ЕКСПЕРТНИЙ ВИСНОВОК

Комплекс засобів захисту інформації від несанкціонованого доступу "Гриф" версії 3 виробництва ТОВ "Інститут комп'ютерних технологій"

Зареєстровано в Адміністрації Державної служби спеціального зв'язку та захисту інформації України "01" липня 2016 р. за № **674**

Дійсний до "01" липня 2019 р.

Перший заступник Голови Служби

О. М. Чаузов

м.п.

За результатами експертизи встановлено, що

комплекс засобів захисту інформації

назва засобу технічного захисту інформації

від несанкціонованого доступу "Гриф" версії 3,

який наданий на експертизу **ТОВ "Інститут комп'ютерних**

назва та адреса організації

технологій", м. Київ, просп. Повітрофлотський, 54,

відповідає

відповідає, не відповідає

вимогам нормативних документів системи технічного захисту інформації в Україні, в тому числі вимогам НД ТЗІ 2.5-008-2002, в обсязі функцій, зазначених в документі "Комплекс засобів захисту інформації від несанкціонованого доступу "Гриф" версія 3. Зміни та доповнення до технічного завдання UA.21541987.00020-01 90 02", сукупність яких визначається функціональним профілем захищеності: **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**, з рівнем гарантій **Г-4** коректності їх реалізації згідно з НД ТЗІ 2.5-004-99, та може бути використаний для захисту інформації з обмеженим доступом, яка обробляється в автоматизованих системах класу "1" та класу "2".

Сфера використання та вимоги до умов експлуатації об'єкта експертизи визначені у відповідному розділі цього експертного висновку.

Директор НДЦ "Тезіс"
НТУУ "КПІ" **М. І. Прокофьєв**

керівник організатора експертизи (НДЦ "ТЕЗІС") підпис ініціали, прізвище

м.п.

1 ЗАГАЛЬНІ ВІДОМОСТІ ЩОДО ОБ’ЄКТА ЕКСПЕРТИЗИ

1.1 Об'єктом експертизи (ОЕ) є комплекс засобів захисту (КЗЗ) інформації від несанкціонованого доступу (НСД) "Гриф" версії 3 (далі – КЗЗ від НСД "Гриф").

1.2 КЗЗ від НСД "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 тощо), оброблюваної в автоматизованих системах (АС) класу "1" та в АС класу "2".

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

1.4 Вид експертизи – додаткова. Експертиза проводилась у зв’язку з закінченням терміну дії експертного висновку за результатами попередньої експертизи, а також у зв’язку з забезпеченням підтримки можливості функціонування КЗЗ від НСД "Гриф" на комп’ютерах під керуванням операційних систем (ОС) із пакетами оновлення, наданими виробником відповідних ОС у період з 01.01.2013 по 31.03.2016.

1.5 Мета експертизи:

– перевірка КЗЗ від НСД "Гриф" на відповідність вимогам НД ТЗІ 2.5-004-99, НД ТЗІ 3.6-001-2000, НД ТЗІ 2.5-008-2002 та документа "Комплекс засобів захисту інформації від несанкціонованого доступу "Гриф" версія 3. Зміни та доповнення до технічного завдання UA.21541987.00020 - 01 90 02", узгодженого Адміністрацією Держспецзв’язку України 18.02.2013 р., з урахуванням порядку реалізації цих вимог, викладеного у документах "Комплекс засобів захисту інформації від несанкціонованого доступу "Гриф" версія 3. Зміни та доповнення до технічного проекту UA.21541987.00020 - 01 81 04" та "Технічні вимоги, на відповідність яким здійснюватиметься державна експертиза комплексу засобів захисту від несанкціонованого доступу "Гриф" версії 3";

– підготовка висновків щодо можливості використання КЗЗ від НСД "Гриф" в АС класу "1" та АС класу "2", побудованих на базі однорангових локальних обчислювальних мереж, для захисту ІзОД, у тому числі службової інформації та інформації, що становить державну таємницю;

– визначення відповідності архітектури, середовища та послідовності розробки, середовища функціонування, документації та методів випробувань КЗЗ від НСД "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 № 08/02/03-887 від 11.05.16 р. щодо проведення державної експертизи в сфері ТЗІ комплексу засобів захисту інформації від несанкціонованого доступу "Гриф" версії 3 та Договір № 3716 Е від 16.05.16 р.

між НТУУ "КПІ" НДЦ "ТЕЗІС" (Організатор експертизи) та ТОВ "Інститут комп'ютерних технологій" (Замовник експертизи).

