1. ІДЕНТИФІКАЦІЯ ОБ'ЄКТА ЕКСПЕРТИЗИ

Об’єктом експертизи є система захисту інформації ЛОЗА™-2, версія 4.X.Y [1] (далі – система «Лоза-2»). Склад програмних засобів, що входять до складу об’єкту експертизи наведено в додатку А до цього документу.

Дія експертного висновку розповсюджується на зразки системи «Лоза-2» версії 4.X.Y (X, Y – цілі невід’ємна числа), склад яких відповідає даним, наведеним в додатку А до цього документу та які виготовлені товариством з обмеженою відповідальністю «Науково-дослідний інститут «Автопром» протягом терміну його дії, з урахуванням умов, зазначених у розділі 8 до цього документу.

Експертним випробуванням підлягає сукупність програмних засобів, які входять до складу системи «Лоза-2» та призначені для реалізації політики безпеки інформації згідно вимог документу «Система захисту інформації ЛОЗА™-2, версія 4.X.Y. Технічне завдання. Редакція 1» (далі – ТЗ).

Державна експертиза в сфері технічного захисту інформації Система «Лоза-2» проводиться на виконання рішення Експертної ради з питань державної експертизи в сфері технічного захисту інформації Адміністрації Держспецзв’язку (протокол засідання від 25.09.2015 № 11-2015) та відповідно до листа ДТЗІ Адміністрації Держспецзв’язку від 15.11.2015 № 08/02/03-2344.

2. ЗАГАЛЬНІ ВІДОМОСТІ ЩОДО ОБ'ЄКТА ЕКСПЕРТИЗИ

2.1. Найменування, відомості про розробника, виробника об’єкту експертизи

Найменування об’єкту експертизи: система захисту інформації ЛОЗА™-2, версія 4.X.Y (далі – система «Лоза-2»).

Розробник, виробник системи «Лоза-2» та замовник експертизи: товариство з обмеженою відповідальністю «Науково-дослідний інститут «Автопром» (далі – ТОВ НДІ «Автопром») (фізична адреса: 03150, м. Київ, вул. Тверська, 6, офіс № 405, код ЄДРПОУ 33102567).

2.2. Призначення та функції об’єкту експертизи

Об’єкт випробувань – система «Лоза-2», що являє собою комплекс програмних засобів, призначений для використання в складі комплексної системи захисту інформації в автоматизованих системах класу 2 та 3[2]. (згідно із класифікацією, наведеною в документі НД ТЗІ 2.5–005–99). Система розроблена у двох конфігураціях: «Підвищена безпека» та «Стандартна безпека». Далі в тексті документа в тих випадках, коли це не може призвести до неоднозначного тлумачення, словом «система» позначається система «Лоза-2».

Система «Лоза-2» може використовуватись для захисту відкритої інформації та інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, у тому числі інформації, що становить державну таємницю (конфігурація «Підвищена безпека»). Обробка інформації, що становить державну таємницю, здійснюється тільки в рамках ІТС класу 2.

Система «Лоза-2» має забезпечувати захист файлів будь-яких форматів, які зберігаються на стаціонарних носіях (жорстких дисках комп’ютера) та на знімних носіях (дискетах, дисках USB Flash та ін.). Захист здійснюється на рівні папки для даних, які зберігаються на жорстких дисках, та на рівні розділу диска для даних, які зберігаються на знімних дисках.

---

[1] X, Y – ціле невід’ємне число.

[2] При застосуванні системи «Лоза-2» у складі ІТС класу 3, передача інформації, вимога щодо захисту якої встановлена законом, через телекомунікаційні мережі загального користування (або іншими незахищеними каналами зв’язку) між взаємодіючими компонентами цієї ІТС повинна здійснюватись по захищеному з'єднанню, що утворюється засобами криптографічного захисту інформації (далі – КЗІ), для яких в експертному висновку зазначена можливість їх використання для захисту інформації з відповідним правовим статусом.

Система ЛОЗА-2 має в своєму складі спеціалізовані засоби захисту текстових документів Microsoft Word та електронних таблиць Microsoft Excel. Захист здійснюється на рівні окремого документа та бази документів. Система надає можливість зберігати документи на стаціонарних та знімних носіях.

Передбачено дві конфігурації системи – «Підвищена безпека» та «Стандартна безпека». Перша з них повинна реалізує більш жорстку політику безпеки інформації.

Система «Лоза-2» має забезпечувати надання послуг безпеки, наведених в таблицях 2.1 та 2.2 (назви та скорочення відповідають документу НД ТЗІ 2.5-004-99).

Таблиця 2.1 Профіль системи «Лоза-2», конфігурація «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
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 2.2 Профіль системи «Лоза-2», конфігурація «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

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

Примітка: *НИ-2/НИ-3 – рівень надання послуги залежить від значень параметрів конфігурації системи «Лоза-2».

Процес розробки системи «Лоза-2» має відповідати рівню гарантій Г-4 згідно з НД ТЗІ 2.5-004-99.

Для супроводження системи «Лоза-2» в складі персоналу автоматизованої системи мають бути передбачені такі особи або групи осіб:

- адміністратор безпеки;
- системний адміністратор;
- адміністратор документів.

3. ЗАГАЛЬНА ХАРАКТЕРИСТИКА ОБ'ЄКТА ЕКСПЕРТИЗИ

3.1. Функціональна структура

3.1.1. *Компоненти внутрішньої архітектури*

Перелік компонентів архітектури системи приведено в таблиці 3.1.

Таблиця 3.1

Компонент архітектури системи	Програмні складові
Ядро системи	*Сервер безпеки для сервера системи* (LOZASec.exe)
	Сервер безпеки для робочих станцій (LOZAGuard.exe)
	Сервер документів (LOZADocProcSrv.exe)
	LOZAStarter (LOZAStarter.exe)
	LOZAGina.dll
	LOZACred.dll
	LOZAFlt.sys
	Агент користувача (UserAgent.exe)
Адміністративні утиліти	*Аудитор* (Auditor.exe)
	Керування захистом (Safety.exe)
	Монітор захисту (SecMon.exe)
Програма для роботи з документами	*Захищені документи* (ProDoc.exe)
Додаткові утиліти	*Відновлення системи* (LOZARecover.exe)
	Реєстрація (Register.exe)

Нижче приведено опис компонентів архітектури системи:

1) **Ядро системи** складається з наступних програмних компонентів:

Сервер безпеки

Головною частиною системи є програма *Сервер безпеки*. Це DCOM-сервер, який виконує основні завдання із захисту інформації.

Програми *Сервер документів*, *LOZAStarter*, *LOZAGina.dll*, *LOZACred.dll*, *Захищені документи* та адміністративні утиліти працюють як клієнти *Сервера безпеки*. На початку роботи всі ці програмні засоби обов'язково реєструються за допомогою виклику відповідного методу інтерфейсу *Сервера безпеки.*

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;
- перевірки цілісності;
- реєстрація подій.

Сервер безпеки надає іншим програмам доступ до технологічної інформації.

Сервер безпеки запускається від імені спеціально створеного користувача, пароль якого є випадковим і постійно змінюється.

LOZAStater

Програма *LOZAStarter* використовується для автоматичного запуску *Сервера безпеки*. Вона є службою (service) Windows, яка запускається автоматично на початку роботи ОС.

Програма *LOZAStarter* запускається від імені системи (System).

Сервер документів

Сервер документів – це служба, яка забезпечує зберігання баз документів та документів і виконує основні завдання із захисту баз документів та документів. Програма *Захищені документи*, яка надає користувачам інтерфейс для роботи з базами документів та документами, отримує доступ до них тільки за допомогою викликів відповідних інтерфейсних методів *Сервера документів.*

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

Сервер документів запускається від імені спеціально створеного користувача, пароль якого є випадковим і постійно змінюється.

Інші компоненти ядра

Бібліотеки *LOZAGina.dll* та *LOZACred.dll* призначені для ідентифікації та автентифікації користувачів.

Перша з них використовується в ОС Widnows XP і заміщує стандартну бібліотеку Windows *Gina.dll*.

Бібліотека *LOZACred.dll* поєднує в собі дві компоненти: вона є провайдером облікових даних (credential provider) і фільтром інших провайдерів.

Драйвер файлової системи *LOZAFlt.sys* 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). Програма *Агент користувача* є DCOM-сервером, який настроєний на запуск від імені інтерактивного користувача.

