Інститут комп’ютерних технологій

"Гриф–Мережа"

Комплекс засобів захисту інформації в локальних обчислювальних мережах від несанкціонованого доступу

версія 3

Опис комплексу

редакція 6

Київ 2023

ІНСТИТУТ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
Тел.: (044) 499-98-44
E-mail: ict@ict.com.ua
http://www.ict.com.ua

СПИСОК ВИКОРИСТАНИХ СКОРОЧЕНЬ

АРМ – автоматизоване робоче місце

АС – автоматизована система

БД – база даних

ІзОД – інформація з обмеженим доступом

КЗЗ – комплекс засобів захисту

ЛОМ – локальна обчислювальна мережа

НД ТЗІ – нормативний документ системи технічного захисту інформації

НСД – несанкціонований доступ

ОКД – основний контролер домену

ОП – оперативна пам’ять

ОС – операційна система

ПБ – політика безпеки

ППЗ – прикладні програмні засоби

ПРД – правила розмежування доступу

ПЗ – програмні засоби

РС – робоча станція

СКБД – система керування базою даних

ТС – технологічна схема

ФС – файловий сервер

ЗМІСТ

СОДЕРЖАНИЕ

1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ЗАСТОСУВАННЯ

КЗЗ **"Гриф–Мережа"** призначений для захисту ІзОД, яка обробляється в АС, побудованих на базі ЛОМ, до складу яких входять РС, що функціонують під керуванням ОС MS Windows 7 (Professional, Enterprise, Ultimate), MS Windows 8.1 (Professional, Enterprise), MS Windows 10 (Professional, Enterprise) MS Windows 11 (Professional, Enterprise) та ФС, що функціонують під керуванням ОС MS Windows Server 2008 R2/ MS Windows Server 2012 R2/ MS Windows Server 2016/ 2019/ 2022, від загроз порушення цілісності, конфіденційності та доступності при реалізації політики адміністративного керування доступом до інформації.

Використання КЗЗ **"Гриф–Мережа"** в ЛОМ забезпечує:

- реєстрацію всіх осіб, які приймають участь в обробці ІзОД, в якості користувачів ЛОМ;
- надання доступу до ІзОД тільки за умови достовірного розпізнання користувача ЛОМ та з урахуванням повноважень, які надані йому згідно зі службовою необхідністю;
- можливість своєчасного доступу зареєстрованих користувачів до ІзОД;
- неможливість неконтрольованого та несанкціонованого ознайомлення, розмноження, розповсюдження, копіювання та відновлення ІзОД в процесі її обробки в ЛОМ;
- неможливість неконтрольованої та несанкціонованої модифікації ІзОД в процесі її обробки в ЛОМ;
- можливість створення в ЛОМ "замкнутого програмного середовища" та використання для обробки ІзОД тільки ПЗ, які пройшли відповідну перевірку;
- можливість запобігання захопленню користувачем надмірного об’єму ресурсів (дискового простору) ФС ЛОМ, при якому стає неможливою подальша робота інших користувачів;
- облік усіх дій користувачів ЛОМ щодо обробки ІзОД, реєстрацію спроб порушення встановленого порядку доступу до інформації, а також можливість блокування доступу до інформації у випадку виявлення таких спроб;
- можливість доступу до функцій адміністрування (керування правами доступу до ІзОД) тільки за умови достовірного розпізнання адміністраторів та з урахуванням наданих їм повноважень;
- облік дій адміністраторів КЗЗ стосовно керування повноваженнями доступу користувачів до ІзОД;
- можливість проведення безперервного контролю з боку уповноважених осіб за всіма подіями, що мають відношення до безпеки оброблюваної ІзОД.

2 СКЛАД ТА АРХІТЕКТУРА КЗЗ

До складу КЗЗ **"Гриф–Мережа"** входять такі основні компоненти:

– засоби розмежування доступу, які встановлюються на РС та ФС ЛОМ, основною функцією яких є реалізація адміністративного керування доступом до захищених інформаційних ресурсів, що містять ІзОД:

  - інтерфейсний модуль автентифікації (провайдер автентифікації);

  - модуль відновлення цілісності та оновлення КЗЗ;

  - модуль контролю запитів доступу до ресурсів та керування правами доступу до ресурсів (системний драйвер та резидентний модуль користувальницького режиму);

  - модуль обслуговування носіїв даних автентифікації користувачів;

  - модуль контролю операцій експорту даних;

  - модуль контролю операцій друку;

– засоби реєстрації даних аудита, які встановлюються на РС та ФС ЛОМ, основною функцією яких є збір, передача та реєстрація, в том числі в реальному часі, інформації про події, що мають відношення до безпеки ІзОД, яка обробляється:

  - агент модуля реєстрації даних аудита (використовується у конфігурації з підвищеними вимогами до забезпечення спостережності);

  - модуль збереження локальних даних аудита;

  - модуль аналізу локальних даних аудита (АРМ аналізу локальних даних аудита);

– модуль реєстрації даних аудита, який встановлюється на ФС-ОКД (використовується у конфігурації з підвищеними вимогами до забезпечення спостережності);

– АРМ адміністратора КЗЗ, яке встановлюється на РС адміністратора КЗЗ та РС адміністратора безпеки, основними функціями якого є: реєстрація користувачів, вироблення даних ідентифікації та автентифікації зі збереженням їх на носіях даних автентифікації; реєстрація захищених ресурсів; керування розмежуванням доступу користувачів до вибраних каталогів; контроль цілісності та самотестування КЗЗ за запитом адміністратора; керування розмежуванням доступу прикладних програм до вибраних каталогів; керування квотами користувачів; увімкнення/ вимкнення режиму контролю програмного забезпечення (заборона запуску незареєстрованих програм), активізація/ деактивізація облікових записів користувачів;

– АРМ адміністратора безпеки, яке встановлюється на РС адміністратора безпеки, основними функціями якого є: налаштування та керування параметрами аудита захищених ресурсів та активного мережевого обладнання; керування параметрами сповіщення та приймання сповіщень про критичні для безпеки події в режимі реального часу; можливість перегляду, аналізу та обробки протоколів аудита; робота з архівом даних аудита (використовується у конфігурації з підвищеними вимогами до забезпечення спостережності);

– модуль взаємодії з ППЗ, який встановлюється на РС та ФС ЛОМ та призначений для реалізації взаємодії між засобами КЗЗ та ППЗ автоматизованих систем, які функціонують в ЛОМ.

Архітектура КЗЗ "Гриф-Мережа" (у конфігурації з підвищеними вимогами до забезпечення спостережності) наведена на рис. 2.1. Детальний опис функцій, які реалізуються компонентами КЗЗ, наведено в розділі 3.