2 ЗАГАЛЬНА ХАРАКТЕРИСТИКА ОБ’ЄКТА ЕКСПЕРТИЗИ

2.1 КЗЗ від НСД "Гриф" призначений для забезпечення захисту ІзОД: інформації, що становить державну таємницю; службової інформації; конфіденційної інформації про особу (персональних даних); інформації, що становить комерційну таємницю тощо), оброблюваної в АС класу "1", побудованих на базі IBM-сумісних персональних електронно-обчислювальних машин (ПЕОМ) або в АС класу "2", побудованих на базі однорангових локальних обчислювальних мереж (ЛОМ), до складу яких входять IBM-сумісні ПЕОМ, від загроз цілісності, конфіденційності та доступності, при реалізації політики адміністративного керування доступом до захищеної інформації.

2.2 КЗЗ від НСД "Гриф" функціонує на ПЕОМ під керуванням ОС MS Windows XP Professional / Windows Vista Professional або Business / Windows 7 Professional, Ultimate або Enterprise (32-розрядна) / Windows 7 Professional, Ultimate або Enterprise (64-розрядна) / Windows 8 Professional або Enterprise (32-розрядна) / Windows 8 Professional або Enterprise (64-розрядна) / Windows 8.1 Professional або Enterprise (32-розрядна) / Windows 8.1 Professional або Enterprise (64-розрядна) / Windows Server 2008 / Windows Server 2008 R2 / Windows Server 2012 / Windows Server 2012 R2.

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

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

– ідентифікацію та автентифікацію користувачів на підставі імені (псевдоніма), пароля та персонального носія даних автентифікації (знімного файлового носія (Flash Drive, CD-RW, DVD-RW, дискета тощо) або пристрою Touch Memory;

– 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, що дозволяє організувати спільну роботу декількох користувачів, які мають різні службові обов’язки та права по доступу до ІзОД;

– керування потоками інформації та блокування потоків інформації, що призводять до зниження рівня її 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 експортом інформації на знімні носії та 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, що дозволяє забезпечити захист ІзОД від випадкового видалення або модифікації та дотримання технології її оброблення;

– 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, що виключає можливість блокування одним із користувачів можливості роботи інших користувачів;

– можливість блокування пристроїв інтерфейсу користувача (клавіатури, миші, монітора) на час його відсутності;

– контроль цілісності та самотестування КЗЗ при старті та за запитом адміністратора, що дозволяє забезпечити стале функціонування КЗЗ і не допустити оброблення ІзОД у випадку порушення працездатності КЗЗ;

– відновлення функціонування КЗЗ після збоїв, що гарантує доступність інформації з забезпеченням дотримання правил доступу до неї;

– реєстрацію, аналіз та оброблення інформації про критичні для безпеки події (вхід користувачів в ОС, спроби несанкціонованого доступу, факти запуску програм, факти роботи з ІзОД, факти імпорту/експорту, факти виведення інформації на друк тощо) у спеціальних протоколах аудиту, що дозволяє адміністраторам контролювати доступ до ІзОД, стежити за тим, як використовується КЗЗ, а також правильно його конфігурувати;

– ведення архіву зареєстрованих даних аудита;

– взаємодію з прикладними програмними системами (ППС) через визначений виробником КЗЗ інтерфейс, що дозволяє забезпечити безперервність захисту ІзОД при її обробленні як у штатних засобах ОС, так і у засобах різних ППС.

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

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

{**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}.

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 та НД ТЗІ 2.5-008-2002.

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	Множинна ідентифікація і автентифікація	НИ-3
11	Однонаправлений достовірний канал	НК-1
12	Розподіл обов'язків адміністраторів	НО-2
13	КЗЗ з гарантованою цілісністю	НЦ-2
14	Самотестування при старті	НТ-2

2.6 Ідентифікація об’єкта експертизи

Версії об’єкта експертизи (ОЕ) ідентифікуються числовим кодом виду "З.хх" за дворівневою схемою, де "З" – номер версії, "хх" - номер підверсії. Нумерація підверсій починається з "07". 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 від НСД "Гриф" версії 3 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 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 2.7-009-09 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.

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

11 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.

12 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.

13 Технічні вимоги, на відповідність яким здійснюватиметься державна експертиза комплексу засобів захисту від несанкціонованого доступу "Гриф" версії 3.

