ЕКСПЕРТНИЙ ВИСНОВОК

Засіб технічного захисту інформації від несанкціонованого доступу «Комплекс «Гриф» версії 4

Зареєстровано в Адміністрації Державної служби спеціального зв'язку та захисту інформації України "20" жовтня 2017 р. за № 767

Дійсний до "20" жовтня 2020 р.

Перший заступник Голови Служби

О. М. Чаузов

м.п.

За результатами експертизи встановлено, що

засіб технічного захисту інформації від несанкціонованого доступу «Комплекс «Гриф» версії 4

назва засобу технічного захисту інформації

виробництва ТОВ «Інститут комп'ютерних технологій»,

який надано на експертизу **ТОВ «Інститут комп'ютерних технологій»,**

назва та адреса організації

м. Київ, просп. Повітрофлотський, 54,

відповідає

відповідає, не відповідає

вимогам нормативних документів системи технічного захисту інформації в Україні, в обсязі функцій, зазначених у документі «Засіб технічного захисту інформації від несанкціонованого доступу «Комплекс «Гриф». Версія 4. Технічне завдання UA.21541987.00025- 01 90 01.

Вимоги до умов експлуатації та сфера використання об'єкта експертизи визначені у відповідних розділах експертного висновку.

Директор НДЦ «ТЕЗІС»
КПІ імені Ігоря Сікорського — **М. І. Прокофьєв**

керівник організатора експертизи — підпис — ініціали, прізвище

м.п.

1 ЗАГАЛЬНІ ВІДОМОСТІ ЩОДО ОБ’ЄКТА ЕКСПЕРТИЗИ

1.1 Об'єктом експертизи (ОЕ) є засіб технічного захисту інформації від несанкціонованого доступу (НСД) "Комплекс "Гриф" версії 4 (далі – комплекс "Гриф").

1.2 Комплекс "Гриф" призначений для забезпечення захисту інформації з обмеженими доступом (ІзОД) (у тому числі інформації, що становить державну таємницю; службової інформації; конфіденційної інформації про особу (персональних даних); інформації, що становить комерційну таємницю і т.п.), оброблюваної в автоматизованих системах (АС) класу "1" та в АС класу "2".

1.3 Розробник – ТОВ "Інститут комп'ютерних технологій", 03151, м. Київ, проспект Повітрофлотський, 54.

1.4 Вид експертизи – первинна.

1.5 Мета експертизи:

– перевірка комплексу "Гриф" на відповідність вимогам НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-012-2015, НД ТЗІ 2.5-008-2002, НД ТЗІ 3.6-001-2000, НД ТЗІ 2.6-001-11 та документа "Засіб технічного захисту інформації від несанкціонованого доступу "Комплекс "Гриф". Версія 4. Технічне завдання" (ТЗ), узгодженого з Адміністрацією Держспецзв’язку України від 01.04.2016 р., з урахуванням порядку реалізації цих вимог, викладеного у документах "Засіб технічного захисту інформації від несанкціонованого доступу "Комплекс "Гриф". Версія 4. Технічний проект UA.21541987.00025 - 01 81 01" (ТП) та "Технічні вимоги на відповідність яким здійснюватиметься державна експертиза засобу технічного захисту інформації від несанкціонованого доступу "Комплекс "Гриф" версії 4 ІАЛЦ.62.09.20.5117.01.ТВ" (ТВ);

– підготовка висновків щодо можливості використання комплексу "Гриф" для захисту ІзОД в АС класу "1" та АС класу "2", побудованих на базі однорангових локальних обчислювальних мереж (ЛОМ);

– визначення відповідності архітектури, середовища та послідовності розробки, середовища функціонування, документації та методів випробувань комплексу "Гриф" вимогам до рівня Г-4 гарантій коректності реалізації функціональних послуг безпеки, викладених в НД ТЗІ 2.5-004-99.

1.6 Підставою для проведення експертизи є доручення Держспецзв’язку № 04/03/04-2174 від 21.06.2017 р. щодо проведення державної експертизи в сфері ТЗІ комплексу "Гриф" та Договору № 5117 Е від 26.06.17 р. між КПІ ім. Ігоря Сікорського НДЦ "ТЕЗІС" (Організатор експертизи) та ТОВ "Інститут комп'ютерних технологій" (Замовник експертизи).

2 ЗАГАЛЬНА ХАРАКТЕРИСТИКА ОБ’ЄКТА ЕКСПЕРТИЗИ

2.1 Комплекс "Гриф" призначений для захисту від загроз цілісності, конфіденційності та доступності ІзОД, в тому числі інформації, яка становить державну таємницю, оброблюваної в

АС класу 1, АС класу 2, побудованих на базі IBM-сумісних ПЕОМ (як стаціонарних, так і мобільних) або однорангових локальних обчислювальних мереж (ЛОМ), до складу яких входять IBM-сумісні ПЕОМ, у яких оброблюється ІзОД різних рівнів конфіденційності та користувачі яких можуть мати різні повноваження щодо доступу до ІзОД.

2.2 Комплекс "Гриф" функціонує на ПЕОМ під керуванням ОС MS Windows 7 Professional, Ultimate або Enterprise (32-розрядна) / Windows 7 Professional, Ultimate або Enterprise (64-розрядна) / Windows 8.1 Professional або Enterprise (32-розрядна) / Windows 8.1 Professional або Enterprise (64-розрядна)/ Windows 10 Professional або Enterprise (32-розрядна) / Windows 10 Professional або Enterprise (64-розрядна) / Windows Server 2008 R2 / Windows Server 2012 R2 / Windows Server 2016.

2.3 До складу комплексу "Гриф" входить програмний модуль криптографічного захисту та розмежування доступу до інформаційних ресурсів "Тайфун-VD" версія 1.01 UA.21541987.00023 - 01 90 02, який має позитивний експертний висновок в сфері КЗІ № 04/03/03-3691 від 14.09.2016 р. і забезпечує розмежування доступу до захищених логічних дисків з використанням механізмів "прозорого" розшифрування/ зашифрування інформації.

2.4 Мінімальні вимоги щодо конфігурації апаратного забезпечення ПЕОМ повинні відповідати вимогам виробника ОС, що встановлюються на відповідних ПЕОМ.

2.5 Комплекс "Гриф" реалізує такі функції захисту:

- ідентифікацію та автентифікацію користувачів на підставі імені (псевдоніма), пароля та персонального носія даних автентифікації (дискети, пристрою Flash Drive, CD-RW, DVD-RW або іншого знімного файлового носія);
- розподіл обов'язків користувачів та виділення декількох ролей адміністраторів, що можуть виконувати різні функції з адміністрування (реєстрацію захищених ресурсів, реєстрацію користувачів, призначення прав доступу, оброблення протоколів аудиту тощо);
- розмежування доступу користувачів до обраних каталогів файлової системи незнімних носіїв ПЕОМ (у тому числі різних ПЕОМ, що функціонують у складі ЛОМ) та файлів, що містяться у них;
- керування потоками інформації та блокування потоків інформації, що призводять до зниження рівня її конфіденційності;
- керування створеними на знімних або незнімних носіях ПЕОМ захищеними логічними дисками, вся інформація на яких зберігається у зашифрованому вигляді, та розмежування доступу до їх вмісту з використанням механізмів "прозорого" розшифрування/ зашифрування даних у момент їх читання/ запису, що дозволяє забезпечити захист конфіденційності збереженої інформації (крім інформації, що становить державну таємницю) навіть у випадку крадіжки ПЕОМ або відповідних носіїв;
- контроль цілісності захищених логічних дисків, що дозволяє забезпечити захист від

несанкціонованої модифікації збереженої на них інформації при відключених засобах захисту або у випадку крадіжки відповідних носіїв;

