1. Загальні відомості щодо об’єкта експертизи

Об’єкт експертизи – система захисту інформації ЛОЗА-1 (версія 3.X.Y) (надалі об’єкт експертизи - ОЕ). ОЕ призначений для використання у складі комплексної системи захисту інформації в автоматизованих системах (АС) класу 1 з технологіями обробки інформації Т1 та Т2 відповідно до НД ТЗІ 2.5-007-2001.

Виробник: ТОВ Науково-дослідний інститут “Автопром”.

Адреса виробника: Україна, м. Київ, вул. Саперне поле, 9а.

Виконавець робіт з експертизи ОЕ: ТОВ НДІАКС “Екотех”. Адреса: 03187, Київ 187, пр. Академіка Глушкова, 40, корп.5.

2. Загальна характеристика об’єкта експертизи

2.1 Об’єкти захисту

ОЕ дозволяє захистити інформацію, яка міститься в таких об’єктах:

1) Бази документів.
2) Документи.
3) Захищені папки.
4) Знімні диски.
5) Захищені процеси.
6) Технологічна інформація:

– база облікових записів:

- список користувачів (перелік користувачів із їхніми атрибутами доступу та даними, необхідними для автентифікації);
- список груп користувачів;

– журнал реєстрації;

– параметри конфігурації системи;

– оперативні дані про роботу системи (дані про поточний стан системи, результати перевірок цілісності, відомості про операції, які наразі виконуються у системі тощо).

2.2 Функції захисту

ОЕ забезпечує виконання таких функцій захисту:

– ідентифікація і автентифікація користувачів на підставі імені та носимого ідентифікатора під час реєстрації у системі;

– адміністрування інформаційних ресурсів та повноважень користувачів;

– адміністративне та довірче керування доступом до захищених інформаційних ресурсів;

– розмежування доступу користувачів до захищених інформаційних ресурсів;

– гарантоване вилучення інформації з обмеженим доступом шляхом затирання вмісту при вилученні;

– контроль цілісності програмного забезпечення та конфігураційних даних системи захисту та відновлення після збоїв;

– реєстрацію подій щодо спроб здійснення санкціонованого та несанкціонованого доступу до захищених інформаційних ресурсів, роботи з програмами, керування доступом та системою, друку тощо, а також здійснення несанкціонованого доступу;

– контроль за експортом та друком документів;

2.3 Засоби захисту ОЕ

ОЕ складається з окремих компонентів, кожний з яких реалізує визначену функціональність, а саме:

1) Ядро системи:

– *Сервер безпеки;*

– *Сервер документів;*

– *LozaStarter;*

– *Бібліотека входу до системи для Windows XP;*

– *Бібліотека входу до системи для Windows Vista/7;*

– *Драйвер файлової системи;*

– *Агент користувача*

2) Адміністративні програми:

– *Аудитор;*

– *Керування захистом;*

– *Монітор захисту.*

3) Програма для роботи з документами:

– *Захищені документи.*

4) Програма для відновлення системи:

– *Відновлення системи*.

Сервер безпеки забезпечує виконання таких функцій:

- загальне керування системою (початок та завершення роботи, зміни стану тощо);
- автентифікація користувачів;
- виконання ПРД під час доступу до всіх об'єктів захисту, крім баз документів та документів;
- перевірка цілісності;
- реєстрація подій.

LOZAStarter призначена для автоматичного запуску Сервера безпеки і розроблена як служба (service) Windows, яка запускається автоматично на початку роботи ОС.

Сервер документів забезпечує виконання правил розмежування доступу до баз документів та документів (крім видів доступу ***Друк*** та ***Експорт*** для документів).

Бібліотеки входу до системи для Windows XP та ***Windows Vista/7*** призначені для ідентифікації та автентифікації користувачів.

Драйвер файлової системи є мініфільтром, який за рахунок взаємодії з Сервером безпеки забезпечує захист об'єктів захисту на рівні файлової системи.