2) **Адміністративні утиліти**

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 коригування технологічної інформації та встановлення настройок системи.

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

Програма Захищені документи

Програма *Захищені документи* надає користувачам інтерфейс для роботи з базами документів та документами. Програми Microsoft Word та Microsoft Excel працюють як незалежні програми, настройками яких керує програма *Захищені документи*. Для доступу до документів програма *Захищені документи* звертається до *Сервера документів*, який передає їй необхідні дані (документ або пов'язані із ним дані) або приймає відкориговані дані для збереження.

Програма *Захищені документи* забезпечує виконання ПРД для видів доступу *Друк* та *Експорт* для документів.

Циркуляція інформаційних потоків між компонентами програми відображено на нижче представленій блок схемі (див. рис. 3.1).

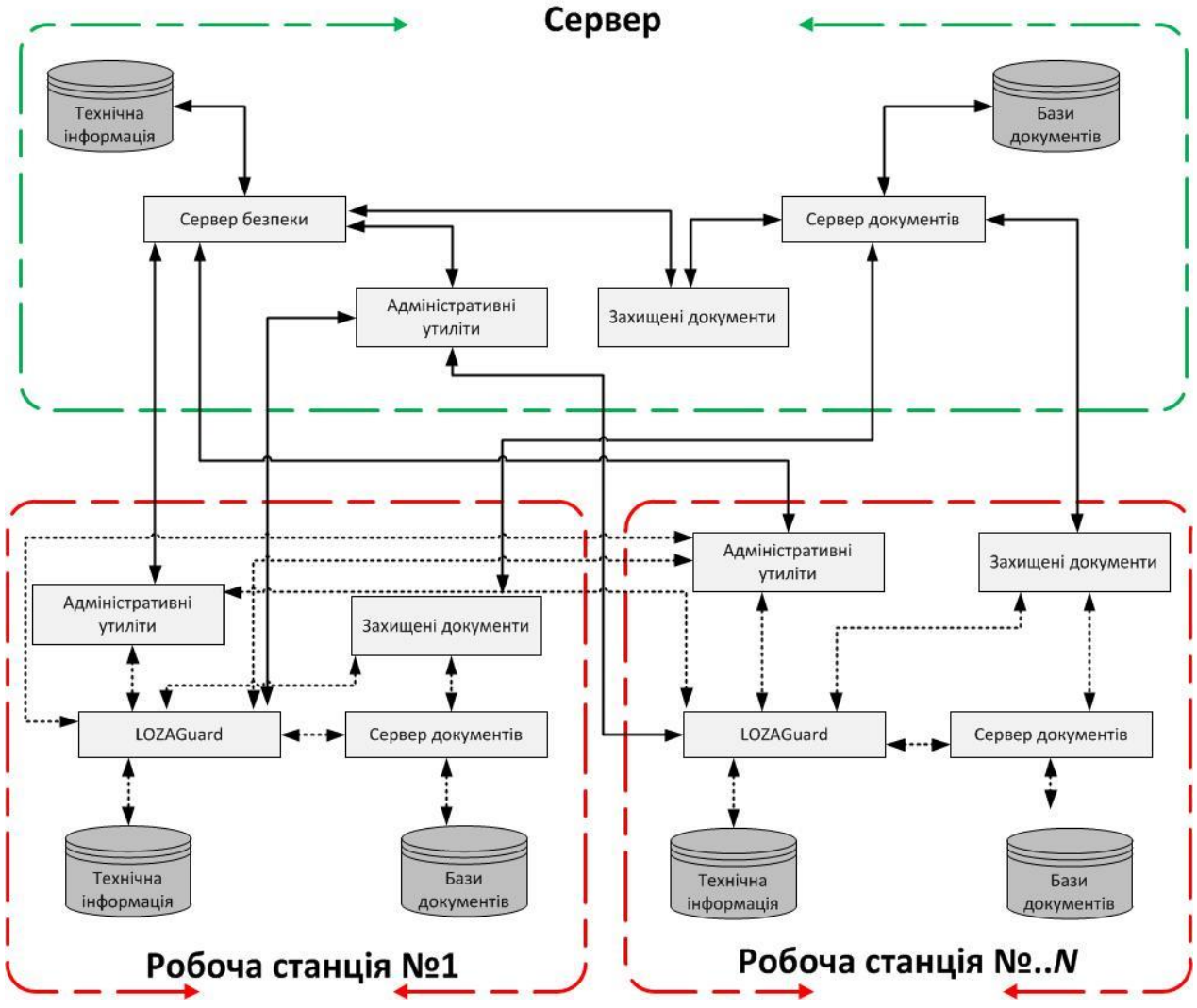

Рис. 3.1. Блок схема роботи програми

3.1.2. *Реалізація функцій підсистеми*

У таблиці 3.3 зазначено, які програмні модулі реалізують функції підсистем, з яких складається система «Лоза-2».

Таблиця 3.2

Підсистема	Програмні модулі
Керуюча підсистема	– Сервер безпеки; – LOZAStarter; – LOZAGina.dll; – LOZACred.dll; – Агент користувача; – Аудитор; – Керування захистом; – Монітор захисту
Підсистема керування доступом	– Сервер безпеки; – Сервер документів; – LOZAFlt.sys; – Агент користувача; – Керування захистом; – Захищені документи
Підсистема забезпечення цілісності	– Сервер безпеки; – LOZAFlt.sys; – Керування захистом; – Монітор захисту
Підсистема реєстрації подій	– Сервер безпеки – Аудитор; – Керування захистом

3.1.3. *Реалізація функцій безпеки*

Система має реалізовувати послуги безпеки наведені в таблицях 2.1 та 2.2. У таблиці 3.3 вказано, які саме компоненти системи «Лоза-2» мають реалізовувати зазначені послуги.

Таблиця 3.3

Послуга	Компоненти системи «Лоза-2»
Довірча конфіденційність – КД-2	– Сервер безпеки; – Сервер документів; – LOZAFlt.sys; – Керування захистом; – Захищені документи
Адміністративна конфіденційність – КА-3/КА-2	– Сервер безпеки; – Сервер документів; – LOZAFlt.sys; – Керування захистом; – Захищені документи
Повторне використання об’єктів – КО-1	– Сервер безпеки; – Сервер документів; – LOZAFlt.sys; – Агент користувача; – Керування захистом

Послуга	Компоненти системи «Лоза-2»
Довірча цілісність – ЦД-1	– Сервер безпеки; – Сервер документів; – LOZAFlt.sys; – Керування захистом
Адміністративна цілісність – ЦА-1	– Сервер безпеки; – Сервер документів; – LOZAFlt.sys; – Керування захистом
Гаряча заміна – ДЗ-1	– Сервер безпеки; – LOZAFlt.sys
Відновлення після збоїв – ДВ-1	– Сервер безпеки; – Монітор захисту
Реєстрація – НР-4	– Сервер безпеки; – Сервер документів; – LOZAFlt.sys; – Аудитор; – Керування захистом; – Захищені документи
Ідентифікація та автентифікація – НИ-3	– Сервер безпеки; – LOZAGina.dll; – LOZACred.dll; – Керування захистом
Достовірний канал – НК-1	– Сервер безпеки; – LOZAGina.dll; – LOZACred.dll; – Керування захистом
Розподіл обов’язків – НО-2	– Сервер безпеки; – Сервер документів; – Керування захистом – Захищені документи
Цілісність комплексу засобів захисту – НЦ-2	– Сервер безпеки; – LOZAFlt.sys; – Керування захистом; – Монітор захисту
Самотестування – НТ-2	– Сервер безпеки; – LOZAFlt.sys; – Керування захистом; – Монітор захисту

3.2. Стани системи

Для проведення різних видів робіт у системі передбачено два стани:

- робочий стан;
- стан відновлення.

Звичайні користувачі мають доступ до даних лише в «*робочому стані*». Цей стан призначений для проведення звичайної роботи системи і в ньому система має перебувати переважну частину часу.

Стан «*відновлення*» призначений для проведення відновлення програмного забезпечення та критичних для роботи системи даних, таких як, наприклад, системний реєстр та технологічна інформація.

На початку роботи система автоматично переходить у стан, який визначається в залежності від того, яким чином була завершена робота в попередньому сеансі, і

відбувається за такими правилами:

– якщо в попередньому сеансі роботи відбулось звичайне або некоректне завершення роботи, початковим є «*робочий стан*».