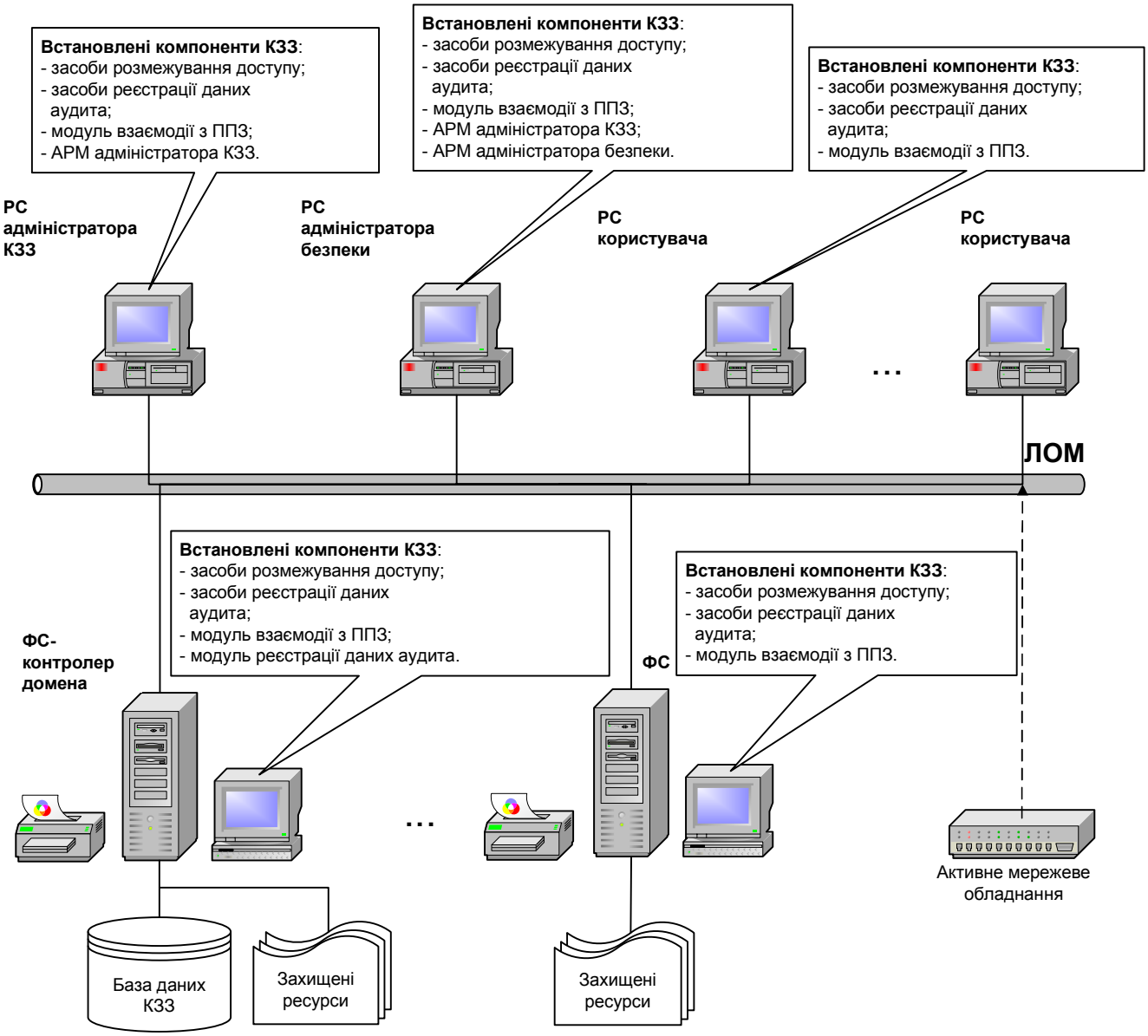

Рисунок 2.1 – *Архітектура КЗЗ "Гриф-Мережа"*

3 ОПИС ФУНКЦІЙ КЗЗ

3.1 Функції комплексу

КЗЗ **"Гриф–Мережа"** реалізує такі функції:

- **ідентифікацію та автентифікацію користувачів** на підставі імені (псевдоніма), паролю та носія даних автентифікації (знімного файлівого носія (пристрою Flash Drive, CD-RW, DVD-RW, дискета тощо)) при завантаженні ОС РС до завантаження будь-яких ПЗ з дисків, що дозволяє заблокувати використання РС сторонньою особою, а також розпізнати конкретного легального користувача та в подальшому реагувати на запити цього користувача відповідно до його повноважень;
- **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 та не допустити обробку ІзОД у випадку порушення його працездатності;
- **розподіл обов'язків користувачів** та виділення декількох ролей адміністраторів, які можуть виконувати різні функції з адміністрування (реєстрацію захищених ресурсів, реєстрацію користувачів, призначення прав доступу, оброблення протоколів аудита, тощо);
- **розмежування доступу користувачів до вибраних каталогів (папок)**, розміщених на РС та ФС ЛОМ, та до файлів, які в них знаходяться, що дозволяє організувати одночасну спільну роботу декількох користувачів ЛОМ, які мають різні службові обов'язки та права по доступу до ІзОД;
- **керування потоками інформації** та блокування потоків інформації, що можуть призвести до зниження рівня її конфіденційності;
- **контроль за виводом інформації на пристрої друку** з можливістю маркування друкованих аркушів документів (в форматі "Office Open XML") відповідно до вимог діючих нормативних документів в сфері охорони державної таємниці;
- **контроль за експортом інформації на знімні носії** з можливістю обмеження переліку знімних носіїв, які використовуються;
- **контроль за імпортом інформації зі знімних носіїв**;
- **гарантоване знищення залишкової інформації** шляхом затирання вмісту файлів, які містять ІзОД, при їх видаленні;
- **розмежування доступу прикладних програм до вибраних каталогів** та файлів, які в них знаходяться, що дозволяє забезпечити захист ІзОД від випадкового видалення, модифікації, а також забезпечити дотримання технології її оброблення;
- **контроль цілісності прикладного та системного програмного забезпечення**, а також блокування завантаження програм, цілісність яких порушена, що дозволяє забезпечити захист від вірусів та дотримання технології оброблення ІзОД;
- **контроль за використанням користувачами дискового простору файлових серверів (квоти)**, що виключає можливість блокування одним із користувачів можливості роботи інших;

- **відновлення функціонування КЗЗ після збоїв**, що гарантує доступність інформації з забезпеченням дотримання правил доступу до неї;
- **безперервну реєстрацію, аналіз та обробку критичних для безпеки подій** (входу користувачів в ОС, спроб несанкціонованого доступу, фактів запуску програм, доступу до захищеної інформації, виводу на друк і т.п.) у спеціальних протоколах аудита, що дозволяє адміністраторам контролювати доступ до ІзОД, слідкувати за тим, як використовується КЗЗ, а також правильно його конфігурувати;
- **негайне оповіщення** адміністратора безпеки про всі виявлені порушення встановлених правил розмежування доступу (у конфігурації для умов з підвищеними вимогами до забезпечення спостережності);
- **ведення архіву зареєстрованих даних аудита;**
- **взаємодію з прикладними програмними системами** через визначений виробником КЗЗ інтерфейс.

3.2 Функціональні профілі захищеності та рівень гарантій

У термінах НД ТЗІ 2.5–004–99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу" КЗЗ **"Гриф–Мережа"** реалізує такі функціональні профілі захищеності.

Функціональний профіль захищеності, який реалізує КЗЗ у базовій конфігурації:

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

Функціональний профіль захищеності, який реалізує КЗЗ у конфігурації з підвищеними вимогами до забезпечення спостережності:

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

де

КА-2 – базова адміністративна конфіденційність;

КО-1 – повторне використання об'єктів;

ЦА-2 – базова адміністративна цілісність;

ЦО-1 – обмежений відкат;

ДР-1 – квоти;

ДС-1 – стійкість при обмежених відмовах;

ДЗ-1 – модернізація;

ДВ-1 – ручне відновлення після збоїв;

НР-2 – захищений журнал;

НР-5 – аналіз в реальному часі;

НИ-3 – множинна ідентифікація та автентифікація

НК-1 – однонаправлений достовірний канал;

НО-2 – розмежування обов’язків адміністраторів;

НЦ-2 – КЗЗ з гарантованою цілісністю;

НТ-2 – самотестування при старті.

Розробка виконана у відповідності з вимогами рівня гарантій Г–4, встановленими НД ТЗІ 2.5– 004–99.

Реалізовані функціональні профілі, політика функціональних послуг безпеки та рівень гарантій відповідають вимогам НД ТЗІ 2.5-008-2002 "Вимоги щодо захисту службової інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2" при використанні технології обробки інформації з підвищеними вимогами до забезпечення конфіденційності, цілісності та доступності інформації та за умови відсутності необхідності реалізації довірчого керування доступом користувачів до інформаційних об’єктів, а також рекомендаціям НД ТЗІ 2.4-015-2018.

3.2.1 Опис політики функціональних послуг безпеки

КА-2 - базова адміністративна конфіденційність

Реалізація цієї послуги забезпечує можливість адміністратору КЗЗ керувати потоками інформації від захищених об’єктів до користувачів.

Політика цієї послуги поширюється на:

- користувачів усіх категорій;
- захищені інформаційні об’єкти (каталоги та файли) на дисках РС та ФС ЛОМ, що містять як ІзОД усіх рівнів конфіденційності, так і відкриту інформацію;
- системні та прикладні ПЗ, які призначені для обробки захищених об’єктів (файлів), що містять ІзОД;
- технологічну інформацію КЗЗ;
- окремі види периферійних пристроїв (принтери, накопичувачі на знімних носіях).

