1. ІДЕНТИФІКАЦІЯ ОБ'ЄКТА ЕКСПЕРТИЗИ

Об'єктом експертизи є система захисту інформації ЛОЗА™-1, версія 4.X.Y[1] (далі – система «Лоза-1»). 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-1» 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.

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™-1, версія 4.X.Y (далі – система «Лоза-1»).

Розробник, виробник системи «Лоза-1» та замовник експертизи: товариство з обмеженою відповідальністю «Науково-дослідний інститут «Автопром» (далі – ТОВ НДІ «Автопром») (фізична адреса: 03150, м. Київ–150, вул. Єжи Ґедройця, 6, код ЄДРПОУ 33102567).

Додаткова експертиза системи «Лоза-1» проводиться у зв'язку із закінченням терміну дії експертного висновку, виданого за результатами первинної державної експертизи системи «Лоза-1» в сфері технічного захисту інформації (№ 740 від 01.06.2017).

2.2. Призначення та функції об'єкту експертизи

Система «Лоза-1» являє собою комплекс програмних засобів, призначений для використання в складі комплексної системи захисту інформації в автоматизованих системах класу «1» (згідно з 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-1».

Система «Лоза-1» функціонує в середовищі операційних систем сімейства Microsoft Windows, побудованих на ядрі NT 6.1 (Windows 7, Server 2008 R2), NT 6.2 (Windows Server 2012), NT 6.3 (Windows 8.1, Windows Server 2012 R2), NT 10.0 (Windows 10, Windows Server 2016, Windows Server 2019).

Система «Лоза-1» забезпечує 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] Кількість та якість прийнятих доопрацювань програмних модулів системи «Лоза-1» попередньої версії, на думку розробників системи, достатньо для зміни номеру версії програмного продукту, тому у ході проведення експертних випробувань було прийняте рішення про змінення назви версії програмного продукту з версії «3.X.Y» на версію «4.X.Y». В зв'язку з цим рішенням далі по тексту протоколу під назвою «система «Лоза-1» буде розумітися «система «Лоза-1», версії 4.X.Y».

Система «Лоза-1» 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.

Система сумісна з наступними версіями Microsoft Office (32- та 64-розрядні):

- Microsoft Office 2007 (SP-2 або вище);
- Microsoft Office 2010;
- Microsoft Office 2013;
- Microsoft Office 2016;
- Microsoft Office 2019.

Разом з Microsoft Word та Microsoft Excel має бути встановлена компонента Visual Basic для приложений.

Детальніші системні вимоги системи «Лоза-1» приведені в Паспорті на систему «Лоза-1».

Передбачено дві конфігурації системи – «Підвищена безпека» та «Стандартна безпека».

Система «Лоза-1» має забезпечувати надання послуг безпеки, наведених в табл. 2.1 та 2.2 (назви та скорочення відповідають документу НД ТЗІ 2.5-004-99).

Таблиця 2.1

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 1.2

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
Цілісність комплексу засобів захисту	НЦ-2	КЗЗ з гарантованою цілісністю
Самотестування	НТ-2	Самотестування при старті

Процес розробки системи «Лоза-1» відповідає рівню гарантій Г-4 згідно з НД ТЗІ 2.5-004-99.

Для супроводження системи «Лоза-1» 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* (LOZASec.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);

Нижче приведено опис компонентів архітектури системи:

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

Сервер безпеки

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 правил розмежування доступу (далі – 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.

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 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

Бібліотека *LOZACred.dll* призначена для ідентифікації та автентифікації користувачів.

Бібліотека *LOZACred.dll* використовується в ОС Windows побудованих на ядрі NT версій 6.1, 6.2, 6.3, 10.0 (7, 2008 Server R2, 8.1, 2012 Server, 2012 Server R2, 10, 2016 Server, 2019 Server) і поєднує в собі дві компоненти: вона є

провайдером облікових даних (credential provider) та 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).

