Прим. № ____

Е К С П Е Р Т Н И Й В И С Н О В О К

Комплекс засобів захисту інформації в локальних обчислювальних мережах від несанкціонованого доступу "Гриф-Мережа" версії 3, виробництва ТОВ "Інститут комп'ютерних технологій"

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

"____"_____ 201__ р. за № _____

Дійсний до "____" _____ 201___ р.

Заступник Голови Державної служби спеціального зв'язку та захисту інформації України

_____ П. П.

М.П

Результати державної експертизи свідчать, що:

комплекс засобів захисту інформації в локальних обчислювальних мережах від несанкціонованого доступу "Гриф-Мережа" версії 3

назва засобу технічного захисту інформації

що наданий на експертизу ТОВ "Інститут комп'ютерних технологій"

назва та адреса організації

03151, Україна, м. Київ, проспект Повітрофлотський, 54

відповідає

відповідає, не відповідає

вимогам нормативних документів системи технічного захисту інформації в Україні, у тому числі вимогам НД ТЗІ 2.5-008-2002 в обсязі функцій, зазначених у документі "Комплекс засобів захисту інформації в локальних обчислювальних мережах від несанкціонованого доступу "Гриф-Мережа" версія 3. Технічне завдання UA.21541987.00019 - 01 90 01", сукупність яких визначається функціональним профілем захищеності:

– у базовій конфігурації:

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

– у конфігурації для умов із підвищеними вимогами щодо забезпечення спостережності:

{КА-2, КО-1, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-5, НИ-3, НК-1, НО-2, НЦ-2, НТ-2}

з рівнем Г-4 гарантій коректності реалізації функціональних послуг безпеки згідно з НД ТЗІ 2.5-004-99 та може використовуватися для захисту інформації з обмеженим доступом, що обробляється в автоматизованих системах класу "2".

Вимоги до умов експлуатації та сфери використання об'єкта експертизи визначені у розділі 8 цього експертного висновку.

Директор НДЦ "ТЕЗІС"
НТУУ "КПІ" _____ **М. І. Прокофьєв**

керівник Організатора експертизи — підпис — ініціали, прізвище

1 ЗАГАЛЬНІ ВІДОМОСТІ ЩОДО ОБ'ЄКТА ЕКСПЕРТИЗИ

1.1 Об'єкт експертизи (ОЕ) – комплекс засобів захисту (КЗЗ) інформації в локальних обчислювальних мережах (ЛОМ) від несанкціонованого доступу (НСД) "Гриф-Мережа" версії 3 (далі – КЗЗ "Гриф-Мережа") призначений для забезпечення захисту інформації, оброблюваної в автоматизованих системах (АС), побудованих на базі ЛОМ, від загроз порушення цілісності, конфіденційності та доступності, при реалізації політики адміністративного керування доступом до інформації.

1.2 Розробник КЗЗ "Гриф-Мережа" - ТОВ "Інститут комп'ютерних технологій", 03151, Україна, м. Київ, пр-т Повітрофлотський, 54.

КЗЗ "Гриф-Мережа" розроблено в ініціативному порядку.

1.3 Вид експертизи – додаткова. Експертиза проводилась у зв'язку з закінченням терміну дії експертного висновку за результатами первинної експертизи, а також у зв'язку з забезпеченням підтримки у КЗЗ "Гриф-Мережа" версії 3.02 можливість функціонування на серверах та робочих станціях ЛОМ під керуванням оновлених операційних систем (ОС) (із пакетами оновлення, наданими виробником відповідних ОС у період з 01.01.2013 по 31.03.2015).

1.4 Мета експертизи – виконання перевірки відповідності КЗЗ "Гриф-Мережа" вимогам НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-008-2002 та документа "Комплекс засобів захисту інформації в локальних обчислювальних мережах від несанкціонованого доступу "Гриф-Мережа" версія 3. Технічне завдання UA.21541987.00019 - 01 90 01" (ТЗ), узгодженого з Державною службою спеціального зв'язку та захисту інформації України (Держспецзв'язку) 10.02.2011 р., з урахуванням порядку реалізації цих вимог, викладеного у документах "Комплекс засобів захисту інформації в локальних обчислювальних мережах від несанкціонованого доступу "Гриф-Мережа" версія 3. Технічний проект UA.21541987.00022 - 01 81 01" (ТП) та "Технічні вимоги, на відповідність яким здійснюватиметься державна експертиза комплексу засобів захисту в локальних обчислювальних мережах від несанкціонованого доступу "Гриф-Мережа" версії 3" (Технічні вимоги), та визначення відповідності архітектури, середовища та послідовності розробки, середовища функціонування, документації та методів випробувань КЗЗ від НСД "Гриф-Мережа" вимогам до рівня Г-4 гарантій коректності реалізації функціональних послуг безпеки, викладених в НД ТЗІ 2.5-004-9.

1.5 Підставою для проведення експертизи є доручення Держспецзв'язку лист № 10/01-2493 від 04.11.2015 р. щодо проведення додаткової державної експертизи комплексу засобів захисту інформації в локальних обчислювальних мережах від несанкціонованого доступу "Гриф-Мережа" версії 3 та Договору № 9515 Е від 18.11.2015 р. між НТУУ "КПІ" (Організатор експертизи - НДЦ "ТЕЗІС") та ТОВ "Інститут комп'ютерних технологій" (Замовник експертизи).

2 ЗАГАЛЬНА ХАРАКТЕРИСТИКА ОБ'ЄКТА ЕКСПЕРТИЗИ

2.1 КЗЗ "Гриф-Мережа" версії 3 призначений для забезпечення захисту інформації з обмеженим доступом (ІзОД): конфіденційної інформації, вимоги щодо захисту якої встановлені законодавством, в тому числі конфіденційної інформації про фізичну особу, службової інформації, створеної в органах владних повноважень, та інформації, яка становить державну таємницю, оброблюваної в АС, побудованих на базі ЛОМ, від загроз порушення цілісності, конфіденційності та доступності, при реалізації політики адміністративного керування доступом до інформації.

2.2 КЗЗ "Гриф-Мережа" версії 3 призначений для функціонування в АС, побудованих на базі ЛОМ, до складу яких входять файлові сервери (ФС) під керуванням ОС MS Windows 2003 Server, MS Windows 2008 Server, MS Windows 2008 Server R2, MS Windows 2012 Server або MS Windows 2012 Server R2 та робочі станції (РС) під керуванням ОС MS Windows XP Professional /MS Windows Vista (Professional, Enterprise, Ultimate) / MS Windows 7 (Professional, Enterprise, Ultimate, у т.ч. 64-розрядних) / MS Windows 8/8.1 (Professional, Enterprise, у т.ч. 64-розрядних).

Як ФС – основний контролер домену (ОКД) використовується IBM-сумісний комп'ютер, що функціонує під керуванням ОС MS Windows 2003 Server, MS Windows 2008 Server, MS Windows 2008 Server R2, MS Windows 2012 Server або MS Windows 2012 Server R2 з

активованою службою Active Directory.

Як ФС використовуються IBM-сумісні комп'ютери, що функціонують під керуванням ОС MS Windows 2003 Server, MS Windows 2008 Server, MS Windows 2008 Server R2, MS Windows 2012 Server або MS Windows 2012 Server R2.

Як РС використовуються IBM-сумісні комп'ютери, що функціонують під керуванням ОС MS Windows XP Professional /MS Windows Vista (Professional, Enterprise, Ultimate)/ MS Windows 7 (Professional, Enterprise, Ultimate, у т.ч. 64-розрядних) / MS Windows 8/8.1 (Professional, Enterprise, у т.ч. 64-розрядних).

2.3 Вимоги до апаратного середовища функціонування ОЕ.

Мінімальні вимоги щодо конфігурації апаратного забезпечення ФС-ОКД, інших ФС та РС повинні відповідати вимогам виробника ОС, що встановлюються на ФС-ОКД, ФС та РС.