– якщо в попередньому сеансі роботи відбулось аварійне завершення роботи, система починає роботу в стані «*відновлення*».

Завершення роботи системи може бути звичайним, аварійним або некоректним.

Вважається, що відбулось звичайне завершення роботи, якщо було здійснене завершення роботи стандартними засобами операційної системи.

У випадку виявлення порушення цілісності під час перебування системи в «*робочому*» стані, система здійснює аварійне завершення роботи (якщо це визначено параметром конфігурації реакція на порушення цілісності).

Під час аварійного завершення роботи користувач, який працює за комп'ютером, впродовж 5 хв. отримує попередження про необхідність закінчити роботу. Після того як зазначений час мине (або користувач припинить роботу), ініціюється завершення роботи операційної системи.

Якщо робота була завершена внаслідок збою або вимкнення комп'ютера, вважається, що система завершила роботу некоректно.

Переходи між переліченими вище станами здійснює адміністратор безпеки та/або системний адміністратор за допомогою програми *Монітор захисту*. Система може змінити стан «із власної ініціативи» лише в одному випадку – після виявлення порушень цілісності. Під час перебування системи в «*робочому*» стані виконується автоматична перевірка цілісності програмного середовища. У стані «*відновлення*» перевірка припиняється.

Під час переходу зі стану відновлення в робочий стан проводиться перевірка цілісності, і перехід здійснюється лише у випадку позитивного результату перевірки.

Вихід та вхід користувачів в операційну систему (logon та logoff) не впливають на стан системи.

Деталізовані відомості щодо архітектури, особливостей побудови та функціонування системи «Лоза-2» наведені в документі «ЛОЗА-2-4.ПД.01.1 Система захисту інформації ЛОЗА-2 (версія 4.2.0). Загальний опис системи».

4. ВИМОГИ НОРМАТИВНИХ ДОКУМЕНТІВ З ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ, НА ВІДПОВІДНІСТЬ ЯКИМ ЗДІЙСНЮЄТЬСЯ ОЦІНКА ОБ'ЄКТА ЕКСПЕРТИЗИ

Експертні роботи здійснювалися на відповідність наступним нормативним документам з технічного захисту інформації:

– «Система захисту інформації ЛОЗА™-2, версія 4.X.Y. Технічне завдання. Редакція 1». Обл. № 101 н/т від 28.04.15р., погоджено Держспецзв'язку від 22.05.2015р;

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

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

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

– НД ТЗІ 2.6-001-11 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах.

5. МЕТОДИКА ПРОВЕДЕННЯ РОБІТ

Державна експертиза в сфері технічного захисту інформації системи «Лоза-2» проводилась Інститутом спеціального зв'язку та захисту інформації НТУУ «КПІ» згідно погоджених Департаментом технічного захисту інформації Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Програма державної експертизи у сфері технічного захисту інформації системи захисту інформації ЛОЗА™-2,

версія 4.X.Y» (№ 25/03-3350 від 05.11.2015) та «Методика державної експертизи у сфері технічного захисту інформації системи захисту інформації ЛОЗА™-2, версія 4.X.Y» (далі – Методика) (№ 25/03-3351 від 05.11.2015).

6. ПЕРЕЛІК ДОКУМЕНТІВ І СПЕЦИФІКАЦІЙ ПРОГРАМНИХ ТА ТЕХНІЧНИХ ЗАСОБІВ, ЯКІ НАДАНО ЗАМОВНИКОМ ОРГАНІЗАТОРУ ЕКСПЕРТИЗИ

Перелік файлів програмного забезпечення системи «Лоза-2», яке представлено для проведення державної експертизи в сфері технічного захисту інформації, наведений в додатку А до цього документу.

Перелік наданих документів щодо системи «Лоза-2»:

Документація з випробувань системи захисту інформації Лоза-2, версія 4.X.Y, проведених Розробником:

1. Технічне завдання на систему захисту інформації ЛОЗА-2 (версія 4.X.Y). Редакція 4; Обл. № 101 н/т від 28.04.15р., погоджено Держспецзв'язку від 22.05.2015р.
2. ЛОЗА-2-4.П1.01.1 Система захисту інформації ЛОЗА-2 (версія 4.X.Y). Пояснювальна записка до ескізного проекту; обл. № 149 н/т від 07.07.15р.
3. ЛОЗА-2-4.ПА.01.1 Система захисту інформації ЛОЗА-2 (версія 4.X.Y). Опис програмного забезпечення; обл. № 151 н/т від 07.07.15р.
4. ЛОЗА-2-4.ПА.02.1 Система захисту інформації ЛОЗА-2 (версія 4.X.Y). Опис інтерфейсу ядра системи; обл. № 152 н/т від 07.07.15р.
5. ЛОЗА-2-4.ПД.01.1 Система захисту інформації ЛОЗА-2 (версія 4.2.0). Загальний опис системи; обл. № 153 н/т від 07.07.15р.
6. ЛОЗА-2-4.І3.01.1 Система захисту інформації ЛОЗА-2 (версія 4.2.0). Інструкція адміністратора безпеки; обл. № 154 н/т від 07.07.15р.
7. ЛОЗА-2-4.І3.02.1 Система захисту інформації ЛОЗА-2 (версія 4.2.0). Інструкція користувача системи; обл. № 155 н/т від 07.07.15р.
8. ЛОЗА-2-4.І3.03.1 Система захисту інформації ЛОЗА-2 (версія 4.2.0). Інструкція системного адміністратора; обл. № 156 н/т від 07.07.15р.
9. ЛОЗА-2-4.І3.04.1 Система захисту інформації ЛОЗА-2 (версія 4.2.0). Інструкція адміністратора документів; обл. № 157 н/т від 07.07.15р.
10. ЛОЗА-2-4.І3.05.1 Система захисту інформації ЛОЗА-2 (версія 4.2.0). Програма «Захищені документи». Інструкція користувача; обл. № 158 н/т від 07.07.15р.
11. ЛОЗА-2-4.І3.06.1 Система захисту інформації ЛОЗА-2 (версія 4.2.0). Програмні засоби адміністрування системи. Інструкція користувача; обл. № 1598 н/т від 07.07.15р.
12. ЛОЗА-2-4.І3.07.1 Система захисту інформації ЛОЗА-2 (версія 4.2.0). Інструкція з інсталяції; обл. № 160 н/т від 07.07.15р.
13. ЛОЗА-2-4.ПМ.01.1 Система захисту інформації ЛОЗА-2 (версія 4). Програма та методика випробувань; обл. № 161 н/т від 07.07.15р.
14. ЛОЗА-2-4.ПД.01.2 Система захисту інформації ЛОЗА-2, версія 4.2.0. Паспорт (проект). обл. № 162 від 07.07.15р.
15. ЛОЗА-2-4.П2.01.1 Система захисту інформації ЛОЗА-2 (версія 4.X.Y). Пояснювальна записка до технічного проекту; обл. № 150 н/т від 07.07.15р.

Документація з випробувань системи захисту інформації Лоза-2, версія 4.X.Y, проведених Розробником:

16. Система захисту інформації ЛОЗА-2, версія 4.2.0. Журнал випробувань програмних засобів; обл. № 163 н/т від 22.08.15р.
17. Система захисту інформації ЛОЗА-2, версія 4.2.0. Звіт про випробування програмного засобу; обл. № 164 н/т від 22.08.15р.
18. Наказ «Про проведення попередніх випробувань системи захисту інформації ЛОЗА-2, версія 4.2.0»; обл. № 165 н/т від 02.06.15р.
19. Протокол №1 випробувань програмного засобу. обл. № 166 н/т від 22.08.15р.

Документація з процедури розробки системи Лоза-2 (версія 4):

20. Інструкція розробника систем захисту інформації «Лоза-2», версія 4.X.Y, та ЛОЗА-2, версія 4.X.Y обл. № 46 від 05.06.14р.

21. Методика забезпечення фізичної, технічної, організаційної та кадрової безпеки у процесі розробки систем захисту інформації ЛОЗА-2, версія 4.X.Y. обл. № 167 н/т від 07.07.15р.

Далі за текстом документу наведені посилання на документи з наведеного переліку.

