Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Герасимова Максима Олеговича*

академічної групи *125-16-3*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Комплекс засобів захисту на базі механізмів операційних систем сімейства RedHat Enterprise Linux*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.т.н., проф. Корнієнко В.І.			
розділів:				
спеціальний	ас. Плєц О.О.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. вик. Тимофєєв Д.С.			

Дніпро
2020

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Герасимову Максиму Олеговичу*** **академічної групи** ***125-16-3***
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Комплекс засобів захисту на базі механізмів операційних систем сімейства RedHat Enterprise Linux***

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № ____

Розділ	Зміст	Термін виконання
Розділ 1	*Актуальність питання. Аналіз існуючих КЗЗ. Аргументація вибору послуг безпеки. Вибір платформи реалізації КЗЗ. Постановка задачі.*	29.03.2020
Розділ 2	*Аналіз механізмів безпеки. Тестування функціональних послуг. Створення комплексу засобів захисту операційної системи.*	24.05.2020
Розділ 3	*Визначення витрат на створення КЗЗ. Розрахунок експлуатаційних витрат. Оцінка величини збитку у разі реалізації загроз. Загальний ефект від впровадження КЗЗ. Визначення та аналіз показників економічної ефективності.*	14.06.2020

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі: 20.04.2020р.

Дата подання до екзаменаційної комісії: 09.06.2020р.

Прийнято до виконання _____ _____

(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: ___ с., ___ рис., __ табл., __ додатка, __ джерел.

Об’єкт дослідження: операційна система RedHat Enterprise Linux 7.

Предмет дослідження: комплекс засобів захисту операційної системи RedHat Enterprise Linux 7.

Мета дипломної роботи: удосконалення захисту інформації в автоматизованих системах.

Перший розділ кваліфікаційної роботи описує стан питання, типову автоматизовану систему та системи керування доступом; порівнює операційні системи сімейства Windows NT і UNIX та аналізує існуючі рішення щодо захисту інформації в автоматизованих системах.

У спеціальній частині наведено основні послуги безпеки та проаналізовано варіанти їх реалізації в RedHat Enterprise Linux. Виконано тестування послуг безпеки відповідно до нормативних документів із ТЗІ.

В економічному розділі було розраховано витрати на створення комплексу засобів захисту та щорічні експлуатаційні витрати на його підтримку. Також було доведено економічну доцільність створення комплексу.

Практичне значення проекту полягає в підвищенні рівня інформаційної безпеки під час обробки інформації в автоматизованих системах.

КОМПЛЕКС ЗАСОБІВ ЗАХИСТУ, ПОСЛУГИ БЕЗПЕКИ, LINUX, КЕРУВАННЯ ДОСТУПОМ, ОПЕРАЦІЙНІ СИСТЕМИ, АВТОМАТИЗОВАНІ СИСТЕМИ

РЕФЕРАТ

Пояснительная записка: ___ стр., __ рис., ___ табл., __ приложений, __ источников.

Объект исследования: операционная система RedHat Enterprise Linux.

Предмет исследования: комплекс средств защиты операционной системы RedHat Enterprise Linux.

Цель дипломной работы: усовершенствование защиты информации в автоматизированных системах.

Первый раздел квалификационной работы описывает состояние вопроса, типичную автоматизированную систему и системы управления доступом; сравнивает операционные системы семейств Windows NT и UNIX и анализирует существующие решения по защите информации в автоматизированных системах.

Во специальной части приведены основные услуги безопасности и проанализировано варианты их реализации в RedHat Enterprise Linux. Выполнено тестирование услуг в соответствии с нормативными документами ТЗИ.

В экономическом разделе было рассчитано затраты на создание комплекса средств защиты и ежегодные эксплуатационные затраты на его поддержку. Также было доказано экономическую целесообразность создания комплекса.

Практическое значение проекта состоит в повышении уровня информационной безопасности во время обработки информации в автоматизированных системах.

КОМПЛЕКС СРЕДСТВ ЗАЩИТЫ, УСЛУГИ БЕЗОПАСНОСТИ, LINUX, УПРАВЛЕНИЕ ДОСТУПОМ, ОПЕРАЦИОННЫЕ СИСТЕМЫ, АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ

ABSTRACT

Explanatory note: __ p., __ fig., __ tab., __ additions, __ sources.

Object of study: RedHat Enterprise Linux operating system.

Subject of study: RedHat Enterprise Linux operating system`s trusted computer base.

Project objective: improving the level of information security in automated systems.

The first section of qualification project describes the state of the issue, a typical automated system and access control systems; compares Windows NT and UNIX family operating systems and analyzes existing solutions for information security in automated systems.

The special section provides basic security services and analyzes their realization. Security services testing performed according to regulatory documents.

In the economic section, the costs of creation of trusted computer base and annual operating costs of its were calculated. The economic feasibility of creating of trusted computer base was proved.

The practical significance of the project is to increase the level of information security in automated systems.

TRUSTED COMPUTER BASE, SECURITY SERVICES, LINUX, ACCESS CONTROL, OPERATING SYSTEMS, AUTOMATED SYSTEMS

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ДСТУ – державний стандарт України;

ЗУ – закон України;

ІзОД – інформація з обмеженим доступом;

ІС – інформаційна система;

КЗЗ – комплекс засобів захисту;

КСЗІ – комплексна система захисту інформації;

НД ТЗІ – нормативний документ в галузі технічний захист інформації;

ОС – операційна система;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер.

ЗМІСТ

ВСТУП

У сучасному світі процес інформатизації охоплює більшість сфер людської діяльності: соціальну, економічну, освітні, тощо. Інформація стрімко набуває значимості, і це пов’язано з розвитком технологій.

Сьогодні в кожній інформаційній системі циркулює інформація, розголошення якої призведе до збитків. Тому створення заходів захисту інформації є одним з найбільш актуальних питань.

Для запобігання витоку інформації під час її обробки в автоматизованій системі використовують комплекси засобів захисту та операційні системи з засобами захисту. Комплекс засобів захисту забезпечує реалізацію політики безпеки, що регламентує порядок захисту інформації.

Аналіз існуючих трендів операційних систем показує поступовий перехід користувачів автоматизованих систем від пропрієтарних програмних засобів до систем з відкритим початковим кодом. Це зумовило до створення відповідних комплексів засобів захисту з певними послугами безпеки не тільки вбудованих в операційну систему але і сторонніх.

Деякі з операційних систем із відкритим початковим кодом мають базові налаштування механізмів захисту, але не завжди вони відповідають критеріям оцінки захищеності інформації, які вказані у НД ТЗІ 2.5-004-99. Проте це не впливає на створення власних критеріїв оцінки захищеності інформації.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Актуальність питання

У сучасному світі в кожній інформаційній системі (ІС) циркулює інформація, розголошення якої може спричинити значні збитки власнику або розпоряднику інформації.

Інформація обробляється в автоматизованій системі (АС), яка являє собою організаційно-технічну систему – поєднання обчислювальної системи (ОС), фізичного середовища, персоналу та оброблюваної інформації.