2.4 КЗЗ від НСД Гриф-Мережа" реалізує такі функції захисту:

– ідентифікацію та автентифікацію користувачів на підставі імені (псевдоніма), паролю та носія даних автентифікації (знімного файлового носія або пристрою Touch Memory);

– розподіл обов'язків користувачів та виділення декількох ролей адміністраторів, які можуть виконувати різні функції з адміністрування (реєстрацію захищених ресурсів, реєстрацію користувачів, призначення прав доступу, оброблення протоколів аудита, тощо);

– розмежування доступу користувачів до обраних каталогів та файлів, що містяться у них, що дозволяє організувати спільну роботу декількох користувачів, які мають різні службові обов'язки та права по доступу до захищеної інформації;

– керування потоками інформації та блокування потоків інформації, що можуть призвести до зниження її рівня конфіденційності;

– контроль за виведенням інформації на пристрої друку з можливістю маркування друкованих аркушів документів (у форматі "Office Open XML") відповідно до вимог діючих нормативних документів в сфері охорони державної таємниці;

– контроль за імпортом інформації зі знімних носіїв;

– контроль за експортом інформації на знімні носії з можливістю обмеження переліку використовуваних знімних носіїв;

– гарантоване знищення інформації з обмеженим доступом при видаленні відповідних файлів;

– розмежування доступу прикладних програм до обраних каталогів та файлів, що містяться у них, що дозволяє забезпечити захист інформації від випадкового видалення або пошкодження, а також забезпечити дотримання технології її оброблення;

– контроль цілісності прикладного програмного забезпечення, а також блокування завантаження програм, цілісність яких порушено, що дозволяє забезпечити захист від вірусів та дотримання технології оброблення захищеної інформації;

– контроль за використанням дискового простору користувачами, що виключає можливість блокування одним із користувачів можливості роботи інших користувачів;

– можливість блокування пристроїв інтерфейсу користувача на час його відсутності;

– контроль цілісності та самотестування КЗЗ при старті та за запитом адміністратора;

– відновлення функціонування КЗЗ у випадку збоїв;

– безперервну реєстрацію, аналіз і обробку критичних для безпеки подій (входу користувачів в ОС, спроб несанкціонованого доступу, фактів запуску програм, доступу до захищеної інформації, виведення на друк і т.п.) у спеціальних протоколах аудита;

– негайне оповіщення адміністратора безпеки про усі виявлені порушення встановлених правил розмежування доступу (у конфігурації із підвищеними вимогами щодо забезпечення спостережності);

– ведення архіву зареєстрованих даних аудита.

2.5 КЗЗ "Гриф-Мережа" реалізує сукупність функціональних послуг безпеки, які, згідно НД ТЗІ 2.5-004-99, становлять такі функціональні профілі захищеності інформації:

– у базовій конфігурації КЗЗ:

{**КА**-2, **КО**-1, **ЦА**-2, **ЦО**-1, **ДР**-1, **ДС**-1, **ДЗ**-1, **ДВ**-1, **НР**-2, **НИ**-3, **НК**-1, **НО**-2, **НЦ**-2, **НТ**-2};

– у конфігурації КЗЗ для умов із підвищеними вимогами щодо забезпечення спостережності:

{**КА**-2, **КО**-1, **ЦА**-2, **ЦО**-1, **ДР**-1, **ДС**-1, **ДЗ**-1, **ДВ**-1, **НР**-5, **НИ**-3, **НК**-1, **НО**-2, **НЦ**-2, **НТ**-2}.

Перелік функціональних послуг безпеки та їх мнемонічне позначення приведені у таблиці 1. Позначення та зміст послуг та їх рівнів відповідають НД ТЗІ 2.5-004-99.

Таблиця 1

№ з. п.	Назва реалізованої послуги безпеки (згідно з НД ТЗІ 2.5-004-99)	Мнемонічне позначення послуги
Конфіденційність		
1	Базова адміністративна конфіденційність	КА-2
2	Повторне використання об’єктів	КО-1
Цілісність		
3	Базова адміністративна цілісність	ЦА-2
4	Обмежений відкат	ЦО-1
Доступність		
5	Квоти	ДР-1
6	Стійкість при обмежених відмовах	ДС-1
7	Модернізація	ДЗ-1
8	Ручне відновлення	ДВ-1
Спостереженість		
9	Захищений журнал	НР-2*
10	Аналіз в реальному часі	НР-5**
11	Множинна ідентифікація і автентифікація	НИ-3
12	Однонаправлений достовірний канал	НК-1
13	Розподіл обов'язків адміністраторів	НО-2
14	КЗЗ з гарантованою цілісністю	НЦ-2
15	Самотестування при старті	НТ-2

* - у базовій конфігурації КЗЗ;

** - у конфігурації КЗЗ для умов із підвищеними вимогами щодо забезпечення спостережності.

2.6 Ідентифікація ОЕ

Версії ОЕ ідентифікуються числовим кодом виду "З.хх" за дворівневою схемою, де "З" – номер версії, "хх" - номер підверсії. Нумерація підверсій починається з "01". Зазначений числовий код доступний для перегляду у всіх інтерактивних компонентах, що входять до складу ОЕ та зазначені у Додатку А.

3 НОРМАТИВНІ ТА ТЕХНІЧНІ ДОКУМЕНТИ, НА ВІДПОВІДНІСТЬ ВИМОГАМ ЯКИХ ЗДІЙСНЮВАЛАСЬ ОЦІНКА ОЕ

Під час підготовки та проведення державної експертизи КЗЗ "Гриф-Мережа" використовувались такі нормативно-методичні документи:

1 Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Затверджені постановою Кабінету Міністрів України від 29.03.2006 р. № 373.

2 Положення про державну експертизу у сфері технічного захисту інформації. Затверджене наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України № 93 від 16.05.2007р. та зареєстроване в Міністерстві юстиції України 16.07.2007 за № 820/14087.

3 ДСТУ 2851-94 Програмні засоби ЕОМ. Документування результатів випробувань.

4 ДСТУ 2853-94 Програмні засоби ЕОМ. Підготовлення і проведення випробувань.

5 ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.

6 ГОСТ 19.301-79 Единая система программной документации. Программа и методика испытаний. Требования к содержанию и оформлению.

7 НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

8 НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

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

10 НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

11 НД ТЗІ 2.5-008-2002 Вимоги із захисту службової інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2.

12 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.

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

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

15 НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.

16 Технічні вимоги, на відповідність яким здійснюватиметься державна експертиза комплексу засобів захисту в локальних обчислювальних мережах від несанкціонованого доступу "Гриф-Мережа" версії 3.

4 МЕТОДИКА ПРОВЕДЕННЯ ЕКСПЕРТНИХ РОБІТ

Експертні роботи виконувались згідно з розробленими Організатором експертизи документами "Програма державної експертизи комплексу засобів захисту інформації в локальних обчислювальних мережах від несанкціонованого доступу "Гриф-Мережа" версія 3 ІАЛЦ.72.10.10.3912.01.П" та "Методики державної експертизи комплексу засобів захисту інформації в локальних обчислювальних мережах від несанкціонованого доступу "Гриф-Мережа" версія 3 ІАЛЦ.72.10.10.3912.01.М", узгодженими з Адміністрацією Держспецзв'язку.

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

5.1 На експертизу КЗЗ "Гриф-Мережа" версії 3 Замовником експертизи надані такі документи, які свідчать, що розроблення КЗЗ здійснювалось у відповідності з вимогами рівня гарантій Г-4, встановлених НД ТЗІ 2.5-004-99.

5.1.1 Експлуатаційна документація:

5.1.1.1 Комплекс засобів захисту інформації в локальних обчислювальних мережах від несанкціонованого доступу "Гриф-Мережа" версія 3. Паспорт.

5.1.1.2 Комплекс средств защиты информации в локальных вычислительных сетях от несанкционированного доступа "Гриф-Мережа" версия 3. Описание комплекса. Редакция 2.