7. РЕЗУЛЬТАТИ РОБІТ ЩОДО КОЖНОГО ПУНКТУ МЕТОДИКИ ЕКСПЕРТИЗИ ОБ'ЄКТА

Висновки щодо відповідності об'єкта експертизи вимогам ТЗ та нормативних документів системи ТЗІ за результатами експертних випробувань по кожному пункту Методики викладені в документі «Протокол виконання робіт відповідно до розділу 3 методики державної експертизи у сфері технічного захисту інформації системи захисту інформації ЛОЗА™-2, версія 4.X.Y».

7.1. Результати перевірки вимог до рівня гарантій

За результатами перевірки вимог до рівня гарантій, визначених у НД ТЗІ 2.5-004-99, експерти зробили висновок, що:

– система «Лоза-2» відповідає вимогам до архітектури рівня гарантій Г-4;

– система «Лоза-2» відповідає вимогам до середовища розробки рівня гарантій Г-4;

– система «Лоза-2» відповідає вимогам до послідовності розробки рівня гарантій Г-4;

– система «Лоза-2» відповідає вимогам до середовища функціонування рівня гарантій Г-4;

– система «Лоза-2» відповідає вимогам до документації рівня гарантій Г-4;

– система «Лоза-2» відповідає вимогам до випробувань рівня гарантій Г-4.

7.2. Результати перевірки вимог до захисту інформації від загроз несанкціонованого доступу

За результатами перевірки системи «Лоза-2» на відповідність вимогам до захисту інформації від загроз несанкціонованого доступу експерти зробили такі висновки:

– система «Лоза-2» відповідає вимогам до об’єктів захисту, суб’єктів доступу та атрибутів, згідно з якими здійснюється їх взаємодія, визначеним в п. 4.1.1, 4.1.4, 4.1.6 ТЗ;

– система «Лоза-2» коректно реалізує послуги безпеки в обсязі функціонального профілю захищеності 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}, та для конфігурації «стандартна безпека» – {КА-2, КД-2, КО-1, ЦА-1, ЦД-1, ДС-1, ДЗ-1, ДВ-1, НР-4, НИ-2/НИ-3, НК-1, НО-2, НЦ-2, НТ-2} відповідно до вимог п. 4.2 ТЗ та НД ТЗІ 2.5-004-99;

– система «Лоза-2» відповідає вимогам п. 6.1 – 6.3, 7.1, 7.2, 8.2 – 8.4, 9.1 – 9.6 НД ТЗІ 2.5-004-99 та ТЗ.

– програмні модулі (класи, функції, методи тощо), які забезпечують реалізацію механізмів ідентифікації та автентифікації користувачів (послуги безпеки НИ-3, НК-1), безпечного використання об’єктів (послуга безпеки КО-1), розмежування доступу до об’єктів захисту (послуги безпеки КД-2, КА-3/КА-2, ЦД-1, ЦА-1) та контролю цілісності КЗЗ (послуга безпеки НЦ-2) містять реалізацію відповідних функціональних послуг безпеки, «недокументовані» можливості в них відсутні.

7.3. Характеристика функціональних послуг безпеки, що реалізуються КЗЗ системи «Лоза-2»

Зауваження до проведення перевірок: Принципи та механізми реалізації функціональних послуг безпеки однакові для серверної та клієнтської версії системи «Лоза-2», тому нижчезазначені перевірки почергово були проведені на серверній ЕОМ та на робочій станції користувача.

7.3.1. Політика адміністративної конфіденційності та цілісності *функціональних послуг безпеки «КА-2»/«КА-3»* та «ЦА-1»*, що реалізується системою «Лоза-2»,

відноситься до об’єктів захисту, наведених в табл. 7.1 окрім довірчих баз документів та документів, які містяться у довірчих базах.

Примітка: * у конфігурації «Стандартна безпека» система «Лоза-2» дозволяє створення об’єктів із довірчим керуванням доступом. Тому у цій конфігурації послуга надається на рівні КА 2 – «Базова адміністративна конфіденційність»

Табл. 7.1

Об’єкт захисту	Умовне позначення
Адміністративні бази документів	{admin_bd}
Довірчі бази документів	{User_bd}
Документи в адміністративних базах (текстові та електронні таблиці)	{admin_doc}
Документи в довірчих базах (текстові та електронні таблиці)	{user_doc}
Захищені папки	{p_folder}
Знімні диски	{r_drive}
Захищені процеси	{p_process}
База облікових записів	{bd_accounts}
Перелік комп’ютерів під’єднаних до серверу системи	{bd_computers}
Дані про бази документів та документи	{bd_config_doc}
Дані про об’єкти захисту (списки захищених папок, зареєстрованих Flash-носіїв, захищених процесів)	{bd_config_sec}
Журнал реєстрації	{log}
Параметри конфігурації системи	{config}
Оперативні данні про роботу системи	{system}
Програмні засоби системи «Лоза-2»	{program}

У системі «Лоза-2» присутні суб’єкти доступу, наведені в табл. 7.2.

Табл. 7.2

Суб’єкт доступу	Умовне позначення
системний адміністратор	[SysAdmin]
адміністратор безпеки	[SecAdmin]
адміністратор документів	[DocAdmin]
звичайні користувачі	[User]

Правила розмежування доступу суб’єктів до адміністративних баз даних, що реалізуються системою «Лоза-2», відображені в табл. 7.3.

Таблиця 7.3

типи доступу / користувачі	Створення	Читання атрибутів	Читання списку документів	Створення папок	Видалення папок	Перейменування папок	Створення документів	Запис атрибутів	перейменування	видалення	Запис власника	Запис списку доступу	Запис списку аудита
[User]	-	+	+	+	+	+	+	-	-	-	-	-	-
[SecAdmin]	-	+*	+*	-	-	-	-	-	-	-	+*	-	-
[SysAdmin]	-	-	-	-	-	-	-	-	-	-	-	-	-
[DocAdmin]	+	+	+	+	+	+	+	+	+	+	+	+	+

Примітка: * - відповідний доступ надається для того, щоб не втратити можливість доступу до бази у випадку відсутності власника. Адміністратор безпеки має право змінити власника бази та документів на іншого користувача за умови що користувач входить до групи «адміністратори» та рівень його допуску не нижчий за максимальний рівень доступу документів цієї бази.

Правила розмежування доступу суб’єктів до документів, що знаходяться в адміністративної базі даних, відображені в табл. 7.4.

Таблиця 7.4

типи доступу / користувачі	Читання	Запис	Читання атрибутів доступу	Запис атрибутів	Видалення	Друк	Експорт	Запис власника	Запис рівня доступу	Запис списку доступу	Запис списку аудита
[User]	+	+	+	+	+	+	+	-	-	-	-
[SecAdmin]	-	-	+	-	-	-	-	-	-	-	-
[SysAdmin]	-	-	-	-	-	-	-	-	-	-	-
[DocAdmin]	+	+	+	+	+	+	+	+	+	+	+

Правила розмежування доступу суб'єктів до захищених папок відображені в табл. 7.5.

Таблиця 7.5

типи доступу / користувачі	Читання	Запис
[User]	+	+
[SecAdmin]	+	+
[SysAdmin]	-	-
[DocAdmin]	-	-

Суб'єкти системи «Лоза-2» мають наступні види доступу до об'єктів, що містять технологічну інформацію, наведені в табл. 7.6.

Таблиця 7.6

типи доступу / користувачі	Читання бази облікових записів	Запис до бази облікових записів	Читання даних про об'єкти захисту	Запис даних про об'єкти захисту	Читання параметрів конфігурації системи	Запис параметрів конфігурації системи	Читання довідника рівнів доступу	Запис довідника рівнів доступу	Читання журналу реєстрації	Читання оперативних даних про роботу системи	Запис оперативних даних про роботу системи
[User]	-	-	-	-	-	-	-	-	-	-	-
[SecAdmin]	+	+	+	+	+	+	+	+	+	+	+
[SysAdmin]	-	-	-	-	+*	-	-	-	-	+	-
[DocAdmin]	-	-	-	-	-	-	-	-	-	-	-

За внутрішніми алгоритмами перевірки повноважень система «Лоза-2» реалізує санкціонування доступу суб'єкта доступу до об'єкта захисту або відмову у такому доступі.

