно політики безпеки цих послуг, визначеної в Технічному завданні [1] для об’єктів захисту, вказаних в розділі 2.4 цього експертного висновку.

7.2 Висновки за результатами оцінювання рівня гарантій коректності реалізації ФПБ

За результатами випробувань визнано, що рівень гарантій коректності реалізації в ОЕ функціональних послуг безпеки відповідає вимогам НД ТЗІ 2.5.004-99 [9] до рівня гарантій Г-4.

7.3 Висновки за результатами оцінювання відповідності ОЕ вимогам чинних нормативних документів щодо забезпечення захисту інформації в ІТС

За результатами випробувань щодо можливості використання ОЕ для забезпечення захисту інформації в певних типах ІТС визнано, що ОЕ надає можливість виконання вимог НД ТЗІ 2.5-008-2002 щодо захисту інформації від несанкціонованого доступу в ІТС класу 2.

ОЕ в конфігураціях „Стандартна безпека” та „Підвищена безпека” в складі комплексних систем захисту інформації в ІТС класу “2” може використовуватись для захисту службової інформації, конфіденційної інформації (у тому числі персональних даних) та іншої інформації з обмеженим доступом.

Для захисту інформації, що становить державну таємницю, рекомендується використовувати ОЕ в конфігурації „Підвищена безпека”. Можливість використання ОЕ для захисту інформації, що становить державну таємницю, в ІТС класу “2” встановлюється окремо для кожної ІТС.

7.4 Висновки за результатами оцінювання відповідності ОЕ в обсязі функцій, визначених у паспорті, вимогам чинних нормативних документів

На підставі експертної оцінки документації ОЕ зроблено висновок про відповідність ОЕ в обсязі функцій, визначених у паспорті, вимогам чинних нормативних документів системи ТЗІ в Україні.

7.5 Висновки щодо сфери застосування результатів експертизи

Дія цього експертного висновку поширюється на систему ЛОЗА-2, версія 3.2.0, а також на всі наступні версії системи ЛОЗА-2, номер яких відповідає шаблону 3.X.Y згідно з правилами, наведеними в пункті 2.6 цього експертного висновку (за умови проведення випробувань нової версії за документом “ЛОЗА-2-3.ПМ.01.1 Система захисту інформації ЛОЗА-2, версія 3.X.Y. Програма та методика випробувань” та передачі до Держспецзв’язку України затвердженого протоколу випробувань).

8 ВИМОГИ ДО УМОВ ВИКОРИСТАННЯ ОБ'ЄКТА ЕКСПЕРТИЗИ

Наведені в п.7 висновки чинні тільки за наступних умов:

– на кожному комп’ютері локальної обчислювальної мережі, в якій використовується ОЕ, встановлена лише одна операційна система (може бути встановлена будь-яка операційна система із переліку, наведеного в пункті 2.3 цього експертного висновку);

– шляхом встановлення параметрів BIOS та/або іншими методами повинна бути забезпечена неможливість завантаження користувачем ОС зі змінних носіїв.

Для реалізації ОЕ в конфігурації „Стандартна безпека” функціонального профілю захищеності КД-2, КА-2, КО-1, ЦД-1, ЦА-1, ДС-1, ДЗ-1, ДВ-1, НР-4, НИ-3, НК-1, НО-2, НЦ-2, НТ-2 для параметра конфігурації “Перевіряти ключовий диск під час входу до Windows” повинно бути встановлення значення “Так”.

У випадку встановлення значення “Ні” для параметра конфігурації ОЕ “Перевіряти ключовий диск під час входу до Windows” послуга “Ідентифікація та автентифікація” реалізується на рівні “НИ-2” – “Одиночна ідентифікація та автентифікація”.

9 ТЕРМІН ДІЇ ЕКСПЕРТНОГО ВИСНОВКУ

Термін дії експертного висновку – три роки з дати реєстрації експертного висновку.

10 ОСОБЛИВІ ДУМКИ ЕКСПЕРТІВ

Протоколи експертизи не містять особливих думок експертів.

11 ПЕРЕЛІК ПОСИЛАНЬ

1) Система захисту інформації ЛОЗА -2 версія 3.X.Y. Технічне завдання.

2) Державна експертиза з технічного захисту інформації системи захисту інформації ЛОЗА-2, версія 3.X.Y, на відповідність вимогам нормативних документів у сфері технічного захисту інформації. Програма експертних випробувань функціональних послуг безпеки та гарантій коректності їх реалізації.

3) Державна експертиза з технічного захисту інформації системи захисту інформації ЛОЗА-2, версія 3.X.Y, на відповідність вимогам нормативних документів у сфері технічного захисту інформації. Методика експертних випробувань функціональних послуг безпеки.

4) Державна експертиза з технічного захисту інформації системи захисту інформації ЛОЗА-2, версія 3.X.Y, на відповідність вимогам нормативних документів у сфері технічного захисту інформації. Методика експертних випробувань щодо гарантій коректності реалізації функціональних послуг безпеки.

5) Державна експертиза з технічного захисту інформації системи захисту інформації ЛОЗА-2, версія 3.X.Y, на відповідність вимогам нормативних документів у сфері технічного захисту інформації. Перелік тестів.

6) Державна експертиза з технічного захисту інформації системи захисту інформації ЛОЗА-2, версія 3.X.Y, на відповідність вимогам нормативних документів у сфері технічного захисту інформації. Протокол експертних випробувань функціональних послуг безпеки.

7) Державна експертиза з технічного захисту інформації системи захисту інформації ЛОЗА-2, версія 3.X.Y, на відповідність вимогам нормативних документів у сфері технічного захисту інформації. Протокол експертних випробувань щодо гарантій коректності реалізації функціональних послуг безпеки.

8) НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 р. № 22.

9) НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від НСД. Затверджені наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.1999 р. за №22.

10) НД ТЗІ 2.5-008-2002 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу “2”. Затверджені наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.2002 р. за №22.

11) НД ТЗІ 2.6-001-11 Порядок проведення робіт із державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. Затверджено наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 25.03.2011 р. № 65.

12) НД ТЗІ 2.7-009-09 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу. Затверджено наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 24.07.2009 р. № 172.

13) НД ТЗІ 2.7-010-09 Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу. Затверджено наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 24.07.2009 р. № 172.