5.1.1.3 Комплекс средств защиты информации в локальных вычислительных сетях от несанкционированного доступа "Гриф-Мережа" версия 3. Руководство по установке и настройке. Редакция 2.

5.1.1.4 Комплекс средств защиты информации в локальных вычислительных сетях от несанкционированного доступа "Гриф-Мережа" версия 3. Автоматизированное рабочее место администратора комплекса средств защиты. Руководство по эксплуатации. Редакция 2.

5.1.1.5 Комплекс средств защиты информации в локальных вычислительных сетях от несанкционированного доступа "Гриф-Мережа" версия 3. Автоматизированное рабочее место администратора безопасности. Руководство по эксплуатации. Редакция 2.

5.1.1.6 Комплекс средств защиты информации в локальных вычислительных сетях от несанкционированного доступа "Гриф-Мережа" версия 3. Автоматизированное рабочее место анализа локальных данных аудита. Руководство по эксплуатации. Редакция 2.

5.1.1.7 Комплекс средств защиты информации в локальных вычислительных сетях от несанкционированного доступа "Гриф-Мережа" версия 3. Руководство системного администратора. Редакция 2.

5.1.1.8 Комплекс средств защиты информации в локальных вычислительных сетях от несанкционированного доступа "Гриф-Мережа" версия 3. Руководство администратора комплекса средств защиты. Редакция 2.

5.1.1.9 Комплекс средств защиты информации в локальных вычислительных сетях от несанкционированного доступа "Гриф-Мережа" версия 3. Руководство администратора безопасности. Редакция 2.

5.1.1.10 Комплекс средств защиты информации в локальных вычислительных сетях от несанкционированного доступа "Гриф-Мережа" версия 3. Руководство пользователя. Ред. 2.

5.1.2 Проектна та супровідна документація:

5.1.2.1 Комплекс засобів захисту інформації в локальних обчислювальних мережах від несанкціонованого доступу "Гриф-Мережа" версія 3. Технічне завдання UA.21541987.00019 - 01 90 01. Узгоджене з Адміністрацією Держспецзв'язку 10.02.2011 р.

5.1.2.2 Комплекс засобів захисту інформації в локальних обчислювальних мережах від несанкціонованого доступу "Гриф-Мережа" версія 3. Технічний проект UA.21541987.00022 - 01 81 01.

5.1.2.3 Комплекс засобів захисту інформації в локальних обчислювальних мережах від несанкціонованого доступу "Гриф-Мережа" версія 3. Опис відповідності специфікацій. Фрагменти вхідного коду. UA.21541987.00022 - 01 81 02.

5.1.2.4 Комплекс засобів захисту інформації в локальних обчислювальних мережах від несанкціонованого доступу "Гриф-Мережа" версія 3. Методики діяльності розробників на протязі життєвого циклу. UA.21541987.00022 - 01 81 03.

5.1.2.5 Комплекс засобів захисту інформації в локальних обчислювальних мережах від несанкціонованого доступу "Гриф-Мережа" версія 3. Програма та методика випробувань UA.21541987.00022 - 01 51 01. Узгоджена з Адміністрацією Держспецзв'язку 28.04.2012 р.

5.1.2.6 Комплекс засобів захисту інформації в локальних обчислювальних мережах від несанкціонованого доступу "Гриф-Мережа" версія 3. Звіт про випробування. UA.21541987.00022 - 01 81 04.

5.1.2.7 Комплекс засобів захисту інформації в локальних обчислювальних мережах від несанкціонованого доступу "Гриф-Мережа" версія 3. Протокол приймальних випробувань UA.21541987.00022 - 01 81 05.

5.1.2.8 Комплекс засобів захисту інформації в локальних обчислювальних мережах від несанкціонованого доступу "Гриф-Мережа" версія 3.02. Звіт про випробування. UA.21541987.00022 - 01 91 01.

5.1.2.9 Комплекс засобів захисту інформації в локальних обчислювальних мережах від несанкціонованого доступу "Гриф-Мережа" версія 3.02. Протокол приймальних випробувань UA.21541987.00022 - 01 92 01.

5.1.2.10 Комплекс засобів захисту інформації в локальних обчислювальних мережах від несанкціонованого доступу "Гриф-Мережа" версія 3. Специфікація UA.21541987.00022-01.

5.1.3 Документація з організації процесу розроблення КЗЗ на підприємстві Розробника:

5.1.3.1 ООО "Институт компьютерных технологий". Положение о порядке разработки, внедрения и сопровождения программного обеспечения. Редакция от 14.07.2005 г.

5.1.3.2 Настанова з якості Товариства з обмеженою відповідальністю "Інститут комп'ютерних технологій".

5.2 КЗЗ Перелік програмних компонентів, що входять до складу інсталяційного пакета КЗЗ "Гриф-Мережа" версії 3.

5.2.1 КЗЗ "Гриф-Мережа" версії 3 постачається на інсталяційному диску (CD-ROM), який має таку структуру каталогів:

– GM3Inst - інсталяція базового ПЗ КЗЗ, автоматизованого робочого місця (АРМ)

адміністратора КСЗ, АРМ адміністратора безпеки, файл ліцензії на базове ПЗ КЗЗ;

– AUDIT - інсталяції модуля реєстрації даних аудиту і агентів модуля реєстрації даних аудиту (у конфігурації для умов із підвищеними вимогами щодо забезпечення спостережності);

– AUDIT\AGENTS - інсталяції агентів модуля реєстрації даних аудита;

– AUDIT\SRV - інсталяції модуля реєстрації даних аудиту, файл ліцензії на ПЗ підсистеми аудиту;

– DOC - документація в електронному вигляді;

– MSDE - інсталяція системи керування базою даних (СКБД) MSDE 2000 (у конфігурації для умов із підвищеними вимогами щодо забезпечення спостережності).

5.2.2 Для експертизи був наданий інсталяційний пакет КЗЗ "Гриф-Мережа" версії 3.02 на інсталяційному диску з серійним номером 007, структура каталогів якого відповідає наведеній у п. 5.2.1. Повний перелік файлів, що містяться на наданому інсталяційному диску із зазначенням їх контрольних сум наведено у Додатку А.

6 РЕЗУЛЬТАТИ ЕКСПЕРТНИХ РОБІТ

6.1 Комплектність штатного програмного забезпечення КЗЗ "Гриф-Мережа" версії 3 відповідає специфікації комплектності, зазначеної у документах на поставку.

6.2 Сукупність реалізованих у КЗЗ "Гриф-Мережа" версії 3 функцій та механізмів захисту інформації визначається згідно з НД ТЗІ 2.5-004-99 такими функціональними профілями захищеності інформації:

– у базовій конфігурації КЗЗ:

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

– у конфігурації КЗЗ для умов із підвищеними вимогами щодо забезпечення спостережності:

{КА-2, КО-1, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-5, НИ-3, НК-1, НО-2, НЦ-2, НТ-2}.

6.3 Результати експертних досліджень та випробувань щодо кожного пункту документа "Методики державної експертизи комплексу засобів захисту інформації в локальних обчислювальних мережах від несанкціонованого доступу "Гриф-Мережа" версія 3 ІАЛЦ.72.10.10.3912.01.М" викладені у документі "Протокол № 9515 додаткової державної експертизи комплексу засобів захисту інформації в локальних обчислювальних мережах від несанкціонованого доступу "Гриф-Мережа" версії 3".

6.4 За результатами експертних досліджень у частині, що стосується оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки (ФПБ) у КЗЗ "Гриф-Мережа" версії 3 встановлено, що:

– рівні реалізованих у КЗЗ "Гриф-Мережа" версії 3 функціональних послуг безпеки (таблиця 1) відповідають з рівнем гарантій Г-4 коректності їх реалізації вимогам, встановленим НД ТЗІ 2.5-004-99;

– архітектура КЗЗ "Гриф-Мережа" версії 3, а також середовище, процедури та послідовність розробки, процедури випробування та розповсюдження КЗЗ "Гриф-Мережа" версії 3 відповідають вимогам рівня Г-4 гарантій коректності реалізації функціональних послуг безпеки, встановленим НД ТЗІ 2.5-004-99;

– експлуатаційна документація на КЗЗ "Гриф-Мережа" версії 3 відповідає вимогам рівня Г-4 гарантій коректності реалізації функціональних послуг безпеки, встановленим НД ТЗІ 2.5-004-99.