Система «Лоза-2» забезпечує можливість визначення користувачам не менше ніж чотири ролі користувача («адміністратор безпеки», «адміністратор документів», «системний адміністратор» та «звичайний користувач»), а також можливість поділу

інформації, що обробляється, не менше ніж на п’ять рівнів конфіденційності («цілком таємна інформація», «таємна інформація», «службова інформація», «конфіденційна інформація» та «відкрита інформація») . Для розподілу користувачів за наведеними рівнями використовуються службові групи:

– «LOZASecAdmins» – для доступу з повноваженнями адміністратора безпеки;
– «LOZADocAdmins» – для доступу з повноваженнями адміністратора документів;
– «LOZASysAdmins» – для доступу з повноваженнями системного адміністратора;
– «LOZAUsers» – для доступу з повноваженнями звичайного користувача.

Користувач має можливість запуску лише тих процесів, які дозволені йому адміністратором безпеки; можливості запускати інші процеси він не має; процес отримує доступ до об’єктів лише згідно тих прав доступу, які має користувач, що здійснив його запуск.

Користувач має можливість використання лише тих пристроїв ЕОМ (принтери, знімні носії інформації типу: гнучкий диск FDD, CD/DVD-диск, або носії USB Flash), які дозволені йому адміністратором безпеки; можливості використання інших пристроїв він не має; в будь-якому випадку спробу використання пристроїв ЕОМ для обробки об’єктів з більш високим рівнем обмеження доступу ніж наявний у користувача буде завершено невдало.

Додатково для об'єктів захисту, що містять технологічну інформацію встановлюються додаткові правила розмежування доступу, які враховують поділ об'єктів та користувачів на локальні та глобальні. Користувачі які мають ознаку «Глобальні» мають всі види доступу, що передбачені роллю користувача, до локальних та глобальних об’єктів захисту. Користувачі які мають ознаку «Локальний» мають доступ тільки на перегляд (читання) глобальних об’єктів, які містять технологічну інформацію та всі види доступу, що передбачені роллю користувача, до локальних об’єктів захисту (за умови, що об'єкт захисту належить до комп'ютера, вказаного в повному переліку комп'ютерів користувача).

Управління правами користувачів та процесів щодо доступу до інформаційних об’єктів здійснюється адміністратором безпеки.

Права доступу до об’єктів захисту встановлюються в момент їх створення (об’єктів файлової системи, об’єктів-процесів, конфігураційних та системних об’єктів) та ініціалізації (пристроїв ЕОМ).

Користувач може здійснено експорт лише об’єктів, які дозволені йому адміністратором безпеки (для об’єктів файлової системи – мають рівень обмеження доступу не вищий за рівень користувача); при експорті об’єктів атрибути доступу, які були встановлені раніше, не зберігаються. Користувач може здійснити імпорт лише об’єктів, які дозволені йому адміністратором безпеки (для об’єктів файлової системи – мають рівень обмеження доступу не вищий за рівень користувача), та лише до каталогів, які дозволені йому адміністратором безпеки та мають рівень обмеження доступу не вищий за рівень користувача. Експлуатаційна документація на системи «Лоза-2» містить рекомендації щодо безпечного поводження із об’єктами файлової системи при проведенні експорту даних з комплексу [6].

Реалізація механізмів адміністративного управління доступом в системі «Лоза-2» забезпечується наступними програмними засобами:

– реалізація механізмів розмежування доступу до захищених документів та баз документів реалізується програмним модулем *Сервер документів* та здійснюється шляхом виклику виконання методу `CheckBaseAction` класу `TLOZADocServerInterface` модулю `LOZADocSrv_IntfUnit.pas`;

– реалізація механізмів захисту буферу обміну реалізується програмним модулем *Захищені документи* та здійснюється шляхом виклику виконання методу `OnCLipCapture` класу `TfmMain` модулю `Main.pas`;

– реалізація механізмів розмежування доступу для захищених папок, знімних дисків, захищених процесів, та технологічної інформації реалізується програмними модулями *Сервер безпеки* та *LOZAGuard* та здійснюється шляхом виклику виконання методу `CheckAccessToProtectedPath` класу `TLOZA` модулю `LOZAType.pas`;

будь-які недокументовані можливості в зазначених методах відсутні.

7.3.2. Політика довірчої конфіденційності та цілісності *функціональних послуг безпеки «КД-2» та «ЦД-1»*, що реалізується системою «Лоза-2», відноситься до наступних об'єктів захисту:

- довірчі бази документів;
- документи, які містяться в довірчих базах.

Правила розмежування доступу суб'єктів до довірчих баз даних, що реалізуються системою «Лоза-2», відображені в табл. 7.7.

Таблиця 7.7

типи доступу / користувачі	Створення	Читання атрибутів	Читання списку документів	Створення папок	Видалення папок	Перейменування папок	Створення документів	Запис атрибутів	перейменування	видалення	Запис власника	Запис списку доступу	Запис списку аудита
[User]	+	+	+	+	+	+	+	+	+	+	+	+	+
[User1]	+	+	+	+	+	+	+	+*	+*	+*	+*	+*	+*
[SecAdmin]	-	+**	+**	-	-	-	-	-	-	-	+**	-	-
[SysAdmin]	-	-	-	-	-	-	-	-	-	-	-	-	-
[DocAdmin]	-	-	-	-	-	-	-	-	-	-	-	-	-

Примітка:

* - користувач отримує відповідний доступ за умови надання йому повного доступу до довірчої бази.

** - додатково, для того, щоб не втратити можливість доступу до бази у випадку відсутності власника, а також для забезпечення можливості реалізації аналогічного додаткового правила доступу до документів встановлюється ці правила, які діють для всіх довірчих баз незалежно від списку доступу бази.

Правила розмежування доступу суб'єктів до документів, що знаходяться в довірчої базі даних, що реалізуються системою «Лоза-2», відображені в табл. 7.8.

Таблиця 7.8

типи доступу / користувачі	Читання	Запис	Читання атрибутів доступу	Запис атрибутів	Видалення	Друк	Експорт	Запис власника	Запис рівня доступу	Запис списку доступу	Запис списку аудита
[User]	+	+	+	+	+	+	+	+	+	+	+
[User1]	+	+	+	+*	+*	+	+	+*	+	+*	+*
[SecAdmin]	-	-	+**	-	-	-	-	+**	-	-	-
[SysAdmin]	-	-	-	-	-	-	-	-	-	-	-
[DocAdmin]	-	-	-	-	-	-	-	-	-	-	-

Права доступу до об'єктів захисту встановлюються в момент їх створення та ініціалізації. Система «Лоза-2» не дозоляє створення об'єктів із невизначеними атрибутами доступу [5].

При експорті об'єктів захисту у вигляді об'єктів файлової системи атрибути доступу не зберігаються; експлуатаційна документація на систему містить рекомендації щодо безпечного поводження із об'єктами файлової системи користувачем, власником цих об'єктів, при проведенні експорту даних з системи [7]. Права доступу до імпортованих об'єктів захисту не зберігаються; імпортовані об'єкти захисту потребують налаштування прав доступу до них.

7.3.3. В рамках реалізації *функціональної послуги безпеки «КО-1»* система «Лоза-2» забезпечує скасування прав доступу для користувачів (процесів), які вони можуть одержати при доступі до об'єктів захисту, звільнених іншим користувачем (процесом), а також очищення змісту об'єктів захисту перш ніж певний користувач (процес) зможе одержати їх в своє розпорядження після звільненням цих об'єктів іншим користувачем (процесом).

Послуга стосується до атрибутів доступу об'єктів захисту, а також до таких файлів:

– файли, в яких зберігаються бази документів;

– файли, в яких зберігаються документи;

– файли, в яких зберігається технологічна інформація;

– тимчасові файли користувачів;

– файли, які зберігаються у захищених папках та на зареєстрованих дисках USB Flash.

Механізм повторного використання об'єктів реалізує взаємну ізоляцію адресного простору процесів, очищення пам'яті після її звільнення, а також ізоляцію тимчасових файлів, що створюються впродовж сесії роботи користувача.

Забезпечення ізоляції адресного простору процесів реалізується шляхом виділення для кожного процесу окремої директорії сторінок фізичної пам'яті та неможливістю прямої зміни процесом цієї директорії та інших структур керування пам'яттю.