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 технологічною інформацією.

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. 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).

3.1.2. *Склад системи*

Система складається з таких частин:

- керуюча підсистема;
- підсистема керування доступом;
- підсистема забезпечення цілісності;
- підсистема реєстрації подій.

Керуюча підсистема

Керуюча підсистема виконує такі функції:

- забезпечення початку та завершення роботи;
- виконання ідентифікації та автентифікації користувачів, у тому числі встановлення достовірного каналу;
- забезпечення можливості поновлення системи;
- забезпечення відновлення після збоїв;

– забезпечення можливості оперативного керування системою;
– забезпечення взаємодії між модулями системи.

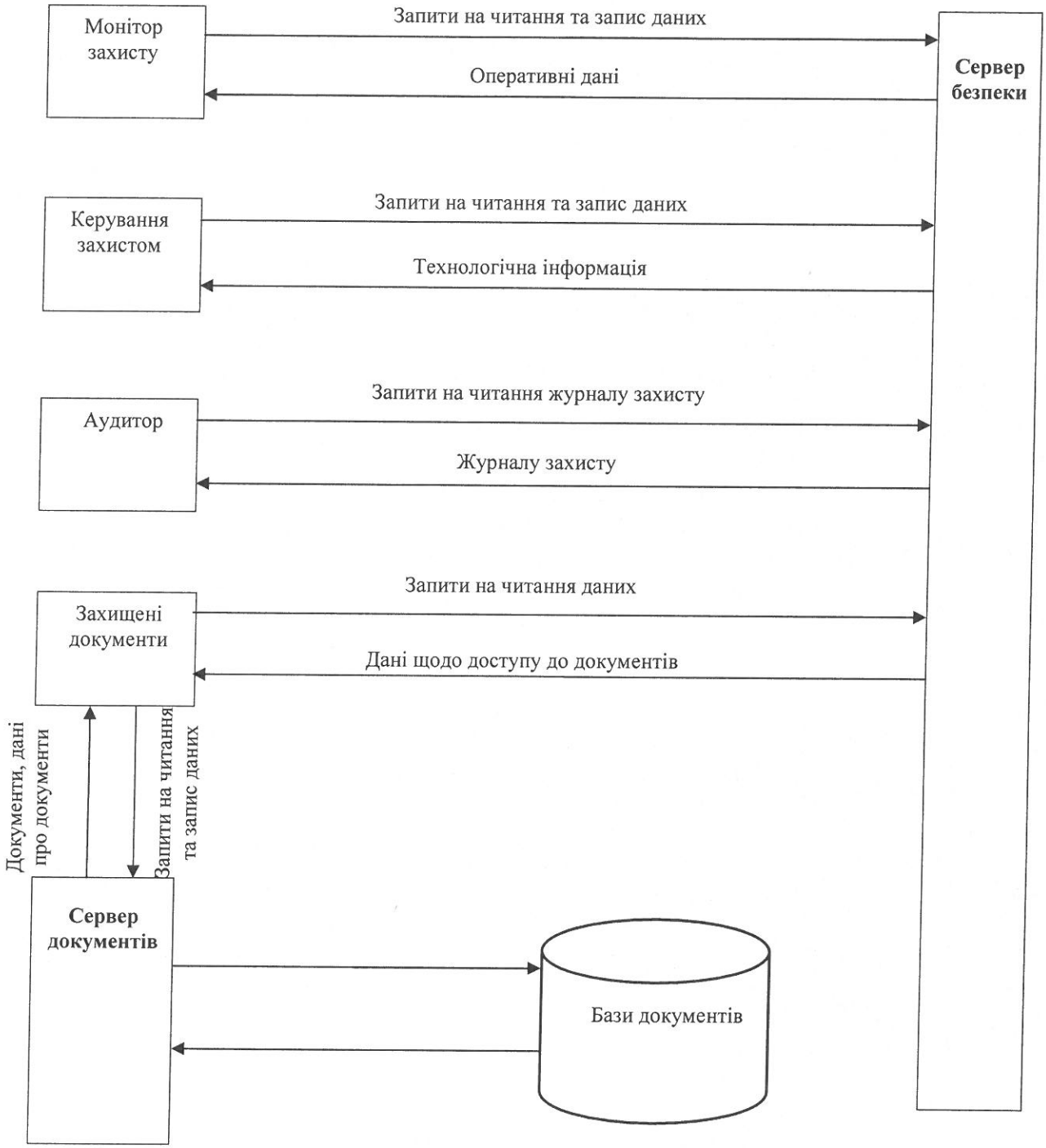


Рис. 3.1. Блок-схема роботи програми

Підсистема керування доступом

Підсистема керування доступом виконує такі функції:
– забезпечення виконання правил розмежування доступу (ПРД);
– унеможливлення повторного використання об'єктів;
– забезпечення розподілу обов'язків користувачів системи;
– забезпечення можливості керування об'єктами захисту (створення, видалення, встановлення атрибутів).