Програма ***Агент користувача*** призначена для виконання деяких завдань, які необхідно виконувати від імені поточного користувача системи (наприклад, видалення тимчасових фалів користувачів).

Програми ***Аудитор, Керування захистом*** та ***Монітор захисту*** призначені для адміністрування системи.

Програма ***Аудитор*** надає можливість переглядати журнал захисту, створювати його резервні копії і працювати зі створеними раніше копіями, а також формувати протоколи роботи системи.

Програма ***Керування захистом*** призначена для роботи з технологічною інформацією.

Програма ***Монітор захисту*** надає інтерфейс для оперативного керування системою (зміни стану системи, виконання перевірок цілісності за запитом адміністратора, обробка помилок, які виникають під час виконання операцій) та спостереження за її роботою.

Програма ***Захищені документи*** надає користувачам інтерфейс для роботи з базами документів та документами. Програма ***Захищені документи*** забезпечує виконання ПРД для видів доступу ***Друк*** та ***Експорт*** для документів, а також здійснює захист даних, які під час роботи знаходяться на екрані монітора (від копіювання у системний буфер обміну, друкування тощо).

2.4 Реалізація послуг безпеки

ОЕ надає послуги безпеки, зазначені в таблиці 2.1

Таблиця 2.1 –Послуг безпеки, що реалізуються ОЕ

Критерій	**Послуга**		**Рівень послуги**	
Конфіденційність	Адміністративна конфіденційність		КА-2	Базова адміністративна конфіденційність
	Довірча конфіденційність		КД-2	Базова довірча конфіденційність
	Повторне використання об’єктів		КО-0	Повторне використання об'єктів
Цілісність	Адміністративна цілісність		ЦА-1	Мінімальна адміністративна цілісність
	Довірча цілісність		ЦД-1	Мінімальна довірча цілісність
	Гаряча заміна		ДЗ-1	Модернізація
	Відновлення після збоїв		ДВ-1	Ручне відновлення
Спостереженість	Реєстрація (аудит)		НР-2	Захищений журнал
	Ідентифікація і автентифікація	підвищена безпека	НИ-3	Множинна ідентифікація і автентифікація
		стандартна безпека	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
	Цілісність КЗЗ		НЦ-2	КЗЗ з гарантованою цілісністю
	Самотестування		НТ-2	Самотестування при старті

*НИ-2/НИ-3 – рівень надання послуги залежить від значень параметрів конфігурації ОЕ.

Перелік компонентів ОЕ відповідно до послуг безпеки, які вони реалізують, зазначено у таблиці 2.2

Таблиця 2.2 – Реалізація послуг безпеки засобами ОЕ

Рівень послуги	**Назва компоненту ОЕ**
Довірча конфіденційність – КД-2	– Сервер безпеки – Сервер документів – Драйвер файлової системи – Керування захистом – Захищені документи
Адміністративна конфіденційність – КА-2	– Сервер безпеки – Сервер документів – Драйвер файлової системи – Керування захистом – Захищені документи
Повторне використання об’єктів – КО-0	– Сервер безпеки – Сервер документів – Драйвер файлової системи – Агент користувача – Керування захистом
Довірча цілісність – ЦД-1	– Сервер безпеки – Сервер документів – Драйвер файлової системи – Керування захистом
Адміністративна цілісність – ЦА-1	– Сервер безпеки – Сервер документів – Драйвер файлової системи – Керування захистом
Гаряча заміна – ДЗ-1	– Сервер безпеки – Драйвер файлової системи
Відновлення після збоїв – ДВ-1	– Сервер безпеки – Монітор захисту
Реєстрація – НР-2	– Сервер безпеки – Сервер документів – Драйвер файлової системи – Аудитор – Керування захистом – Захищені документи
Ідентифікація та автентифікація – НИ-3/НИ-2	– Сервер безпеки – Бібліотека входу до системи для Windows XP – Бібліотека входу до системи для Windows Vista/7 – Керування захистом