Для захисту інформації в АС від несанкціонованого доступу використовуються ОС з комплексом засобів захисту (КЗЗ), що являє собою сукупність програмно-апаратних засобів, що забезпечує реалізацію політики безпеки інформації. Існують різні варіанти реалізації КЗЗ, що побудовані для роботи на базі операційних систем сімейств Windows NT та UNIX.

Метою кваліфікаційної роботи є підвищення рівня захищеності інформації за допомогою створення комплексу засобів захисту на базі захисних механізмів операційних систем сімейства RedHat Enterprise Linux (RHEL).

1.2 Класифікація АС

Згідно з НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» [1], АС поділяються на три класи:

- АС-1 (клас «1) – одномашинний однокористувачевий комплекс, який обробляє інформацію однієї або кількох категорій конфіденційності. Особливості: в кожен момент часу з комплексом може працювати тільки один користувач;
- АС-2 (клас «2») – локалізований багатомашинний багатокористувачевий комплекс, який обробляє інформацію

різних категорій конфіденційності. Особливості: в кожен момент часу з комплексом можуть працювати декілька користувачів з різними повноваженнями, які можуть одночасно виконувати обробку інформації різних категорій конфіденційності;

- АС-3 (клас «3») – розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності. Особливості: передача інформації через незахищене середовище або наявність вузлів, що реалізують різну політику безпеки.

Вимоги до функціонального складу послуг безпеки, що реалізує КЗЗ для кожного з класів АС відрізняються, але базові послуги співпадають.

Для обробки інформації з обмеженим доступом (ІзОД) частіше за все використовуються АС класу «1», оскільки не завжди необхідно виконувати передачу ІзОД через незахищені канали зв'язку. Також вартість створення та обслуговування КСЗІ АС класу «1» набагато нижче.

1.3 Типова АС класу «1»

АС класу «1» найчастіше використовується для обробки інформації, імпорту/експорту на зовнішні носії та друку. Таким чином, до складу прикладного програмного забезпечення (ПЗ) типової АС класу «1» можуть входити:

- офісні пакети (Microsoft Office, LibreOffice);
- ПЗ для обробки графіки (GIMP, AutoCAD);
- засоби розборки (gcc, java);
- ПЗ для перегляду документів (Adobe Acrobat, PDF-viewer);
- бази даних (PostgreSQL, MySQL).

Потенційними загрозами для АС класу «1» є:

- помилки, що виникають при роботі ПЗ, можуть призвести до втрати або пошкодження інформації;
- помилки при введені даних користувачем;

- збої та відмови в роботі апаратного забезпечення;
- встановлення і використання стороннього ПЗ, що не дозволено політикою безпеки;
- встановлення шкідливого ПЗ;
- викрадення носіїв інформації;
- несанкціоноване копіювання інформації на зовнішні носії;
- несанкціоноване копіювання інформації у каталоги, що мають загальний доступ;
- доступ до інформації, яка залишилась в оперативній пам'яті чи запам'ятовуючих пристроях після її видалення;
- розголошення даних автентифікації користувачів;
- несанкціонований доступ до інформації та її модифікація.

1.4 Аналіз існуючих рішень

У «Переліку засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом» («Перелік...») [2] наразі існують операційні системи з засобами захисту та окремі комплекси засобів захисту:

- Комплекс засобів захисту операційної системи Microsoft Windows 10 Professional – ТОВ «Майкрософт Україна». Функціональний профіль: КД-2, КВ-1, КО-1, ЦД-1, ЦА-1, ЦВ-1, ЦО-1, ДР-1, ДЗ-2, ДВ-2, НР-1, НР-2, НИ-1, НК-1, НО-3, НЦ-2, НТ-2, НВ-1. Рівень гарантій Г-2.
- Комплекс засобів захисту програмного забезпечення «Операційна система Січ» – ТОВ «Трайбекс». Функціональний профіль: КД-2, КА-1, КА-2, КО-1, КВ-1, ЦД-1, ЦА-1, ЦА-2, ЦВ-1, ДР-3, ДС-1, ДЗ-2, ДВ-1, НР-2, НИ-2, НИ-3, НК-1, НО-3, НЦ-2, НВ-1. Рівень гарантій Г-3.

- Комплекс засобів захисту програмного забезпечення «Операційна система Ubuntu*Pack 18.04» – ТОВ «УАЛІНУКС». Функціональний профіль: КД-2, КА-1, КА-2, КО-1, КВ-2, ЦД-1, ЦА-1, ЦА-2, ЦВ-2, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-3, НИ-3, НК-1, НО-3, НЦ-2, НТ-3, НВ-1. Рівень гарантій Г-3.
- Засіб технічного захисту інформації від несанкціонованого доступу «Комплекс «Гриф» версії 4» – ТОВ «Інститут комп'ютерних технологій». Функціональний профіль: КА-2, КО-1, КВ-2, ЦА-1, ЦО-1, ЦВ-2, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-3, НИ-3, НК-1, НО-2, НЦ-2, НТ-2. Рівень гарантій Г-4.

1.5 Порівняння операційних систем

Для обробки інформації частіше за все використовують операційні системи сімейств Windows NT та UNIX (GNU/Linux та BSD системи).

Операційні системи сімейства UNIX побудовані на відкритому коді, який проходить багато перевірок як розробниками, так і співтовариством користувачів. Сімейство Windows NT – розробка з закритим початковим кодом.

У Windows користувачу зазвичай автоматично надається високий рівень повноважень. UNIX-системи мають чітке розмежування повноважень: користувачу надається найнижчий рівень доступу, а наявність облікового запису адміністратора – обов'язкова.

Згідно з даними NetMarketShare [3], станом на травень 2020 року операційні системи сімейства GNU/Linux встановлені лише на 3,17% персональних комп'ютерів. У той же час, сімейство операційних систем Windows NT займає 86,69% ринку (рис. 1.1). Через свою поширеність та недосконаліть підходів до безпеки інформації, Windows NT стає ціллю для різноманітних атак.

Згідно з базою даних загальновідомих вразливостей Common Vulnerabilities and Exposures (CVE) організації MITRE, у 2019-му році в

продукті Microsoft Windows 10 було знайдено 357 вразливості [4], а у RedHat Enterprise Linux (RHEL) – 52 [5]. Графіки кількості знайдених вразливостей за рік у системах Windows 10 та RHEL наведено в Додатку Д та Додатку Е відповідно.

Рис. 1.1 – Ринок операційних систем персональних комп'ютерів

У «Переліку...» представлено лише кілька рішень на базі операційних систем GNU/Linux, які не використовують на повну потенціал цих систем та їх захисних механізмів. RedHat Enterprise Linux з системою керування доступом SELinux здатна забезпечити більш високий рівень захисту та надійності.

1.6 Аналіз профілів захищеності КЗЗ

В АС класу «1» з підвищеними вимогами до забезпечення конфіденційності, цілісності та доступності інформації, в першу чергу приділяється увага адміністративному керуванню доступом. Тому профіль захищеності повинен мати послуги «Адміністративна конфіденційність» (КА) та «Адміністративна цілісність» (ЦА).

Послуга «Цілісність комплексу засобів захисту» (НЦ) є необхідною умовою абсолютно для всіх рівнів інших послуг.