6.5 За результатами експертних випробувань засобів реалізації ФПБ встановлено, що зміст реалізованих ФПБ, їх рівні та політика відповідають вимогам НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-008-2002 та документа "Комплекс засобів захисту інформації в локальних обчислювальних мережах від несанкціонованого доступу "Гриф-Мережа" версія 3. Технічне завдання UA.21541987.00019 - 01 90 01" з урахуванням порядку реалізації цих вимог, викладеного у документах "Комплекс засобів захисту інформації в локальних обчислювальних мережах від несанкціонованого доступу "Гриф-Мережа" версія 3. Технічний проект UA.21541987.00022 - 01 81 01" та "Технічні вимоги, на відповідність яким здійснюватиметься державна експертиза комплексу засобів захисту в локальних обчислювальних мережах від несанкціонованого доступу "Гриф-Мережа" версії 3" (далі – Технічні вимоги). Результати експертних робіт

свідчать, що:

6.5.1 Політика ФПБ "Адміністративна конфіденційність" рівня КА-2, яка реалізується КЗЗ, визначена стосовно таких об’єктів:

- користувачі усіх категорій;
- об’єкти-процеси:
  - прикладні програмні засоби (ППЗ) АС, що використовуються для оброблення інформації з обмеженим доступом (ІзОД) та відкритої інформації, яка потребує захисту (ВІПЗ);
- інформаційні об’єкти (ІО):
  - ІО у вигляді структурованих та неструктурованих файлів, що містять ІзОД (ВІПЗ) та зберігаються в каталогах файлової системи незнімних носіїв;
  - ІО у вигляді структурованих та неструктурованих файлів, що містять ІзОД (ВІПЗ) та зберігаються на зареєстрованих або незареєстрованих знімних носіях;
  - ІО, що містять технологічну інформацію КЗЗ;
  - ІО у вигляді файлів виконуваного коду ППЗ АС, що зберігаються в каталогах файлової системи незнімних носіїв;
- периферійне обладнання (пристрої друку, плотери і т.п.), підключене до відповідних портів введення – виведення ФС та РС;
- накопичувачі на знімних носіях, підключені до відповідних портів введення – виведення ФС та РС.

Засоби КЗЗ надають можливість адміністратору КЗЗ, що має відповідні повноваження, для кожного захищеного ІО шляхом керування належністю користувачів та ІО до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від ІО.

Засоби КЗЗ надають можливість адміністратору КЗЗ, для кожного процесу через керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес.

Засоби КЗЗ забезпечують реалізацію політики ФПБ за допомогою механізму керування доступом з використанням атрибутів користувачів, процесів та захищених ІО та за правилами, наведеними у п. 3.1 Технічних вимог.

6.5.2 Політика ФПБ "Повторне використання об’єктів" рівня КО-1, яка реалізується засобами КЗЗ, поширюється на об'єкти, що містять ІзОД та зберігаються на поділюваних між різними користувачами і процесами ресурсах, а також на відповідні ресурси:

- сегменти дискового простору незнімних носіїв, які використовуються для зберігання ІО у вигляді структурованих та неструктурованих файлів, що містять ІзОД;
- сегменти дискового простору знімних носіїв, які використовуються для зберігання ІО у вигляді структурованих та неструктурованих файлів, що містять ІзОД;
- простір сховища технологічної інформації КЗЗ, який використовуються для зберігання облікових записів користувачів.

Засоби КЗЗ при видаленні захищених ІО у вигляді файлів, які зберігаються в каталогах файлової системи незнімних носіїв, забезпечують очищення вмісту видалених ІО шляхом перезапису кластерів диску, які займав видалений файл, послідовністю нульових байт.

Засоби КЗЗ при видаленні (з використанням засобів КЗЗ) ІО у вигляді файлів, що зберігаються на зареєстрованих або незареєстрованих знімних носіях, забезпечують очищення вмісту видалених ІО шляхом перезапису кластерів диску, які займав видалений файл, послідовністю нульових байт.

Засоби КЗЗ забезпечують неможливість успадкування новим користувачем із псевдонімом, який співпадає з псевдонімом користувача, обліковий запис якого було видалено, прав доступу до захищених ІО, призначених користувачу, обліковий запис якого було видалено.

Засоби КЗЗ забезпечують реалізацію політики ФПБ за допомогою механізму очищення вмісту видалених ІО та за правилами, наведеними у п. 3.2 Технічних вимог.

6.5.3 Політика ФПБ "Адміністративна цілісність" рівня ЦА-2, яка реалізується КЗЗ, визначена стосовно таких об’єктів:

- користувачі усіх категорій;
- об’єкти-процеси:
  - ППЗ АС, що використовуються для оброблення ІзОД та ВІПЗ;
- інформаційні об’єкти:
  - ІО у вигляді структурованих та неструктурованих файлів, що містять ІзОД (ВІПЗ) та зберігаються в каталогах файлової системи незнімних носіїв;
  - ІО у вигляді структурованих та неструктурованих файлів, що містять ІзОД (ВІПЗ) та зберігаються на зареєстрованих або незареєстрованих знімних носіях;
  - ІО, що містять технологічну інформацію КЗЗ;
  - ІО у вигляді файлів виконуваного коду ППЗ АС, що зберігаються в каталогах файлової системи незнімних носіїв.
- накопичувачі на знімних носіях, підключені до відповідних портів введення – виведення ФС та РС.

Засоби КЗЗ надають можливість адміністратору КЗЗ, що має відповідні повноваження, для кожного захищеного ІО шляхом керування належністю користувачів, процесів та ІО до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право, за допомогою відповідних процесів, модифікувати ІО.

Засоби КЗЗ надають можливість адміністратору КЗЗ, для кожного процесу через керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес.

Засоби КЗЗ забезпечують реалізацію політики ФПБ за допомогою механізму керування доступом з використанням атрибутів користувачів, процесів та захищених ІО та за правилами, наведеними у п. 3.3 Технічних вимог.

6.5.4 Політика ФПБ "Відкат" рівня ЦО-1, яка реалізується КЗЗ, визначена стосовно таких об’єктів:

- користувачі таких категорій:
  - системний адміністратор КЗЗ;
  - адміністратори КЗЗ;
- набори даних, що містяться у сховищах технологічної інформації КЗЗ.

Засоби КЗЗ забезпечують можливість автоматизованого здійснення відкату баз даних (БД) технологічної інформації КЗЗ до попереднього стану, якщо в процесі встановлення захисту на каталог файлової системи або включенням захищеного каталогу до технологічної схеми виникли збої і ця послідовність операцій не була повністю завершена, за правилами, наведеними у п. 3.4 Технічних вимог.

6.5.5 Політика ФПБ "Використання ресурсів" рівня ДР-1, яка реалізується КЗЗ, визначена стосовно таких об’єктів:

- користувачі усіх категорій;
- дисковий простір незнімних носіїв, який використовується користувачами для зберігання створених ними ІО у вигляді структурованих та неструктурованих файлів, що зберігаються у каталогах файлової системи незнімних носіїв.

Засоби КЗЗ надають можливість адміністратору КЗЗ за правилами, наведеними у п. 3.5 Технічних вимог, встановити обмеження на обсяг дискового простір незнімних носіїв, що може бути використаний користувачами для зберігання створених ними ІО.

Засоби КЗЗ здатні проконтролювати встановлені обмеження та зареєструвати факт спроби перевищення користувачем встановленого обмеження в журналі реєстрації з використанням засобів реалізації ФПБ "Реєстрація".