- 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 експортом інформації на знімні носії та за імпортом інформації зі знімних носіїв з можливістю обмеження переліку використовуваних знімних носіїв;
- гарантоване видалення ІзОД шляхом затирання вмісту файлів при їхньому видаленні;
- розмежування доступу прикладних програм до обраних каталогів файлової системи незнімних носіїв ПЕОМ (у тому числі різних ПЕОМ, що функціонують у складі ЛОМ) та файлів, що містяться у них;
- контроль цілісності прикладного програмного забезпечення, а також блокування завантаження програм, цілісність яких порушено, що дозволяє забезпечити захист від шкідливих програм (комп'ютерних вірусів) та дотримання технології оброблення ІзОД;
- контроль за використанням дискового простору ПЕОМ користувачами;
- можливість блокування пристроїв інтерфейсу користувача (клавіатури, миші, монітора) на час його відсутності;
- контроль цілісності та самотестування комплексу при старті та за запитом адміністратора;
- відновлення функціонування комплексу після збоїв;
- реєстрацію, аналіз та оброблення (у т.ч. в режимі реального часу з блокуванням можливості повторення спроб НСД) інформації про критичні для безпеки події, що дозволяє адміністраторам контролювати доступ до ІзОД, слідкувати за тим, як використовується комплекс, а також правильно його конфігурувати;
- ведення архівів зареєстрованих даних аудита;
- взаємодію з прикладними програмними системами через визначений виробником КЗЗ інтерфейс.

Усі зазначені вище функції захисту реалізуються Комплексом "Гриф" у повному обсязі для всіх ОС, зазначених у п. 2.2.

2.6 Комплекс "Гриф" реалізує сукупність функціональних послуг безпеки, які, згідно НД ТЗІ 2.5-004-99, становлять такий функціональний профіль захищеності інформації:

{**КА**-2, **КО**-1, **КВ**-2, **ЦА**-1, **ЦА**-2, **ЦО**-1, **ЦВ**-2, **ДР**-1, **ДС**-1, **ДЗ**-1, **ДВ**-1, **НР**-3, **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
3	Базова конфіденційність при обміні	КВ-2
Цілісність		
4	Мінімальна адміністративна цілісність	ЦА-1
5	Базова адміністративна цілісність	ЦА-2
6	Обмежений відкат	ЦО-1
7	Базова цілісність при обміні	ЦВ-2
Доступність		
8	Квоти	ДР-1
9	Стійкість при обмежених відмовах	ДС-1
10	Модернізація	ДЗ-1
11	Ручне відновлення	ДВ-1
Спостереженість		
12	Сигналізація про небезпеку	НР-3
13	Множинна ідентифікація і автентифікація	НИ-3
14	Однонаправлений достовірний канал	НК-1
15	Розподіл обов'язків адміністраторів	НО-2
16	КЗЗ з гарантованою цілісністю	НЦ-2
17	Самотестування при старті	НТ-2

2.7 Ідентифікація об’єкта експертизи

Версії об’єкта експертизи (ОЕ) ідентифікуються числовим кодом виду "4.xx" за дворівневою схемою, де "4" – номер версії, "xx" - 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 комплексу "Гриф" 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 Держспецзв'язку № 93 від 16.05.2007р.

3 ДСТУ 3396.2 Захист інформації. Технічний захист інформації. Терміни та визначення.

4 НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу;

5 НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу;

6 НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу;

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

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

9 НД ТЗІ 2.5-012-2015.

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

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

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

14 Технічні вимоги на відповідність яким здійснюватиметься державна експертиза засобу технічного захисту інформації від несанкціонованого доступу "Комплекс "Гриф" версії 4 обл № _____ від ___.___. 2017 р.

4 МЕТОДИКА ПРОВЕДЕННЯ ЕКСПЕРТНИХ РОБІТ

Експертні роботи виконувались згідно з розробленими Організатором експертизи документами "Програма державної експертизи засобу технічного захисту інформації від несанкціонованого доступу "Комплекс "Гриф" версії 4. ІАЛЦ.62.09.20.5117.01.П" та "Методики державної експертизи засобу технічного захисту інформації від несанкціонованого доступу "Комплекс "Гриф" версії 4 ІАЛЦ.62.09.20.5117.01.М", які узгоджені листом Держспецзв'язку № _____ від 08.08.2017 р.

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

5.1 На експертизу комплексу "Гриф" версії 4 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 Засіб технічного захисту інформації від несанкціонованого доступу "Комплекс "Гриф" версія 4. Паспорт (проект).А

5.1.1.2 Засіб технічного захисту інформації від несанкціонованого доступу "Комплекс "Гриф" версія 4. Опис комплексу. Редакція 1.

5.1.1.3 Засіб технічного захисту інформації від несанкціонованого доступу "Комплекс "Гриф" версія 4. Скорочена настанова з експлуатації (швидкий старт). Редакція 1.

5.1.1.4 Засіб технічного захисту інформації від несанкціонованого доступу "Комплекс "Гриф" версія 4. Настанова адміністратора засобів захисту. Редакція 1.

5.1.1.5 Засіб технічного захисту інформації від несанкціонованого доступу "Комплекс "Гриф" версія 4. Настанова адміністратора безпеки. Редакція 1.

5.1.1.6 Засіб технічного захисту інформації від несанкціонованого доступу "Комплекс "Гриф" версія 4. Настанова системного адміністратора. Редакція 1.

5.1.1.7 Засіб технічного захисту інформації від несанкціонованого доступу "Комплекс "Гриф" версія 4. Настанова користувача. Редакція 1.

5.1.1.8 Засіб технічного захисту інформації від несанкціонованого доступу "Комплекс "Гриф" версія 4. Модуль взаємодії з прикладними програмними системами. Настанова програміста. Редакція 1.

5.1.2 Проектна та супровідна документація:

5.1.2.1 Засіб технічного захисту інформації від несанкціонованого доступу "Комплекс "Гриф". Версія 4. Технічне завдання UA.21541987.00025 - 01 90 01, узгоджене з Адміністрацією Держспецзв’язку 01.04.2016 р.

5.1.2.2 Засіб технічного захисту інформації від несанкціонованого доступу "Комплекс "Гриф". Версія 4. Технічний проект UA.21541987.00025 - 01 81 01.

5.1.2.3 Засіб технічного захисту інформації від несанкціонованого доступу "Комплекс "Гриф". Версія 4. Опис відповідності специфікацій. Фрагменти вхідного коду. UA.21541987.00025 - 01 81 02.

5.1.2.4 Засіб технічного захисту інформації від несанкціонованого доступу "Комплекс "Гриф". Версія 4. Специфікація UA.21541987.00025 - 01.

5.1.2.5 Засіб технічного захисту інформації від несанкціонованого доступу "Комплекс "Гриф". Версія 4. Методики діяльності розробників на протязі життєвого циклу. UA.21541987.00025 - 01 81 03.

5.1.3 Документація щодо проведених приймальних випробувань:

5.1.3.1 Засіб технічного захисту інформації від несанкціонованого доступу "Комплекс "Гриф". Версія 4. Програма та методика випробувань UA.21541987. 00025 - 01 51 01, узгоджена з Адміністрацією Держспецзв'язку 01.11.2016 р.

5.1.3.2 Експертний висновок про відповідність програмного модуля криптографічного захисту та розмежування доступу до інформаційних ресурсів "Тайфун-VD" версія 1.01 UA.21541987.00023 - 01 90 02 вимогам нормативних документів системи криптографічного захисту інформації від 14.09.2016 № 04/03/03-3691.

5.1.3.3 Засіб технічного захисту інформації від несанкціонованого доступу "Комплекс "Гриф". Версія 4.01. Звіт про випробування UA.21541987.00025 - 01 91 01.