Для послуг КА та ЦА необхідною умовою будуть послуги «Розподіл обов'язків» (НО) та «Ідентифікація і автентифікація» (НИ), а для високих рівнів реалізації цих послуг – також і «Повторне використання об'єктів» (КО).

У разі відмови або переривання обслуговування, система повинна мати можливість повернутися в захищений стан. Для цього необхідною умовою буде послуга «Відновлення після збоїв» (ДВ).

Для контролю небезпечних подій, профіль має включати послугу НР «Реєстрація».

Також необхідно гарантувати користувачу безпосередню взаємодію з комп'ютерною системою та правильність її функціонування. Для цього в профіль повинен включати послугу «Самотестування» (НТ) та «Достовірний канал» (НК).

1.7 Системи керування доступом

Традиційно, операційні системи сімейства UNIX використовують модель безпеки засновану на вибірковому керуванні доступом (Discretionary Access Control, DAC) [6] – кожен користувач контролює, які користувачі можуть отримати доступ до його файлів. Тобто користувачі можуть надавати доступ не залучаючи до цього адміністратора [7].

В UNIX-реалізації моделі DAC доступи до файлів описані в спрощеній формі списків контролю доступу (Access Control List, ACL). У той час, коли повна форма ACL описує кожен об'єкт окремо та вказує який користувач може виконувати які дії (наприклад, користувач alice має право на читання, а користувач bob має право на запис), UNIX ACL визначає узагальнені правила для трьох типів суб'єктів [7]:

- користувач-власник;
- група-власник;
- інші користувачі.

Розвитком DAC стала модель керування доступом на основі ролей (Role Based Access Control, RBAC). Складається з трьох відношень [8]:

- користувач-роль – зіставлення користувача і відведеної йому ролі (ролей);
- роль-дозвіл – дія, дозволеній даній ролі;

- роль-роль – спадкова ієрархія ролей.

RBAC відрізняється від ACL тим, що може надавати привілеї на складні операції (наприклад, заповнення медичних карток пацієнтів мед. працівником), а не тільки на операції з низькорівневими об’єктами (наприклад, запис даних до директорії).

Для забезпечення більш високого рівню захисту, в деяких UNIX системах опціонально або за замовченням використовується модель примусового керування доступом (Mandatory Access Control, MAC) [7]. В цій моделі політика безпеки централізовано керується адміністраторами, а розмежування доступу засновується на мітках конфіденційності об’єктів та наявності допуску у суб’єктів.

1.8 Керування доступом в ОС GNU/Linux

В дистрибутивах сімейства RedHat Enterprise Linux та у деяких інших сімействах за замовчанням використовується реалізація системи примусового контролю доступу з покращеним рівнем безпеки (Security-Enhanced Linux, SELinux) [9].

SELinux – це проект з відкритим вихідним кодом, який був розроблений Агентством національної безпеки США.

Поряд з SELinux, ядро Linux підтримує різні моделі, такі як AppArmor, Smack та TOMOYO. Підтримку реалізовано фреймворком Linux Security Modules (LSM). Виклик функції LSM відбувається тільки якщо він пройшов перевірку DAC [10]. Тому SELinux працює спільно з вибірковим керуванням доступом.

SELinux реалізує політику безпеки, яку адміністратор налаштував самостійно або використав одну з вже існуючих:

- цільова (Targeted) – стандартна політика, контроль застосовується тільки до певних (цільових) процесів. Інші об’єкти не обмежуються;

- політика багатокатегорійної безпеки (Multicategory security, MCS) – політика посиленої безпеки, при якій усім об’єктам системи присвоюються категорії (наприклад, «Бухгалтерія» або «Конфіденційно», тощо). Тільки користувачі з доступом до відповідної категорії можуть отримати доступ до інформації. В даній політиці категорії не ієрархічні;
- політика багаторівневої безпеки (Multilevel security, MLS) – політика, яка використовує модель примусового контролю доступу Бела-ЛаПадули. Кожному суб’єкту надається рівень доступу, який повинен відповідати рівню конфіденційності об’єкту. На відміну від політики MCS, рівні конфіденційності MLS ієрархічні. Використовується принцип «no read up, no write down» (заборона читання вгору, заборона запису вниз). Ця модель унеможливлює утворення потоків інформації від суб’єктів з вищим рівнем доступу до суб’єктів з нижчим рівнем доступу.

SELinux може визначати права доступу на основі:

- ролі (рис. 1.2);
- користувача SELinux (рис. 1.3);
- збігу типів суб’єкта (вихідний домен – користувач і/або процес) та об’єкта (цільовий домен – файл, каталог, мережевий порт, тощо) (Type Enforcement) (рис. 1.4);
- позначок категорій (рис. 1.5).

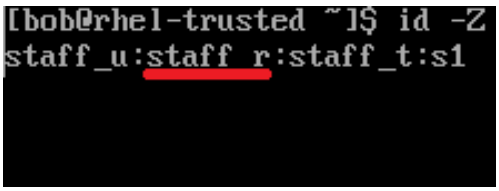


Рис. 1.2 – Роль в контексті SELinux

SELinux має 14 визначених ролей [10], які відображені в таблиці 1.1:

Таблиця 1.1 – Ролі SELinux

№	Роль SELinux	Описання
1	auditadm_r	Роль адміністратора аудиту безпеки. Надає доступ до лог-файлів, які зберігають інформацію виключно про події безпеки.
2	dbadm_r	Роль адміністратора бази даних. Надає доступ до керування та конфігурації встановлених баз даних (MySQL, PostgreSQL та інші).
3	guest_r	Гостьова роль. Надає найбільш обмежений доступ до консолі.
4	user_r	Роль звичайного користувача. Надає повноцінний доступ до системи та можливість використовувати додатки для кінцевого користувача. Користувачі з даною роллю не можуть виконувати дію від імені іншого користувача (наприклад, адміністратора).
5	staff_r	Роль звичайного користувача. Має ті ж самі властивості, що й роль user_r, проте користувач з даною роллю може виконувати дію від імені іншого користувача (наприклад, адміністратора).
6	logadm_r	Роль адміністратора аудиту системи. Надає доступ до лог-файлів, які зберігають інформацію виключно про системні події.
7	object_r	Роль об’єкту (інформації). Оскільки SELinux вимагає наявності контексту у всіх суб’єктів і об’єктів системи, то роль object_r було створено виключно для файлів.
8	secadm_r	Роль адміністратора безпеки. Надає контроль над SELinux та іншими засобами безпеки. Користувач з даною роллю може змінювати політику SELinux.
9	sysadm_r	Роль адміністратора системи. Надає контроль над системними процесами і конфігурацією операційної системи. Проте користувач з даною роллю не має доступу до механізмів безпеки та більшості додатків для кінцевого користувача.
10	system_r	Роль, яку відведено для системних процесів та демонів. Не відноситься до додатків для кінцевого користувача та адміністративних об’єктів.
12	xguest_r	Гостьова роль. Надає найбільш обмежений доступ до графічної оболонки.
13	nx_server_r	Роль, яку відведено для серверу віддаленого доступу NX.
14	unconfined_r	Роль користувача з повним набором повноважень. Дана роль не обмежується SELinux.