6.5.6 Політика ФПБ "Стійкість до відмов" рівня ДС-1, яка реалізується КЗЗ, визначена стосовно всіх зазначених у детальному проекті структурних компонентів (модулів) КЗЗ, що входять до складу:

- модуля обслуговування носіїв даних автентифікації користувачів;
- інтерфейсного модуля ідентифікації та автентифікації (провайдера автентифікації);
- модуля контролю запитів доступу до ресурсів та керування доступом до ресурсів (системного драйвера);

- модуля контролю запитів доступу до ресурсів та керування доступом до ресурсів (системного сервісу);
- модуля контролю операцій експорту даних;
- модуля контролю операцій друку;
- модуля адміністрування (АРМ адміністратора КЗЗ);
- модуля відновлення цілісності та оновлення КЗЗ;
- модуля зберігання локальних даних аудита;
- модуля аналізу локальних даних аудита (АРМ аналізу локальних даних аудита);
- агента модуля реєстрації даних аудита;
- модуля реєстрації даних аудита;
- модуля оброблення та аналізу даних аудита (АРМ адміністратора безпеки);
- інтерфейсного модуля взаємодії з ППЗ.

У випадку виникнення певних відмов ПЗ КЗЗ решта засобів КЗЗ не втрачають працездатність та забезпечують реалізацію відповідних ФПБ.

Засоби КЗЗ здатні зареєструвати факт відмови певних структурних компонентів КЗЗ та повідомити про це адміністраторів за правилами, наведеними у п. 3.6 Технічних вимог.

6.5.7 Політика ФПБ "Гаряча заміна" рівня ДЗ-1, яка реалізується КЗЗ, визначена стосовно всіх зазначених у детальному проекті структурних компонентів (модулів) КЗЗ, що входять до складу:

- модуля обслуговування носіїв даних автентифікації користувачів;
- інтерфейсного модуля ідентифікації та автентифікації (провайдера автентифікації);
- модуля контролю запитів доступу до ресурсів та керування доступом до ресурсів (системного драйвера);
- модуля контролю запитів доступу до ресурсів та керування доступом до ресурсів (системного сервісу);
- модуля контролю операцій експорту даних;
- модуля контролю операцій друку;
- модуля адміністрування (АРМ адміністратора КЗЗ);
- модуля відновлення цілісності та оновлення КЗЗ;
- модуля зберігання локальних даних аудита;
- модуля аналізу локальних даних аудита (АРМ аналізу локальних даних аудита);
- агента модуля реєстрації даних аудита;
- модуля реєстрації даних аудита;
- модуля оброблення та аналізу даних аудита (АРМ адміністратора безпеки);
- інтерфейсного модуля взаємодії з ППЗ.

Засоби КЗЗ надають можливість системному адміністратору КЗЗ провести модернізацію (оновлення) ПЗ КЗЗ за правилами, наведеними у п. 3.7 Технічних вимог..

Засоби оновлення ПЗ КЗЗ в процесі виконання модернізації не здійснюють зміни або видалення раніше встановлених атрибутів користувачів і захищених ІО, які використовуються при реалізації інших ФПБ. Результати виконання операцій по модернізації (оновленню) ПЗ КЗЗ реєструються у журналі реєстрації з використанням засобів реалізації ФПБ "Реєстрація".

6.5.8 Політика ФПБ "Відновлення після збоїв" рівня ДВ-1, яка реалізується КЗЗ, визначена стосовно всіх зазначених у детальному проекті структурних компонентів (модулів) КЗЗ, що входять до складу:

- модуля обслуговування носіїв даних автентифікації користувачів;
- інтерфейсного модуля ідентифікації та автентифікації (провайдера автентифікації);
- модуля контролю запитів доступу до ресурсів та керування доступом до ресурсів (системного драйвера);
- модуля контролю запитів доступу до ресурсів та керування доступом до ресурсів (системного сервісу);
- модуля контролю операцій експорту даних;
- модуля контролю операцій друку;
- модуля адміністрування (автоматизованого робочого місця (АРМ) адміністратора КЗЗ);
- модуля відновлення цілісності та оновлення КЗЗ;

- модуля зберігання локальних даних аудита;
- модуля аналізу локальних даних аудита (АРМ аналізу локальних даних аудита);
- агента модуля реєстрації даних аудита;
- модуля реєстрації даних аудита;
- модуля оброблення та аналізу даних аудита (АРМ адміністратора безпеки);
- інтерфейсного модуля взаємодії з ППЗ.

Засоби КЗЗ надають можливість системному адміністратору КЗЗ провести відновлення цілісності та працездатності КЗЗ за правилами, наведеними у п. 3.8 Технічних вимог.

Засоби відновлення цілісності та працездатності ПЗ КЗЗ в процесі відновлення цілісності та працездатності не здійснюють зміни або видалення раніше встановлених атрибутів користувачів і захищених ІО, які використовуються при реалізації інших ФПБ. Результати виконання операцій щодо відновленню цілісності та працездатності ПЗ КЗЗ реєструються у журналі реєстрації з використанням засобів реалізації ФПБ "Реєстрація".

6.5.9 Політика ФПБ "Реєстрація" рівня НР-2 та НР-5, яка реалізується засобами КЗЗ, визначає такий перелік подій (які реєструються у відповідних журналах), що мають безпосереднє або непряме відношення до безпеки та стосуються функціонування ПЗ КЗЗ, а саме:

- факти входу/виходу або спроби входу/виходу до/із ОС користувачів будь-яких категорій;
- факти реєстрації та видалення або спроби реєстрації та видалення облікових записів користувачів будь-якої категорії;
- факти призначення/зміни прав доступу користувачів до захищених ресурсів;
- факти порушення встановлених прав доступу користувачів;
- факти зміни даних ідентифікації та автентифікації користувачів будь-яких категорій;
- факти отримання або намагання отримання користувачем будь-якої категорії доступу до будь-яких ПЗ, що використовуються для оброблення ІО, що містять ІзОД або ВІПЗ;
- факти отримання або намагання отримання користувачем будь-якої категорії доступу до будь-яких ІО, які містять ІзОД або ВІПЗ;
- факти виведення або спроби виведення користувачем будь-якої категорії документа, що містить ІзОД, на пристрій друку;
- факти або спроби імпорту ІО зі знімних носіїв;
- факти або спроби експорту ІО на знімні носії;
- факти порушення цілісності засобів КЗЗ;
- факти перезавантаження, вимикання комп’ютера та інші системні події;
- події, пов'язані зі спостереженням за процесами (запуск, завершення);
- інші події, обов’язковість реєстрації яких передбачена політикою реалізації окремих ФПБ.

Засоби КЗЗ надають можливість адміністраторам безпеки провести перегляд та аналіз зареєстрованої інформації про події за правилами, наведеними у пп. 3.9, 3.10 Технічних вимог.

Засоби КЗЗ здатні за правилами, наведеними у п. 3.10 Технічних вимог, контролювати одиничні або повторювані події, які можуть свідчити про прямі (істотні) порушення політики безпеки інформації, оброблюваної в АС, негайно інформувати адміністратора безпеки про перевищення порогів безпеки та, якщо небезпечні події повторюються, надати йому можливість здійснити неруйнівні дії щодо припинення повторення цих подій.

6.5.10 Політика ФПБ "Достовірний канал" рівня НК-1, яка реалізується засобами КЗЗ, визначена стосовно:

- користувачів усіх категорій;
- ПЗ КЗЗ.

Засоби КЗЗ забезпечують створення достовірного каналу, використовуваного при початковій ідентифікації та автентифікації користувачів у засобах реалізації ФПБ "Ідентифікація та автентифікація" рівня НИ-3, за правилами, наведеними у п. 3.11 Технічних вимог. Ініціювання достовірного каналу взаємодії меж користувачем і засобами КЗЗ здійснюється виключно користувачем з використанням реалізованого в ОС механізму ініціювання достовірного каналу взаємодії з користувачем при натисканні комбінації клавіш "Ctrl+Alt+Del".