Рівень послуги	**Назва компоненту ОЕ**
Достовірний канал – НК-1	– Сервер безпеки – Бібліотека входу до системи для Windows XP – Бібліотека входу до системи для Windows Vista/7 – Керування захистом
Розподіл обов'язків – НО-2	– Сервер безпеки – Сервер документів – Керування захистом – Захищені документи
Цілісність комплексу засобів захисту – НЦ-2	– Сервер безпеки – Драйвер файлової системи – Керування захистом – Монітор захисту
Самотестування – НТ-2	– Сервер безпеки – Драйвер файлової системи – Керування захистом – Монітор захисту

2.5 Ідентифікація ОЕ

Версії З ОЕ нумеруються за шаблоном 3.X.Y, де X позначає номер редакції, Y – номер модифікації.

Початкова версія ОЕ нумерується 3.0.0

Випуск нової редакції залишає незмінними такі характеристики ОЕ:

– вимоги, сформульовані в технічному завданні на створення ОЕ;

– 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 залишає незмінними рішення технічного проекту ОЕ.

Документація, що є незмінною при новій модифікації має позначку (версія 3.X), де X приймає значення 0,1,2 і т.д.

Інша документація має позначку (версія 3.X.У). X, Y залежать від номера версії та номера модифікації та приймають значення 0,1,2 і т.д.

ОЕ поставляється Замовнику у наступному вигляді:

– дистрибутив системи на компакт-диску;

– ліцензійна угода;

– документація в електронному вигляді на компакт-диску в такому складі:

- Паспорт;
- Інструкція з інсталяції;
- Загальний опис системи;
- Інструкція адміністратора безпеки;
- Інструкція системного адміністратора;
- Інструкція адміністратора документів;
- Інструкція користувача;
- Програма “Захищені документи”. Інструкція користувача;
- Програмні засоби адміністрування системи. Інструкція користувача;
- Типове технічне завдання на створення комплексної системи захисту інформації;

– документація у друкованому вигляді в такому складі:

- Паспорт;
- Інструкція з інсталяції.

3. Нормативні та технічні документи з технічного захисту інформації, на відповідність вимогам яких здійснювалась оцінка ОЕ

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

– НД ТЗІ 2.5-007-2007 Вимоги до комплексу засобів захисту інформації, що становить державну таємницю, від несанкціонованого доступу при її обробці в автоматизованих системах класу “1”. Чинний від 21.09.2007 р.;

– НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від НСД. Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.99 р. за №22;

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

– 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;

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

4. Назва окремої методики, згідно з якою здійснювалася оцінка КСЗІ

Експертні роботи виконувалися згідно з Програмою експертних випробувань функціональних послуг та гарантій безпеки, погодженою із Замовником експертизи та Державною службою спеціального зв'язку та захисту інформації України, Методикою експертних випробувань функціональних послуг безпеки та Методикою експертних випробувань щодо рівня гарантій, погодженими з Державною службою спеціального зв'язку та захисту інформації України України.

5. Склад програмно-технічних засобів та документів, які надано на експертизу

5.1 Склад програмних засобів, наданих на випробування.

1) Дистрибутиви LOZA-1_HS_Setup.exe та LOZA-1_Setup.exe, за допомогою яких здійснюється інсталяція ОЕ та наприкінці інсталяції виконується початкова настройка системи – створення адміністратора безпеки системи ЛОЗА-1, виконання настройок Windows, необхідних для роботи системи ЛОЗА-1, та встановлення для параметрів конфігурації, визначених у документі ЛОЗА-1.ПД.01.1 Загальний опис системи (Додаток А. Параметри конфігурації системи), значень за умовчанням.

Під час початкової настройки ведеться журнал, у якому фіксуються всі дії, які виконуються під час початкової настройки, і зазначається успішність або неуспішність виконання цих дій.