Розмежування доступу користувачів до захищених об’єктів виконується на підставі атрибутів захищених об’єктів, які характеризують ступінь конфіденційності інформації, що міститься в цих об’єктах, та атрибутів користувача, які характеризують рівень його повноважень по доступу до інформації. Атрибути доступу захищених об’єктів (каталогів та файлів) призначаються при їх створенні.

Запити на призначення та зміну прав доступу оброблюються тільки у випадку, якщо вони надходять від адміністраторів КЗЗ.

КЗЗ надає можливість адміністратору КЗЗ для кожного захищеного каталогу шляхом включення (виключення) користувачів до (із) списку користувачів, які мають права доступу до даного каталогу по читанню, визначити конкретних користувачів, які мають право отримувати інформацію із файлів, що містяться в захищеному каталозі, або запускати програми, виконувані коди яких у вигляді файлів зберігаються в даному каталозі.

КЗЗ реалізує керування потоками інформації з метою заборони потоків, які приводять до зниження рівня конфіденційності інформації, шляхом блокування копіювання та

переміщення (перейменування) файлів із каталогів з більш високим рівнем конфіденційності до каталогів з більш низьким рівнем конфіденційності, а також заборони можливості використання системного буфера обміну (clipboard) ОС для переносу даних із файлів з більш високим рівнем конфіденційності до файлів із більш низьким рівнем конфіденційності.

КЗЗ надає можливість адміністратору КЗЗ надавати/ відміняти користувачам повноваження імпорту/ експорту ІзОД з використанням знімних носіїв та повноваження виводу інформації на друк. Крім безпосереднього керування доступом користувачів до пристроїв імпорту/ експорту та пристроїв друку, КЗЗ, з метою підвищення достовірності реєстрації фактів виконання операцій експорту та друку, забороняє експорт інформації та друк з використанням довільних застосувань і дозволяє виконувати такі операції тільки з використанням:

- модуля контролю операцій експорту даних та модуля контролю операцій друку, що входять до складу КЗЗ;
- спеціально зареєстрованих програм.

КО-1 - повторне використання об'єктів

Реалізація цієї послуги забезпечує коректність повторного використання поділюваних об'єктів, гарантуючи, що у випадку, якщо поділюваний об'єкт виділяється новому користувачу або процесу, у ньому не міститься інформація, яка залишилась після використання його попереднім користувачем або процесом.

Політика цієї послуги поширюється на:

- сегменти ОП РС та ФС ЛОМ;
- носії інформації (жорсткі диски) РС та ФС, які використовуються системними та прикладними ПЗ при обробленні ІзОД;
- технологічну інформацію КЗЗ (облікові записи користувачів).

Відносно сегментів ОП РС та ФС послуга реалізується шляхом очистки вмісту об'єкта перед виділенням його іншому користувачу або процесу.

Відносно носіїв інформації (жорстких дисків) послуга реалізується шляхом очищення дискового простору, який займає файл з ІзОД, одразу після видалення відповідного файлу.

При реалізації послуги відносно облікових записів користувачів забезпечена неможливість успадкування новим користувачем з псевдонімом, який співпадає з псевдонімом раніше видаленого користувача, призначених видаленому користувачу прав.

ЦА-2 - базова адміністративна цілісність

Реалізація цієї послуги забезпечує можливість адміністратору КЗЗ керувати потоками інформації від користувачів до захищених об'єктів.

Політика цієї послуги поширюється на:

- користувачів усіх категорій;
- захищені інформаційні об'єкти (каталоги та файли) на дисках РС та ФС ЛОМ, які містять як ІзОД усіх рівнів конфіденційності, так і відкриту інформацію;
- системні та прикладні ПЗ, які призначені для обробки захищених об'єктів (файлів), що містять ІзОД;
- технологічну інформацію КЗЗ.

Розмежування доступу користувачів з використанням відповідних процесів до захищених об’єктів виконується на підставі атрибутів захищених об’єктів та процесів, які характеризують їх приналежність до однієї та тієї ж ТС, під якою розуміється певна іменована сукупність захищених об’єктів та процесів (програм), з використанням яких дозволено здійснення модифікації цих захищених об’єктів, а також атрибутів користувача, які характеризують рівень його повноважень по модифікації інформації. Атрибути доступу захищених об’єктів (каталогів та файлів) призначаються при їх створенні.

Запити на призначення та зміну прав доступу обробляються тільки у випадку, якщо вони надходять від адміністраторів КЗЗ.

КЗЗ надає можливість адміністратору КЗЗ для кожного захищеного каталогу шляхом включення (виключення) користувачів до (із) списку користувачів, які мають права доступу до даного каталогу по запису, визначити конкретних користувачів, які мають право модифікувати інформацію у файлах, що містяться в захищеному каталозі, або видаляти файли.

КЗЗ надає можливість адміністратору КЗЗ шляхом включення захищених каталогів та каталогів, що містять виконувані модулі програм, в одну й ту саму ТС, визначати процеси, тільки з використанням яких дозволено створення, зміна або видалення файлів в захищеному каталозі.

ЦО-1 - обмежений відкат

Реалізація цієї послуги забезпечує можливість відміни послідовності певних операцій та повернення (відката) захищеного об’єкта в попередній стан.

Політика цієї послуги поширюється на технологічну інформацію КЗЗ та на послідовність операцій, які виконуються КЗЗ при встановленні захисту на каталог.

КЗЗ забезпечує можливість автоматизованого здійснення відкату БД технологічної інформації КЗЗ в попередній стан, якщо в процесі виконання послідовності операцій, зв’язаних з встановленням захисту на каталог, виникли збої та дана послідовність операцій не була повністю завершена.

ДР-1 - квоти

Реалізація цієї послуги забезпечує запобігання захвату користувачами надмірного об’єму ресурсів.

Політика цієї послуги поширюється на:

- користувачів усіх категорій;
- захищені інформаційні об’єкти (файли) у каталогах, розміщених на ФС ЛОМ, які містять як ІзОД усіх рівнів конфіденційності, так і відкриту інформацію.

КЗЗ надає адміністраторам КЗЗ засоби для керування максимально допустимим розміром дискового простору для одного користувача на будь-якому із дисків ФС, а також встановлення граничного значення розміру зайнятого користувачем дискового простору.

При перевищенні користувачем граничного значення генерується відповідний запис у протоколі аудита, спроби виділення користувачу дискового простору понад квоти блокуються.

Запити на зміну значень дискових квот обробляються тільки в тому випадку, якщо вони надходять від адміністраторів КЗЗ.

ДС-1 - стійкість при обмежених відмовах

Реалізація цієї послуги забезпечує можливість використання окремих функцій КЗЗ після відмови його компонента (з погіршенням характеристик обслуговування).

Політика цієї послуги поширюється на компоненти КЗЗ, які реалізують рівень НР-5 (аналіз в реальному часі) послуги "Реєстрація" (агент модуля реєстрації даних аудита, модуль реєстрації даних аудита, модуль обробки та аналіза даних аудита).

При виникненні будь-яких відмов компонентів КЗЗ, які реалізують послугу "Реєстрація", КЗЗ в змозі продовжувати функціонування зі зниженням рівня послуги до НР-2 (захищений журнал).

ДЗ-1 - модернізація

Реалізація цієї послуги забезпечує можливість використання КЗЗ після заміни окремих його компонентів.

Політика цієї послуги поширюється на:

- ПЗ КЗЗ;
- технологічну інформацію КЗЗ.

Системному адміністратору КЗЗ з використанням спеціальних ПЗ надана можливість виконання модернізації (upgrade) ПЗ КЗЗ. Модернізація ПЗ КЗЗ не призводить до необхідності повторної інсталяції ПЗ КЗЗ або повторного налаштування КЗЗ.

ДВ-1 - ручне відновлення

Реалізація цієї послуги забезпечує повернення КЗЗ у відомий захищений стан після відмови або переривання обслуговування.

Політика цієї послуги поширюється на:

- ПЗ КЗЗ;
- технологічну інформацію КЗЗ.

При реалізації цієї послуги у випадку відмови ПЗ КЗЗ або порушення цілісності БД технологічної інформації КЗЗ переводиться до стану, в якому заборонена обробка ІзОД. Повернути КЗЗ до нормального функціонування може тільки системний адміністратор КЗЗ.

Системному адміністратору КЗЗ з використанням спеціальних ПЗ надана можливість відновлення працездатності ПЗ КЗЗ (із еталонної копії), а також відновлення коректності вмісту БД технологічної інформації КЗЗ.