6.5.11 Політика ФПБ "Цілісність комплексу засобів захисту" рівня НЦ-2, яка реалізується засобами КЗЗ, визначена стосовно всіх зазначених в детальному проекті

структурних компонентів (модулів) КЗЗ, що входять до складу:
- модуля обслуговування носіїв даних автентифікації користувачів;
- інтерфейсного модуля ідентифікації та автентифікації (провайдера автентифікації);
- модуля контролю запитів доступу до ресурсів та керування доступом до ресурсів (системного драйвера);
- модуля контролю запитів доступу до ресурсів та керування доступом до ресурсів (системного сервісу);
- модуля контролю операцій експорту даних;
- модуля контролю операцій друку;
- модуля адміністрування (АРМ адміністратора КЗЗ);
- модуля відновлення цілісності та оновлення КЗЗ;
- модуля зберігання локальних даних аудита;
- модуля аналізу локальних даних аудита (АРМ аналізу локальних даних аудита);
- агента модуля реєстрації даних аудита;
- модуля реєстрації даних аудита;
- модуля оброблення та аналізу даних аудита (АРМ адміністратора безпеки);
- інтерфейсного модуля взаємодії з ППЗ.

Засоби КЗЗ з метою захисту від зовнішніх впливів на несанкціонованої модифікації підтримують власний домен виконання, відмінний від доменів всіх інших процесів, за правилами, наведеними у п. 3.12 Технічних вимог.

Додатково до виділення домену виконання, засоби КЗЗ забезпечують контроль цілісності програмних модулів КЗЗ з використанням механізму розрахунку кодів контролю цілісності (ККЦ) програмних модулів КЗЗ при старті та порівняння розрахованого ККЦ з еталонним значенням, яке було вироблене розробником при підготовці інсталяційного пакету. У випадку невідповідності ККЦ фіксується порушення цілісності, запуск відповідного програмного модуля блокується, реєструється факт порушення цілісності програмних модулів КЗЗ, повідомляється про це системний адміністратор КЗЗ та КЗЗ переводиться до стану, в якому заборонене оброблення ІзОД. Повернення до нормального режиму роботи може виконати тільки системний адміністратор КЗЗ з використанням спеціальних програмних засобів (модуля відновлення цілісності та оновлення КЗЗ).

6.5.12 Політика ФПБ "Самотестування" рівня НТ-2, яка реалізується засобами КЗЗ, визначена стосовно всіх зазначених у детальному проекті структурних компонентів (модулів) КЗЗ, що входять до складу:
- модуля обслуговування носіїв даних автентифікації користувачів;
- інтерфейсного модуля ідентифікації та автентифікації (провайдера автентифікації);
- модуля контролю запитів доступу до ресурсів та керування доступом до ресурсів (системного драйвера);
- модуля контролю запитів доступу до ресурсів та керування доступом до ресурсів (системного сервісу);
- модуля контролю операцій експорту даних;
- модуля контролю операцій друку;
- модуля адміністрування (АРМ адміністратора КЗЗ);
- модуля відновлення цілісності та оновлення КЗЗ;
- модуля зберігання локальних даних аудита;
- модуля аналізу локальних даних аудита (АРМ аналізу локальних даних аудита);
- агента модуля реєстрації даних аудита;
- модуля реєстрації даних аудита;
- модуля оброблення та аналізу даних аудита (АРМ адміністратора безпеки);
- інтерфейсного модуля взаємодії з ППЗ.

Засоби КЗЗ за правилами, наведеними у п. 3.13 Технічних вимог, здійснюють перевірку працездатності шляхом автоматичної перевірки цілісності ПЗ КЗЗ при старті відповідного модуля (модулем контролю запитів доступу до ресурсів та керування доступом до ресурсів (системним драйвером) та іншими модулями самостійно), за запитом системного адміністратора КЗЗ (з використанням модуля адміністрування), а також цілісності БД технологічної інформації КЗЗ при доступі до неї з боку модулів КЗЗ.

6.5.13 Політика ФПБ "Ідентифікація та автентифікація" рівня НИ-3, яка реалізується

засобами КЗЗ, визначена стосовно користувачів таких категорій:
- системний адміністратор КЗЗ;
- адміністратори КЗЗ;
- адміністратори безпеки;
- користувачі з різними рівнями повноважень.

Засоби КЗЗ забезпечують автентифікацію користувачів на підставі введених ними паролів (принцип "щось знаю") та пред'явлених носіїв даних автентифікації (принцип "чимось володію") за правилами, наведеними у п. 3.14 Технічних вимог.

6.5.14 Політика ФПБ "Розподіл обов'язків" рівня НО-2, яка реалізується засобами КЗЗ, визначає функції, притаманні таким ролям користувачів:
- системний адміністратор КЗЗ;
- адміністратори КЗЗ;
- адміністратори безпеки;
- користувачі з різними рівнями повноважень.

Засобами КЗЗ, за правилами, наведеними у п. 3.15 Технічних вимог, здійснюється, згідно з результатами виконаної ідентифікації та автентифікації, призначення користувачів на певні ролі.

7 ВИСНОВКИ

За результатами експертизи за критеріями технічного захисту інформації КЗЗ "Гриф-Мережа" версії 3 встановлено:
- наданий для випробувань КЗЗ "Гриф-Мережа" версії 3 відповідає вимогам нормативних документів системи технічного захисту інформації в Україні, у тому числі НД ТЗІ 2.5-008-2002, та Технічного завдання;
- сукупність реалізованих у КЗЗ "Гриф-Мережа" версії 3 функцій та механізмів захисту інформації з рівнем гарантій Г-4 коректності реалізації функціональних послуг безпеки забезпечує реалізацію наведених у п. 6.2 функціональних профілів захищеності інформації;
- результати експертизи КЗЗ "Гриф-Мережа" версії 3 дійсні для складу КЗЗ, наведеного у п. 5.2, для версій структурних компонентів КЗЗ, що містяться в інсталяційному пакеті КЗЗ "Гриф-Мережа" версії 3.02, склад якого наведено у Додатку А, а також для пакетів оновлення КЗЗ "Гриф-Мережа" версій 3.xx, встановлення яких здійснюється з використанням засобів реалізації функціональної послуги безпеки "Гаряча заміна" (ДЗ-1), за умов проведення випробувань оновлених ПЗ за узгодженою з Адміністрацією Держспецзв'язку програмою та методикою приймальних випробувань "Комплекс засобів захисту інформації в локальних обчислювальних мережах від несанкціонованого доступу "Гриф-Мережа" версія 3. Програма та методика випробувань UA.21541987.00022 - 01 51 01" та надання до Адміністрації Держспецзв'язку відповідного Протоколу випробувань.

8 ВИМОГИ ЩОДО СФЕРИ ВИКОРИСТАННЯ ТА УМОВ ЕКСПЛУАТАЦІЇ

8.1 На підставі встановленої за результатами експертизи відповідності КЗЗ "Гриф-Мережа" версії 3 вимогам НД ТЗІ 2.5-008-2002 він без обмежень може бути використаний для захисту службової інформації; таємної інформації, що не становить державної таємниці; конфіденційної інформації, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України "про доступ до публічної інформації"; іншої інформації з обмеженим доступом, необхідність захисту якої встановлена законом; конфіденційної інформації фізичних та юридичних осіб.

Використання КЗЗ "Гриф-Мережа" версії 3 для захисту інформації, що становить державну таємницю, можливо за умов відповідності КЗЗ вимогам щодо політики та порядку реалізації функціональних послуг безпеки, висунутим у Технічному завданні на створення відповідної комплексної системи захисту інформації.