4 МЕТОДИКА ПРОВЕДЕННЯ ЕКСПЕРТНИХ РОБІТ

Експертні роботи виконувались згідно з розробленими Організатором експертизи документами "Програма державної експертизи комплексу засобів захисту інформації від несанкціонованого доступу "Гриф" версії 3. ІАЛЦ.72.10.10.5013.01.П" та "Методики державної експертизи комплексу засобів захисту інформації від несанкціонованого доступу "Гриф" версії 3 ІАЛЦ.72.10.10.5013.01.М", які узгоджені листами Держспецзв'язку № 08/02/04-3810 від 08.08.2013 р. та 08/02/03-1106 від 06.06.2016 р.

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

5.1 На експертизу КЗЗ від НСД "Гриф" 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 від несанкціонованого доступу "Гриф" версії 3. Паспорт (проект).

5.1.1.2 Комплекс средств защиты информации от несанкционированного доступа "Гриф" версии 3. Описание комплекса. Редакция 10.

5.1.1.3 Комплекс средств защиты информации от несанкционированного доступа "Гриф" версии 3. Краткое руководство по эксплуатации (быстрый старт). Редакция 8.

5.1.1.4 Комплекс средств защиты информации от несанкционированного доступа "Гриф" версии 3. Руководство по эксплуатации. Редакция 8.

5.1.1.5 Комплекс средств защиты информации от несанкционированного доступа "Гриф" версии 3. Руководство администратора КСЗ. Редакция 8.

5.1.1.6 Комплекс средств защиты информации от несанкционированного доступа "Гриф" версии 3. Руководство администратора безопасности. Редакция 8.

5.1.1.7 Комплекс средств защиты информации от несанкционированного доступа "Гриф" версии 3. Руководство системного администратора. Редакция 8.

5.1.1.8 Комплекс средств защиты информации от несанкционированного доступа "Гриф" версии 3. Руководство пользователя. Редакция 8.

5.1.1.9 Комплекс средств защиты информации от несанкционированного доступа "Гриф" версии 3. Модуль взаимодействия с прикладными программными системами. Руководство программиста. Редакция 4.

5.1.2 Проектна та супровідна документація:

5.1.2.1 Комплекс засобів захисту інформації від несанкціонованого доступу "Гриф" версія 3. Зміни та доповнення до технічного завдання UA.21541987.00020 - 01 90 02, погоджені з Державною службою спеціального зв’язку та захисту інформації України 18.02.2013 р.

5.1.2.2 Комплекс засобів захисту інформації від несанкціонованого доступу "Гриф" версія 3. Зміни та доповнення до технічного проекту UA.21541987.00020 - 01 81 04.

5.1.2.3 Комплекс засобів захисту інформації від несанкціонованого доступу "Гриф" версія 3. Опис відповідності специфікацій. Фрагменти вхідного коду. UA.21541987.00020 - 01 81 05.

5.1.2.4 Комплекс засобів захисту інформації від несанкціонованого доступу "Гриф" версія 3. Специфікація програмного забезпечення КЗЗ (UA.21541987.00020 - 02).

5.1.2.5 Комплекс засобів захисту інформації від несанкціонованого доступу "Гриф" версія 3. Методики діяльності розробників на протязі життєвого циклу. UA.21541987.00020 - 01 81 06.

5.1.3 Документація щодо проведених приймальних випробувань:

5.1.3.1 Комплекс засобів захисту інформації від несанкціонованого доступу "Гриф" версія 3. Зміни та доповнення до програми та методики випробувань UA.21541987. 00020 - 01 51 02, погоджені з Державною службою спеціального зв’язку та захисту інформації України 25.04.2013 р.

5.1.3.2 Комплекс засобів захисту інформації від несанкціонованого доступу "Гриф" версія 3. Звіт про випробування. UA.21541987.00020 - 01 91 01.

5.1.3.3 Комплекс засобів захисту інформації від несанкціонованого доступу "Гриф" версія 3. Протокол приймальних випробувань UA.21541987.00020 - 01 92 01.

5.1.4 Документація, яка стосується організації процесу розроблення КЗЗ

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

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 КЗЗ від НСД "Гриф" версії 3.

5.2.1 КЗЗ від НСД "Гриф" версії 3 версії 3 постачається на інсталяційному диску (CD-ROM), який має структуру та вміст каталогів, зазначених у таблиці 2.