Підсистема забезпечення цілісності

Підсистема забезпечення цілісності виконує такі функції:

– забезпечення цілісності програмних засобів та даних системи;

– забезпечення можливості перевірки цілісності будь-яких файлів, папок, параметрів та розділів реєстру, а також облікових записів Windows.

– забезпечення автоматичного реагування на порушення цілісності;

– забезпечення виконання самотестування системи.

Підсистема реєстрації подій

Підсистема реєстрації подій виконує такі функції:

– реєстрація всіх подій, які мають безпосереднє або непряме відношення до безпеки інформації;

– ведення журналу реєстрації подій;

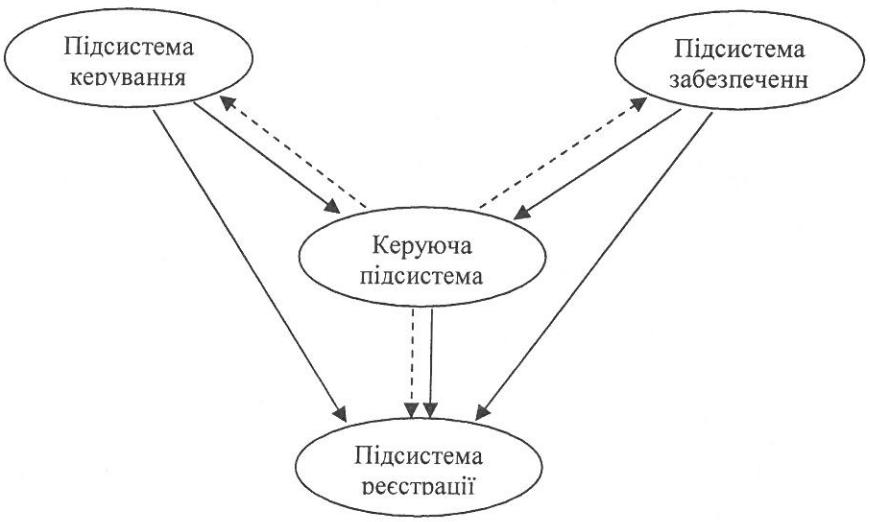
– забезпечення можливості встановлення політики аудита;

– реагування на виникнення небезпечних подій;

– забезпечення можливості зручної роботи з журналом реєстрації.

Взаємодія між підсистемами

Зв'язки між підсистемами схематично зображені на рис. 3.2.



Умовні позначення

----------►	Керуючі зв'язки
——————►	Інформаційні зв'язки

Рис. 3.2. Зв'язки між підсистемами системи «Лоза-1»

Керуюча підсистема здійснює керування іншими підсистемами: запускає і зупиняє відповідні процеси, а також змінює режими роботи підсистем.