Обнуління сторінок пам'яті при їхньому звільненні забезпечується потоком обнуління сторінок, який переводить очищенні сторінки в список, з якого потім проводиться їхнє видалення. Такий механізм гарантує обнуління звільненої пам'яті в визначений проміжок часу (цей проміжок залежить від завантаження системи), навіть у випадку відсутності запитів на виділення пам'яті.

Забезпечення ізоляції тимчасових файлів, що можуть створюватись програмним забезпеченням під час свого виконання впродовж сесії роботи користувача, реалізується шляхом розміщення тимчасових файлів в окремій системній директорії відповідного профілю користувача та їх видалення по закінченні сесії роботи користувача.

Реалізація механізмів примусового очищення оперативної пам'яті в системі «Лоза-2» забезпечується наступними програмними засобами:

– реалізація механізмів безповоротного видалення файлів реалізується програмними модулями *Сервер документів та Сервер безпеки* і *LOZAGuard* (в залежності від типу обєкту) та здійснюється шляхом виклику виконання методу `NTWipe` модулю `NIIWiper.pas`;

будь-які недокументовані можливості в зазначених методах відсутні.

7.3.4. В рамках реалізації *функціональної послуги безпеки «ДС-1»* система «Лоза-2» забезпечує реалізацію послуги для таких видів відмов:

– відмови компонентів системи «Лоза-2», які забезпечують реєстрацію подій у журналі;

– відмови компонентів системи «Лоза-2» та компонентів ОС, які призводять до неможливості звичайного завантаження ОС і дозволяють завантажити ОС лише у безпечному режимі (safe mode);

– відмови компонентів ОС та/або мережного обладнання, які призводять до неможливості взаємодії ПЗ робочих станцій з ПЗ сервера.

Відмови компонентів системи «Лоза-2» приводять систему в стан «відновлення» в якому робота системи продовжується в обсязі цього стану (доступ до системи має тільки адміністратор безпеки для проведення відновлення). Після відмови компонентів ОС має можливість завантажити ОС у безпечному режимі та працювати з програмами *Керування захистом, Аудитор, Монітор захисту*. Всі інші користувачі системи мають можливість війти до системи, але не мають можливості працювати з програмою *Захищені документи.* За допомогою програмного модулю *Монітор захисту,* адміністратор безпеки має можливість відновити пошкоджені компоненти, що привели до збою, з еталонних копій.

При відмові мережевого обладнання, робота робочої станції можлива в автономному режимі (адміністратор безпеки має можливість ввійти до системи та працювати з адміністративними засобами системи «Лоза-2», користувачі мають можливість ввійти до

системи тільки у разі, якщо в налаштуваннях доступу дозволено роботу звичайних користувачів в «автономному» режимі).

7.3.5. В рамках реалізації *функціональної послуги безпеки «ДЗ-1»* система «Лоза-2» забезпечує можливість оновлення програмного забезпечення Система «Лоза-2». Модернізація здійснюється адміністратором безпеки без переривання функцій із захисту інформації в порядку, наведеному в [12, розділ 4].

Модернізація системи «Лоза-2» може бути проведена в будь-який момент часу для всіх програмних пакетів. Для оновлення системи «Лоза-2» повинен переводитись з нормального режиму роботи до режиму відновлення. Проведення оновлень не призводять до переривання функцій із захисту інформації та не викликає необхідності повторної інсталяції комплексу. Після проведення оновлень є необхідним лише переведення системи «Лоза-2» зі режиму відновлення до нормального режиму роботи.

При модернізації системи «Лоза-2» на нього також розповсюджується дія цього експертного висновку за таких умов:

– версія модернізованої системи «Лоза-2» залишається в межах версії 4.X.Y (X, Y – ціле невід’ємне число);

– склад КЗЗ оновленого комплексу відповідає даним, наведеним в додатку А до цього документу.

7.3.6. В рамках реалізації *функціональної послуги безпеки «ДВ-1»* система «Лоза-2» забезпечує можливість відновлення роботи. Відновлення здійснюється адміністратором безпеки за допомогою програмного компоненту *Монітор захисту*, або якщо в наслідок системного збою, завантаження графічного інтерфейсу, або ядра системи «Лоза-2» неможливе, відновлення здійснюється адміністратором безпеки за допомогою службової утиліти LOZARecover.exe, яка знаходиться у службовому каталозі системи «Лоза-2» %LOZA%\LIB. Відновлення налаштувань здійснюється шляхом імпорту конфігураційних файлів з резервної копії При цьому відновлене функціонування здійснюється з безпечного стану шляхом застосування визначеної та реалізованої по замовчанню політики безпеки інформації у порядку описаному [11, розділ 4; 12 розділ 4].

7.3.7. В рамках реалізації *функціональної послуги безпеки «НР-4»* система «Лоза-2» забезпечує можливість реєстрації подій, які мають безпосереднє відношення до безпеки:

– вхід користувача до системи та вихід користувача з системи;
– зміна паролю користувача самим користувачем;
– спроби доступу до об’єктів захисту, зокрема:
  – зміни списку користувачів та списку груп користувачів;
  – зміни атрибутів доступу об’єктів захисту;
  – зміни параметрів конфігурації системи;
  – створення та видалення документів та баз документів;
  – читання та коригування документів;
  – друк документів;
  – експорт документів;
– виявлення порушень цілісності;
– робота з робочими станціями.

Журнал реєстрації подій системи містить інформацію про події, які мають непряме відношення до безпеки (перелік подій наведений в додатку Б документу «Система захисту інформації «Лоза-2», версії 4.X.Y, Загальний опис системи. Лоза-2-4.ПД.01.1» [5]).

В журналах подій системи «Лоза-2» міститься інформація стосовно дати, часу, місця, типу і наслідків зареєстрованої події (успішність/неуспішність), ім’я та/або ідентифікатор причетного до цієї події користувача.

Журнали подій робочих станцій зберігаються локально на робочих станціях користувачів, але адміністратор безпеки має можливість налаштувати перелік «важливих» подій, які будуть копіюватись до загального журналу подій, який зберігається на сервері системи «Лоза-2».

Для всіх подій, які заносяться до журналу реєстрації подій адміністратором безпеки можуть бути налаштовані рівні, при перевищенні яких виконуються дії із формування

інформаційного повідомлення користувачу та переведення системи до стану *«відновлення»*; контроль здійснюється за типом події, а не об’єктом, якого вона стосується; періодом накопичення даних про повторюваність події є сесія роботи пакету системи «Лоза-2», при функціонуванні якого виникла відповідна подія.

Деталізовані відомості про реалізовані технології моніторингу файлових об’єктів, процесів, контролю за завданнями друку, пристроїв, структури локальної обчислювальної мережі наведені в [5, розділ 5].

Система «Лоза-2» надає можливість перегляду журналу реєстрації подій лише адміністратору безпеки.

7.3.8. В рамках реалізації *функціональних послуг безпеки «НИ-3» та «НК-1»* система «Лоза-2» забезпечує можливість однозначної ідентифікації та автентифікації адміністраторів та користувачів з використанням таких атрибутів доступу:

– ідентифікатор (логін) користувача;

– пароль;

– носії даних автентифікації (ключовий диск) (CD-R/DVD-R, CD-RW/DVD-RW, Flash-носій).

В конфігурації «Стандартна безпека» існує можливість відключення вимоги перевірки носія даних автентифікації. При відключенні даної функції, послуга безпеки реалізується на рівні НИ-2 (здійснюється перевірка лише ідентифікатора користувача та паролю).

Політика безпеки облікових записів користувачів визначає політику паролів та політику блокування облікового запису. Політика паролів визначає наступні параметри та їх значення:

– мінімальний термін дії паролю – 0 дні;

– мінімальна довжина паролю – 6 символів;

– максимальний термін дії паролю – 45 діб;

– паролі повинні відповідати вимогам складності (пароль повинен містити цифри, букви малого та великого регістру та спецсимволи);

– журнал (не повторювальність) паролів – 2 збережених пароля.

Управління обліковими записами користувачів, реєстрацією первинних паролів доступу та ідентифікаційних носіїв інформації здійснюється адміністратором безпеки.

Успішний доступ користувача можливий лише за умови введення правильних значень ідентифікатора, пароля та підключення коректного носія даних автентифікації а також якщо дана ЕОМ внесена до його переліку комп’ютерів[3]; будь-які інші спроби доступу завершуються невдало. Також у вході до системи «Лоза-2» може бути відмовлено у наступних випадках:

– у випадку, коли носій даних автентифікації пошкоджений або відсутній;

– якщо носій, що використовується для ідентифікації користувача, при вході в систему, не належить йому;

– якщо намагатися увійти в систему у режимі «відновлення» під обліковим записом, що не має повноважень адміністратора безпеки.