Роль SELinux – це контекст, який призначається усім суб’єктам та об’єктам. Кожен користувач SELinux має одну або більше ролей. Наприклад (табл. 1.2):

Таблиця 1.2 – Користувачі SELinux та їх ролі SELinux

Користувач SELinux	Роль SELinux
guest_u	guest_r
root	auditadm_r, secadm_r, staff_r, sysadm_r
staff_u	staff_r, sysadm_r, user_r
sysadm_u	sysadm_r
system_u	system_r
user_u	user_r
xguest_u	xguest_r

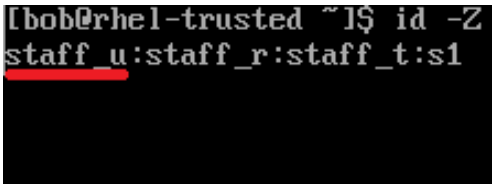


Рис. 1.3 – Користувач в контексті SELinux

SELinux має 7 визначених користувачів. Ці користувачі зазначені в таблиці 1.3:

Таблиця 1.3 – Користувачі SELinux

№	Користувач SELinux	Описання
1	sysadm_u	Користувач, який має загальну роль системного адміністратора. Основна роль – sysadm_r
2	system_u	Користувач-системний процес. Основна роль – system_r
3	xguest_u	Користувач, який має загальну роль гостя. Основна роль – xguest_r
4	root	Суперкористувач. Основна роль – sysadm_r
5	guest_u	Користувач, який має загальну роль гостя. Основна роль – guest_r
6	staff_u	Непривілейований користувач адміністратора. Цей контекст використовується адміністратором для звичайних дій. При виконанні адміністративних обов’язків контекст змінюється на sysadm_u (або інший). Основна роль – staff_r
7	user_u	Непривілейований користувач. Основна роль – user_r

Користувач SELinux – це контекст, якому призначаються ролі. Користувачі системи зіставляються з користувачами SELinux. Наприклад (табл. 1.4):

Таблиця 1.4 – Співставлення користувачів системи

Користувач системи	Користувач SELinux
root	sysadm_u
alice	staff_u
bob	staff_u
john	user_u

SELinux також оперує контекстом користувача. Кожен користувач може отримати тільки визначені політикою ролі. Адміністратор має можливість створити нового користувача SELinux та надати йому бажані ролі.

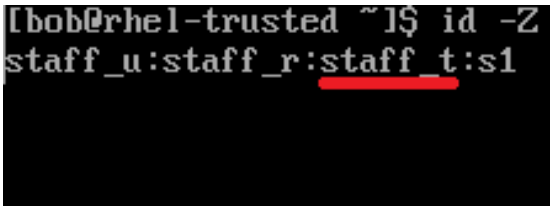


Рис. 1.4 – Тип в контексті SELinux

SELinux має 3605 визначених типів. Доступ до домену можливий за умови відповідного правила політики. Адміністратор має можливість створити новий тип та визначити нові правила як для нових, так і для вже існуючих типів.

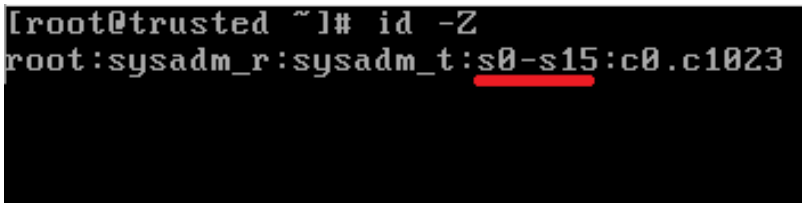


Рис. 1.5 – Позначка конфіденційності в контексті SELinux

При використання політики MLS, SELinux визначає 16 рівнів конфіденційності (s0-s15). Також як і в політиці MCS, в MLS використовуються категорії (1024 категорії для кожного з рівнів конфіденційності). Адміністратор має можливість змінити кількість рівнів

конфіденційності та призначити їм імена (наприклад, рівень s10 «Конфіденційно»).

1.9 Постановка задачі

Беручи до уваги вищезазначені пункти, задля доцільної розробки КЗЗ необхідно виконати аналіз та тестування механізмів безпеки операційної системи сімейства RHEL згідно з НД ТЗІ 2.7-009-09 [11] та реалізувати послуги: КА, КО, КВ, ЦА, ЦО, ЦВ, ДР, ДЗ, ДВ, НР, НИ, НК, НО, НЦ, НТ [12].

Виконати техніко-економічне обґрунтування доцільності створення комплексу засобів захисту на базі RHEL із застосуванням SELinux.

1.10 Висновки

У цьому розділ розглянуто та проаналізовано наступні питання:

- актуальність розробки КЗЗ;
- класифікацію АС;
- типову АС класу «1»;
- порівняння операційних систем;
- аналіз профілів захищеності КЗЗ;
- системи керування доступом;
- керування доступом в GNU/Linux;
- постановку задачі.

Таким чином визначено доцільність створення КЗЗ для захисту інформації в автоматизованих системах класу «1» на основі механізмів безпеки операційних систем сімейства RHEL.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

Для послуг безпеки, що зазначені у Розділі 1 цієї роботи, необхідно виконати налаштування та перевірку реалізації цих послуг у відповідності до НД ТЗІ 2.5-004 та НД ТЗІ 2.7-009

2.1 Адміністративна конфіденційність

Реалізація послуги забезпечує адміністратору можливість керувати потоками інформації від захищених об’єктів до користувачів. Політика послуги поширюється на:

- користувачів усіх категорій;
- процеси;
- інформаційні об’єкти;
- програмні засобі;
- зовнішні та внутрішні носії інформації.

Послугу реалізує система мандатного керування доступом SELinux з використанням політики MLS на рівні КА-3 «Повна адміністративна конфіденційність».

Керування доступом до об’єктів виконується на підставі атрибутів об’єкту та користувача. Атрибути призначаються при створенні об’єктів/користувачів.

Виконаємо перевірку реалізації послуги безпеки КА:

В стандартній конфігурації, політика MLS має такі рівні конфіденційності:

- s0 – системна низька;
- s1 – відкрита інформація;
- s2 – інформація з обмеженим доступом;
- s15 – системна висока.

Створимо користувача SELinux з допуском до ІзОД:

#: semanage user -a -L s2 -r s0-s2 -R user_r secret_u

Створимо користувача *john* з допуском до ІзОД:

#: useradd -m -G users -Z secret_u john

Маємо директорії */data/Unclassified* з рівнем конфіденційності s1 та */data/Secret* з рівнем конфіденційності s2 (рис. 2.1):

```
[root@rhel-trusted ~]# ls -Z /data/
drwxr-xr-x. root root root:object_r:user_home_dir_t:s2 Secret
drwxr-xr-x. root root root:object_r:user_home_dir_t:s1 Unclassified
```

Рис. 2.1 – Директорії

Надамо користувачеві *john* доступ до директорії */data/Secret* з правами на читання:

#: setfacl -m "u:john:r" /data/Secret

Тепер користувач *john* може читати інформацію в директорії */data/Secret* (рис. 2.2):

```
[john@rhel-trusted ~]$ cat /data/Secret/confidential-information.txt
Confidential text
```