Крім того, між підсистемами існують такі інформаційні зв'язки:

– підсистема реєстрації подій отримує від всіх інших підсистем інформацію про події, які необхідно зареєструвати в журналі;

– підсистема керування доступом передає керуючій підсистемі дані про користувачів системи;

– підсистема забезпечення цілісності передає керуючій підсистемі дані про результати перевірок цілісності, зокрема дані про порушення цілісності.

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-1» наведені в документі «ЛОЗА-1-4.ПД.01.1 Система захисту інформації ЛОЗА-1 (версія 4.0.0). Загальний опис системи».

Експертним випробуванням підлягає сукупність програмних засобів, які входять до складу системи «Лоза-1» та призначені для реалізації політики безпеки інформації згідно вимог документу «Система захисту інформації ЛОЗА™-1, версія 3.X.Y. Технічне завдання. Редакція 4» (далі – ТЗ).

Додаткова експертиза системи «Лоза-1» проводиться на виконання рішення Експертної ради з питань державної експертизи в сфері технічного захисту інформації Адміністрації Держспецзв'язку (протокол засідання від 24.01.2020 № 02-2020).

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™-1, версія 3.X.Y. Технічне завдання. Редакція 4» В/вих. № 08/02/02-4970 від 15.10.13;

– 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

Додаткова державна експертиза в сфері технічного захисту інформації системи «Лоза-1» проводилась відповідно до «Програми додаткової державної експертизи в сфері технічного захисту інформації системи захисту інформації ЛОЗА™-1, версія 4.X.Y (№ 2502/д-1 від 25.02.2020) та «Методики додаткової державної експертизи в сфері технічного захисту інформації системи захисту інформації ЛОЗА™-1, версія 4.X.Y (№ 2502/д-2 від 25.02.2020, далі – Методика).

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

Перелік файлів програмного забезпечення системи «Лоза-1», яке представлено для проведення державної експертизи в сфері технічного захисту інформації, наведений в додатку А до цього документу.

Перелік наданих документів щодо системи «Лоза-1»:

Документація з випробувань системи захисту інформації ЛОЗА-1, версія

4.X.Y, проведених Розробником:

1. Технічне завдання на систему захисту інформації ЛОЗА-1 (версія 3.X.Y). Редакція 4 В/вих. № 08/02/02-4970 від 15.10.13.
2. ЛОЗА-1-4.П1.01.1 Система захисту інформації ЛОЗА-1 (версія 4.X.Y). Пояснювальна записка до ескізного проекту від 14.01.20.
3. ЛОЗА-1-4.ПА.01.1 Система захисту інформації ЛОЗА-1 (версія 4.X.Y). Опис програмного забезпечення від 14.01.20.
4. ЛОЗА-1-4.ПА.02.1 Система захисту інформації ЛОЗА-1 (версія 4.X.Y). Опис інтерфейсу ядра системи від 14.01.20.
5. ЛОЗА-1-4.ПД.01.1 Система захисту інформації ЛОЗА-1 (версія 4.4.0). Загальний опис системи.
6. ЛОЗА-1-4.І3.01.1 Система захисту інформації ЛОЗА-1 (версія 4.4.0). Інструкція адміністратора безпеки.
7. ЛОЗА-1-4.І3.02.1 Система захисту інформації ЛОЗА-1 (версія 4.4.0). Інструкція користувача системи.
8. ЛОЗА-1-4.І3.03.1 Система захисту інформації ЛОЗА-1 (версія 4.4.0). Інструкція системного адміністратора.
9. ЛОЗА-1-4.І3.04.1 Система захисту інформації ЛОЗА-1 (версія 4.4.0). Інструкція адміністратора документів.
10. ЛОЗА-1-4.І3.05.1 Система захисту інформації ЛОЗА-1 (версія 4.4.0). Програма «Захищені документи». Інструкція користувача.
11. ЛОЗА-1-4.І3.06.1 Система захисту інформації ЛОЗА-1 (версія 4.4.0). Програмні засоби адміністрування системи. Інструкція користувача.
12. ЛОЗА-1-4.І3.07.1 Система захисту інформації ЛОЗА-1 (версія 4.4.0). Інструкція з інсталяції системи.
13. ЛОЗА-1-4.ПМ.01.1 Програма та методика випробувань системи захисту ЛОЗА-1 (версія 4.X.Y) від 14.01.20.
14. ЛОЗА-1-4.ПД.01.1 Система захисту інформації ЛОЗА-1, версія 4.X.Y. Паспорт.
15. ЛОЗА-1-4.П2.01.1 Система захисту інформації ЛОЗА-1 (версія 4.X.Y). Пояснювальна записка до технічного проекту від 14.01.20.