Система «Лоза-2» забезпечує захист даних автентифікації користувачів від несанкціонованого доступу, модифікації або руйнування; доступ до даних автентифікації користувачів (до відповідних механізмів управління обліковими записами користувачів) має лише адміністратор безпеки.

При спробі підключення до системи «Лоза-2» користувач повинен ввести власний ідентифікатор та пароль у спеціальній програмній формі, яка унеможливлює перехоплення цих даних іншим програмним забезпеченням; для цього використовується інтерфейсний модуль ідентифікації та автентифікації (провайдер автентифікації) системи «Лоза-2»; додатково до зазначених дій користувачу необхідно підключити носій даних автентифікації; цей носій є фізичним знімним носієм, який неможливо емулювати; виконання зазначених дій ініціюється виключно користувачем.

[3] Локальний користувач має можливість працювати тільки за тими комп'ютерами, які містяться в його «повному переліку комп'ютерів». Глобальний користувач може працювати за будь-яким комп'ютером мережі.

Реалізація механізмів ідентифікації та автентифікації користувачів системи «Лоза-2» забезпечується наступними програмними засобами:

– реалізація механізмів ідентифікації та автентифікації реалізується програмними модулями *Сервер безпеки* і *LOZAGuard* та здійснюється шляхом виклику виконання методу `LogonUser` класу `TLogonManager` модулю `LOZAType.pas`, що забезпечує постачання облікових даних відповідного користувача та перевірку їх достовірності;

– організація достовірного каналу здійснюється тими ж самими механізмами, що й ідентифікація та автентифікації користувачів;

будь-які недокументовані можливості в зазначених механізмах відсутні.

7.3.9. В рамках реалізації *функціональної послуги безпеки «НО-2»* система «Лоза-2» забезпечує виділення ролей користувачів, які мають адміністративні права (адміністратор безпеки, системний адміністратор, адміністратор документів) та звичайних користувачів:

– *системний адміністратор* – здійснює встановлення, налаштування та керування компонентами обчислювального середовища функціонування системи «Лоза-2»;

– *адміністратор безпеки* – здійснює управління налаштуваннями безпеки системи «Лоза-2», управління користувачами та групами користувачів, управління їх правами доступу щодо доступу до об'єктів захисту;

– *адміністратор документів* – здійснює управління правами доступу користувачів до об'єктів захисту;

– *звичайні користувачі* – в рамках виконання функціональних обов'язків працюють з об'єктами захисту (за винятком тих, що належать до технологічної інформації), в обсязі, який дозволений для них адміністраторами; також, в конфігурації «Стандартна безпека», вони мають можливість створення довірчих баз даних та керування доступом до документів, які містяться в довірчих базах даних (за умови, що користувач є власником даної бази).

Система «Лоза-2», незалежно від конфігурації, підтримує наступні вбудовані ролі (групи) користувачів:

– Адміністратори безпеки;
– Системні адміністратори;
– Адміністратори документів;
– Звичайні користувачі;
– Всі;
– Власник бази;
– Власник документа.

Приналежність користувачів до вбудованих груп визначається наступним чином:

– членами групи *Адміністратори безпеки*, *Системні адміністратори*, *Адміністратори документів* або *Звичайні користувачі* є всі користувачі системи, яким надана відповідна роль;

– членами групи *Всі* є всі користувачі системи;

– єдиним членом групи *Власник бази* є користувач – власник бази документів;

– єдиним членом групи Власник документа є користувач – власник документа.

Дозволяється суміщати виконання адміністративних ролей, але заборонено суміщати виконання адміністративної ролі з роллю звичайного користувача.

Управління обліковими записами користувачів, ролями користувачів та їх правами доступу здійснюється в порядку, визначеному в [5].

7.3.10. В рамках реалізації *функціональної послуги безпеки «НЦ-2»* система «Лоза-2» забезпечує контроль цілісності власного програмного забезпечення. Крім того, система забезпечує можливість контролю цілісності будь-яких об'єктів таких типів:

– файли та папки;
– параметри та розділи системного реєстру;
– облікові записи системи «Лоза-2» (операційної системи).

З метою захисту від зовнішніх впливів системи «Лоза-2» виділяє домен для власного виконання, відмінний від доменів всіх інших процесів. Додатково до виділення домену засоби системи «Лоза-2» забезпечують реалізацію механізмів розрахунку кодів контролю

цілісності програмних модулів при старті та порівняння розрахованого коду контролю цілісності з еталонним значенням, яке було вироблене при встановленні та реєстрації відповідного програмного модуля засобів системи «Лоза-2».

При виявленні порушень цілісності програмного забезпечення системи «Лоза-2» його функціонування припиняється; відновлення працездатності може бути здійснено лише адміністратором безпеки за допомогою програми *Монітор захисту,* яка входить до складу програмного забезпечення «Лоза-2» або, коли неможливо завантажити інтерфейс системи «Лоза-2», за допомогою службової утиліти LOZARecover.exe, яка знаходиться у службовому каталозі системи «Лоза-2» %LOZA%\LIB.

Тільки адміністратор безпеки має можливість відновлення цілісності програмних модулів системи «Лоза-2»; при виявленні порушень в цілісності окремих файлів або налаштувань система автоматично переводиться до стану *«відновлення»*, з якого повернути його до нормального функціонування може тільки адміністратор безпеки; експлуатаційна документація містить опис порядку відновлення цілісності програмних модулів системи «Лоза-2» [12, розділ 4].

Обмеження, виконання яких дозволяє гарантувати, що всі послуги безпеки доступні лише через інтерфейс системи «Лоза-2» і всі запити на доступ до захищених об’єктів контролюються цим КЗЗ, наведені в розділі 8 цього документу.

Реалізація механізмів контролю цілісності в системі «Лоза-2» забезпечується наступними програмними засобами:

– реалізація механізмів контролю цілісності файлів та папок в системі «Лоза-2» здійснюється програмними модулями *Сервер безпеки* та *LOZAGuard* завдяки виконанню методу `CheckFiles` класу `TIntegrityChecker` модулю `Checker.pas`;

– реалізація механізмів контролю цілісності розділів та параметрів системного реєстру в системі «Лоза-2» здійснюється програмними модулями *Сервер безпеки* та *LOZAGuard* завдяки виконанню методу `CheckRegistry` класу `TIntegrityChecker` модулю `Checker.pas`;

– реалізація механізмів контролю цілісності завантажувальних секторів в системі «Лоза-2» здійснюється програмними модулями *Сервер безпеки* та *LOZAGuard* завдяки виконанню методу `CheckBoots` класу `TIntegrityChecker` модулю `Checker.pas`;

– реалізація механізмів контролю цілісності облікових записів в системі «Лоза-2» здійснюється програмними модулями *Сервер безпеки* та *LOZAGuard* завдяки виконанню методу `CheckAccounts` класу `TIntegrityChecker` модулю `Checker.pas`;

будь-які недокументовані можливості в зазначених механізмах відсутні.

7.3.11. В рамках реалізації *функціональної послуги безпеки «НТ-2»* система «Лоза-2» реалізує процедури самотестування, що полягають у перевірці цілісності програмного забезпечення КЗЗ в такому обсязі:

– виконуваних модулів системи «Лоза-2»;
– бібліотек динамічної компоновки системи «Лоза-2»;
– записів системного реєстру;
– цілісності програмних каталогів;
– облікових записів користувачів;
– завантажувальних секторів жорсткого диску;

зазначені перевірки проводяться в автоматичному режимі при запуску програмного забезпечення системи «Лоза-2» (одночасно із запуском операційної системи) та за відповідним запитом адміністратора безпеки.

Система «Лоза-2» за запитом адміністратора безпеки виявляє факт порушення цілісності відповідного пакету, переводить систему до стану «відновлення», програма *Монітор захисту* відображає короткий звіт про знайдені порушення цілісності та пропонує прийняти зміни або поновити модифікований пакет з еталонної копії програмного забезпечення системи «Лоза-2».