5.1.3.4 Засіб технічного захисту інформації від несанкціонованого доступу "Комплекс "Гриф". Версія 4.01. Протокол приймальних випробувань UA.21541987.00025 - 01 92 01.

5.1.4 Документація, яка стосується організації процесу розроблення КЗЗ

5.1.4.1 ТОВ "Інститут комп'ютерних технологій". Положення про порядок розроблення, впровадження та супроводження програмного забезпечення. Редакція від 08.09.2016 р.

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

5.2 Перелік програмних компонентів, що входять до складу інсталяційного пакета комплексу "Гриф" версії 4.

5.2.1 Комплекс "Гриф" версії 4 постачається на інсталяційному диску (CD-ROM), який має структуру та вміст каталогів, зазначені у таблиці 2.

Таблиця 2

Ім'я файлу/ каталогу	**Назва файлу/ документа**
_readme	Файл-довідка з підготовки до інсталяції
Ver_4_01	**каталог**
g4local.exe	Інсталяційний файл-архів
DOC	**каталог**
grif_401a.pdf	Засіб технічного захисту інформації від несанкціонованого доступу "Комплекс "Гриф" версія 4. Настанова адміністратора засобів захисту
grif_401b.pdf	Засіб технічного захисту інформації від несанкціонованого доступу "Комплекс "Гриф" версія 4. Настанова адміністратора безпеки
grif_401i.pdf	Засіб технічного захисту інформації від несанкціонованого доступу "Комплекс "Гриф" версія 4. Настанова системного адміністратора
grif_401q.pdf	Засіб технічного захисту інформації від несанкціонованого доступу "Комплекс "Гриф" версія 4. Скорочена настанова з експлуатації (швидкий старт)
grif_401r.pdf	Засіб технічного захисту інформації від несанкціонованого доступу "Комплекс "Гриф" версія 4. Опис комплексу
grif_401supp.pdf	Засіб технічного захисту інформації від несанкціонованого доступу "Комплекс "Гриф" версія 4. Модуль взаємодії з прикладними програмними системами. Настанова програміста
grif_401u.pdf	Засіб технічного захисту інформації від несанкціонованого доступу "Комплекс "Гриф" версія 4. Настанова користувача

5.2.2 Для експертизи був наданий інсталяційний пакет Комплексу "Гриф" версії 4.01 на інсталяційному диску з серійним номером №0001, структура каталогів якого відповідає наведеній у Таблиці 2. Повний перелік файлів, що містяться в інсталяційному файлі-архіві (g4local.exe) на наданому інсталяційному диску із зазначенням їх контрольних сум наведено у Додатку А.

6 РЕЗУЛЬТАТИ ЕКСПЕРТНИХ РОБІТ

6.1 Комплектність штатного програмного забезпечення комплексу "Гриф" відповідає специфікації комплектності, зазначеної у документах на поставку.

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

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

6.3 Результати експертних випробувань щодо кожного пункту документа "Методики державної експертизи засобу технічного захисту інформації від несанкціонованого доступу "Комплекс "Гриф" версії 4 ІАЛЦ.62.09.20.5117.01.М" викладені у документі "Протокол № 5117 первинної державної експертизи засобу технічного захисту інформації від несанкціонованого доступу "Комплекс "Гриф" версії 4".

6.4 За результатами експертних досліджень у частині, що стосується оцінювання рівня

гарантій коректності реалізації функціональних послуг безпеки (ФПБ) у комплексі "Гриф" встановлено, що:

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

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

– експлуатаційна документація на комплекс "Гриф" 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, НД ТЗІ 2.5-012-2015 та документа "Засіб технічного захисту інформації від несанкціонованого доступу "Комплекс "Гриф". Версія 4. Технічне завдання UA.21541987.00025 - 01 90 01", узгодженого з Адміністрацією Держспецзв'язку України від 01.04.2016 р. з урахуванням порядку реалізації цих вимог, викладеного у документах "Засіб технічного захисту інформації від несанкціонованого доступу "Комплекс "Гриф". Версія 4. Технічний проект UA.21541987.00025 - 01 81 01" та "Технічні вимоги, на відповідність яким здійснюватиметься державна експертиза засобу технічного захисту інформації від несанкціонованого доступу Комплекс "Гриф". Версія 4" (далі – Технічні вимоги). Результати експертних робіт свідчать, що:

6.6 Політика ФПБ "Адміністративна конфіденційність" рівня КА-2, яка реалізується комплексом, визначена стосовно таких об'єктів:

– об'єкти-користувачі, що відповідають користувачам усіх категорій;

– пасивні об'єкти, що відповідають:

– інформаційним об'єктам (ІО) у вигляді структурованих та неструктурованих файлів, що містять ІзОД (відкриту інформацію, що потребує захисту (ВІПЗ)) та зберігаються в каталогах файлової системи логічних дисків, які розміщені на незнімних носіях;

– ІО у вигляді структурованих та неструктурованих файлів, що містять ІзОД (ВІПЗ) та зберігаються в каталогах файлової системи захищених логічних дисків, які розміщені на незнімних та знімних носіях;

– ІО у вигляді структурованих та неструктурованих файлів, що містять ІзОД (ВІПЗ) та зберігаються на зареєстрованих або незареєстрованих знімних носіях;

– ІО у вигляді файлів виконуваного коду ППЗ АС, що зберігаються в каталогах файлової системи логічних дисків, які розміщені на незнімних носіях;

– об’єкти-процеси, що відповідають окремим виконуваним модулям ППЗ АС, за допомогою яких здійснюється доступ до пасивних об’єктів у вигляді ІО відповідного типу;

– периферійне обладнання (пристрої друку, плотери і т.п.), підключене до відповідних портів введення – виведення ПЕОМ;

– накопичувачі на знімних носіях, підключені до відповідних портів введення – виведення ПЕОМ.

Засоби комплексу надають можливість адміністратору засобів захисту, 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 комплексу надають можливість адміністратору засобів захисту, 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 комплексу 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.

6.7 Політика ФПБ "Повторне використання об’єктів" рівня КО-1, яка реалізується засобами комплексу, 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 комплексу, який використовуються для зберігання облікових записів користувачів.

Засоби комплексу 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 комплексу при видаленні (з використанням засобів комплексу) 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 комплексу 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 комплексу забезпечують реалізацію політики ФПБ за правилами, наведеними у п. 3.2 Технічних вимог.

6.8 Політика ФПБ "Конфіденційність при обміні" рівня КВ-2, яка реалізується засобами КЗЗ, визначена стосовно таких об’єктів:

– об’єкти-користувачі, що відповідають користувачам таких категорій;
  – адміністратори засобів захисту;
  – звичайні користувачі;
– захищені логічні диски, які розміщені на знімних та незнімних носіях та у каталогах файлової системи яких зберігаються ІО у вигляді структурованих та неструктурованих файлів, що містять ІзОД (ВІПЗ);
– інтерфейсні процеси, що відповідають окремим виконуваним модулям ППЗ АС, за допомогою яких здійснюється доступ до ІО у вигляді файлів, що зберігаються в каталогах файлової системи захищених логічних дисків.

Політика ФПБ "Конфіденційність при обміні" рівня КВ-2, яка реалізується засобами КЗЗ, не поширюється на захищені логічні диски, на яких зберігаються ІО у вигляді структурованих та неструктурованих файлів, що містять інформацію, яка становить службову інформацію та державну таємницю.