Таблиця 2

Ім’я файлу/ каталогу	Назва файлу/ документа
_readme	Файл-довідка з підготовки до інсталяції
Ver_3_07	**каталог**
g3local.exe	Інсталяційний файл-архів
DOC	**каталог**
grif_307a.pdf	Комплекс средств защиты информации от несанкционированного доступа "Гриф" версии 3. Руководство администратора комплекса средств защиты
grif_307b.pdf	Комплекс средств защиты информации от несанкционированного доступа "Гриф" версии 3. Руководство администратора безопасности
grif_307i.pdf	Комплекс средств защиты информации от несанкционированного доступа "Гриф" версии 3. Руководство системного администратора
grif_307q.pdf	Комплекс средств защиты информации от несанкционированного доступа "Гриф" версии 3. Краткое руководство по эксплуатации (быстрый старт)
grif_307r.pdf	Комплекс средств защиты информации от несанкционированного доступа "Гриф" версии 3. Описание комплекса
grif_307s.pdf	Комплекс средств защиты информации от несанкционированного доступа "Гриф" версии 3. Руководство по эксплуатации
grif_307supp.pdf	Комплекс средств защиты информации от несанкционированного доступа "Гриф" версии 3. Модуль взаимодействия с прикладными программными системами. Руководство программиста
grif_307u.pdf	Комплекс средств защиты информации от несанкционированного доступа "Гриф" версии 3. Руководство пользователя

5.2.2 Для експертизи був наданий інсталяційний пакет КЗЗ від НСД "Гриф" версії 3.07 на інсталяційному диску з серійним номером №2945, структура каталогів якого відповідає наведеній у Таблиці 2. 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 від НСД "Гриф" версії 3 відповідає специфікації комплектності, зазначеної у документах на поставку.

6.2 Сукупність реалізованих у КЗЗ від НСД "Гриф" версії 3 функцій та механізмів захисту інформації визначається згідно з НД ТЗІ 2.5-004-99 таким функціональним профілем захищеності інформації:

{**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}.

6.3 Результати експертних випробувань щодо кожного пункту документа "Методики державної експертизи комплексу засобів захисту інформації від несанкціонованого доступу "Гриф" версії 3 ІАЛЦ.72.10.10.5013.01.М" викладені у документі "Протокол № 3716 додаткової державної експертизи комплексу засобів захисту інформації від несанкціонованого доступу "Гриф" версії 3".

6.4 За результатами експертних досліджень у частині, що стосується оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки (ФПБ) у "Гриф" версія 3

встановлено, що:

– рівні реалізованих у КЗЗ "Гриф" 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" версії 3, а також середовище, процедури та послідовність розробки, процедури випробування та розповсюдження КЗЗ "Гриф" 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" 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 від несанкціонованого доступу "Гриф". Версія 3. Зміни та доповнення до технічного завдання UA.21541987.00020 - 01 90 02", узгодженого Адміністрацією Держспецзв'язку України від 18.02.2013 р., з урахуванням порядку реалізації цих вимог, викладеного у документах "Комплекс засобів захисту інформації від несанкціонованого доступу "Гриф". Версія 3. Зміни та доповнення до технічного проекту UA.21541987.00020 - 01 81 04" та "Технічні вимоги, на відповідність яким здійснюватиметься державна експертиза комплексу засобів захисту від несанкціонованого доступу "Гриф" версії 3" (далі – Технічні вимоги). Результати експертних робіт свідчать, що:

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

- користувачі всіх категорій;
- інформаційні об'єкти (ІО):
  - ІО у вигляді структурованих та неструктурованих файлів, що містять ІзОД та зберігаються в каталогах файлової системи незнімних носіїв;
  - ІО у вигляді структурованих та неструктурованих файлів, що містять ІзОД та зберігаються на зареєстрованих або незареєстрованих знімних носіях;
  - ІО, що містять технологічну інформацію КЗЗ;
  - ІО у вигляді файлів виконуваного коду прикладних програмних засобів (ППЗ) АС, що зберігаються в каталогах файлової системи незнімних носіїв;
- 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 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.

6.7 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.

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

- користувачів усіх категорій;
- об’єкти-процеси:

  - ППЗ АС, що використовуються для оброблення ІзОД та відкритої інформації, що потребує захисту (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 ПЕОМ.

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.

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

- 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.

6.10 Політика ФПБ "Використання ресурсів" рівня ДР-1, яка реалізується КЗЗ, 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 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".

6.11 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 контролю запитів доступу до ресурсів та керування доступом до ресурсів (системного драйвера);
- інтерфейсного модуля ідентифікації та автентифікації (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 адміністрування (автоматизованого робочого місця (АРМ) адміністратора КЗЗ);
- модуля обслуговування носіїв даних автентифікації користувачів;
- модуля відновлення цілісності та оновлення КЗЗ;
- модуля зберігання даних аудита;
- модуля аналізу даних аудита (АРМ аналізу даних аудита).