Рис. 2.2 – Читання файлу confidential-information.txt користувачем john

Також якщо користувачеві *john* надати доступ до директорії */data/Unclassified*, він зможе читати дані в цій директорії, тому що має рівень конфіденційності вищий за рівень директорії */data/Unclassified* (рис. 2.3):

```
[john@rhel-trusted ~]$ cat /data/Unclassified/unclassified-information.txt
Unclassified text
```

Рис. 2.3 – Читання файлу unclassified-information.txt користувачем john

Створимо користувача SELinux без допуску до ІзОД:

#: semanage user -a -L s1 -r s0-s1 -R user_r unclassified_u

Створимо користувача *alice* без допуску до ІзОД:

#: useradd -m -G users -Z unclassified_u alice

Надамо користувачеві *alice* доступ до директорії */data/Unclassified* з правами на читання:

#: setfacl -m "u:alice:r" /data/Unclassified

Тепер користувач *alice* може читати інформацію в директорії */data/Unclassified* (рис. 2.4):

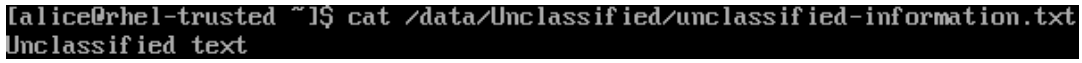


Рис. 2.4 – Читання файлу unclassified-information.txt користувачем alice

Надамо користувачеві *alice* доступ до директорії */data/Secret* з правами на читання:

#: setfacl -m "u:alice:r" /data/Secret

Користувач *alice* намагається отримати доступ до файлу *confidential-information.txt* в директорії */data/Secret* (рис. 2.5):

Рис. 2.5 – Спроба читання файлу confidential-information.txt користувачем alice

І хоча користувач *alice* має доступ до файлів в директорії */data/Secret*, він отримує відмову у доступі на підставі контексту SELinux – користувач не має необхідного рівню допуску.

2.2 Повторне використання об'єктів

Реалізація послуги унеможливлює отримання залишкової інформації з розділюваних об'єктів. Політика послуги поширюється на:

- сторіни оперативної пам'яті;
- зовнішні та внутрішні носії інформації.

Операційна система реалізує очищення сторінок оперативної пам'яті при їх звільненні наступними опціями ядра Linux:

CONFIG_DEBUG_PAGEALLOC=n

CONFIG_PAGE_POISONING=y

CONFIG_PAGE_POISONING_NO_SANITY=n

CONFIG_PAGE_POISONING_ZERO=y

CONFIG_SLUB_DEBUG=y

Очищення увімкнено на етапі завантаження системи такими параметрами ядра: page_poisoning=on, slub_debug=PF.

Видалення інформації, яка зберігається на зовнішніх та внутрішніх носіях, реалізовано за допомогою багаторазового перезапису даних ПЗ shred.

Виконаємо перевірку реалізації послуги безпеки КО для оперативної пам’яті:

Вбудована підсистема тестування ядра Linux Kernel Dump Test Module (lkdtm) дозволяє проводити тести на читання залишкової інформації з сторінок оперативної пам’яті після їх звільнення.

Результати тесту для системи без очищення сторінок пам’яті відображені на рис. 2.6:

```
[  131.984376] lkdtm: Performing direct entry READ_AFTER_FREE
[  131.984379] lkdtm: Value in memory before free: 12345678
[  131.984381] lkdtm: Attempting bad read from freed memory
[  131.984381] lkdtm: Memory correctly poisoned (0)
```

Рис. 2.6 – Тест №1 «Очищення сторінок пам’яті»

Результатом тесту є «0», тобто негативним. Значення «12345678» було знайдено в звільненій сторінці пам’яті – отже очищення сторінки не відбулось.

Результати тесту для системи з очищенням сторінок пам’яті відображені на рис. 2.7:

```
[   61.805998] lkdtm: Performing direct entry READ_AFTER_FREE
[   61.806005] lkdtm: Value in memory before free: 12345678
[   61.806006] lkdtm: Attempting bad read from freed memory
[   61.806006] lkdtm: Memory correctly poisoned (6b6b6b6b)
```

Рис. 2.7 – Тест №2 «Очищення сторінок пам’яті»

Як видно з рис. 2.7, результат «6b» – позитивний. Значення «12345678» не було знайдено в звільненій пам’яті – сторіни очищено.

Виконаємо перевірку реалізації послуги безпеки КО для жорсткого диску АС:

Маємо файл *test,* який має у своєму складі інформацію (рис. 2.8):

```
[root@trusted ~]# hexdump -C test
00000000  46 4f 52 20 54 45 53 54  49 4e 47 20 50 55 52 50  |FOR TESTING PURP|
00000010  4f 53 45 53 20 4f 4e 4c  59 0a                    |OSES ONLY.|
0000001a
```

Рис. 2.8 – Представлення файлу test в пам’яті внутрішнього накопичувача

Для видалення файлу необхідно виконати команду:

#: shred -n 10 -z test

де ключ «n» – це кількість повторів перезапису пам’яті, «z» – запис нулів при останньому повторі перезапису пам’яті.

Результат видалення відображений на рис. 2.9:

```
[root@trusted ~]# hexdump -C test
00000000  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00001000
```

Рис. 2.9 – Зміст файлу test після його видалення з пам’яті внутрішнього накопичувача

2.3 Конфіденційність при обміні

Реалізація послуги забезпечує захист інформації, яка зберігається на внутрішніх чи зовнішніх носіях, від несанкціонованого ознайомлення у разі вилучення носіїв з-під контролю засобів захисту. Політика послуги поширюється на:

- користувачів усіх категорій;
- логічні диски на внутрішніх та зовнішніх носіях.

Послугу реалізовано інфраструктурою ядра Linux Device-mapper (dm-crypt) на рівні КВ-2 «Базова конфіденційність при обміні».

Ця інфраструктура забезпечує «прозоре» шифрування блокових пристроїв завдяки створенню віртуальних рівнів блокових пристроїв. Користувач має можливість обрати для шифрування один із симетричних шифрів (AES, ANUBIS, TWOFISH, ARC4 та інш.), режим шифрування, ключ та вектор ініціалізації.

З використанням стандартних опцій, dm-crypt шифрує пристрій з такими параметрами (рис. 2.10):

- шифр – AES-XTS-PLAIN64;
- розмір ключа – 256 біт;
- хеш алгоритм для створення ключа – SHA256.

Рис. 2.10 – Параметри шифрованого блокового пристрою sda5

Зашифрований блоковий пристрій на внутрішньому носії може бути розшифровано при:

- ініціалізації системи (рис. 2.11);
- штатному режимі роботи системи (рис. 2.12).

Рис. 2.11 – Вікно вводу паролю для розшифрування при ініціалізації системи

Рис. 2.12 – Розшифрування блокового пристрою при штатному режимі роботи системи

Для шифрування може бути використано пароль або ключ-файл, який може зберігатися на жорсткому диску АС або на зовнішніх носіях.

2.4 Адміністративна цілісність

Реалізація послуги забезпечує адміністратору можливість керувати потоками інформації процесів, ініційованих користувачами, до захищених об’єктів. Політика послуги поширюється на:

- користувачів усіх категорій;
- процеси;
- інформаційні об’єкти;
- програмні засоби;

- зовнішні та внутрішні накопичувачі інформації.