Засоби комплексу забезпечують захист від несанкціонованого ознайомлення з умістом ІО (файлів), що збережені в каталогах файлової системи захищених логічних дисків, шляхом підтримки створення та керування доступом до файлових контейнерів, розміщених як на знімних, так і на незнімних носіях, які доступні через засоби ОС у вигляді захищених логічних диків, за допомогою механізмів "прозорого" розшифрування/ зашифрування даних у момент їх читання/ запису та використання відповідної схеми керування криптографічними ключами. У якості алгоритму розшифрування/ зашифрування даних використовується алгоритм гамування зі зворотним зв’язком, встановлений ДСТУ 7624:2014. Коректність реалізації цієї послуги досягається за рахунок використання програмного модуля "Тайфун-VD" версія 1.01, який реалізує:

– криптографічні алгоритми, визначені ДСТУ 7564:2014, ДСТУ 7624:2014 (у режимах "Калина-128/128-CFB", "Калина-128/128-KW", "Калина-128/128-CMAC"), ДСТУ 4145-2002 (в частині генерації особистих ключів та обчислення відкритих ключів електронного цифрового підпису);
– генерацію випадкових послідовностей при генерації особистих ключів, які використовуються у протоколі узгодження ключів;
– вироблення секретних ключів шифрування даних для зашифрування/ розшифрування даних за алгоритмом, визначеним ДСТУ 7624:2014;
– вироблення секретних ключів шифрування ключів для зашифрування/ розшифрування секретних ключів шифрування даних за алгоритмом, визначеним ДСТУ 7624:2014, на підставі особистих ключів комплексу засобів захисту та відкритих ключів користувачів або відкритих ключів комплексу засобів захисту та особистих ключів користувачів за схемою Діффі-Гелмана, що базується на криптографічних перетвореннях у групі точок еліптичної кривої;

– вироблення секретних ключів шифрування ключів для зашифрування/ розшифрування особистих ключів комплексу засобів захисту за алгоритмом, визначеним ДСТУ 7624:2014, на підставі особистих ключів адміністраторів та відкритих ключів адміністраторів за схемою Діффі-Гелмана, що базується на криптографічних перетвореннях у групі точок еліптичної кривої;

– вироблення секретних ключів шифрування ключів для зашифрування/ розшифрування особистих ключів користувачів та особистих ключів адміністраторів за алгоритмом, визначеним ДСТУ 7624:2014;

– генерацію та зберігання ключових даних.

Програмний модуль "Тайфун-VD" версія 1.01 відповідає вимогам технічного завдання (UA.21541987.00023 – 01 90 01) із доповненням № 1 до нього UA.21541987.00023 – 01 90 02 в частині реалізації функцій криптографічних перетворень.

Програмний модуль "Тайфун-VD" версія 1.01 як засіб криптографічного захисту інформації категорії "Р" і категорії "К" (що використовується у засобах категорії "Р") може бути використаний для криптографічного захисту інформації з обмеженим доступом (крім інформації, що становить державну таємницю) та відкритої інформації, вимога щодо захисту якої встановлена законом.

Програмний модуль "Тайфун-VD" версія 1.01 має позитивний експертний висновок в сфері КЗІ № 04/03/03-3691 від 14.09.2016 р.

Засоби комплексу забезпечують реалізацію політики ФПБ за правилами, наведеними у п. 3.3 Технічних вимог.

6.9 Політика ФПБ "Адміністративна цілісність" рівня ЦА-1, яка реалізується засобами комплексу, визначена стосовно таких об’єктів:

– об’єкти-користувачі, що відповідають користувачам усіх категорій;

– пасивні об’єкти, що відповідають:

– ІО у вигляді структурованих та неструктурованих файлів, що містять ІзОД (ВІПЗ) та зберігаються в каталогах файлової системи логічних дисків, які розміщені на незнімних носіях;

– ІО у вигляді структурованих та неструктурованих файлів, що містять ІзОД (ВІПЗ) та зберігаються в каталогах файлової системи захищених логічних дисків, які розміщені на незнімних та знімних носіях;

– ІО у вигляді структурованих та неструктурованих файлів, що містять ІзОД (ВІПЗ) та зберігаються на зареєстрованих або незареєстрованих знімних носіях;

– ІО у вигляді файлів виконуваного коду ППЗ АС, що зберігаються в каталогах файлової системи логічних дисків, які розміщені на незнімних носіях;

– накопичувачі на знімних носіях, підключені до відповідних портів введення – виведення ПЕОМ.

Засоби комплексу надають можливість адміністратору засобів захисту, що має відповідні повноваження, для кожного захищеного ІО шляхом керування належністю користувачівта ІО до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати ІО.

Засоби комплексу забезпечують реалізацію політики ФПБ за допомогою механізму керування доступом з використанням атрибутів користувачів та захищених ІО та за правилами, наведеними у п. 3.4 Технічних вимог.

6.10 Політика ФПБ "Адміністративна цілісність" рівня ЦА-2, яка реалізується засобами комплексу, визначена стосовно таких об’єктів:

– об’єкти-користувачі, що відповідають користувачам усіх категорій;

– пасивні об’єкти, що відповідають:

– ІО у вигляді структурованих та неструктурованих файлів, що містять ІзОД (ВІПЗ) та зберігаються в каталогах файлової системи логічних дисків, які розміщені на незнімних носіях;

– ІО у вигляді структурованих та неструктурованих файлів, що містять ІзОД (ВІПЗ) та зберігаються в каталогах файлової системи захищених логічних дисків, які розміщені на незнімних та знімних носіях;

– ІО у вигляді структурованих та неструктурованих файлів, що містять ІзОД (ВІПЗ) та зберігаються на зареєстрованих або незареєстрованих знімних носіях;

– ІО у вигляді файлів виконуваного коду ППЗ АС, що зберігаються в каталогах файлової системи логічних дисків, які розміщені на незнімних носіях;

– об’єкти-процеси, що відповідають окремим виконуваним модулям ППЗ АС, за допомогою яких здійснюється доступ до пасивних об’єктів у вигляді ІО відповідного типу;

– накопичувачі на знімних носіях, підключені до відповідних портів введення – виведення ПЕОМ.

Засоби комплексу надають можливість адміністратору засобів захисту, 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 комплексу надають можливість адміністратору засобів захисту, 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 комплексу забезпечують реалізацію політики ФПБ за допомогою механізму керування доступом з використанням атрибутів користувачів, процесів та захищених ІО та за правилами, наведеними у п. 3.5 Технічних вимог.

6.11 Політика ФПБ "Відкат" рівня ЦО-1, яка реалізується засобами комплексу, визначена стосовно таких об’єктів:

– адміністратори засобів захисту;

– набори даних, що містяться у сховищах технологічної інформації комплексу.

Засоби комплексу забезпечують можливість автоматизованого здійснення відкату баз даних (БД) технологічної інформації комплексу 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. 3.6 Технічних вимог.

6.12 Політика ФПБ "Цілісність при обміні" рівня ЦВ-2, яка реалізується засобами

комплексу, визначена стосовно таких об’єктів:

– об’єкти-користувачі, що відповідають користувачам таких категорій;

– адміністратори засобів захисту;

– звичайні користувачі;

– захищені логічні диски, які розміщені на знімних та незнімних носіях та у каталогах файлової системи яких зберігаються ІО у вигляді структурованих та неструктурованих файлів, що містять ІзОД (ВІПЗ);

– інтерфейсні процеси, що відповідають окремим виконуваним модулям ППЗ АС, за допомогою яких здійснюється доступ до ІО у вигляді файлів, що зберігаються в каталогах файлової системи захищених логічних дисків.

Політика ФПБ "Цілісність при обміні" рівня ЦВ-2, яка реалізується засобами КЗЗ, не поширюється на захищені логічні диски, на яких зберігаються ІО у вигляді структурованих та неструктурованих файлів, що містять інформацію, яка становить службову інформацію та державну таємницю.