У випадку виникнення певних відмов програмних засобів (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.

6.12 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 контролю запитів доступу до ресурсів та керування доступом до ресурсів (системного драйвера);
- інтерфейсного модуля ідентифікації та автентифікації (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 адміністрування (АРМ адміністратора КЗЗ);
- модуля обслуговування носіїв даних автентифікації користувачів;
- модуля відновлення цілісності та оновлення КЗЗ;
- модуля зберігання даних аудита;
- модуля аналізу даних аудита (АРМ аналізу даних аудита).

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".

6.13 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 контролю запитів доступу до ресурсів та керування доступом до ресурсів (системного драйвера);
- інтерфейсного модуля ідентифікації та автентифікації (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 адміністрування (АРМ адміністратора КЗЗ);
- модуля обслуговування носіїв даних автентифікації користувачів;
- модуля відновлення цілісності та оновлення КЗЗ;
- модуля зберігання даних аудита;
- модуля аналізу даних аудита (АРМ аналізу даних аудита).

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".

6.14 Політика ФПБ "Реєстрація" рівня НР-2, 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 п. 3.9 Технічних вимог.

6.15 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. 3.10 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".

6.16 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 контролю запитів доступу до ресурсів та керування доступом до ресурсів (системного драйвера);
- інтерфейсного модуля ідентифікації та автентифікації (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 адміністрування (АРМ адміністратора КЗЗ);
- модуля обслуговування носіїв даних автентифікації користувачів;
- модуля відновлення цілісності та оновлення КЗЗ;
- модуля зберігання даних аудита;
- модуля аналізу даних аудита (АРМ аналізу даних аудита).

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. 3.11 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).

6.17 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);
- інтерфейсного модуля ідентифікації та автентифікації (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 адміністрування (АРМ адміністратора КЗЗ);
- модуля обслуговування носіїв даних автентифікації користувачів;
- модуля відновлення цілісності та оновлення КЗЗ;
- модуля зберігання даних аудита;
- модуля аналізу даних аудита (АРМ аналізу даних аудита).

Засоби КЗЗ за правилами, наведеними у п. 3.12 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.

6.18 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. 3.13 Технічних вимог.

6.19 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. 3.14 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" версії 3 встановлено:

- наданий для випробувань КЗЗ "Гриф" версії 3 відповідає вимогам нормативних

документів системи технічного захисту інформації в Україні, у тому числі НД ТЗІ 2.5-008-2002 (крім вимог щодо розмежування доступу до сильнозв’язаних об’єктів у вигляді записів баз даних, які можуть бути реалізовані лише у засобах систем керування базами даних, та для умов, коли, відповідно до п. 6.5.15 НД ТЗІ 2.5-008-2002, немає потреби у реалізації функціональних послуг безпеки, що базуються на довірчому принципі розмежування доступу), та Технічного завдання;

– сукупність реалізованих у КЗЗ "Гриф" версії 3 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 КЗЗ "Гриф" версії 3 дійсні для складу КЗЗ, наведеного у Таблиці 2, для версій структурних компонентів КЗЗ, що містяться в інсталяційному пакеті КЗЗ "Гриф" версії 3.07, склад якого наведено у Додатку А, а також для пакетів оновлення КЗЗ "Гриф" 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 від несанкціонованого доступу "Гриф" версія 3. Зміни та доповнення до програми та методики випробувань UA.21541987. 00020 - 01 51 02" та надання до Адміністрації Держспецзв’язку відповідного Протоколу випробувань.

8 ВИМОГИ ЩОДО СФЕРИ ВИКОРИСТАННЯ ТА УМОВ ЕКСПЛУАТАЦІЇ

8.1 КЗЗ "Гриф" версії 3 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, оброблюваної в АС класу "1".

8.2 КЗЗ "Гриф" версії 3 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, оброблюваної в АС класу "2".

Використання КЗЗ "Гриф" версії 3 для захисту інформації, що становить державну таємницю, оброблюваної в АС класу "2", 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.

8.3 При функціонуванні КЗЗ "Гриф" версії 3 має бути забезпечено дотримання таких умов: на ПЕОМ, на яких встановлені засоби КЗЗ, організаційними та/або технічними заходами має бути заблокована можливість завантаження ОС зі знімних носіїв.

9 ТЕРМІН ДІЇ ЕКСПЕРТНОГО ВИСНОВКУ

Термін дії експертного висновку – до _____ 2019 р.