Дистрибутив LOZA-1_HS_Setup.exe призначений для інсталяції ОЕ в конфігурації „Підвищена безпека". Ця конфігурація системи призначена для захисту інформації, що становить державну таємницю.

Дистрибутив LOZA-1_Setup.exe призначений для інсталяції ОЕ в конфігурації „Стандартна безпека". Ця конфігурація системи може використовуватися для захисту інформації, що не становить державну таємницю.

Зазначені дистрибутиви дозволяють також здійснити автоматичне поновлення програмних засобів КЗЗ відповідно до внесених Розробником змін.

5.2 1. Документи на ОЕ:

Система захисту інформації ЛОЗА-1 (версія 3.X.Y). Технічне завдання, погоджене з ДССЗЗІ України, вих. 8/3-1325 від 26.04.2010;

ЛОЗА-1.П1.01.3 Пояснювальна записка до ескізного проекту;

ЛОЗА-1.П2.01.3 Пояснювальна записка до технічного проекту;

ЛОЗА-1.ПД.01.3 Загальний опис системи;

ЛОЗА-1.ПА.01.3 Опис програмного забезпечення;

ЛОЗА-1.ПА.02.3 Опис інтерфейсу ядра системи;

ЛОЗА-1.І3.01.3 Інструкція адміністратора безпеки;

ЛОЗА-1.І3.02.3 Інструкція користувача системи;

ЛОЗА-1.І3.03.3 Інструкція системного адміністратора;

ЛОЗА-1.І3.04.3 Інструкція адміністратора документів;

ЛОЗА-1.І3.05.3 Програма “Захищені документи”. Інструкція користувача;

ЛОЗА-1.І3.06.3 Програмні засоби адміністрування системи. Інструкція користувача.;

ЛОЗА-1.І3.07.3 Інструкція з інсталяції системи;

ЛОЗА-1.ПМ.01.3 Програма та методика випробувань погоджена з ДССЗЗІ України, вих. 8/3-1836 від 11.06.2010.

Фрагменти вихідного коду

2. Документація з випробувань ОЕ, проведених Розробником:

– Система захисту інформації ЛОЗА-1 (версія 3.0.0). Журнал випробувань програмних засобів;

– Система захисту інформації ЛОЗА-1 (версія 3.0.0). Звіт про випробування програмних засобів;

– Протокол №1 випробувань програмних засобів системи захисту інформації ЛОЗА-1 (версія 3.0.0).

3. Документація з процедури розробки ОЕ:

– Інструкція розробника.

6. Результати експертних робіт

6.1 Комплектність ОЕ відповідає специфікації комплектності, визначеній у документах на поставку.

6.2 Сукупність реалізованих у ОЕ функцій та механізмів захисту інформації визначається згідно з НД ТЗІ 2.5-004-99 таким функціональним профілем:

Для конфігурації «Підвищена безпека»

КД-2, КА-2, КО-0, ЦД-1, ЦА-1, ДВ-1, ДЗ-1, НР-2, НИ-3, НК-1, НО-2, НЦ-2, НТ-2.

Для конфігурації «Стандартна безпека безпека»

КД-2, КА-2, КО-0, ЦД-1, ЦА-1, ДВ-1, ДЗ-1, НР-2, 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».

6.3 За результатами експертних випробувань ОЕ встановлено, що:

– рівні реалізованих у ОЕ послуг безпеки (таблиця 2.1) відповідають з рівнем гарантій Г-3 вимогам НД ТЗІ 2.5.004-99 в обсязі функцій, зазначених у документі Система захисту інформації ЛОЗА-1 (версія 3.X.Y). Технічне завдання;

– впроваджені виробником архітектура системи, середовище, процедура та послідовність розробки, процедури випробування та розповсюдження системи відповідають специфікаціям рівня гарантій Г-3 згідно з НД ТЗІ 2.5.004-99;

– експлуатаційна документація на КЗЗ ОЕ відповідає специфікаціям рівня гарантій Г3 згідно з НД ТЗІ 2.5.004-99.