Документація з випробувань системи захисту інформації ЛОЗА-1, версія 4.X.Y, проведених Розробником:

16. Система захисту інформації ЛОЗА-1, версія 4.4.0. Журнал випробувань від 28.01.20.
17. Система захисту інформації ЛОЗА-1, версія 4.4.0. Звіт про випробування програмного засобу від 28.01.20.
18. Наказ «Про проведення попередніх випробувань системи захисту інформації ЛОЗА-1, версія 4.4.0» від 14.01.20.
19. Протоколи випробувань програмного засобу від 28.01. 20.

Документація з процедури розробки системи ЛОЗА-1 (версія 4):

20. Інструкція розробника систем захисту інформації ЛОЗА-1, версія 4.X.Y,та ЛОЗА-2, версія 4.X.Y від 05.06.14.
21. Методика забезпечення фізичної, технічної, організаційної та кадрової безпеки у процесі розробки систем захисту інформації ЛОЗА-1, версія 4.X.Y від 05.06.14.

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™-1, версія 3».

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-1» відповідає вимогам до архітектури рівня гарантій Г-4;

– система «Лоза-1» відповідає вимогам до середовища розробки рівня гарантій Г-4;

– система «Лоза-1» відповідає вимогам до послідовності розробки рівня гарантій Г-4;

– система «Лоза-1» відповідає вимогам до середовища функціонування рівня гарантій Г-4;

– система «Лоза-1» відповідає вимогам до документації рівня гарантій Г-4;

– система «Лоза-1» 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-1» на відповідність вимогам до захисту інформації від загроз несанкціонованого доступу експерти зробили такі висновки:

– система «Лоза-1» відповідає вимогам до об'єктів захисту, суб'єктів доступу та атрибутів, згідно з якими здійснюється їх взаємодія, визначеним в п. 4.3, 4.4, 4.6 ТЗ;

– система «Лоза-1» 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-1» 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-1»

7.3.1. Політика адміністративної конфіденційності та цілісності *функціональних послуг безпеки «КА-2»/«КА-3»* та «ЦА-1»*, що реалізується системою «Лоза-1», 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-1» дозволяє створення об'єктів із довірчим керуванням доступом. Тому у цій конфігурації послуга надається на рівні КА 2 – «Базова адміністративна конфіденційність»*

Таблиця 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}
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-1»	{program}

У системі «Лоза-1» присутні суб'єкти доступу, наведені в табл. 7.2.

Таблиця 7.2

Суб'єкт доступу	Умовне позначення
системний адміністратор	[sys_admin]
адміністратор безпеки	[sec_admin]
адміністратор документів	[doc_admin]
звичайні користувачі	[user]

Правила розмежування доступу суб'єктів до адміністративних баз даних, що реалізуються системою «Лоза-1», 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]	-	+	+	+	+	+	+	-	-	-	-	-	-
[sec_admin]	-	+*	+*	-	-	-	-	-	-	-	+*	-	-
[sys_admin]	-	-	-	-	-	-	-	-	-	-	-	-	-
[doc_admin]	+	+	+	+	+	+	+	+	+	+	+	+	+

*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 адміністративній 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]	+	+	+	+	+	+	+	-	-	-	-
[sec_admin]	-	-	+	-	-	-	-	-	-	-	-
[sys_admin]	-	-	-	-	-	-	-	-	-	-	-
[doc_admin]	+	+	+	+	+	+	+	+	+	+	+

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

Таблиця 7.5

типи доступу / користувачі	Читання	Запис
[user]	+	+

[sec_admin]	+	+
[sys_admin]	-	-
[doc_admin]	-	-

Суб'єкти системи «Лоза-1» мають наступні види доступу до об'єктів, що містять технологічну інформацію, наведені в табл. 7.6.