8. СФЕРА ВИКОРИСТАННЯ (ВИМОГИ ДО УМОВ ЕКСПЛУАТАЦІЇ) ОБ'ЄКТА ЕКСПЕРТИЗИ

Використання системи «Лоза-2» можливе лише за умови дотримання вимог та положень експлуатаційної документації, а також наступних положень:

– відсутність потенційно небезпечних програмних засобів на ЕОМ, на яких застосовується система «Лоза-2», до яких належать:

- засоби прямого доступу до інформації, що зберігається на жорстких дисках ЕОМ;
- засоби розробки, відлагодження та тестування програмного забезпечення;
- засоби аналізу змісту оперативної пам’яті;
- засоби аналізу виконуємого коду програмного забезпечення;
- засоби злому комп’ютерних систем;

– фізична охорона ЕОМ, на яких застосовується система «Лоза-2», мережевого обладнання, зовнішніх пристроїв (накопичувачів), носіїв інформації та фізичних ліній зв’язку; фізична охорона повинна передбачати контроль доступу сторонніх осіб до приміщення, де знаходяться об’єкти охорони, наявність надійних перешкод для несанкціонованого проникнення до приміщень та сховищ носіїв інформації, особливо в неробочий час;

– обмеження доступу користувачів до пристроїв введення інформації з зовнішніх джерел; в разі необхідності, введення інформації повинно здійснюватись під контролем адміністратора безпеки;

– дотримуються вимоги щодо умов застосування системи «Лоза-2», наведені в п. 2.2 цього документу та експлуатаційної документації [21];

– налаштування операційної системи, спільно з якою використовується система «Лоза-2», відповідають вимогам експлуатаційної документації на систему [12];

– дія експертного висновку розповсюджується на зразки системи «Лоза-2» версії 4.X.Y (X, Y – ціле невід’ємне число), склад яких відповідає даним, наведеним у додатку А до цього документу;

– модернізація системи «Лоза-2» повинна проводитись його розробником (виробником) з урахуванням наступних вимог:

- модернізована версія системи «Лоза-2» має значення 4.X.Y (X, Y – ціле невід’ємне число);
- модернізована система «Лоза-2» пройшла випробування на підприємстві-виробнику в порядку, визначеному в документі [13], погодженому із Адміністрацією Держспецзв’язку; за результатами випробувань встановлено відповідність модернізованої системи «Лоза-2» вимогам ТЗ, про що в паспорті на систему «Лоза-2» зроблено відповідні відмітки.

9. ТЕРМІН ДІЇ ЕКСПЕРТНОГО ВИСНОВКУ

Термін дії висновку становить 3 роки за умови виконання вимог розділу 8 цього висновку.

Провідний науковий співробітник науково-дослідної лабораторії сертифікаційних та експертних робіт науково-дослідного центру

С.С. Анпілогов

Начальник науково-дослідного центру

Ю.В. Сергієнко

Додаток А
до Експертного висновку на систему захисту інформації ЛОЗА™-2, версія 4.X.Y

Склад програмних засобів, наданих для виконання робіт

Для виконання робіт наданий комплект інсталяцій пакетів, що містять файли компонент комплексу засобів захисту інформації від несанкціонованого доступу в інформаційно-телекомунікаційній системі «Лоза-2», склад якого наведений в табл. А.1.

Таблиця А.1

№ з/с	Назва і шлях	Опис
1.	%loza%\HELP\ProDoc**Prodoc.chm**	Інтерактивна довідка для програми «Захищені документи»
2.	%loza%\LIB\1058(1049)**Res_Auditor.dll**	Мовні ресурси програми «Аудитор»
3.	%loza%\LIB\1049**Res_LozaDoc.dll**	Мовні ресурси програми «Захищені документи»
4.	%loza%\LIB**AdminAssistant.exe**	Утиліта «Помічник адміністратора» - для тимчасового дозволу друку та доступу до захищених баз документів
5.	%loza%\LIB**CdsPad.exe**	Утиліта для відкриття та редагування .cds - файлів
6.	%loza%\LIB**ConvertorToProdocNewFormat.exe**	Конвертор баз документів старого формату в новий
7.	%loza%\LIB**devxexec.exe**	Додаткова утиліта, яка використовується для запуску агента користувача UserAgent.exe
8.	%loza%\LIB**ExtractText.exe**	Додаткова утиліта для контекстного пошуку по тексту документів, що знаходяться у базі документів
9.	%loza%\LIB**GetSID.exe**	Додаткова утиліта для отримання SID користувача
10.	%loza%\LIB**KillPrcs.exe**	Додаткова утиліта для видалення процесів (для Windows XP)
11.	%loza%\LIB**LOZA-2.inf**	Шаблон безпеки Windows, необхідний для того, щоб налаштувати Windows XP/Vista/7/8/8.1/10/2003/ 2008/2012/2012 r2 стандартними засобами адміністрування Windows (тільки на сервері)
12.	%loza%\LIB**LOZACryst.dll**	Бібліотека для роботи з ключем Кристал-1
13.	%loza%\LIB**LOZAHook.dll**	Бібліотека, яка використовується для захисту від копіювання інформації до буферу обміну Windows
14.	%loza%\LIB**LozaHookOffice_2.dll**	Бібліотека для роботи з MS Office
15.	%loza%\LIB**LOZAKeygen.exe**	Утиліта,яка генерує файли для ініціалізації CD/DVD ключових дисків
16.	%loza%\LIB**LOZALib.dll**	Бібліотека для зв’язку інших

№ з/с	Назва і шлях	Опис
		систем з системою ЛОЗА-2
17.	%loza%\LIB**LOZARecover.exe**	Утиліта «Відновлення системи ЛОЗА-2»
18.	%loza%\LIB**LOZAReg.dll**	Бібліотека, яка використовується для реєстрації системи ЛОЗА-2
19.	%loza%\LIB**LOZAWinSec.exe**	Утиліта для застосування шаблону безпеки LOZA.inf
20.	%loza%\LIB**loza_excel2007.xlam**	Файл надбудови Excel, який використовується налаштування заборони деяких функцій Excel 2007
21.	%loza%\LIB**Register.exe**	Утиліта «Реєстрації системи ЛОЗА-2»
22.	%loza%\LIB**UserAgent.exe**	Утиліта «Агент користувача»
23.	%loza%\LIB**WFolders.exe**	Додаткова утиліта для видалення файлів
24.	%loza%\PROGRAMS\ProDoc**ProDoc.exe**	Програма «Захищені документи»
25.	%loza%\Security\HELP**auditor.chm**	Інтерактивна довідка для програми «Аудитор»
26.	%loza%\Security\HELP**safety.chm**	Інтерактивна довідка для програми «Керування захистом»
27.	%loza%\Security\HELP**secmon.chm**	Інтерактивна довідка для програми «Монітор захисту»
28.	%loza%\Security\PROGRAMS**auditor.exe**	Програма «Аудитор»
29.	%loza%\Security\PROGRAMS**safety.exe**	Програма «Керування захистом»
30.	%loza%\Security\PROGRAMS**secmon.exe**	Програма «Монітор захисту»
31.	%loza%\Security\SAFETY	Технологічна інформація системи «ЛОЗА-2»
32.	%loza%\Security\SAFETY\Workstations\	Технологічна інформація робочих станцій системи «ЛОЗА-2»
33.	%loza%\Security\Server**LOZAGuard.exe**	Сервер безпеки для робочих станцій (для автоматичного поновлення програмного забезпечення системи «ЛОЗА-2»)
34.	%loza%\Security\Server**LOZASec.exe**	Сервер безпеки (тільки на сервері)
35.	%loza%\Security\Server**LOZAStarter.exe**	Служба для запуску сервера безпеки
36.	%loza%\Servers\DOC**LOZADocProcSrv.exe**	Сервер документів
37.	%loza%\SysTemp\	Тимчасова інформація, необхідна для функціонування системи «ЛОЗА-2»
38.	%windir%\system32\drivers**LOZAFilt.sys**	Драйвер файлової системи
39.	%windir%\system32**LOZAGina.dll**	Бібліотека входу до системи для Windows XP/2003
40.	%windir%\system32**LOZACred.dll**	Бібліотека входу до системи для Windows Vista/7/8/8.1/10/2008/2012/2012 r2
41.	%windir%\system32**LOZAMsg.dll**	Бібліотека ресурсів повідомлень для журналів Windows, які генерує ЛОЗА-2