Засоби комплексу забезпечують можливість виявлення фактів несанкціонованої модифікації ІО (файлів), що збережені в каталогах файлової системи захищених логічних дисків, а також фактів їх видалення/дублювання за допомогою механізмів вироблення/ перевіряння кодів контролю цілісності (ККЦ) умісту захищених логічних дисків при їх демонтуванні (відключенні), монтуванні (підключенні) як видимих у засобах файлової системи. У якості алгоритму вироблення ККЦ використовується алгоритм вироблення імітовставки, встановлений ДСТУ 7624:2014. Коректність реалізації цієї послуги досягається за рахунок використання програмного модуля "Тайфун-VD" версія 1.01, функції якого описані в п. 6.8.

Засоби комплексу забезпечують реалізацію політики ФПБ за правилами, наведеними у п. 3.7 Технічних вимог.

6.13 Політика ФПБ "Використання ресурсів" рівня ДР-1, яка реалізується засобами комплексу, визначена стосовно таких об’єктів:

– користувачів усіх категорій;

– дискового простору незнімних носіїв, який використовується користувачами для зберігання створених ними ІО у вигляді структурованих та неструктурованих файлів, що зберігаються у каталогах файлової системи логічних дисків.

Засоби комплексу надають можливість адміністратору засобів захисту за правилами, наведеними у п. 3.8 Технічних вимог, встановити обмеження на обсяг дискового простору логічних дисків, що може бути використаний користувачами для зберігання створених ними ІО.

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

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

– модуля контролю запитів доступу до ресурсів та керування доступом до ресурсів (системного драйвера);

– провайдера автентифікації;

– модуля контролю запитів доступу до ресурсів та керування доступом до ресурсів (системного сервісу);

– модуля контролю операцій експорту даних;

– модуля контролю операцій друку;

– інтерфейсного модуля взаємодії з ППС;

– модуля підтримки захищених логічних дисків;

– модуля керування захищеними логічними дисками;

– модуля адміністрування;

– модуля обслуговування носіїв даних автентифікації користувачів;

– модуля відновлення цілісності та оновлення;

– модуля зберігання даних аудита;

– модуля аналізу даних аудита.

У випадку виникнення певних відмов програмних засобів (ПЗ) комплексу решта засобів комплексу не втрачають працездатність та забезпечують реалізацію відповідних ФПБ.

Засоби комплексу здатні зареєструвати факт відмови певних структурних компонентів комплексу та повідомити про це адміністраторів за правилами, наведеними у п. 3.9 Технічних вимог.

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

– модуля контролю запитів доступу до ресурсів та керування доступом до ресурсів (системного драйвера);

– провайдера автентифікації;

– модуля контролю запитів доступу до ресурсів та керування доступом до ресурсів (системного сервісу);

– модуля контролю операцій експорту даних;

– модуля контролю операцій друку;

– інтерфейсного модуля взаємодії з ППС;

– модуля підтримки захищених логічних дисків;

– модуля керування захищеними логічними дисками;

– модуля адміністрування;

– модуля обслуговування носіїв даних автентифікації користувачів;

– модуля відновлення цілісності та оновлення;

– модуля зберігання даних аудита;

– модуля аналізу даних аудита.

Засоби комплексу надають можливість системному адміністратору провести модернізацію (оновлення) ПЗ комплексу за правилами, наведеними у п. 3.10 Технічних вимог.

Засоби оновлення ПЗ комплексу 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 комплексу реєструються у журналі реєстрації з використанням засобів реалізації ФПБ "Реєстрація".

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

– модуля контролю запитів доступу до ресурсів та керування доступом до ресурсів (системного драйвера);

– провайдера автентифікації;

– модуля контролю запитів доступу до ресурсів та керування доступом до ресурсів (системного сервісу);

– модуля контролю операцій експорту даних;

– модуля контролю операцій друку;

– інтерфейсного модуля взаємодії з ППС;

– модуля підтримки захищених логічних дисків;

– модуля керування захищеними логічними дисками;

– модуля адміністрування;

– модуля обслуговування носіїв даних автентифікації користувачів;

– модуля відновлення цілісності та оновлення;

– модуля зберігання даних аудита;

– модуля аналізу даних аудита.

Засоби комплексу надають можливість системному адміністратору провести відновлення цілісності та працездатності ПЗ комплексу за правилами, наведеними у п. 3.11 Технічних вимог.

Засоби відновлення цілісності та працездатності ПЗ комплексу 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 комплексу реєструються у журналі реєстрації з використанням засобів реалізації ФПБ "Реєстрація".

6.17 Політика ФПБ "Реєстрація" рівня НР-3, яка реалізується засобами комплексу, визначає такий перелік подій (які реєструються у відповідних журналах), що мають безпосереднє відношення до безпеки та стосуються функціонування комплексу, 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 доступу та виконання певних дій або факти 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 комплексу;

– факти перезавантаження, вимикання ПЕОМ 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 комплексу повідомляють адміністраторів безпеки про виявлені засобами аналізу зареєстрованих подій, реалізованими у складі модуля контролю запитів доступу до ресурсів та керування доступом до ресурсів (системний сервіс), факти виникнення одиночних або повторюваних подій, які можуть свідчити про прямі (істотні) порушення політики безпеки, шляхом негайного виведення відповідних повідомлень на екран, а також виведення відповідних повідомлень на екран під час першого (після реєстрації відповідного факту) входу в систему

Засоби комплексу надають можливість адміністраторам безпеки провести перегляд та аналіз зареєстрованої інформації про зареєстровані події.

Засоби комплексу забезпечують реалізацію політики ФПБ за правилами, наведеними у п. 3.12 Технічних вимог.

6.18 Політика ФПБ "Ідентифікація та автентифікація" рівня НИ-3, яка реалізується засобами комплексу, визначена стосовно користувачів таких категорій:

– системний адміністратор;

– адміністратори засобів захисту;

– адміністратори безпеки;

– користувачі з різними рівнями повноважень.

Засоби комплексу 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. 3.13 Технічних вимог.

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

– користувачів усіх категорій;

– ПЗ комплексу.

Засоби комплексу 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. 3.14 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".

6.20 Політика ФПБ "Розподіл обов'язків" рівня НО-2, яка реалізується засобами

комплексу, визначає функції, притаманні таким ролям користувачів:

- системний адміністратор;
- адміністратори засобів захисту;
- адміністратори безпеки;
- користувачі з різними рівнями повноважень.

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

6.21 Політика ФПБ "Цілісність комплексу засобів захисту" рівня НЦ-2, яка реалізується засобами комплексу, визначена стосовно всіх зазначених в детальному проекті структурних компонентів (модулів) комплексу, що входять до складу:

- модуля контролю запитів доступу до ресурсів та керування доступом до ресурсів (системного драйвера);
- провайдера автентифікації;
- модуля контролю запитів доступу до ресурсів та керування доступом до ресурсів (системного сервісу);
- модуля контролю операцій експорту даних;
- модуля контролю операцій друку;
- інтерфейсного модуля взаємодії з ППС;
- модуля підтримки захищених логічних дисків;
- модуля керування захищеними логічними дисками;
- модуля адміністрування;
- модуля обслуговування носіїв даних автентифікації користувачів;
- модуля відновлення цілісності та оновлення;
- модуля зберігання даних аудита;
- модуля аналізу даних аудита.

Засоби комплексу з метою захисту від зовнішніх впливів на несанкціонованої модифікації підтримують власний домен виконання, відмінний від доменів всіх інших процесів, за правилами, наведеними у п. 3.16 Технічних вимог.

Додатково до виділення домену виконання, засоби комплексу забезпечують контроль цілісності програмних модулів комплексу з використанням механізму розрахунку ККЦ програмних модулів 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 комплексу, повідомляється про це системний адміністратор та комплекс переводиться до стану, в якому заборонене оброблення ІзОД. Повернення до нормального режиму роботи може виконати тільки системний

адміністратор з використанням спеціальних програмних засобів (модуля відновлення цілісності та оновлення).