Таблиця 7.6

користувачі \ типи доступу	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]	-	-	-	-	-	-	-	-	-	-	-
[sec_admin]	+	+	+	+	+	+	+	+	+	+	+
[sys_admin]	-	-	-	-	+*	-	-	-	-	+	-
[doc_admin]	-	-	-	-	-	-	-	-	-	-	-

За внутрішніми алгоритмами перевірки повноважень система «Лоза-1» реалізує санкціонування доступу суб'єкта доступу до об'єкта захисту або відмову у такому доступі.

Система «Лоза-1» 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.

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-1» містить рекомендації щодо безпечного поводження із об'єктами файлової системи при проведенні експорту даних з комплексу [6].

7.3.2. Політика довірчої конфіденційності та цілісності *функціональних послуг безпеки «КД-2» та «ЦД-1»*, що реалізується системою «Лоза-1», 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-1», 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]	+	+	+	+	+	+	+	+*	+*	+*	+*	+*	+*
[sec_admin]	-	+**	+**	-	-	-	-	-	-	-	+**	-	-
[sys_admin]	-	-	-	-	-	-	-	-	-	-	-	-	-
[doc_admin]	-	-	-	-	-	-	-	-	-	-	-	-	-

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-1», 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]	+	+	+	+*	+*	+	+	+*	+	+*	+*
[sec_admin]	-	-	+**	-	-	-	-	+**	-	-	-
[sys_admin]	-	-	-	-	-	-	-	-	-	-	-
[doc_admin]	-	-	-	-	-	-	-	-	-	-	-

Права доступу до об'єктів захисту встановлюються в момент їх створення та ініціалізації. Система «Лоза-1» 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-1» 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 очищення пам'яті після її звільнення, а також видалення тимчасових файлів, що створюються впродовж сесії роботи користувача.

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 видалення тимчасових файлів, що можуть створюватись програмним забезпеченням під час свого виконання впродовж сесії роботи користувача, реалізується шляхом видалення тимчасових файлів, що були створені впродовж сесії роботи користувача, по її закінченні.

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

– відмови компонентів системи «Лоза-1», які забезпечують реєстрацію подій у журналі;

– відмови компонентів системи «Лоза-1» та компонентів ОС, які призводять до неможливості звичайного завантаження ОС і дозволяють завантажити ОС лише у безпечному режимі (safe mode).

Відмови компонентів системи «Лоза-1» 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.

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

Модернізація системи «Лоза-1» може бути проведена в будь-який момент часу для всіх програмних пакетів. Для оновлення системи «Лоза-1» 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-1» зі режиму відновлення до нормального режиму роботи.

При модернізації системи «Лоза-1» на нього також розповсюджується дія цього експертного висновку за таких умов:

– версія модернізованої системи «Лоза-1» залишається в межах версії 4.X.Y (X, Y – ціле невід'ємне число);

– склад КЗЗ оновленого комплексу відповідає даним, наведеним в табл. 7.9.