Додаток А
(обов'язковий)

Вміст інсталяційного диску КЗЗ від НСД "Гриф" версії 3.07**, наданого на експертизу**

Ім'я файлу	**Назва**	**Розмір файлу (байт)**	CRC*	**Дата створення**
_README	Файл-довідка з підготовки до інсталяції	2899	C768F531	07.04.2016
DOC	**Каталог**			
GRIF_307A.PDF	Комплекс средств защиты информации от несанкционированного доступа "Гриф" версии 3. Руководство администратора КСЗ	2259778	215B7058	04.04.2016
GRIF_307B.PDF	Комплекс средств защиты информации от несанкционированного доступа "Гриф" версии 3. Руководство администратора безопасности	978426	B70B7C3E	04.04.2016
GRIF_307I.PDF	Комплекс средств защиты информации от несанкционированного доступа "Гриф" версии 3. Руководство системного администратора	965624	D6ED2805	04.04.2016
GRIF_307Q.PDF	Комплекс средств защиты информации от несанкционированного доступа "Гриф" версии 3. Краткое руководство по эксплуатации (быстрый старт)	517393	C811B61F	04.04.2016
GRIF_307R.PDF	Комплекс средств защиты информации от несанкционированного доступа "Гриф" версии 3. Описание комплекса	532093	CAF7A486	04.04.2016
GRIF_307S.PDF	Комплекс средств защиты информации от несанкционированного доступа "Гриф" версии 3. Руководство по эксплуатации	569400	206BEBE1	04.04.2016
GRIF_307SUPP.PDF	Комплекс средств защиты информации от несанкционированного доступа "Гриф" версии 3. Модуль взаимодействия с прикладными программными системами. Руководство программиста	168573	5AFCB72E	04.04.2016
GRIF_307U.PDF	Комплекс средств защиты информации от несанкционированного доступа "Гриф" версии 3. Руководство пользователя	452057	56A6005D	05.05.2016
Ver_3_07	**Каталог**			
G3LOCAL.EXE	Інсталяційний файл-архів	5154960	05507DCA	04.04.2016
GNGInst	Каталог в інсталяційному файлі-архіві			

Ім’я файлу	Назва	Розмір файлу (байт)	CRC*	Дата створення
ALLFILES.IMM	Файл кодів контролю цілісності пакету інсталяції (повний)	1191	6025796B	01.04.2016
ARMG2K.INI	Файл початкових настроювань	140	89958725	17.09.2009
AUDITLOG.DLL	Динамічна бібліотека обробки даних аудита для ОС Windows XP	122880	543F96A2	20.08.2010
AUDITLOG60.DLL	Динамічна бібліотека обробки даних аудита для ОС Windows Vista, Windows Server 2008, Windows 7, Windows 8, Windows Server 2008 R2, Windows Server 2012	163840	95AC34F1	29.02.2012
CBUTIL.EXE	Програма контролю буферу обміну	65616	2B710FAE	03.06.2013
CBUTILX64.EXE	Програма контролю буферу обміну	174080	4A1F0AB2	03.06.2013
DEMANDS.TXT	Файл із описом необхідних умов для інсталяції комплексу	3451	0227769A	31.03.2016
ERRORS.HTM	Файл довідкової інформації щодо помилок під час інсталяції	76814	00A1C5D8	13.04.2010
GLARMEV.EXE	Програма АРМ аналізу даних аудита	1319424	985E9F42	15.02.2016
GLARMRA.EXE	Програма автоматизованого АРМ адміністратора КЗЗ	1204224	4F9A6B02	22.02.2016
GLARMRAX64.EXE	Програма АРМ адміністратора КЗЗ	1783808	79E5CE3B	17.02.2016
GLCP.DLL	Провайдер автентифікації	319488	9613FBB4	17.02.2016
GLCPX64.DLL	Провайдер автентифікації	670720	E5508394	17.02.2016
GLGINA.DLL	Динамічна бібліотека ідентифікації та автентифікації з графічним інтерфейсом (GINA)	286720	5A1C8D39	10.03.2016
GMEXPORT.EXE	Програма експорту даних	98304	9DB45803	20.03.2015
GMPRINT.EXE	Програма друку даних	176128	B98F97D1	24.02.2012
GMSHEXT.DLL	Динамічна бібліотека розширення Windows Explorer	98304	01EA0C67	24.02.2012
GMSHEXTX64.DLL	Динамічна бібліотека розширення Windows Explorer	105984	5DEF4C48	20.07.2012
GMSUPP.DLL	Динамічна бібліотека взаємодії з ППС	208896	4D03B512	08.09.2010
GMSUPPX64.DLL	Динамічна бібліотека взаємодії з ППС	393216	27431082	24.02.2012
GNCAT.DLL	Динамічна бібліотека розбору повідомлень комплексу	90112	60642AE5	12.04.2010
GRIF51ON.SYS	Системний драйвер для ОС Windows XP	125952	11CF1965	12.09.2014
GRIF51ROMI.SYS	Системний драйвер для ОС Windows XP	168576	211559F6	18.02.2016
GRIF60ON.SYS	Системний драйвер для 32-розрядних ОС Windows Vista, Windows Server 2008	50176	E1302E4E	02.03.2012
GRIF60ROMI.SYS	Системний драйвер для 32-розрядних ОС Windows Vista, Windows Server 2008	101376	FA48EF44	07.06.2013
GRIF61ON.SYS	Системний драйвер для 32-розрядної ОС Windows 7	51104	A68D2CFC	10.09.2014