8.2 При функціонуванні КЗЗ "Гриф-Мережа" версії 3 має бути забезпечено дотримання таких умов:
- якщо в ЛОМ використовуються ФС та РС, на яких не встановлені засоби КЗЗ "Гриф-Мережа", то, шляхом відповідного конфігурування активного мережевого обладнання на канальному рівні стеку протоколів ЛОМ має бути заборонений доступ з таких ФС та РС до ФС та РС, на яких встановлені засоби КЗЗ від НСД "Гриф-Мережа", та навпаки;

- у випадках, коли захищені інформаційні ресурси (захищені каталоги) розміщуються на жорстких дисках РС ЛОМ, на яких встановлені засоби КЗЗ "Гриф-Мережа", організаційними та/або технічними заходами має бути заблокована можливість завантаження ОС цих РС зі знімних носіїв;
- організаційними та/або технічними заходами має бути забезпечений захист ФС-ОКД та інших ФС ЛОМ від несанкціонованого вимикання або перезавантаження ОС.

9 ТЕРМІН ДІЇ ЕКСПЕРТНОГО ВИСНОВКУ

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

Додаток А

(обов'язковий)

Вміст інсталяційного диску КЗЗ "Гриф-Мережа" версії 3.02, наданого на експертизу

Ім’я файлу	Назва	Розмір файлу(байт)	CRC*	Дата створення
DOC	каталог	6922937		01.12.2015
gm_3_a_2.pdf	"Руководство администратора комплекса средств защиты"	252617	0555474A	24.04.2015
gm_3_armab_2.pdf	"Автоматизированное рабочее место администратора безопасности. Руководство по эксплуатации"	1474697	F87AF8ED	24.04.2015
gm_3_armar_2.pdf	"Автоматизированное рабочее место администратора комплекса средств защиты. Руководство по эксплуатации"	2058206	7C741C5D	24.04.2015
gm_3_armvj_2.pdf	"Автоматизированное рабочее место анализа локальных данных аудита. Руководство по эксплуатации"	921034	DD371902	23.04.2015
gm_3_aud_2.pdf	"Руководство администратора безопасности"	212574	455EABCB	24.04.2015
gm_3_op_2.pdf	"Описание комплекса"	303813	42F7D79E	24.04.2015
gm_3_s_2.pdf	"Руководство по установке и настройке"	756033	3A74FAD9	24.04.2015
gm_3_sa_2.pdf	"Руководство системного администратора комплекса средств защиты"	356899	8CAC2F4E	24.04.2015
gm_3_supp_2.pdf	"Модуль взаимодействия с прикладными программными системами. Руководство программиста"	193834	28973980	24.04.2015
gm_3_u_2.pdf	"Руководство пользователя"	393230	79F4F01D	24.04.2015
GM3Inst	каталог	14541624		01.12.2015
AUDIT	підкаталог	1853361		01.12.2015
AGENTS	підкаталог	497909		01.12.2015
GM3_Ai.exe	Модуль інсталяції агента модуля реєстрації даних аудиту	497909	BEE37BBD	25.04.2012
SRV	підкаталог	3288266		01.12.2015
inst_srv.exe	Модуль інсталяції модуля реєстрації даних аудиту	3288266	7E03B27B	25.04.2012
GM3_saud.exe	Модуль інсталяції модуля аналізу локальних даних аудиту	1853361	0479620E	10.04.2015
SecLev.dat	Файл бази даних рівнів конфіденційності	4962	B1FE77AE	21.11.2002
auditlog.dll	Динамічна бібліотека для роботи з локальними протоколами аудиту	122880	FBC84A5A	14.06.2012
auditlog60.dll	Динамічна бібліотека для роботи з локальними протоколами аудиту	167936	60D65D67	14.06.2012
gmbacres.dll	Допоміжна бібліотека збереження/відновлення стану ОС	94208	EA45603D	04.02.2010
gmcp.dll	Динамічна бібліотека провайдера аутентифікації	569344	4DB86E4C	27.03.2015
gmcpx64.dll	Динамічна бібліотека провайдера аутентифікації	858112	C5F5AB33	27.03.2015
GMGina.dll	Динамічна бібліотека інтерфейсного модуля ідентифікації та аутентифікації	425984	30AC9AFC	27.03.2015
GMShExt.dll	Динамічна бібліотека розширення Windows Explorer	98304	C1C56792	25.06.2012
GMShExtx64.dll	Динамічна бібліотека розширення Windows Explorer	105472	4D7B68C3	22.06.2012
GMSUPP.dll	Динамічна бібліотека взаємодії з прикладними програмними системами	208896	F19C2241	15.06.2012
gmsuppx64.dll	Динамічна бібліотека взаємодії з прикладними програмними системами	393728	1D7D573C	15.06.2012
gncat.dll	Динамічна бібліотека для роботи з локальними протоколами аудиту	90112	60642AE5	12.04.2010
log2krus.dll	Динамічна бібліотека з ресурсами для повідомлень протоколу аудиту	20480	B7D0D2B3	10.08.2010
ntdsmir.dll	Динамічна бібліотека для роботи з	90112	E61A5B2B	19.03.2008

	локальними протоколами аудиту			
NTWDBLIB.DLL	Допоміжна бібліотека для роботи з базами даних	278800	697434AA	05.07.2006
RecoverDLL.dll	Модуль відновлення цілісності і оновлення КЗЗ	163840	ECD01605	28.03.2015
RecoverDLLx64.dll	Модуль відновлення цілісності і оновлення КЗЗ	278016	45DB63D6	28.03.2015
savedat.dll	Динамічна бібліотека для роботи з локальними протоколами аудиту	786944	02145825	14.06.2012
ZLIB.DLL	Допоміжна бібліотека для роботи з архівами	53760	8FA6E740	13.04.2006
CBUtil.exe	Допоміжний резидентний модуль для роботи з буфером обміну (Clipboard)	77912	EE2581F4	15.06.2012
CBUtilx64.exe	Допоміжний резидентний модуль для роботи з буфером обміну (Clipboard)	177152	EAB8C589	13.09.2012
checkmod.exe	Допоміжний модуль перевірки цілісності файлів підсистеми аудиту	53248	25D2CACD	06.11.2006
GMArmEV.exe	Модуль АРМ аналізу локальних даних аудиту	1319424	7513EA1F	16.01.2015
GMArmRA.exe	Модуль АРМ адміністратора КЗЗ	1445888	AF97979D	08.04.2015
GMArmRAx64.exe	Модуль АРМ адміністратора КЗЗ	2692096	AAB69D25	08.04.2015
GMExport.exe	Програма експорту КЗЗ «Гриф-Мережа»	98304	9DB45803	20.03.2015
gmprint.exe	Програма друку КЗЗ «Гриф-Мережа»	176128	A8B5D112	12.09.2012
gmsrv.exe	Резидентний модуль режиму користувача	168010	2007F33E	20.03.2015
gmsrvx64.exe	Резидентний модуль режиму користувача	321536	A8AB03BD	20.03.2015
Grif_Ser.exe	Допоміжний резидентний модуль режиму користувача	172032	9AE8FFF8	11.09.2012
setup.exe	Програма інсталяції «Гриф-Мережа»	425984	571A1EF5	27.03.2015
51TemplALL.imm	Файл кодів контролю цілісності пакету інсталяції	716	D15554B7	16.04.2015
51TemplM.imm	Файл кодів контролю цілісності пакету інсталяції	624	FABDFD46	16.04.2015
51TemplMAR.imm	Файл кодів контролю цілісності пакету інсталяції	716	D15554B7	16.04.2015
52TemplALL.imm	Файл кодів контролю цілісності пакету інсталяції	716	C3A009B0	16.04.2015
52TemplM.imm	Файл кодів контролю цілісності пакету інсталяції	624	9BCF3E39	16.04.2015
52TemplMAR.imm	Файл кодів контролю цілісності пакету інсталяції	716	C3A009B0	16.04.2015
60TemplALL.imm	Файл кодів контролю цілісності пакету інсталяції	846	D5A20AAA	16.04.2015
60TemplM.imm	Файл кодів контролю цілісності пакету інсталяції	754	F3E3122E	16.04.2015
60TemplMAR.imm	Файл кодів контролю цілісності пакету інсталяції	846	D5A20AAA	16.04.2015
61Tempi ALL.imm	Файл кодів контролю цілісності пакету інсталяції	846	2C7B6E60	16.04.2015
61Tempi ALLx64.imm	Файл кодів контролю цілісності пакету інсталяції	902	74D55BCF	16.04.2015
61TemplM.imm	Файл кодів контролю цілісності пакету інсталяції	754	9EF80850	16.04.2015
61TemplMAR.imm	Файл кодів контролю цілісності пакету інсталяції	846	2C7B6E60	16.04.2015
61TemplMARx64.imm	Файл кодів контролю цілісності пакету інсталяції	902	74D55BCF	16.04.2015
61TemplMx64.imm	Файл кодів контролю цілісності пакету інсталяції	807	2B091567	16.04.2015
62Tempi ALL.imm	Файл кодів контролю цілісності пакету інсталяції	846	771C3070	16.04.2015
62Tempi ALLx64.imm	Файл кодів контролю цілісності пакету інсталяції	902	0307035A	16.04.2015
62TemplM.imm	Файл кодів контролю цілісності пакету інсталяції	754	F3C32616	16.04.2015
62TemplMAR.imm	Файл кодів контролю цілісності пакету інсталяції	846	771C3070	16.04.2015