Таблиця 7.9

	Назва і шлях	Опис
1.	%loza%\LIB\1058(1049)**Res_Auditor.dll**	Мовні ресурси «Аудитор»
2.	%loza%\LIB\1058(1049)**Res_LozaDoc.dll**	Мовні ресурси «Захищені документи»
3.	%loza%\LIB**AdminAssistant.exe**	Утиліта «Помічник адміністратора» - для тимчасового дозволу друку та доступу до захищених баз документів
4.	%loza%\LIB**CdsPad.exe**	Утиліта для відкриття та редагування .cds - файлів
5.	%loza%\LIB**ConvertorToProdocNewFormat.exe**	Конвертор баз старого формату в новий
6.	%loza%\LIB**devxexec.exe**	Додаткова утиліта, яка використовується для запуску агента користувача UserAgent.exe
7.	%loza%\LIB**GetSID.exe**	Додаткова утиліта для отримання SID користувача
8.	%loza%\LIB**LOZACryst.dll**	Бібліотека для роботи з ключем Кристал-1
9.	%loza%\LIB**LOZAHook.dll**	Бібліотека, яка використовується для захисту від копіювання інформації до буферу обміну Windows
10.	%loza%\LIB**LozaHookOffice_2.dll**	Бібліотека для роботи з MS Office
11.	%loza%\LIB**LOZAKeygen.exe**	Утиліта,яка генерує файли для ініціалізації CD/DVD ключових дисків
12.	%loza%\LIB**LOZALib.dll**	Бібліотека для зв'язку інших систем з системою ЛОЗА-1
13.	%loza%\LIB**LOZARecover.exe**	Утиліта «Відновлення системи ЛОЗА-1»
14.	%loza%\LIB**LOZAReg.dll**	Бібліотека, яка використовується для реєстрації системи ЛОЗА-1
15.	%loza%\LIB**LOZAWinSec.exe**	Утиліта для застосування шаблону безпеки LOZA.inf
16.	%loza%\LIB**loza_excel2007.xlam**	Файл надбудови Excel, який використовується налаштування заборони деяких функцій Excel 2007
17.	%loza%\LIB**Register.exe**	Утиліта «Реєстрації системи ЛОЗА-1»
18.	%loza%\LIB**UserAgent.exe**	Утиліта «Агент користувача»
19.	%loza%\LIB**WFolders.exe**	Додаткова утиліта для видалення файлів
20.	%loza%\PROGRAMS\ProDoc**ProDoc.exe**	Програма «Захищені документи»
21.	%loza%\Security\PROGRAMS**auditor.exe**	Програма «Аудитор»
22.	%loza%\Security\PROGRAMS**safety.exe**	Програма «Керування захистом»
23.	%loza%\Security\PROGRAMS**secmon.exe**	Програма «Монітор захисту»
24.	%loza%\Security\Server**LOZASec.exe**	Сервер безпеки
25.	%loza%\Security\Server**LOZAStarter.exe**	Служба для запуску сервера безпеки
26.	%loza%\Servers\DOC**LOZADocProcSrv.exe**	Сервер документів
27.	%windir%\system32\drivers**LOZAFilt.sys**	Драйвер файлової системи
28.	%windir%\system32**LOZAGina.dll**	Бібліотека входу до системи для Windows XP/2003
29.	%windir%\system32**LOZACred.dll**	Бібліотека входу до системи для Windows Vista/7/2008/2012

7.3.6. В рамках реалізації *функціональної послуги безпеки «ДВ-1»* система «Лоза-1» 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-1» неможливе, відновлення здійснюється адміністратором безпеки за допомогою службової утиліти LOZARecover.exe, яка знаходиться у службовому каталозі системи «Лоза-1» %LOZA%\LIB. 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-1» 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.

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-1, версії 4.0.0, Загальний опис системи. ЛОЗА-1-4.ПД.01.1» [5]).

В журналах подій системи «Лоза-1» міститься інформація стосовно дати, часу, місця, типу і наслідків зареєстрованої події (успішність/неуспішність), ім'я та/або ідентифікатор причетного до цієї події користувача.

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-1», 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-1» 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-1» 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; будь-які інші спроби доступу завершуються невдало. Також у вході до системи «Лоза-1» 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-1» 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-1» 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-1»; додатково до зазначених дій користувачу необхідно підключити підключити носій даних автентифікації; цей носій є фізичним знімним носієм, який неможливо емулювати; виконання зазначених дій ініціюється виключно користувачем.