6.4. Результати експертних випробувань пунктів Методики експертних випробувань функціональних послуг безпеки та Методики експертних випробувань щодо рівня гарантій, викладені у Протоколі випробувань функціональних послуг безпеки та Протоколі випробувань щодо гарантій безпеки. Матеріали протоколів свідчать, що зміст реалізованих функціональних послуг безпеки та їх рівні відповідають вимогам НД ТЗІ 2.5.004-99 стосовно визначеної в ОЕ політики безпеки.

6.5. ОЕ в конфігурації „Підвищена безпека” реалізує функціональний профіль захищеності з рівнем реалізації послуг, що відповідають функціональному профілю СФП (Т2), визначеному згідно з НД ТЗІ 2.5-007-2001 як стандартний функціональний профіль захищеності від загроз НСД до інформації, що становить державну таємницю. Конфігурація „Підвищена безпека” повинна також використовуватися для захисту інформації, що становить державну таємницю, при технології обробки інформації Т1.

6.6 Середовище розробки ОЕ є довіреним, що дозволяє Розробнику ОЕ здійснювати модифікацію системи та випускати нову її редакцію без проведення додаткової державної експертизи.

У випадку зміни рішень ескізного проекту та/або вимог ТЗ випускається нова версія ОЕ - версія 4, для якої повинна бути проведена державна експертиза.

7 Висновки щодо відповідності об'єкта експертизи вимогам нормативних документів системи ТЗІ

На підставі експертної оцінки за критеріями ТЗІ ОЕ встановлюється наступне:

Наданий на випробування ОЕ відповідає вимогам нормативних документів з питань ТЗІ та технічного завдання.

Сукупність реалізованих КЗЗ ОЕ функцій та механізмів захисту з рівнем гарантій Г-3 забезпечує реалізацію наведеного у п.6.2 функціонального профілю захищеності інформації.

Розробка виконана у відповідності до вимог НД ТЗІ 2.5-007-2007 Вимоги до комплексу засобів захисту інформації, що становить державну таємницю, від несанкціонованого доступу при її обробці в автоматизованих системах класу “1”.

ОЕ в конфігурації „Підвищена безпека” може використовуватися для захисту інформації в АС класу “1”, у яких здійснюється обробка інформації, що становить державну таємницю.

8 Сфера використання (вимоги до умов експлуатації) об'єкта експертизи

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

- на комп’ютері, на якому використовується ОЕ, має бути встановлена тільки одна операційна система. У випадку необхідності використовувати додаткову операційну систему, її завантаження має бути повністю контрольованим адміністратором;
- шляхом встановлення параметрів BIOS та/або іншими методами повинна бути забезпечена неможливість завантаження користувачем ОС зі змінних носіїв;
- каталоги, в яких розміщується ОЕ, та каталоги даних, із якими працює система, якщо вони зберігаються на жорсткому диску, повинні знаходитися на NTFS розділах жорсткого диску.

Для реалізації ОЕ в конфігурації „Стандартна безпека” функціонального профілю захищеності КД-2, КА-2, КО-0, ЦД-1, ЦА-1, ДВ-1, ДЗ-1, НР-2, НИ-3, НК-1, НО-2, НЦ-2, НТ-2 для параметру конфігурації “Перевіряти ключовий диск під час входу до Windows” повинно бути встановлення значення “Так”.

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

9 Термін дії експертного висновку

Термін дії експертного висновку до 17.09.2013.

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;

КЗЗ - комплекс засобів захисту;

КСЗІ – комплексна система захисту інформації;

НД ТЗІ - нормативний документ системи технічного захисту інформації;

НСД - несанкціонований доступ;

ОС - операційна система;

ПЗ - програмне забезпечення.