В повній аналогії з адміністративною конфіденційністю, керування доступом до об'єктів виконується на підставі атрибутів користувача та об'єкту. Атрибути призначаються при створенні об'єктів/користувачів.

Послугу реалізує система мандатного керування доступом SELinux з використанням політики MLS на рівні ЦА-3 «Повна адміністративна цілісність».

Виконаємо перевірку реалізації послуги безпеки ЦА:

Створимо користувача SELinux з допуском до ІзОД:

#: semanage user -a -L s2 -r s0-s2 -R user_r secret_u

Створимо користувача *john* з допуском до ІзОД:

#: useradd -m -G users -Z secret_u john

Маємо директорії */data/Unclassified* з рівнем конфіденційності s1 та */data/Secret* з рівнем конфіденційності s2 (рис. 2.13):

```
[root@rhel-trusted ~]# ls -Z /data/
drwxr-xr-x. root root root:object_r:user_home_dir_t:s2 Secret
drwxr-xr-x. root root root:object_r:user_home_dir_t:s1 Unclassified
```

Рис. 2.13 – Директорії

Надамо користувачеві *john* доступ до директорії */data/Secret* з правами на запис:

#: setfacl -m "u:john:w" /data/Secret

Тепер користувач *john* може редагувати та записувати дані в директорії */data/Secret* (рис. 2.14):

```
[john@rhel-trusted ~]$ echo "Secret information" > /data/Secret/secret-info.txt
[john@rhel-trusted ~]$ cat /data/Secret/secret-info.txt
Secret information
```

Рис. 2.14 – Запис даних в файл secret-info.txt користувачем john

Надамо користувачеві *john* доступ до директорії */data/Unclassified* з правами на запис:

#: setfacl -m "u:john:w" /data/Unclassified

Користувач *john* намагається скопіювати файл з ІзОД *secret-info.txt* із директорії */data/Secret* в директорію */data/Unclassified* (рис. 2.15):

```
[john@rhel-trusted ~]$ cp /data/Secret/secret-info.txt /data/Unclassified/
cp: cannot create regular file '/data/Unclassified/secret-info.txt': Permission denied
```

Рис. 2.15 – Спроба копіювання файлу з ІзОД користувачем john

І хоча користувач *john* має доступ до файлів в директорії */data/Unclassified*, він отримує помилку *«Відказано в доступі»* на підставі контексту SELinux – файл не може бути скопійовано в директорію з міткою конфіденційності нижче, ніж у файлу.

2.5 Відкат

Реалізація послуги забезпечує можливість відміни послідовності операцій над захищеним об’єктом. Політика послуги поширюється на послідовність операцій, які виконуються при встановленні захисту на файл або каталог.

Послугу реалізує ПЗ системи SELinux на рівні ЦО-1 «Обмежений відкат».

Спеціалізоване ПЗ «restorecon» дозволяє відновити контекст безпеки файлу або директорії. Оригінальний контекст об’єкту та усі зміни зберігаються в директорії */etc/selinux/<policy>/contexts/*. Усі зміні контексту та відміна операцій зберігаються в журналі аудиту.

2.6 Цілісність при обміні

Реалізація послуги забезпечує виявлення фактів несанкціонованої модифікації інформації, яка зберігається на внутрішніх чи зовнішніх носіях, у разі вилучення носіїв з-під контролю засобів захисту. Політика послуги поширюється на:

- користувачів усіх категорій;
- логічні диски на внутрішніх та зовнішніх носіях.

Послугу реалізовано хостовою системою виявлення атак (Host-Based Intrusion Detection System, HIDS) AIDE на рівні ЦВ-2 «Базова цілісність при обміні».

AIDE використовується для моніторингу змін в файлових системах внутрішніх та зовнішніх носіїв. Гнучка система конфігураційних файлів AIDE дозволяє проводити перевірку окремих логічних дисків, директорій чи файлів.

Виконаємо перевірку реалізації послуги безпеки ЦВ:

Поточна конфігурація AIDE відстежує зміни у внутрішньому носії, який змонтовано в */data*, та у зовнішньому USB накопичувачі, який змонтовано в */usb*. Первинна ініціалізація бази даних контрольних сум за поданою конфігурацією:

#: aide –init –config=aide.conf

Перевірка цілісності даних в директоріях */data* та */usb* після створення, зміни та видалення окремих файлів (рис. 2.16):

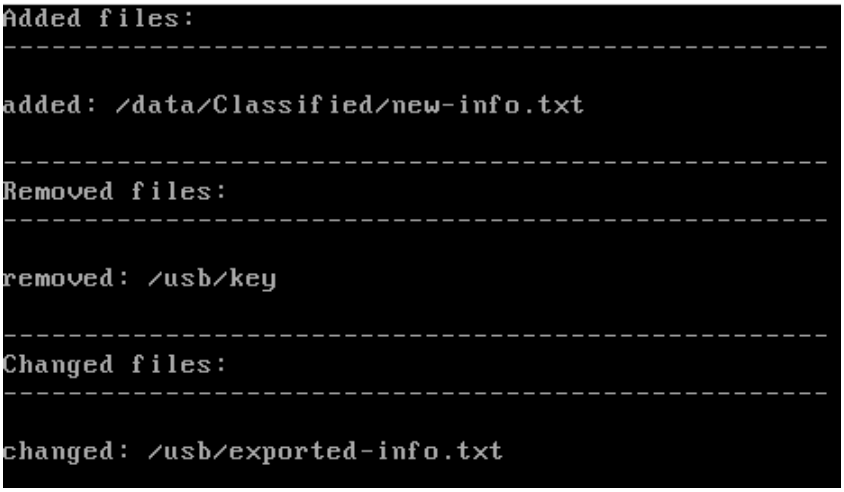


Рис. 2.16 – Зміни в директоріях /data та /usb

2.7 Використання ресурсів

Реалізація послуги унеможливлює захоплення користувачами надмірного об’єму ресурсів. Політика послуги поширюється на:

- користувачів усіх категорій;
- дисковий простір внутрішніх носіїв, що зберігають створені користувачами захищені інформаційні об’єкти.

Послугу реалізовано файловою системою XFS на рівні ДР-1 «Квоти».

Адміністратор має можливість встановити максимально допустимий розмір дискового простору для кожного користувача окремо і/або групи користувачів.

Виконаємо перевірку реалізації послуги безпеки ДР:

Встановимо ліміт на використання дискового простору для користувача *john* в 2 ГБ:

#: xfs_quota limit bsoft=1g bhard=2g john

Звіт по встановленим лімітам файлової системи відображено на рис. 2.17:

```
xfs_quota> report -h -u
User quota on /storage (/dev/sda5)
                        Blocks
User ID      Used   Soft   Hard Warn/Grace
---------- --------------------------------
root            0      0      0  00 [------]
john            0     1G     2G  00 [------]
```

Рис. 2.17 – Ліміти, встановлені для користувачів

Користувач *john* намагається створити файл розміром 2 ГБ, що ілюструє рис. 2.18:

```
[john@trusted storage]$ fallocate -l 2G test
fallocate: fallocate failed: Disk quota exceeded
[john@trusted storage]$
```

Рис. 2.18 – Спроба користувача john створити файл

Завдяки контролю займаного користувачами дискового простору, користувач *john* отримує помилку «Квоту на дисковий простір вичерпано».