НР-2 – захищений журнал

Реалізація цієї послуги забезпечує можливість контролю небезпечних для КЗЗ та системи в цілому подій.

Політика цієї послуги поширюється на:

- користувачів усіх категорій;
- захищені інформаційні об’єкти (каталоги та файли), які містять як ІзОД усіх рівнів конфіденційності, так і відкриту інформацію;
- системні та прикладні ПЗ, призначені як для обробки захищених об’єктів, що містять ІзОД, так і об’єктів, що містять відкриту інформацію;
- ПЗ КЗЗ;
- технологічну інформацію КЗЗ.

Засоби КЗЗ забезпечують реєстрацію у відповідних протоколах, аналіз та обробку у відкладеному режимі таких подій, які мають пряме відношення до безпеки:

- вхід користувача в ОС та завершення роботи користувача (вихід);
- запуск АРМ адміністратора КЗЗ;
- зміна стану БД технологічної інформації та ПЗ КЗЗ:
- реєстрація, видалення користувачів;
- реєстрація, видалення захищених ресурсів (встановлення/ зняття захисту на каталог);
- факти призначення/ зміни прав доступу користувачів до захищених ресурсів;
- факти доступу користувачів до захищених каталогів та файлів;
- факти виводу файлів з ІзОД на друк;
- факти експорту файлів з ІзОД на знімні носії;
- факти імпорту файлів з ІзОД зі знімних носіїв;
- факти порушення прав доступу користувачів до захищених ресурсів;
- факти перезавантаження, вимкнення РС та ФС та виникнення інших системних подій;
- подій, пов’язаних зі спостереженням за процесами (запуск, завершення).

У кожному записі протоколу аудита фіксується дата та час події, тип та атрибути операції, атрибути процесу та користувача, які ініціювали подію, признак успішності завершення операції, у випадку відмови – причина, а також інша інформація.

Засобами КЗЗ забезпечений захист протоколів аудита від несанкціонованого доступу (ознайомлення, модифікації або руйнування), а також можливість аналізу протоколів уповноваженими адміністраторами.

НР-5 - аналіз в реальному часі

Реалізація цієї послуги забезпечує можливість контролю небезпечних для КЗЗ та системи в цілому подій.

Політика цієї послуги поширюється на:

- користувачів усіх категорій;
- захищені інформаційні об’єкти (каталоги та файли), що містять як ІзОД усіх рівнів конфіденційності, так і відкриту інформацію;
- системні та прикладні ПЗ, призначені як для обробки захищених об’єктів, що містять ІзОД, так і об’єктів, що містять відкриту інформацію;
- ПЗ КЗЗ;
- технологічну інформацію КЗЗ.

Засоби КЗЗ забезпечують реєстрацію у відповідних протоколах, аналіз та обробку в реальному часі таких подій, які мають пряме або непряме відношення до безпеки:

- вхід користувача в ОС та завершення роботи користувача (вихід);
- запуск АРМ адміністратора КЗЗ;
- запуск АРМ адміністратора безпеки;
- зміна стану БД технологічної інформації та ПЗ КЗЗ:
- реєстрація, видалення користувачів;
- реєстрація, видалення захищених ресурсів (встановлення/ зняття захисту на каталог);
- факти призначення/ зміни прав доступу користувачів до захищених ресурсів;
- факти доступу користувачів до захищених каталогів та файлів;
- факти виводу файлів з ІзОД на друк;
- факти експорту файлів з ІзОД на знімні носії;
- факти імпорту файлів з ІзОД зі знімних носіїв;
- факти порушення прав доступу користувачів до захищених ресурсів;
- факти перезавантаження, вимкнення РС та ФС та виникнення інших системних подій;
- подій, пов’язаних з спостереженням за процесами (запуск, завершення);
- подій, пов'язаних з функціонуванням активного мережевого обладнання.

В кожному записі протоколу аудита фіксується дата та час події, тип та атрибути операції, атрибути процесу та користувача, які ініціювали подію, признак успішності завершення операції, у випадку відмови – причина, а також інша інформація.

Засобами КЗЗ забезпечений захист протоколів аудита від несанкціонованого доступу (ознайомлення, модифікації або руйнування), а також можливість аналізу протоколів уповноваженими адміністраторами.

Засоби КЗЗ забезпечують можливість контролю одиничних або повторюваних реєстраційних подій, що свідчать про прямі порушення ПБ інформації, яка обробляється в ЛОМ, та негайного інформування адміністратора безпеки про перевищення встановлених порогів безпеки. У складі КЗЗ реалізовані засоби, які дозволяють адміністратору безпеки здійснити неруйнівні дії по припиненню повторення цих подій (шляхом блокування облікового запису відповідного користувача).

З метою виключення можливості втрати інформації аудита при збоях засобами КЗЗ реалізується можливість збереження локальних даних аудита у вигляді відповідних протоколів безпосередньо на ФС або РС, на яких були зареєстровані відповідні події. У складі КЗЗ реалізовані засоби, які дозволяють адміністратору безпеки здійснювати перегляд та аналіз збережених протоколів аудита.

НИ-3 - множинна ідентифікація та автентифікація

Політика цієї послуги поширюється на користувачів усіх категорій, які намагаються отримати доступ до:

- засобів КЗЗ;
- захищених інформаційних об’єктів (каталогів та файлів), які містять ІзОД усіх рівнів конфіденційності та відкриту інформацію;

- системних та прикладних ПЗ, призначених як для обробки захищених об'єктів, що містять як ІзОД усіх рівнів конфіденційності, так і відкриту інформацію;
- периферійного обладнання, яке задіяне в обробці ІзОД;
- технологічної інформації КЗЗ.

Послуга реалізована шляхом ідентифікації користувачів на підставі введеного псевдоніма та автентифікації за встановленим протоколом на підставі пред'явленого носія з даними автентифікації та введеного пароля.

Дані автентифікації захищені від несанкціонованого доступу, модифікації або руйнування з використанням тих самих механізмів, що і при реалізації послуг КА-2, ЦА-2. З цією метою у КЗЗ реалізована вбудована ТС КЗЗ, в яку включені ПЗ КЗЗ та файли БД технологічної інформації КЗЗ.

НК-1 - однонаправлений достовірний канал

Реалізація цієї послуги гарантує користувачам усіх категорій можливість безпосередньої взаємодії з КЗЗ в процесі виконання їх ідентифікації та автентифікації.

Політика цієї послуги поширюється на:

- користувачів усіх категорій;
- ПЗ КЗЗ.

Достовірний канал реалізується в компонентах КЗЗ, через які здійснюється взаємодія з користувачем в процесі його ідентифікації та автентифікації. Зв'язок з використанням даного каналу ініціюється користувачем безпосередньо перед виконанням вводу даних автентифікації при вході в ОС.

НО-2 - розподіл обов'язків адміністраторів

Реалізація цієї послуги забезпечує можливість розподілу повноважень користувачів шляхом визначення категорій користувачів з певними для кожної категорії функціями (ролями).

Політика цієї послуги поширюється на користувачів усіх категорій та визначає такі ролі:

- системний адміністратор КЗЗ;
- адміністратори КЗЗ;
- адміністратори безпеки;
- користувачі.

Користувач, який встановлює КЗЗ, є Системним адміністратором КЗЗ. Обліковий запис Системного адміністратора КЗЗ не може бути видалений або відключений. В обов'язки Системного адміністратора входить інсталяція та початкова ініціалізація КЗЗ, оновлення за необхідності ПЗ КЗЗ, відновлення за необхідності цілісності ПЗ та БД КЗЗ, відновлення за необхідності працездатності ОС, встановлення та налаштування додаткових прикладних ПЗ. В процесі штатного функціонування КЗЗ обліковий запис Системного адміністратора КЗЗ не використовується.

В обов'язки адміністраторів КЗЗ, яких може бути декілька, входить керування користувачами, захищеними ресурсами та правами доступу до них. За кожним

адміністратором КЗЗ можуть бути закріплені повноваження на виконання різних функцій адміністрування, при цьому на дії адміністраторів КЗЗ накладаються обмеження:

- адміністратори КЗЗ можуть призначати права доступу до захищених каталогів тільки іншим користувачам, але не собі;
- адміністратори КЗЗ не можуть змінювати свої адміністративні повноваження;
- зміни атрибутів інших адміністраторів КЗЗ (прав доступу та адміністративних повноважень) та користувачів (прав доступу) вступають в силу тільки після санкції (підтвердження) зроблених змін адміністратором безпеки.