Ім’я файлу	Назва	Розмір файлу (байт)	CRC*	Дата створення
GRIF61ONX64.SYS	Системний драйвер для 64-розрядних ОС Windows 7/Windows Server 2008 R2	78240	F282E020	10.09.2014
GRIF61ROMI.SYS	Системний драйвер для 32-розрядної ОС Windows 7	104352	43DFC395	29.02.2016
GRIF61ROMIX64.SYS	Системний драйвер для 64-розрядних ОС Windows 7/Windows Server 2008 R2	156064	69880198	01.04.2016
GRIF62ON.SYS	Системний драйвер для 32-розрядної ОС Windows 8	51104	FE6761CB	10.09.2014
GRIF62ONX64.SYS	Системний драйвер для 64-розрядних ОС Windows 8/Windows Server 2012	78240	54E133A6	10.09.2014
GRIF62ROMI.SYS	Системний драйвер для 32-розрядної ОС Windows 8	100768	0FFB02E1	03.06.2015
GRIF62ROMIX64.SYS	Системний драйвер для 64-розрядних ОС Windows 8/Windows Server 2012	154016	65729C01	03.06.2015
GRIF63ON.SYS	Системний драйвер для 32-розрядної ОС Windows 8.1	45848	CDAB42A0	09.09.2014
GRIF63ONX64.SYS	Системний драйвер для 64-розрядних ОС Windows 8.1/Windows Server 2012 R2	84000	3108FEA2	22.08.2014
GRIF63ROMI.SYS	Системний драйвер для 32-розрядної ОС Windows 8.1	139072	A078DDD1	30.03.2016
GRIF63ROMIX64.SYS	Системний драйвер для 64-розрядних ОС Windows 8.1/Windows Server 2012 R2	189560	9DA990FF	31.03.2016
GRIFLOCAL51.INF	Файл параметрів конфігурації для програми інсталяції	16036	9A755E6F	12.03.2016
GRIFLOCAL60.INF	Файл параметрів конфігурації для програми інсталяції	19129	01D0F11A	12.03.2016
GRIFLOCAL61.INF	Файл параметрів конфігурації для програми інсталяції	19936	CC34E066	12.03.2016
GRIFLOCAL62.INF	Файл параметрів конфігурації для програми інсталяції	21014	1C3121D3	12.03.2016
GRIFLOCALX64_61.INF	Файл параметрів конфігурації для програми інсталяції	24381	C3FD59D9	12.03.2016
GRIFLOCALX64_62.INF	Файл параметрів конфігурації для програми інсталяції	25186	8F39FC1F	12.03.2016
GRIFLOCALX64_63.INF	Файл параметрів конфігурації для програми інсталяції	26252	D8A6903E	12.03.2016
GRIFPOLAS2_T51.INF	Файл параметрів конфігурації для програми інсталяції	51064	73C6804B	16.07.2014
GRIFPOLAS2_T60.INF	Файл параметрів конфігурації для програми інсталяції	119082	212FE4C6	16.07.2014
GRIFPOLAS2_T61.INF	Файл параметрів конфігурації для програми інсталяції	119090	4CD90E15	28.04.2015
GRIFPOLAS2_T62.INF	Файл параметрів конфігурації для програми інсталяції	110618	4E31C7EA	16.07.2014
GRIFPOLAS2_T63.INF	Файл параметрів конфігурації для програми інсталяції	110618	4E31C7EA	16.07.2014
GRIFPOL_T51.INF	Файл параметрів конфігурації для програми інсталяції	50880	A372914C	16.07.2014
GRIFPOL_T60.INF	Файл параметрів конфігурації для програми інсталяції	118926	6E4FEB1A	16.07.2014
GRIFPOL_T61.INF	Файл параметрів конфігурації для програми інсталяції	118934	3974DD6D	28.04.2015
GRIFPOL_T62.INF	Файл параметрів конфігурації для програми інсталяції	110462	5E7EF527	16.07.2014