2.8 Гаряча заміна

Реалізація послуги забезпечує можливість використання системи після заміни окремих компонентів. Політика послуги поширюється на програмне забезпечення.

Послугу реалізовано менеджером пакетів ПЗ YUM на рівні ДЗ-1 «Модернізація».

Адміністратор має можливість виконувати модернізацію системи без повторної інсталяції чи налаштування.

2.9 Відновлення після збоїв

Реалізація послуги забезпечує повернення системи у захищений стан у разі відказу або переривання обслуговування. Політика послуги поширюється на:

- програмне забезпечення;
- БД контрольних сум виконуваних файлів.

Послугу реалізовано ядром системи на рівні ДВ-1 «Ручне відновлення».

У разі відмови ПЗ системи або порушення цілісності БД контрольних сум система переходить у стан, в якому неможлива обробка ІзОД. Повернути систему до нормального функціонування може тільки системний адміністратор, працездатність ПЗ з копії або відновивши цілісність БД.

2.10 Реєстрація

Реалізація послуги забезпечує контроль подій в системі. Політика послуги поширюється на:

- користувачів усіх категорій;
- інформаційні ресурси;
- системне та прикладне ПЗ.

Послугу реалізовано службою аудиту системи auditd на рівні НР-4 «Детальна реєстрація».

Служба забезпечує реєстрацію та аналіз таких подій:

- вхід/вихід (або спроби входу) в/із системи (рис. 2.19-21);
- реєстрація/видалення облікових записів (рис. 2.22);
- порушення встановлених правил доступу (рис. 2.23);
- зміна даних автентифікації (рис. 2.24);
- встановлення/зміна прав доступу до ресурсів (рис. 2.25);

- доступ та виконання операцій над захищеними об’єктами (рис. 2.26);
- системні події (рис. 2.27-28);

```
[root@trusted ~]# tail -n 3 /var/log/secure
May 15 12:46:52 trusted login: pam_unix(login:session): session opened for user
john by LOGIN(uid=0)
May 15 12:46:52 trusted login: LOGIN ON tty2 BY john
May 15 12:48:44 trusted login: pam_unix(login:session): session closed for user
john
```

Рис. 2.19 – Вхід та вихід користувача john в/із системи

```
[root@trusted ~]# tail -n 3 /var/log/secure
May 15 12:51:24 trusted unix_chkpwd[1855]: password check failed for user (john)
May 15 12:51:24 trusted login: pam_unix(login:auth): authentication failure; log
name=LOGIN uid=0 euid=0 tty=tty2 ruser= rhost=  user=john
May 15 12:51:26 trusted login: FAILED LOGIN 1 FROM tty2 FOR john, Authentication
 failure
```

Рис. 2.20 – Невдала спроба входу в систему користувача john

```
[root@trusted ~]# ausearch -m USER_LOGIN -ts 12:46
----
time->Fri May 15 12:46:52 2020
type=USER_LOGIN msg=audit(1589536012.460:187): pid=1820 uid=0 auid=1000 ses=5 su
bj=system_u:system_r:local_login_t:s0-s15:c0.c1023 msg='op=login id=1000 exe="/u
sr/bin/login" hostname=trusted.local addr=? terminal=tty2 res=success'
----
time->Fri May 15 12:51:26 2020
type=USER_LOGIN msg=audit(1589536286.468:195): pid=1849 uid=0 auid=4294967295 se
s=4294967295 subj=system_u:system_r:local_login_t:s0-s15:c0.c1023 msg='op=login
id=1000 exe="/usr/bin/login" hostname=trusted.local addr=? terminal=tty2 res=fai
led'
----
time->Fri May 15 12:55:54 2020
type=USER_LOGIN msg=audit(1589536554.493:207): pid=1861 uid=0 auid=1000 ses=6 su
bj=system_u:system_r:local_login_t:s0-s15:c0.c1023 msg='op=login id=1000 exe="/u
sr/bin/login" hostname=trusted.local addr=? terminal=tty2 res=success'
```

Рис. 2.21 – Аналіз події «USER_LOGIN» з позначкою часу 12:46 та вище

```
[root@trusted ~]# ausearch -m USER_LOGIN -ts 12:46
----
time->Fri May 15 12:46:52 2020
type=USER_LOGIN msg=audit(1589536012.460:187): pid=1820 uid=0 auid=1000 ses=5 su
bj=system_u:system_r:local_login_t:s0-s15:c0.c1023 msg='op=login id=1000 exe="/u
sr/bin/login" hostname=trusted.local addr=? terminal=tty2 res=success'
----
time->Fri May 15 12:51:26 2020
type=USER_LOGIN msg=audit(1589536286.468:195): pid=1849 uid=0 auid=4294967295 se
s=4294967295 subj=system_u:system_r:local_login_t:s0-s15:c0.c1023 msg='op=login
id=1000 exe="/usr/bin/login" hostname=trusted.local addr=? terminal=tty2 res=fai
led'
----
time->Fri May 15 12:55:54 2020
type=USER_LOGIN msg=audit(1589536554.493:207): pid=1861 uid=0 auid=1000 ses=6 su
bj=system_u:system_r:local_login_t:s0-s15:c0.c1023 msg='op=login id=1000 exe="/u
sr/bin/login" hostname=trusted.local addr=? terminal=tty2 res=success'
```

Рис. 2.22 – Створення користувачем root облікового запису alice

```
type=PROCTITLE msg=audit(05/16/2020 12:38:41.941:160) : proctitle=nano /data/Secret/secr
type=SYSCALL msg=audit(05/16/2020 12:38:41.941:160) : arch=x86_64 syscall=open success=no exit=EACCE
S(Permission denied) a0=0xf11b40 a1=O_WRONLY|O_CREAT|O_TRUNC a2=0666 a3=0x7ffc23bc2b20 items=0 ppid=
1648 pid=1738 auid=alice uid=alice gid=alice euid=alice suid=alice fsuid=alice egid=alice sgid=alice
 fsgid=alice tty=tty2 ses=2 comm=nano exe=/usr/bin/nano subj=user_u:user_r:user_t:s0 key=(null)
type=AVC msg=audit(05/16/2020 12:38:41.941:160) : avc:  denied  { search } for  pid=1738 comm=nano n
ame=Secret dev="dm-2" ino=67 scontext=user_u:user_r:user_t:s0 tcontext=root:object_r:user_home_dir_t
:s2 tclass=dir permissive=0
```

Рис. 2.23 – Спроба користувача alice записати дані в директорії, до якої він не має доступу

```
[root@rhel-trusted ~]# ausearch --start recent -m USER_CHAUTHTOK -i
----
type=USER_CHAUTHTOK msg=audit(05/16/2020 12:49:38.183:181) : pid=1762 uid=alice auid=alice ses=2 sub
j=user_u:user_r:passwd_t:s0 msg='op=PAM:chauthtok grantors=pam_pwquality,pam_unix acct=alice exe=/us
r/bin/passwd hostname=rhel-trusted addr=? terminal=tty2 res=success'
[root@rhel-trusted ~]# _
```