В обов'язки адміністраторів безпеки входить контроль за дотриманням правил доступу до ІзОД шляхом контролю встановлених прав доступу, керування правилами аудита та аналізу зареєстрованих даних аудита. Тільки адміністратор безпеки може активізувати облікові записи інших адміністраторів та користувачів після зміни їх атрибутів.

Користувач, який успішно пройшов ідентифікацію та автентифікацію та не призначений КЗЗ на роль Системного адміністратора КЗЗ, адміністратора КЗЗ або адміністратора безпеки, призначається на роль звичайного користувача. Звичайному користувачу можуть бути надані права доступу до захищених інформаційних об'єктів (каталогів та файлів), які містять ІзОД та відкриту інформацію, повноваження друку, імпорту/ експорту інформації.

НЦ-2 - КЗЗ з гарантованою цілісністю

Реалізація цієї послуги забезпечує КЗЗ можливість захищати себе від зовнішніх впливів та гарантувати свою здатність керувати захищеними об'єктами.

Політика цієї послуги поширюється на:

- ПЗ КЗЗ;
- системні та прикладні ПЗ, призначені як для обробки захищених об'єктів, що містять ІзОД, так і об'єктів, що містять відкриту інформацію;
- технологічну інформацію КЗЗ.

З метою захисту від зовнішніх впливів КЗЗ визначає та підтримує власний домен виконання, відмінний від доменів усіх інших процесів, та реалізує механізми розмежування доменів.

У власному домені КЗЗ забезпечує захист від несанкціонованої модифікації засобів КЗЗ, які реалізують механізми КЗЗ, та/ або втрати керування КЗЗ, а також від НСД до технологічної інформації КЗЗ з використанням тих самих механізмів, що і при реалізації послуг КА-2, ЦА-2. З цією метою у КЗЗ реалізована вбудована ТС КЗЗ, до якої включені ПЗ КЗЗ та файли БД технологічної інформації КЗЗ.

Додатково до виділення домену КЗЗ, реалізовано контроль цілісності ПЗ КЗЗ та БД технологічної інформації КЗЗ при старті та за запитом адміністратора КЗЗ.

У випадку виявлення порушення цілісності ПЗ КЗЗ або порушення цілісності БД технологічної інформації КЗЗ переводиться до стану, в якому заборонена обробка ІзОД. Повернути КЗЗ до нормального функціонування може тільки Системний адміністратор КЗЗ.

Системному адміністратору КЗЗ з використанням спеціальних ПЗ надана можливість відновлення працездатності ПЗ КЗЗ (із еталонної копії), а також відновлення коректності вмісту БД технологічної інформації КЗЗ.

Додатково в рамках політики цієї послуги у КЗЗ реалізовано контроль цілісності всіх системних та прикладних ПЗ при старті, що забезпечує:

- виключення спроб пошуку та використання уразливостей КЗЗ та ОС;
- неможливість доступу до ресурсів з використанням недокументованих інтерфейсів та засобів безпосереднього звернення до функціональних рівнів ОС, на яких базується КЗЗ;
- виключення можливості впровадження програмних закладок та реалізації прихованих каналів;
- дотримання встановленої технології обробки ІзОД.

НТ-2 - самотестування при старті

Реалізація цієї послуги забезпечує КЗЗ можливість перевірити та на основі цього гарантувати правильність функціонування та цілісність певної множини своїх функцій.

Політика цієї послуги поширюється на:

- ПЗ КЗЗ;
- технологічну інформацію КЗЗ.

При старті та за запитом адміністратора КЗЗ виконує набор тестів з метою оцінки правильності функціонування своїх критичних функцій (шляхом перевірки цілісності відповідних ПЗ та БД технологічної інформації КЗЗ).

У випадку неуспішного виконання тестів (виявлення порушення цілісності ПЗ КЗЗ або порушення цілісності БД технологічної інформації) КЗЗ переводиться до стану, в якому заборонена обробка ІзОД. Повернути КЗЗ до нормального функціонування може тільки Системний адміністратор КЗЗ.

Системному адміністратору КЗЗ з використанням спеціальних ПЗ надана можливість відновлення працездатності ПЗ КЗЗ (із еталонної копії), а також відновлення коректності вмісту БД технологічної інформації КЗЗ.

3.3 Опис реалізованих функцій КЗЗ

3.3.1 Ідентифікація та автентифікація користувачів

Перш ніж здійснювати розмежування доступу, КЗЗ повинен розпізнати користувача та блокувати доступ неавторизованих користувачів. Для цього при вході користувача в систему виконується його ідентифікація (розпізнання) та автентифікація (перевірка результатів ідентифікації).

Ідентифікація користувача виконується на підставі імені (псевдоніма), яке (який) користувач вводить з клавіатури. Автентифікація користувача виконується на підставі пароля, який вводиться з клавіатури, та носія даних автентифікації, який пред’являється. В якості носія даних автентифікації може виступати перезаписуваний знімний файловий носій будь-якого типу (дискета, пристрій Flash Drive, CD-RW/DVD-RW тощо). Таким чином, реалізується автентифікація користувача з використанням механізмів, які функціонують на основі двох різних принципів: "володію чимось" – носій даних автентифікації та "знаю щось" – пароль (множинна ідентифікація та автентифікація).

У випадку, якщо надана користувачем інформація автентифікації не відповідає еталону, який зберігається в БД КЗЗ, доступ користувача в ОС блокується.

Крім того, КЗЗ виконує контроль за закінченням терміну дії повноважень користувача та його пароля, а також за відповідністю дня тижня та часового інтервалу, на протязі якого користувач здійснює вхід в ОС, тим, які задані адміністратором.

Важливою особливістю є те, що ідентифікація та автентифікація користувача здійснюється з використанням достовірного каналу. При цьому жодна стороння програма не може перехопити інформацію автентифікації, яку вводить користувач.

3.3.2 Можливість блокування пристроїв інтерфейсу користувача

Ідентифікація та автентифікація користувача виконується не тільки при вході в ОС, але і після блокування пристроїв інтерфейсу користувача (клавіатури, миші та монітора). Блокування пристроїв інтерфейсу може здійснюватись користувачем, наприклад, у випадку необхідності покинути на певний час робоче місце. Для розблокування пристроїв інтерфейсу користувачу необхідно пред’явити свій носій даних автентифікації та ввести пароль.

3.3.3 Контроль цілісності та самотестування КЗЗ

Контроль цілісності КЗЗ виконується шляхом перевірки цілісності ПЗ КЗЗ при кожному завантаженні ОС. Крім того, дана операція може виконуватись за бажанням адміністратора КЗЗ з використанням АРМ адміністратора КЗЗ. При цьому може бути виконана перевірка як ПЗ КЗЗ, розміщених на тій РС, на якій встановлений АРМ адміністратора КЗЗ, так і ПЗ КЗЗ, розміщених на будь-якій іншій РС ЛОМ або на будь-якому іншому ФС ЛОМ. У випадку виявлення порушення цілісності користувачу, який виконує перевірку (вхід в ОС), видається відповідне повідомлення. Відновлення цілісності ПЗ КЗЗ може бути виконано Системним адміністратором КЗЗ за допомогою спеціальних ПЗ, які входять до складу КЗЗ.

3.3.4 Розмежування обов’язків користувачів

Будь-яка ПБ крім ПРД встановлює правила керування засобами захисту. Функції керування покладаються на довірених осіб, які несуть відповідальність за безпеку обробки інформації в системі. Для комп’ютерних систем осіб, за якими закріплені права на виконання певних функцій керування, прийнято називати адміністраторами.

Відповідно з ПБ, яка реалізується КЗЗ, функції адміністратора можуть бути доступні конкретному користувачу на підставі його членства в певній групі та/ або конкретних привілеїв, які закріплені за даним користувачем та записані в його обліковому записі.