Ім'я файлу	**Назва**	**Розмір файлу (байт)**	CRC*	**Дата створення**
GRIFPOL_T63.INF	Файл параметрів конфігурації для програми інсталяції	110658	97B22133	11.08.2014
GRIFSRV.EXE	Системний сервіс	176206	305E91B0	18.02.2016
GRIFSRVX64.EXE	Системний сервіс	256000	EA46369B	28.03.2016
GRIFTEMPL51.IMM	Файл кодів контролю цілісності пакету інсталяції (частковий)	696	BAB41C51	01.04.2016
GRIFTEMPL60.IMM	Файл кодів контролю цілісності пакету інсталяції (частковий)	824	D88B012D	01.04.2016
GRIFTEMPL61.IMM	Файл кодів контролю цілісності пакету інсталяції (частковий)	824	8D742710	01.04.2016
GRIFTEMPL62.IMM	Файл кодів контролю цілісності пакету інсталяції (частковий)	824	EE1447AD	01.04.2016
GRIFTEMPL63.IMM	Файл кодів контролю цілісності пакету інсталяції (частковий)	824	2C9AEDB2	01.04.2016
GRIFTEMPLX64_61.IMM	Файл кодів контролю цілісності пакету інсталяції (частковий)	824	5D678FFC	01.04.2016
GRIFTEMPLX64_62.IMM	Файл кодів контролю цілісності пакету інсталяції (частковий)	824	98FE3470	01.04.2016
GRIFTEMPLX64_63.IMM	Файл кодів контролю цілісності пакету інсталяції (частковий)	824	F17B09C6	01.04.2016
GRIF_SER.EXE	Системний сервіс	245760	FE47F558	18.03.2016
LICENSE.TXT	Файл з текстом ліцензійної угоди	1028	F5C18079	19.05.2010
LOG2KRUS.DLL	Службова динамічна бібліотека	20480	8CD63A9C	26.08.2011
NTDSMIR.DLL	Динамічна бібліотека розбору GUID	90112	AD27B847	17.09.2009
RECOVER51.IMM	Файл кодів контролю цілісності пакету інсталяції (частковий)	72	DDE05BC1	01.04.2016
RECOVER60.IMM	Файл кодів контролю цілісності пакету інсталяції (частковий)	72	2FC822C3	01.04.2016
RECOVER61.IMM	Файл кодів контролю цілісності пакету інсталяції (частковий)	72	FC2FAB88	01.04.2016
RECOVER62.IMM	Файл кодів контролю цілісності пакету інсталяції (частковий)	72	1594F939	01.04.2016
RECOVER63.IMM	Файл кодів контролю цілісності пакету інсталяції (частковий)	72	B176ADA5	01.04.2016
RECOVERDLL.DLL	Динамічна бібліотека відновлення цілісності та оновлення КЗЗ	217088	604B0BE2	17.02.2016
RECOVERDLLX64.DLL	Динамічна бібліотека відновлення цілісності та оновлення КЗЗ	583680	9F5A9CE7	17.02.2016
RECOVERX64_61.IMM	Файл кодів контролю цілісності пакету інсталяції (частковий)	72	EA00919C	01.04.2016

Ім’я файлу	**Назва**	**Розмір файлу (байт)**	CRC*	**Дата створення**
RECOVERX64_62.IMM	Файл кодів контролю цілісності пакету інсталяції (частковий)	72	D9EA82FB	01.04.2016
RECOVERX64_63.IMM	Файл кодів контролю цілісності пакету інсталяції (частковий)	72	DDD7B482	01.04.2016
RESETTM.EXE		86016	F073434D	26.03.2010
SAVEDAT.DLL	Динамічна бібліотека збереження даних аудита	785920	60CCAADB	24.11.2009
SECLEV.DAT	Файл бази даних рівнів конфіденційності	4962	B1FE77AE	21.11.2002
SETUP.EXE	Програма інсталяції комплексу	532480	0748B1DF	18.03.2016
STPINF64.INF	Файл параметрів конфігурації для програми інсталяції	164864	AC959123	01.07.2013
ZLIB.DLL	Динамічна бібліотека архівування / розархівування даних	53760	8FA6E740	13.04.2006

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