6.22 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 контролю запитів доступу до ресурсів та керування доступом до ресурсів (системного драйвера);

– провайдера автентифікації;

– модуля контролю запитів доступу до ресурсів та керування доступом до ресурсів (системного сервісу);

– модуля контролю операцій експорту даних;

– модуля контролю операцій друку;

– інтерфейсного модуля взаємодії з ППС;

– модуля підтримки захищених логічних дисків;

– модуля керування захищеними логічними дисками;

– модуля адміністрування;

– модуля обслуговування носіїв даних автентифікації користувачів;

– модуля відновлення цілісності та оновлення;

– модуля зберігання даних аудита;

– модуля аналізу даних аудита.

Засоби комплексу за правилами, наведеними у п. 3.17 Технічних вимог, здійснюють перевірку працездатності шляхом автоматичної перевірки цілісності ПЗ комплексу 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 (з використанням модуля адміністрування), а також цілісності БД технологічної інформації комплексу при доступі до неї з боку модулів комплексу.

7 ВИСНОВКИ

За результатами експертизи за критеріями технічного захисту інформації комплексу "Гриф" версії 4 встановлено:

– наданий для випробувань комплекс "Гриф" версії 4 відповідає вимогам нормативних документів системи технічного захисту інформації в Україні, у тому числі НД ТЗІ 2.5-012-2015, НД ТЗІ 2.5-008-2002 та Технічного завдання;

– сукупність реалізованих у комплексі "Гриф" версії 4 функцій та механізмів захисту інформації з рівнем гарантій Г-4 коректності реалізації функціональних послуг безпеки забезпечує реалізацію наведеного у п. 6.2 функціонального профілю захищеності інформації;

– результати експертизи Комплексу "Гриф" версії 4 дійсні для складу програмних засобів комплексу, наведеного у Таблиці 2, для версій структурних компонентів комплексу, що містяться в інсталяційному файлі комплексу "Гриф" версії 4.01, склад якого наведено у Додатку А, а також для пакетів оновлення КЗЗ "Гриф" версій 4.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 "Засіб технічного захисту інформації від несанкціонованого доступу Комплекс "Гриф" версія 4. Програма та методика випробувань UA.21541987. 00025 - 01 51 02" 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 Комплексу "Гриф" версія 4 вимогам НД ТЗІ 2.5-012-2015 він без обмежень може бути використаний в АС класу "1" для захисту інформації, що становить державну таємницю; 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.

При цьому засоби реалізації ФПБ "Конфіденційність при обміні" рівня КВ-2 та "Цілісність при обміні" рівня ЦВ-2 можуть використовуватися лише для захисту 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.

8.2 На підставі встановленої за результатами експертизи відповідності Комплексу "Гриф" версія 4 вимогам НД ТЗІ 2.5-008-2002 він без обмежень може бути використаний в АС класу "2" 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 Комплексу "Гриф" версія 4 для захисту інформації, що становить державну таємницю, оброблюваної в АС класу "2" можливо за умов відповідності комплексу вимогам щодо політики та порядку реалізації функціональних послуг безпеки, висунутим у

Технічному завданні на створення відповідної комплексної системи захисту інформації.

При цьому засоби реалізації ФПБ "Конфіденційність при обміні" рівня КВ-2 та "Цілісність при обміні" рівня ЦВ-2 можуть використовуватися лише для захисту 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.

8.3 При функціонуванні комплексу "Гриф" версія 4 має бути забезпечено дотримання таких умов: на ПЕОМ, на яких встановлені засоби комплексу, організаційними та/або технічними заходами має бути заблокована можливість завантаження ОС зі знімних носіїв.

9 ТЕРМІН ДІЇ ЕКСПЕРТНОГО ВИСНОВКУ

Термін дії експертного висновку – до _____ 2020 р., за умови наявності чинного експертного висновку в сфері КЗІ на програмний модуль криптографічного захисту та розмежування доступу до інформаційних ресурсів "Тайфун-VD" версія 1.01.

Додаток А
(обов'язковий)

Вміст інсталяційного файлу-архіву комплексу "Гриф" версії 4.01, наданого на експертизу

Ім’я файлу	Назва	Розмір файлу (байт)	Геш-вектор за ГОСТ 28147-89*	Дата створення
ALLFILES.IMM	Файл кодів контролю цілісності пакету інсталяції (повний)	1270	A491E817 B68ECE46 278984F8 F3D16473 DDF44900 F4B3B5DA 5183FD47 24C35724	01-09-2017
ARMG4.INI	Файл початкових настроювань	136	12482CC9 CDD3055B E64CEFD7 FD5E2E68 2D7D0B2A A1DC37D9 6095C854 841B4170	21-09-2016
AUDITLOG60.DLL	Динамічна бібліотека обробки даних аудита	167936	7875E826 15FD79EC 60F8F160 8217FF3D 22DF310B B183AD61 F1E149F6 72719C6B	04-10-2016
CBUTIL.EXE	Програма контролю буферу обміну для 32-х розрядних ОС	221184	1E81B6F6 517A77AD 01116800 82642932 C2084D0F 77667D7A 99EC5A9C 84313812	18-07-2017
CBUTILX64.EXE	Програма контролю буферу обміну для 64-х розрядних ОС	389632	89632BA1 84F5E9FD 338A891B 5C5F649B CB46B9D3 6970F30A FA0AF6D8 851581E8	19-07-2017
DEMANDS.TXT	Файл із описом необхідних умов для інсталяції комплексу	2484	E4D4861E F472405B 6E60ADDA B4D098A5 BFFC467F 494E468A 72E521D5 37ADA8B8	18-07-2017
ERRORS.HTM	Файл довідкової інформації щодо помилок під час інсталяції	77353	AC697328 0FD9AC87 DF631A2C 0680A1C1 779883FF 025BAF34 935948D1 8D18652C	22-09-2016
G4_061ON.SYS	Системний драйвер для 32-розрядної ОС Windows 7	84384	09915FC7 7A5A0DA7 0320018C 9900FE4F C7D337FA 3CA31919 AF6D516B 205D9ACA	06-06-2017
G4_061ONX64.SYS	Системний драйвер для 64-розрядних ОС Windows 7/ Windows Server 2008 R2	129952	B53858F7 3D92DD3C 4297A40C 9759CBE2 ECE13095 F813BEF2 CAB1FB30 3279DE27	09-06-2017
G4_061ROMI.SYS	Системний драйвер для 32-розрядної ОС Windows 7	139680	2558ED0E 6813E00D 16A8DA1E AC923208 0AEF196D AA53B1AC BB4C0F72 101EF12D	02-06-2017
G4_061ROMIX64.SYS	Системний драйвер для 64-розрядних ОС Windows 7/ Windows Server 2008 R2	210336	CE3023DA B00610BB 00540808 2697B22E 1900BF7C DCD774FC FF0DF364 DCA045DF	09-06-2017
G4_063ON.SYS	Системний драйвер для 32-розрядної ОС Windows 8.1	85512	655C74F7 BF6AFD29 EA86B488 1A044893 09D6BEEE C8BA55F6 B89C7689 5A8A096C	08-06-2017
G4_063ONX64.SYS	Системний драйвер для 64-розрядних ОС Windows 8.1/ Windows Server 2012 R2	135976	C4DFCC04 4EFD0A25 E2DBD49B 3774743D 55E783BD 9DFEBDF9 916E573B 2619F016	12-06-2017
G4_063ROMI.SYS	Системний драйвер для 32-розрядної ОС Windows 8.1	185464	DF0C416C AB1E74E2 70C7C004 72F6BA0D 63B67218 4C24B6DA CF1FEE26 B1988329	10-07-2017
G4_063ROMIX64.SYS	Системний драйвер для 64-розрядних ОС Windows 8.1/ Windows Server 2012 R2	244680	A736D913 A2D574F7 AB8288BE A42D015E 015F0FC7 C27AFC17 AFCE531D 3AA13ABC	10-07-2017
G4_100ON.SYS	Системний драйвер для 32-розрядної ОС Windows 10	85512	BD27924B 58FC8928 79F07926 071072F6 913F84B4 4A49FE59 DD8EE281 A0C89DEA	08-06-2017
G4_100ONX64.SYS	Системний драйвер для 64-розрядних ОС Windows 10/ Windows Server 2016	135464	AD84E4B9 9C288D90 73688920 64500677 EF0C93D5 8975CAC1 7908600C 8006EC7C	12-06-2017
G4_100ROMI.SYS	Системний драйвер для 32-розрядної ОС Windows 10	192656	A11DB55F D85BA4FF 7D012698 69AAE6A0 0406C17D B60E5CEC 01336C71 27E9005B	10-07-2017
G4_100ROMIX64.SYS	Системний драйвер для 64-розрядних ОС Windows 10/ Windows Server 2016	232296	6EEEFC9B 00A6F35A E1F782D2 CFD31669 DB8EF1D9 C5753424 E57926A2 883BA286	10-07-2017
G4ARMEV.EXE	Програма модуля аналізу даних аудита	1320448	E1EAAB8B 930CAB09 6D049748 3F9984BE F4C7875F B695CE05 F4A4708F 7B6209A6	20-07-2017