Відповідно з ПБ, яка реалізується КЗЗ **"Гриф–Мережа"**, всі адміністратори діляться на:

- Системного адміністратора КЗЗ, який виконує встановлення та налаштування КЗЗ;
- адміністраторів КЗЗ, які виконують керування засобами КЗЗ, захищеними інформаційними ресурсами та правами доступу користувачів до захищених ресурсів;

- адміністраторів безпеки, які контролюють дії адміністраторів КЗЗ та користувачів та дотримання ними вимог встановленої ПБ.

Всі адміністратори включаються в групу адміністраторів ОС.

Користувач, який встановлює КЗЗ (обліковий запис адміністратора домену "Адміністратор"), є Системним адміністратором КЗЗ. Обліковий запис Системного адміністратора КЗЗ не може бути видалений. Тільки Системний адміністратор КЗЗ має право на відновлення цілісності ПЗ та БД КЗЗ у випадку збоїв.

Системний адміністратор КЗЗ **"Гриф–Мережа"** має повноваження по роботі з даними аудита, зареєстрованими засобами КЗЗ. За допомогою АРМ аналізу локальних даних аудита він може здійснювати аналіз інформації аудита. Крім того, він має такі повноваження:

- керування користувачами (реєстрація, видалення неактивізованих облікових записів, модифікація атрибутів облікового запису, зміна пароля, перегенерація інформації автентифікації на носій, активізація/ деактивізація облікових записів сервісів та активізація одного адміністратора безпеки);
- керування правами доступу користувачів до захищених каталогів;
- керування правами доступу до захищених каталогів з боку програм або технологічними схемами (див. п. 3.3.10);
- керування рівнями конфіденційності оброблюваної інформації;
- керування обліковими записами РС, ФС та квотами дискового простору на них;
- керування увімкненням/ вимкненням режиму повного контролю цілісності виконуваного програмного забезпечення.

Адміністратор КЗЗ може мати такі повноваження:

- керування користувачами (реєстрація, видалення неактивізованих облікових записів, модифікація атрибутів облікового запису, зміна пароля, перегенерація інформації автентифікації на носій, активізація/ деактивізація облікових записів сервісів);
- керування правами доступу користувачів до захищених каталогів;
- керування правами доступу до захищених каталогів з боку програм або технологічними схемами (див. п. 3.3.10);
- керування рівнями конфіденційності оброблюваної інформації;
- керування обліковими записами РС, ФС та квотами дискового простору на них;
- керування увімкненням/ вимкненням режиму повного контролю цілісності виконуваного програмного забезпечення.

Системний адміністратор КЗЗ та адміністратори КЗЗ можуть призначати права доступу до захищених каталогів тільки іншим користувачам, але не собі. При призначенні прав доступу користувачу його обліковий запис деактивується. Призначені права доступу вступають в силу тільки після підтвердження адміністраторами безпеки (шляхом активізації облікового запису відповідного користувача).

Адміністратори безпеки мають повноваження по роботі з даними аудита, зареєстрованими засобами КЗЗ. За допомогою АРМ адміністратора безпеки вони можуть міняти налаштування аудита КЗЗ, здійснювати аналіз інформації аудита, отримувати в режимі реального часу сповіщення про порушення встановленої ПБ. Крім цього, адміністратори безпеки мають повноваження на керування користувачами (активізація/ деактивізація облікових записів користувачів та сервісів).

3.3.5 Розмежування доступу користувачів до каталогів

Відповідно до ПБ, яка реалізується КЗЗ, захищеними об’єктами є каталоги жорстких дисків РС та ФС ЛОМ та файли, які в знаходяться в них. Розмежування доступу користувачів до каталогів та файлів, які в них знаходяться, реалізовано у відповідності з принципами адміністративного керування доступом. При цьому всі розділи всіх жорстких дисків РС та ФС ЛОМ повинні бути розділами з файловою системою NTFS.

При реєстрації захищеного каталогу адміністратор КЗЗ вказує рівень його конфіденційності, який далі не може бути змінений. Каталоги, які не зареєстровані як захищені, вважаються за замовченням відкритими (такими, що не мають рівня конфіденційності) та доступ до них дозволяється всім користувачам.

Для кожного захищеного каталогу адміністратор КЗЗ може створити список доступу, в якому перелічені користувачі, що мають права доступу до даного каталогу та файлів, що містяться в ньому та в його підкаталогах, а також дозволені для цих користувачів типи доступу (тільки читання, читання та запис).

Користувач потенційно може отримати доступ до каталогу, якщо рівень його допуску (також задається адміністратором КЗЗ при реєстрації користувача) не нижчий, ніж рівень конфіденційності відповідного каталогу.

За замовченням у КЗЗ введені такі рівні конфіденційності інформації та рівні допуску користувачів:

- "КОНФІДЕНЦІЙНА ІНФОРМАЦІЯ";
- "ДСК";
- "ТАЄМНО";
- "ЦІЛКОМ ТАЄМНО";
- "ОСОБЛИВОЇ ВАЖЛИВОСТІ".

Крім того, адміністратор КЗЗ може створити до 29 довільних рівнів конфіденційності між рівнями "КОНФІДЕНЦІЙНО" та "ДСК".

Кожному користувачу, який має відповідний рівень допуску, адміністратор КЗЗ може надати доступ до захищеного каталогу по читанню або по читанню та запису.

Користувачі мають тільки ті права доступу до захищених каталогів, а значить і до файлів з ІзОД, що містяться в них, які явно визначені адміністратором КЗЗ. Захист поширюється на всю гілку дерева, починаючи з вказаного в БД КЗЗ захищеного каталогу, включно з його підкаталогами. Тому не допускається вказувати в якості нового захищеного каталогу каталог, який є підкаталогом вже захищеного каталогу. КЗЗ забороняє виконувати перейменування та видалення захищеного каталогу і тих каталогів, які його містять, аж до того, що знаходиться в корні диску.

Доступ по запису до каталогів КЗЗ дозволений тільки ПЗ КЗЗ (АРМ адміністратора КЗЗ). Доступ по запису до каталогів ОС дозволений тільки адміністраторам.

При спробі користувача отримати заборонений вид доступу (наприклад, видалити файл в каталозі, до якого дозволений доступ тільки по читанню) спроба доступу блокується та в протоколі аудита реєструється факт НСД.

3.3.6 Керування потоками інформації

КЗЗ підтримує можливість керування потоками інформації, яке полягає в тому, що КЗЗ слідкує за тим, щоб процеси, у яких є відкриті для читання файли, які містяться у захищених каталогах, не могли відкрити для запису файли, які містяться у незахищених (відкритих або спільних) каталогах або каталогах з меншим рівнем конфіденційності. Це, частково, дозволяє блокувати копіювання файлів із захищених каталогів до незахищених або із каталогів з більш високим рівнем конфіденційності до каталогів з меншим рівнем, що дозволяє уникнути випадкового або умисного зниження рівня конфіденційності інформації.

Крім цього, КЗЗ дозволяє заблокувати можливість переносу даних з використанням системного буфера обміну ОС (Clipboard) із файлів з більш високим рівнем конфіденційності до файлів з меншим рівнем конфіденційності.

3.3.7 Контроль за виведенням інформації на друк

Адміністратори КЗЗ мають можливість явним чином вказати, кому із користувачів дозволено виведення інформації на друк. Всі факти виведення інформації на пристрій друку фіксуються в протоколах аудита (із зазначенням імені файлу, який виводиться на друк, та імені пристрою друку, який використовується). При цьому, виведення на друк може здійснюватися тільки з використанням спеціальної програми, яка входить до складу КЗЗ, а також спеціально зареєстрованих адміністратором КЗЗ програм.

3.3.8 Контроль за імпортом/ експортом інформації з використанням знімних носіїв

Всі знімні носії (жорсткі диски, які підключаються через USB-інтерфейс, дискети, пристрої Flash Drive, CD-ROM, DVD-ROM тощо), встановлені на РС та ФС ЛОМ, розглядаються КЗЗ як пристрої імпорту/ експорту. Доступ до цих пристроїв мають тільки ті користувачі, яким адміністраторами КЗЗ дозволено виконувати операції експорту інформації на знімні носії або імпорту інформації з них. Всі факти імпорту/ експорту інформації (із зазначенням імені файлу та типу пристрою, який використовується) фіксуються в протоколах аудита. При цьому, експорт даних на знімні носії може здійснюватися тільки з використанням спеціальної програми, яка входить до складу КЗЗ, а також спеціально зареєстрованих адміністратором КЗЗ програм.