62TemplMARx64.imm	Файл кодів контролю цілісності пакету інсталяції	902	0307035A	16.04.2015
62TemplMx64.imm	Файл кодів контролю цілісності пакету інсталяції	807	EA8B812F	16.04.2015
63Tempi ALL.imm	Файл кодів контролю цілісності пакету інсталяції	846	85594388	16.04.2015
63Tempi ALLx64.imm	Файл кодів контролю цілісності пакету інсталяції	902	54BCBFA5	16.04.2015
63TemplM.imm	Файл кодів контролю цілісності пакету інсталяції	754	5D6DC8CE	16.04.2015
63TemplMAR.imm	Файл кодів контролю цілісності пакету інсталяції	846	85594388	16.04.2015
63TemplMARx64.imm	Файл кодів контролю цілісності пакету інсталяції	902	54BCBFA5	16.04.2015
63TemplMx64.imm	Файл кодів контролю цілісності пакету інсталяції	807	88AED77A	16.04.2015
ALLFILES.imm	Файл кодів контролю цілісності пакету інсталяції	2020	D35A2E0A	16.04.2015
Recover51.imm	Файл кодів контролю цілісності пакету інсталяції	53	F0713300	16.04.2015
Recover52.imm	Файл кодів контролю цілісності пакету інсталяції	53	748D410B	16.04.2015
Recover60.imm	Файл кодів контролю цілісності пакету інсталяції	53	86065CA3	16.04.2015
Recover61.imm	Файл кодів контролю цілісності пакету інсталяції	53	4D0A889A	16.04.2015
Recover62.imm	Файл кодів контролю цілісності пакету інсталяції	53	074261FA	16.04.2015
Recover63.imm	Файл кодів контролю цілісності пакету інсталяції	53	92999A22	16.04.2015
Recoverx64_61.imm	Файл кодів контролю цілісності пакету інсталяції	59	1D234D10	16.04.2015
Recoverx64_62.imm	Файл кодів контролю цілісності пакету інсталяції	59	05C2E530	16.04.2015
Recoverx64_63.imm	Файл кодів контролю цілісності пакету інсталяції	59	8E4851A8	16.04.2015
gm_m51.inf	Файл параметрів конфігурації для інсталяції системи	31830	76558BA1	06.02.2015
gm_m52.inf	Файл параметрів конфігурації для інсталяції системи	32119	3549E5C9	06.02.2015
gm_m60.inf	Файл параметрів конфігурації для інсталяції системи	37222	FB7C9C86	06.02.2015
gm_m61.inf	Файл параметрів конфігурації для інсталяції системи	37256	BC65A113	06.02.2015
gm_m62.inf	Файл параметрів конфігурації для інсталяції системи	38556	DF939DBF	06.02.2015
gm_m63.inf	Файл параметрів конфігурації для інсталяції системи	42325	13DDFC43	06.02.2015
gmmpdcpol.inf	Файл параметрів конфігурації для інсталяції системи	13572	7578458E	02.02.2015
gmmpdcpolrf_T.inf	Файл параметрів конфігурації для інсталяції системи	40522	AF26E1F7	21.01.2015
gmmwspol_t.inf	Файл параметрів конфігурації для інсталяції системи	57854	A96E4A99	02.02.2015
gmx64_m61.inf	Файл параметрів конфігурації для інсталяції системи	49659	5E627F96	06.02.2015
gmx64_m62.inf	Файл параметрів конфігурації для інсталяції системи	51148	92B18300	06.02.2015
gmx64_m63.inf	Файл параметрів конфігурації для інсталяції системи	53289	CA130957	16.04.2015
stpinf64.inf	Файл параметрів конфігурації для інсталяції системи	175616	346A6978	27.03.2015
armg2k.ini	Файл параметрів конфігурації для інсталяції системи	158	B68A6932	21.06.2005
GMDRV51.sys	Модуль контролю та розмежування доступу до ресурсів	178176	BA7DEA11	05.12.2014
GMDRV510N.sys	Допоміжний модуль аутентифікації користувачів у режимі відновлення цілісності	125696	B139C689	05.12.2014
GMDRV52.sys	Модуль контролю та розмежування	97280	00230328	19.03.2015

	доступу до ресурсів			
GMDRV520N.sys	Допоміжний модуль аутентифікації користувачів у режимі відновлення цілісності	47616	B9051D09	19.03.2015
GMDRV60.sys	Модуль контролю та розмежування доступу до ресурсів	108032	9253E58D	03.07.2012
GMDRV60ON.sys	Допоміжний модуль аутентифікації користувачів у режимі відновлення цілісності	49152	0E2A9954	15.06.2012
GMDRV61.sys	Модуль контролю та розмежування доступу до ресурсів	112128	E3B1B207	07.04.2015
GMDRV610N.sys	Допоміжний модуль аутентифікації користувачів у режимі відновлення цілісності	49664	43466390	17.12.2014
GMDRV610NX64.sys	Допоміжний модуль аутентифікації користувачів у режимі відновлення цілісності	78752	BD34DC7B	19.12.2014
GMDRV61X64.sys	Модуль контролю та розмежування доступу до ресурсів	163232	48945EBB	10.04.2015
GMDRV62.sys	Модуль контролю та розмежування доступу до ресурсів	112544	302AA347	26.02.2015
GMDRV620N.sys	Допоміжний модуль аутентифікації користувачів у режимі відновлення цілісності	49664	87416242	17.02.2015
GMDRV620NX64.sys	Допоміжний модуль аутентифікації користувачів у режимі відновлення цілісності	78752	C02A9EDD	27.02.2015
GMDRV62X64.sys	Модуль контролю та розмежування доступу до ресурсів	161184	397CA415	05.03.2015
GMDRV63.sys	Модуль контролю та розмежування доступу до ресурсів	147824	B6DE750F	16.04.2015
GMDRV630N.sys	Допоміжний модуль аутентифікації користувачів у режимі відновлення цілісності	69520	A9C0C7F9	16.04.2015
GMDRV630NX64.sys	Допоміжний модуль аутентифікації користувачів у режимі відновлення цілісності	82952	A0DC4932	16.04.2015
GMDRV63X64.sys	Модуль контролю та розмежування доступу до ресурсів	203456	2F2C4939	16.04.2015
License.txt	Файл з текстом ліцензійної угоди	1026	FCD6A3F8	21.10.2003
MSDE	каталог	72503896		01.12.2015
sql2kdesksp3.exe	Модуль інсталяції ПО для роботи з базою даних MS SQL Server	72503896	54440D17	21.08.2003

*) CRC розраховано за допомогою програми-архіватора WinRar 3.71.