Ім’я файлу	Назва	Розмір файлу (байт)	Геш-вектор за ГОСТ 28147-89*	Дата створення
G4ARMRA.EXE	Програма модуля адміністрування для 32-х розрядних ОС	1654784	09F225FB 8338912B 2A22B99F 0CEB5856 1454B3E4 979D6298 E07B79DC 5B550CFE	01-09-2017
G4ARMRAX64.EXE	Програма модуля адміністрування для 64-х розрядних ОС	2605568	CD7FB25F 23ACE694 14551A7A BC6D381E A9C95D21 5F1B8465 32A4EB4E F5CB3162	01-09-2017
G4CONTROL.DLL	Динамічна бібліотека модуля керування захищеними логічними дисками для 32-х розрядних ОС	180224	60868642 99E451DB A577C228 3543A458 9A334F87 C571A528 02C39403 DBC3782E	19-07-2017
G4CONTROL.EXE	Програма модуля керування захищеними логічними дисками для 32-х розрядних ОС	331776	E020DA6F 1AB96731 A99BEA53 913B706E 484EBDEF 21C3D864 BBF3AE9D CE988C2B	17-07-2017
G4CONTROLX64.DLL	Динамічна бібліотека модуля керування захищеними логічними дисками для 64-х розрядних ОС	240640	AF7B3DFD E65EC4A8 36BB7AE7 A95A294C 617B49DB 9F55071A 15ADC6DF EA29335D	19-07-2017
G4CONTROLX64.EXE	Програма модуля керування захищеними логічними дисками для 64-х розрядних ОС	574464	2B2FCD50 F66C01D2 137DD413 3D03E343 217972F3 ABFC6D3F 1F64FE60 59F11F51	19-07-2017
G4CP.DLL	Провайдер автентифікації для 32-х розрядних ОС	356352	A25007D2 945C3D07 833CF7B6 6B2C61C9 6AA4E81E C7FC8D2D E6B6AB4A CF4ACC18	17-07-2017
G4CPX64.DLL	Провайдер автентифікації для 64-х розрядних ОС	786944	1C885654 B793D8A4 E8280A41 E989F8EE 1ABFFFFC C66FEF40 76B63519 29A216E7	19-07-2017
G4EXPORT.EXE	Програма експорту даних	167936	B94E95DD 8D8A944E D18EF93B 4120AA7C 77A316BF 9EE62F5D 9F1A8FE8 0EE28E59	17-07-2017
G4PRINT.EXE	Програма друку даних	253952	0951491D 165708EF 0F4B5DBB FCBA97DA E6E9F636 B99A8C7B F166A11F 2AE65817	17-07-2017
G4RECOVER.DLL	Модуль відновлення цілісності та оновлення для 32-х розрядних ОС	434176	DD38E317 FC8B9B0C 540EC0E2 06F13882 9F5C6151 E8EA86B6 C5863D48 64EC221B	19-07-2017
G4RECOVER061.IMM	Файл кодів контролю цілісності пакету інсталяції (частковий)	51	AFE4BFCF 4638A4DD 061F128D 00D1B2A7 F6A2B17E EE84B6D4 DF1566E7 AF92FADE	01-09-2017
G4RECOVER063.IMM	Файл кодів контролю цілісності пакету інсталяції (частковий)	51	AD688A3B A4794DBB C7C00CD7 DC09728E 227055F1 318FC0DE FBB01373 EC224BB1	01-09-2017
G4RECOVER100.IMM	Файл кодів контролю цілісності пакету інсталяції (частковий)	51	1B6C8743 55C6EF07 9CED7208 A90266D3 27025097 91BBC36A E6A230BF 3375B686	01-09-2017
G4RECOVERX64.DLL	Модуль відновлення цілісності та оновлення для 64-х розрядних ОС	686080	D48B7C18 5A634964 181588AB 7DFCAD3A 4A9BA3B8 DE5CB491 4724B905 1DB98663	19-07-2017
G4RECOVERX64_061.IMM	Файл кодів контролю цілісності пакету інсталяції (частковий)	57	19D166A5 C00DD0A4 B04C3BD0 34C5FBE5 40F79EBB D4F9EC5E CB9CED68 C2545543	01-09-2017
G4RECOVERX64_063.IMM	Файл кодів контролю цілісності пакету інсталяції (частковий)	57	68AA45DB 741CFDC6 33D77ED8 910F7F35 5CC42209 B7D958A4 14EBA23E 078C805C	01-09-2017
G4RECOVERX64_100.IMM	Файл кодів контролю цілісності пакету інсталяції (частковий)	57	31B9FF99 534DED5B 018D9B7B B989E428 A2743A7C 3A9F8E25 F823A8DD 80964A33	01-09-2017