Крім того, додаткові обмеження на виконання операцій імпорту та експорту вводяться при використанні режиму реєстрації знімних носіїв, які допускають багаторазове зчитування/ запис інформації (дискети, пристрої Flash Drive тощо). У цьому випадку адміністратор КЗЗ може зареєструвати в БД комплексу знімні носії, попередньо поставлені на облік в режимно-секретному органі або канцелярії, та дозволити певнім користувачам виконання операцій імпорту / експорту тільки з використанням таких носіїв.

3.3.9 Гарантоване видалення залишкової інформації

У КЗЗ реалізовано гарантоване видалення залишкової інформації при видаленні файлів, що містять ІзОД. Додатково до реалізованої в ОС функції очистки дискового простору перед його виділенням для розміщення нового файлу реалізована функція очищення займаного файлом дискового простору безпосередньо при видаленні файлу, що міститься в захищеному каталозі (так званий wiping). Затирання даних реалізовано шляхом запису поверх цих даних

послідовності нульових байтів. Реалізація даної функції перешкоджає проведенню атак типа "збирання сміття".

3.3.10 Розмежування доступу прикладних програм до каталогів

У КЗЗ реалізовано розмежування доступу до захищених каталогів та файлів, які містяться в них, з боку створюваних користувачем процесів, що дозволяє забезпечити захист ІзОД від випадкового видалення або модифікації та дотриматись технології її оброблення.

Дана функція реалізується шляхом створення ТС. ТС являє собою іменовану сукупність захищених каталогів, що містять файли даних, та каталогів, що містять файли програм, з використанням яких дозволена модифікація цих даних. Якщо каталог входить в ТС, то, навіть якщо користувач має право доступу до даного каталогу, він зможе здійснити доступ до даних тільки за допомогою певних, включених в ТС програм. В одну ТС можуть включатися каталоги, розміщені як на одній, так і на різних РС ЛОМ, один і той же каталог може входити в декілька ТС.

З використанням даного механізму обмежується також доступ до каталогу КЗЗ та налаштуванням реєстру, які впливають на безпеку. Доступ до них по запису можуть отримати тільки адміністратори КЗЗ та тільки з використанням АРМ адміністратора КЗЗ, який в свою чергу, дозволяє виконувати операції тільки при наявності у адміністратора КЗЗ відповідних повноважень та у відповідності з встановленими правилами.

3.3.11 Контроль цілісності прикладного та системного програмного забезпечення

Реалізація контролю цілісності прикладного та системного програмного забезпечення у КЗЗ **"Гриф–Мережа"** переслідує одразу декілька цілей:

- по-перше, це перешкоджає розповсюдженню вірусів, а значить порушенню цілісності ОС, КЗЗ та оброблюваної інформації;
- по-друге, це дозволяє уникнути витоку інформації за рахунок використання прихованих каналів, порушення встановленої технології оброблення інформації, а також інших дій, пов’язаних з впровадженням шкідливих програм (закладок, "троянських коней" тощо);
- по-третє, це дозволяє створити умови, коли в системі працює тільки перевірене програмне забезпечення, яке не виконує жодних дій, які могли б призвести до відключення або подолання засобів захисту, що дозволяє виконати вимоги більш високих рівнів послуги "цілісність КЗЗ".

Контроль цілісності програмного забезпечення полягає у перевірці цілісності виконуваних модулів при їх завантаженні з використанням попередньо розрахованих кодів контролю цілісності. Завантаження модулів, цілісність яких порушена, блокується.

3.3.12 Контроль за використанням дискового простору

КЗЗ підтримує можливість квотування ресурсів та дозволяє реалізувати контроль за використанням дискового простору ФС та РС ЛОМ користувачами. Адміністратор має можливість для кожного логічного диску на будь-якій РС або будь-якому ФС вказати, який максимальний об’єм дискового простору може використовувати кожний користувач.

Використання даної функції дозволяє виключити можливість блокування одним із користувачів ЛОМ можливості роботи інших.

3.3.13 Відновлення функціонування КЗЗ після збоїв

У випадку виявлення в процесі самотестування при старті порушення працездатності КЗЗ, цілісності ПЗ або БД КЗЗ користувачу видається відповідне повідомлення і подальша робота блокується. В такій ситуації необхідне втручання Системного адміністратора КЗЗ, який має можливість (з використанням відповідних ПЗ) відновити цілісність засобів КЗЗ на РС або на ФС (із еталонної копії) або БД КЗЗ із резервної копії.

Адміністратор КЗЗ при роботі з АРМ адміністратора КЗЗ має можливість виконувати відкат невдало завершених операцій по встановленню захисту на каталог.

3.3.14 Безперервна реєстрація, аналіз та обробка подій

Засоби КЗЗ забезпечують реєстрацію таких подій, які мають пряме або непряме відношення до безпеки:

- вхід користувача в ОС та завершення роботи користувача (вихід);
- запуск АРМ адміністратора КЗЗ;
- запуск АРМ адміністратора безпеки;
- зміна стану БД та ПЗ КЗЗ:
- реєстрація, видалення користувачів;
- реєстрація, видалення захищених ресурсів (встановлення/ зняття захисту на каталог);
- факти призначення/ зміни прав доступу користувачів до захищених ресурсів;
- факти доступу користувачів до захищених каталогів та файлів;
- факти виведення файлів з ІзОД на друк;
- факти імпорту/ експорту файлів з ІзОД з використанням знімних носіїв;
- факти порушення прав доступу користувачів до захищених ресурсів;
- факти перезавантаження, вимкнення РС та ФС та виникнення інших системних подій;
- подій, пов’язаних з спостереженням за процесами (запуск, завершення);
- подій, пов’язаних з функціонуванням активного мережевого обладнання.

У кожному запису протоколу аудита фіксується дата та час події, тип та атрибути операції (наприклад, відкриття файлу для читання/ запису), атрибути процесу та користувача, які ініціювали подію, ознака успішності завершення операції і, у випадку відмови – причина, а також інша інформація.

Збір інформації аудита та її аналіз в реальному часі реалізується з використанням агентів модуля реєстрації даних аудита, які входять до складу КЗЗ і функціонують на РС та ФС ЛОМ, а також модуля реєстрації даних аудита, який функціонує на ФС-ОКД ЛОМ.

Перегляд та аналіз протоколів реєстрації (у конфігурації з підвищеними вимогами до забезпечення спостережності) виконується з допомогою АРМ адміністратора безпеки, яке входить до складу КЗЗ.

Дані аудита зберігаються в БД КЗЗ та можуть бути використані для подальшого аналізу.

З метою виключення можливості втрати інформації аудита при збоях засобами КЗЗ реалізується можливість збереження локальних даних аудита (за допомогою модулів збереження локальних даних аудита) у вигляді відповідних протоколів безпосередньо на ФС або РС, на яких були зареєстровані відповідні події.

У складі КЗЗ реалізовані засоби (АРМ аналізу локальних даних аудита), які дозволяють адміністратору безпеки здійснювати перегляд та аналіз збережених протоколів аудита.

3.3.15 Негайне сповіщення адміністратора безпеки про порушення встановлених ПРД

Для оперативної реакції на порушення встановлених ПРД у КЗЗ **"Гриф–Мережа"** (у конфігурації з підвищеними вимогами до забезпечення спостережності) реалізована можливість негайного сповіщення адміністратора безпеки про зареєстровані факти таких порушень. Адміністратор безпеки з використанням АРМ адміністратора безпеки, який входить до складу КЗЗ, може встановлювати відповідні правила сповіщення. У випадку, якщо подія, яка виникла та зареєстрована в протоколах аудита, задовольняє заданому правилу сповіщення, інформація про неї негайно поступає на консоль АРМ адміністратора безпеки.

3.3.16 Ведення архіву зареєстрованих даних аудита

За допомогою АРМ адміністратора безпеки (у конфігурації з підвищеними вимогами до забезпечення спостережності) або АРМ аналізу локальних даних аудита адміністратор безпеки може створити архівну копію даних аудита і, відповідно, за необхідності відновити дані із архівної копії.