7.3.9. В рамках реалізації *функціональної послуги безпеки «НО-2»* система «Лоза-1» забезпечує виділення ролей користувачів, які мають адміністративні права (адміністратор безпеки, системний адміністратор, адміністратор документів) та звичайних користувачів:

– *системний адміністратор* – супроводжує програмне забезпечення обчислювальної системи, в якій використовується система ЛОЗА-1, він може читати значення параметрів конфігурації системи ЛОЗА-1 та спостерігати за її роботою;

– *адміністратор безпеки* – веде базу облікових записів та дані про об'єкти захисту (зокрема, здійснює керування доступом до всіх об'єктів захисту, крім баз документів та документів), працює з журналом реєстрації подій, змінює значення параметрів конфігурації системи, може спостерігати за її роботою та здійснювати оперативне керування системою;

– *адміністратор документів* – здійснює керування доступом до адміністративних баз документів та документів, які містяться в адміністративних базах;

– *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-1», 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-1» 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-1» (операційної системи).

З метою захисту від зовнішніх впливів системи «Лоза-1» виділяє домен для власного виконання, відмінний від доменів всіх інших процесів. Додатково до виділення домену засоби системи «Лоза-1» 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-1».

При виявленні порушень цілісності програмного забезпечення системи «Лоза-1» його функціонування припиняється; відновлення працездатності може бути здійснено лише адміністратором безпеки за допомогою програми *Монітор захисту,* яка входить до складу програмного забезпечення «Лоза-1» або, коли неможливо завантажити інтерфейс системи «Лоза-1», за допомогою службової утиліти LOZARecover.exe, яка знаходиться у службовому каталозі системи «Лоза-1» %LOZA%\LIB.

Тільки адміністратор безпеки має можливість відновлення цілісності програмних модулів системи «Лоза-1»; 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-1» [12, розділ 4].

Обмеження, виконання яких дозволяє гарантувати, що всі послуги безпеки доступні лише через інтерфейс системи «Лоза-1» і всі запити на доступ до захищених об'єктів контролюються цим КЗЗ, наведені в розділі 8 цього документу.

7.3.11. В рамках реалізації *функціональної послуги безпеки «НТ-2»* система «Лоза-1» реалізує процедури самотестування, що полягають у перевірці цілісності програмного забезпечення КЗЗ в такому обсязі:

- виконуваних модулів системи «Лоза-1»;
- бібліотек динамічної компоновки системи «Лоза-1»;
- 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-1» (одночасно із запуском операційної системи) та за відповідним запитом адміністратора безпеки.

Система «Лоза-1» 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-1».

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

Використання системи «Лоза-1» 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-1», 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-1», 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-1», наведені в п. 2.2 цього документу та експлуатаційної документації;

– налаштування операційної системи, спільно з якою використовується система «Лоза-1», відповідають вимогам експлуатаційної документації на систему [12];

– дія експертного висновку розповсюджується на зразки системи «Лоза-1» версії 4.X.Y (X, Y – ціле невід'ємне число), склад яких відповідає даним, наведеним в табл. 7.9;

– модернізація системи «Лоза-1» повинна проводитись його розробником (виробником) з урахуванням наступних вимог:

- модернізована версія системи «Лоза-1» має значення 4.X.Y (X, Y – ціле невід'ємне число);
- модернізована система «Лоза-1» пройшла випробування на підприємстві-виробнику в порядку, визначеному в документі [13], погодженому із Адміністрацією Держспецзв'язку; за результатами випробувань встановлено відповідність модернізованої системи «Лоза-1» вимогам ТЗ, про що в паспорті на систему «Лоза-1» зроблено відповідні відмітки.

9. ТЕРМІН ДІЇ ЕКСПЕРТНОГО ВИСНОВКУ

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

Експерт В.П. Приказчик