Ім’я файлу	Назва	Розмір файлу (байт)	Геш-вектор за ГОСТ 28147-89*	Дата створення
G4SHEXT.DLL	Динамічна бібліотека розширення Windows Explorer для 32-х розрядних ОС	102400	F36A6F91 3AB9ACD1 8F02FF9E B5053019 66B47A6D A31C2BA0 6447761C 3ECF66FB	17-07-2017
G4SHEXTX64.DLL	Динамічна бібліотека розширення Windows Explorer для 64-х розрядних ОС	110080	B1A6DEA5 F5B4B081 D3B880CF 64B102B2 27310EE6 32E79204 418D2750 D9E13B67	19-07-2017
G4SUPP.DLL	Динамічна бібліотека взаємодії з ППС для 32-х розрядних ОС	315392	1C05117B 27650508 06B39A35 EEC76D03 303ED39A 6E89D8FB BB8ADD5F 4988746F	18-10-2016
G4SUPPX64.DLL	Динамічна бібліотека взаємодії з ППС для 64-х розрядних ОС	388608	B376BDDE 5BA5B566 8F13E188 38BF9801 3267A7B8 DBD54679 82EFB285 D184ACB2	25-04-2017
GNCAT.DLL	Динамічна бібліотека розбору повідомлень комплексу	61440	D972E75B 3CE39A82 B605C3A2 A899D4AF 3EF375F4 8E326D9C 9A20BDE7 5D4A3C78	05-10-2016
GRIF_SER.EXE	Допоміжний системний сервіс	237568	C6A42926 1CC3289F 95B41CA2 BA03A0C1 55444D68 284C0816 BB8244F7 0B8277A7	04-01-2017
GRIFLOCAL061.INF	Файл параметрів конфігурації для програми інсталяції	20407	F31ABA34 3DC62A62 4ABA3CE7 98252AD2 80C4FFAA C033B6DA 5DAAE1DA BFC68BC9	20-04-2017
GRIFLOCAL063.INF	Файл параметрів конфігурації для програми інсталяції	22292	1A3606E6 24A6EBBC 1AFC8A03 D163E230 2C03327E 491D5413 462CE479 3CB41F7D	20-04-2017
GRIFLOCAL100.INF	Файл параметрів конфігурації для програми інсталяції	22292	E4F190F0 DC71ACF1 7C638B56 4B7C4558 D500D4CE B25BB2CA 8AEC9930 8F57969C	20-04-2017
GRIFLOCALX64_061.INF	Файл параметрів конфігурації для програми інсталяції	25880	C65CE722 78072FD1 D34C3864 EA02987E 34BCD7E7 70F28D35 5FB9063B 8E04506F	20-04-2017
GRIFLOCALX64_063.INF	Файл параметрів конфігурації для програми інсталяції	27763	CC6BFABE DB2E8E3E 7D4852CB 2ED68BEA 03E4AF9F 7197024B 770958ED 42D0FE8F	20-04-2017
GRIFLOCALX64_100.INF	Файл параметрів конфігурації для програми інсталяції	27763	F87D41F5 2E8D3CB4 EB49C19A 8D54CA91 EE694983 E42E53DE 6680FA23 492ECC24	20-04-2017
GRIFPOL_T061.INF	Файл параметрів конфігурації для програми інсталяції	119358	F3CCD909 D473B85E 9A8A8E98 CD6662B3 5EFFC38D 56F6ECB1 7A8D57AF 9173423C	21-09-2016
GRIFPOL_T063.INF	Файл параметрів конфігурації для програми інсталяції	111082	0D619DCD 89B03C0C 5847156F CC2AA0B8 40374891 F4BD144D 063CC358 3EDB5EE3	21-09-2016
GRIFPOL_T100.INF	Файл параметрів конфігурації для програми інсталяції	45148	BD318D37 BC00C9F0 B412DE3A E2EABAA4 D3C4885B C553E2A1 D95B6E7C 4A8D8EE3	27-12-2016
GRIFPOLAS2_T061.INF	Файл параметрів конфігурації для програми інсталяції	119514	7221B401 570994DA A5EDA472 8D059D4B AADFF029 151DB90F AC1B962B 7F2A2C59	21-09-2016
GRIFPOLAS2_T063.INF	Файл параметрів конфігурації для програми інсталяції	111042	8E8ABECA 0FECF9CA C448CE2E 8572B9C5 75056AFB 0598599C 06065CDA 459EFCC2	21-09-2016
GRIFPOLAS2_T100.INF	Файл параметрів конфігурації для програми інсталяції	45102	B6579608 C73D6D56 52CEF691 071FEF73 35A2158D 840CABA2 C60953FF EA2FB69D	27-12-2016
GRIFSRV.EXE	Системний сервіс для 32-х розрядних ОС	245760	3E458AA1 7D8B577B 973F2D76 0F29D398 F509EC31 F489227E 5EB4CE61 B0A52A3A	25-04-2017
GRIFSRVX64.EXE	Системний сервіс для 64-х розрядних ОС	308224	E2A7599B FB8CAA2E 9EB8502D 809CE5CC F3CA6D03 DBD726EB E6CDD965 693631E6	26-04-2017

Ім’я файлу	Назва	Розмір файлу (байт)	Геш-вектор за ГОСТ 28147-89*	Дата створення
GRIFTEMPL061.IMM	Файл кодів контролю цілісності пакету інсталяції (частковий)	828	26B8713D 80E4BF81 ADB092A7 6C39FF2B FC327818 5AB6ADF9 B360DA2D 1BA1FD2E	01-09-2017
GRIFTEMPL063.IMM	Файл кодів контролю цілісності пакету інсталяції (частковий)	828	A3182602 4D429C05 20FD2E36 C2CD651A 11C2FA48 2D918BF8 4F0AD500 54B33C77	01-09-2017
GRIFTEMPL100.IMM	Файл кодів контролю цілісності пакету інсталяції (частковий)	828	180A5E61 68240904 EC8FC90A A2D01436 97AD6B3B 0F6AB673 55B9DB56 10ABFD81	01-09-2017
GRIFTEMPLX64_061.IMM	Файл кодів контролю цілісності пакету інсталяції (частковий)	897	35A80A77 A6052A54 E9852464 BA3F7ED0 B131BD9E C970F193 569BC56C D0E54AC9	01-09-2017
GRIFTEMPLX64_063.IMM	Файл кодів контролю цілісності пакету інсталяції (частковий)	897	4ABDC248 FBDF78B9 E3B12CF8 BB306030 FBB7330D 072009F8 3D47F5A2 7D162A12	01-09-2017
GRIFTEMPLX64_100.IMM	Файл кодів контролю цілісності пакету інсталяції (частковий)	897	6B97FC03 7342763B 9E3EB226 C3AEE23A F73C1890 9EACD0A7 244BD838 201BF459	01-09-2017
LICENSE.TXT	Файл з текстом ліцензійної угоди	1017	EDF8F5F1 D8DF34DB 548CE056 B6AB2844 56118A35 6BCAA61D A8333244 2F5FB5CE	18-07-2017
LOG2KRUS.DLL	Службова динамічна бібліотека	12800	02F30E1E D297DBD0 2E46BF5D 38318658 DC530EA6 10D9B11E 1A3DAD2C 2DF4C90B	01-10-2016
NTDSMIR.DLL	Динамічна бібліотека розбору GUID	90112	0DE0C1C7 B5FEEFAF 61EE1747 C3E849AC BC42320D C1486EEB 8425DEAC 64FDA77E	17-09-2009
SAVEDAT.DLL	Динамічна бібліотека збереження даних аудита	786944	FDF49F78 2DC3D182 2236D7FF 9DC77BD9 2312FF5C F041BAAA A4D25FDD 0D1E9B3D	23-09-2016
SECLEV.DAT	Файл бази даних рівнів конфіденційності	4962	2463D233 C64D46C7 7322E88D 160BDB13 D5C2EB11 3EAD0DF1 59DDC347 ED1F7CE4	13-07-2017
SETUP.EXE	Програма інсталяції комплексу	716800	0B29D108 85958ADD C5C56332 E5DDC6AA 765A41E0 605602F7 F8EB301A E9D08FA8	29-08-2017
STPINF64.INF	Файл параметрів конфігурації для програми інсталяції	164864	F546B910 CE26401F E4E7E692 F8A074B0 C1A96445 004E0B56 A525C21E CC9C71CB	11-05-2017
TFN_VD.SYS	Модуль підтримки захищених логічних дисків для 32-х розрядних ОС	202936	E72F90F2 9CCE4644 7E7803B2 62A0590F 987B8726 E2CCDC52 D81DD57C 428DF289	21-03-2017
TFN_VDX64.SYS	Модуль підтримки захищених логічних дисків для 64-х розрядних ОС	256008	E104282C 51659D0E 47C934E5 D2F02237 A9458F56 BF17A7FE CE712485 34D533B3	22-03-2017
ZLIB.DLL	Динамічна бібліотека архівування / розархівування даних	53760	3F334974 125B9915 6B66A9C2 78FFD66E B5A2C230 294F0C14 22F9EC51 F1B7CDFF	13-04-2006

*) Геш-вектори розраховано за допомогою програмного виробу реалізації функцій контролю цілісності даних "HashCounter" (UA.DEKZI.00001 01-01), експертний висновок № 05/02/02-4323 від 28.11.2013 р.