4 ВАРИАНТИ ВИКОРИСТАННЯ КЗЗ

4.1 Застосування КЗЗ для захисту інформації у вигляді слабозв'язаних об'єктів

При використанні КЗЗ **"Гриф–Мережа"** для захисту оброблюваної в ЛОМ із використанням відповідних ППЗ інформації, представленої у вигляді слабозв'язаних об'єктів (окремих файлів), ресурси, що підлягають захисту (каталоги, що містять файли з ІзОД), можуть бути розміщені як на жорстких дисках ФС ЛОМ, так і на жорстких дисках РС ЛОМ (рис. 2.1).

Доступ до захищених каталогів (та, відповідно, збережених у них файлів) повинен надаватися користувачам у відповідності зі службовою необхідністю. Якщо для обробки файлів з ІзОД передбачається використовувати обмежений набір ПЗ, можна також зареєструвати ці ПЗ як технологічні програми та створити відповідні ТС.

4.2 Застосування КЗЗ для захисту інформації у вигляді сильнозв'язаних об'єктів

При використанні КЗЗ **"Гриф–Мережа"** для захисту оброблюваної в ЛОМ із використанням відповідних ППЗ інформації, представленої у вигляді сильнозв'язаних об'єктів, які зберігаються у сховищах даних (наприклад, таблиць БД), ресурси, які необхідно захистити (каталоги, що містять файли з сильнозв'язаними об'єктами), повинні бути розміщені тільки на жорстких дисках ФС ЛОМ (рис. 2.1).

Доступ до захищених каталогів (та, відповідно, збережених у них файлів) повинен бути наданий тільки тому службовому обліковому запису (сервісу), під яким функціонує відповідний сервер СКБД та, у випадку необхідності виконання операцій резервного копіювання даних, користувачам, які виконують цю операцію. З метою запобігання можливості модифікації файлів, що містять сильнозв'язані об'єкти, в обхід сервера СКБД, повинні бути створені відповідні ТС, до яких повинні бути включені каталоги з ПЗ сервера СКБД та захищені каталоги з файлами, які містять сильносв'язані об'єкти.

Розмежування доступу до об'єктів всередині прикладної системи повинно реалізовуватись її прикладними програмними засобами. Для забезпечення надійного безперервного захисту ІзОД ці прикладні програмні засоби повинні забезпечувати:

- взаємодію з КЗЗ **"Гриф–Мережа"** (через відповідний інтерфейс, який реалізується інтерфейсним модулем взаємодії з ППЗ) для отримання ідентифікаторів зареєстрованих користувачів ОС та їх атрибутів доступу до ІзОД;
- призначення прав доступу до інформаційних об'єктів, які обробляються у прикладній системі, у відповідності з отриманими ідентифікаторами та атрибутами доступу користувачів до ІзОД, а також згідно з встановленими для системи вимогами;
- взаємодію з КЗЗ **"Гриф–Мережа"** (через відповідний інтерфейс, який реалізується інтерфейсним модулем взаємодії з ППЗ) для отримання ідентифікатора та атрибутів доступу поточного користувача ОС;
- керування доступом користувача до інформаційних об'єктів, які обробляються у прикладній системі, на підставі отриманих від КЗЗ **"Гриф–Мережа"** ідентифікатора та атрибутів доступу поточного користувача ОС (в тому числі рівня допуску користувача та рівня конфіденційності інформаційного об'єкта);
- реєстрацію всіх критичних для безпеки інформації подій в протоколах аудита ОС;
- взаємодію з КЗЗ **"Гриф–Мережа"** для отримання списку та атрибутів доступу захищених ресурсів ОС (захищених каталогів ОС) через відповідний інтерфейс, який реалізується інтерфейсним модулем взаємодії з ППЗ;

- контроль відповідності атрибутів доступу (рівня конфіденційності) захищених інформаційних об’єктів, які обробляються у прикладній системі, та атрибутів доступу захищених каталогів ОС при експорті інформаційних об’єктів зі сховища даних прикладної системи до каталогів ОС або імпорті інформаційних об’єктів із каталогів ОС до сховища даних прикладної системи.

5 ВИМОГИ ДО УМОВ ЕКСПЛУАТАЦІЇ

У випадку, якщо в ЛОМ використовуються ФС та РС, на яких не встановлені засоби КЗЗ **"Гриф–Мережа",** шляхом відповідного адміністрування активного мережевого обладнання (пристроїв комутації пакетів) на канальному рівні стека протоколів ЛОМ повинен бути заборонений доступ з таких ФС та РС до ФС та РС, на яких встановлені засоби КЗЗ **"Гриф–Мережа"**.

Якщо захищені каталоги розміщуються на жорстких дисках РС ЛОМ, відповідними організаційними та/ або технічними заходами (вилучення пристроїв вводу/ виводу; підключення дисковода до контролера таким чином, щоб він розпізнавався як дисковод, з якого неможливо виконати завантаження ОС; встановлення заборони на завантаження зі знімних носіїв в SETUP BIOS та пароля для доступу до SETUP тощо) повинна бути заблокована можливість завантаження ОС зі знімних носіїв. У випадку розміщення захищених каталогів тільки на жорстких дисках ФС ЛОМ, у зазначених вище заходах по відношенню до РС немає необхідності.

Крім цього, з використанням відповідних організаційних заходів (наприклад, механічного блокування доступу до панелі управління та клавіатури) повинен бути забезпечений захист ФС-ОКД ЛОМ від несанкціонованого вимкнення або перезавантаження.

6 УМОВИ ПОСТАЧАННЯ

6.1 Комплект поставки

В комплект поставки входять:

- паспорт – 1 шт;
- CD-ROM із програмним забезпеченням та документацією в електронному вигляді (опис комплексу, настанова з встановлення та налаштування, настанова системного адміністратора КЗЗ, настанова адміністратора КЗЗ, настанова адміністратора безпеки, настанова користувача, настанова з експлуатації автоматизованого робочого місця адміністратора КЗЗ, настанова з експлуатації автоматизованого робочого місця адміністратора безпеки, настанова з експлуатації автоматизованого робочого місця аналізу локальних даних аудита, настанова програміста) – 1 шт;
- упаковка – 1 шт.

6.2 Сумісність

Програмні засоби КЗЗ **"Гриф–Мережа"** сумісні із засобами, які входять до комплекту постачання ОС:

- Windows 7 (Professional, Enterprise, Ultimate) без пакетів оновлення та з пакетом оновлення SP1;
- Windows Server 2008 R2 без пакетів оновлення та з пакетом оновлення SP1;
- Windows 8.1 (Professional, Enterprise);
- Windows 10 (Professional, Enterprise);
- Windows 11 (Professional, Enterprise);
- Windows Server 2012 / 2012 R2;
- Windows Server 2016 / 2019/ 2022,

а також з іншим системним, інструментальним та прикладним програмним забезпеченням, яке використовує стандартні інтерфейси зазначених ОС (у тому числі з усіма версіями Microsoft Office – до Microsoft Office 2021 включно).

КЗЗ **"Гриф–Мережа"** може використовуватись разом з антивірусними засобами Eset Smart Security (Nod32) версії 4.0 та вище; Symantec Endpoint Protection версії 12.0 та вище; Zillya! Антивірус для бізнесу версії 1.1 та вище.

КЗЗ **"Гриф–Мережа"** може використовуватись з такими системами управління базами даних: Microsoft SQL Server; Oracle; IBM DB2; Informix.

КЗЗ **"Гриф–Мережа"** може бути не сумісний з іншими засобами захисту від несанкціонованого доступу, антивірусним програмним забезпеченням та програмним забезпеченням, яке працює з дисками та файлами на низькому рівні в обхід файлової системи.

Після установки КЗЗ **"Гриф–Мережа"** обмежується можливість відновлення та оновлення програмного забезпечення ОС (тобто, для проведення оновлення програмного забезпечення ОС може бути необхідно провести деінсталяцію програмних засобів КЗЗ **"Гриф–Мережа"** з відповідної РС або ФС). Після установки КЗЗ **"Гриф–Мережа"**

обмежуться можливість використання штатних засобів збереження/відновлення системних даних ОС.

6.3 Гарантійні зобов’язання

Гарантійні зобов’язання Розробника наведені у Паспорті на КЗЗ **"Гриф-Мережа"**. Додаткова взаємна відповідальність Замовника та Розробника може бути визначена на договірних умовах.

6 УМОВИ ПОСТАЧАННЯ