Рис. 2.24 – Зміна паролю користувача alice

```
type=PROCTITLE msg=audit(05/18/2020 13:23:38.777:166) : proctitle=setfacl -m u:b
ob:rwx /data/Classified/info.txt
type=PATH msg=audit(05/18/2020 13:23:38.777:166) : item=0 name=/data/Classified/
info.txt inode=131077 dev=08:03 mode=file,674 ouid=root ogid=root rdev=00:00 obj
=root:object_r:default_t:s0 objtype=NORMAL cap_fp=none cap_fi=none cap_fe=0 cap_
fver=0
type=CWD msg=audit(05/18/2020 13:23:38.777:166) :  cwd=/root
type=SYSCALL msg=audit(05/18/2020 13:23:38.777:166) : arch=x86_64 syscall=getxat
tr success=yes exit=44 a0=0x7ffe5c58a870 a1=0x7fcc4b4dae2f a2=0x7ffe5c58a4a0 a3=
0x84 items=1 ppid=1374 pid=1895 auid=root uid=root gid=root euid=root suid=root
fsuid=root egid=root sgid=root fsgid=root tty=tty1 ses=1 comm=setfacl exe=/usr/b
in/setfacl subj=root:sysadm_r:sysadm_t:s0-s15:c0.c1023 key=info-mon
```

Рис. 2.25 – Надання доступу до файлу info.txt користувачеві bob

```
type=PROCTITLE msg=audit(05/18/2020 13:37:05.212:228) : proctitle=nano /data/Unc
lassified/info.txt
type=PATH msg=audit(05/18/2020 13:37:05.212:228) : item=1 name=/data/Unclassifie
d/info.txt inode=131078 dev=08:03 mode=file,664 ouid=john ogid=john rdev=00:00 o
bj=classified_u:object_r:default_t:s2 objtype=NORMAL cap_fp=none cap_fi=none cap
_fe=0 cap_fver=0
type=PATH msg=audit(05/18/2020 13:37:05.212:228) : item=0 name=/data/Unclassifie
d/ inode=131075 dev=08:03 mode=dir,775 ouid=root ogid=root rdev=00:00 obj=root:o
bject_r:default_t:s0 objtype=PARENT cap_fp=none cap_fi=none cap_fe=0 cap_fver=0
type=CWD msg=audit(05/18/2020 13:37:05.212:228) :  cwd=/home/john
type=SYSCALL msg=audit(05/18/2020 13:37:05.212:228) : arch=x86_64 syscall=open s
uccess=yes exit=3 a0=0x23d4940 a1=O_WRONLY|O_CREAT|O_TRUNC a2=0666 a3=0x7fff959a
f260 items=2 ppid=1951 pid=1981 auid=john uid=john gid=john euid=john suid=john
fsuid=john egid=john sgid=john fsgid=john tty=tty2 ses=4 comm=nano exe=/usr/bin/
nano subj=classified_u:user_r:user_t:s2 key=data-monitor
```

Рис. 2.26 – Запис даних користувачем john у файл info.txt

```
[root@trusted ~]# last reboot
reboot   system boot  3.10.0-1127.el7. Mon May 18 13:53 - 17:08  (03:15)
```

Рис. 2.27 – Останнє перезавантаження системи

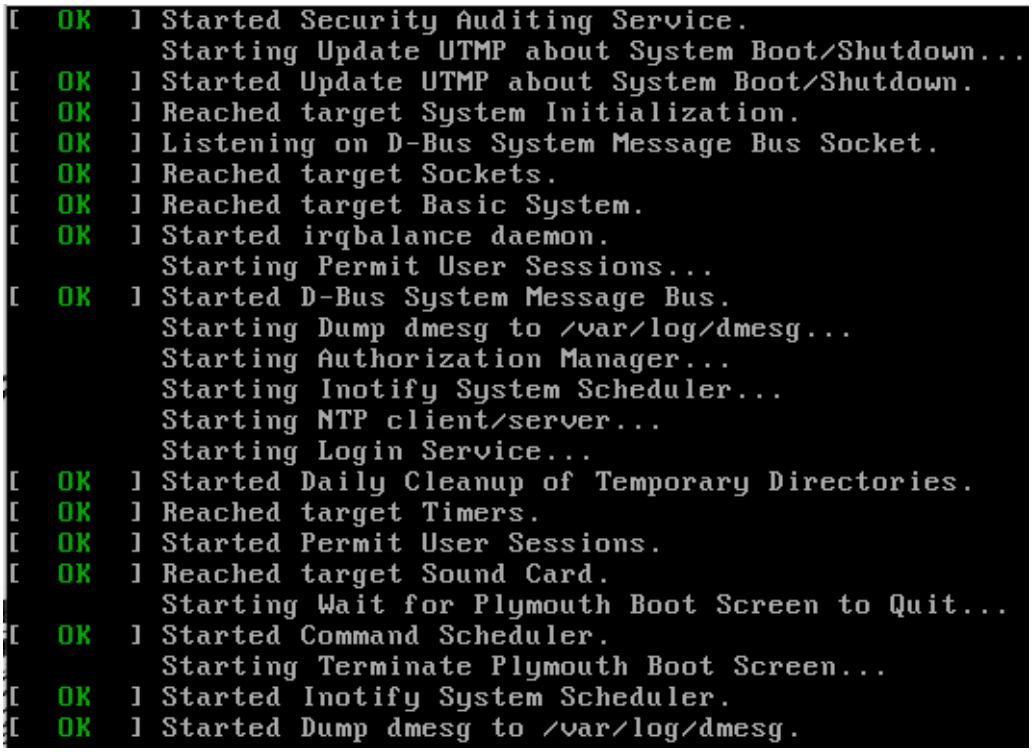


Рис. 2.28 – Старт сервісів при ініціалізації системи

Засобами системи контролю доступу SELinux забезпечено захист протоколів реєстрації від несанкціонованого доступу. Аналіз протоколів виконує вповноважена особа (адміністратор безпеки).

Можливий контроль у реальному часі подій, що стосуються безпеки: аутентифікація користувачів, операції над захищеними об’єктами, порушення правил доступу.

2.11 Ідентифікація і автентифікація

Реалізація послуги дозволяє визначити і перевірити особистість користувача. Політика послуги поширюється на усіх користувачів системи, які намагаються:

- одержати доступ до КС;
- виконати дію з правами адміністратора.

Послугу реалізовано ідентифікацією користувача на основі введеного їм псевдоніму та автентифікації за встановленим протоколом на рівні НИ-3 «Множинна ідентифікація і автентифікація».

Для автентифікації в системі користувач повинен пред'явити змінний носій з даними автентифікації та ввести пароль.

Дані автентифікації захищені від несанкціонованого доступу, модифікації чи знищення з використанням механізмів, що використовуються для реалізації послуг «Адміністративна конфіденційність» та «Адміністративна цілісність».

Паролі користувачів зберігаються у вигляді контрольних сум SHA-512 (рис. 2.29):

```
john:$6$XUz/5fn4$T0Vq0X.KGD08WuW3hRu4a.hZqfx6M/24IkSrqpZIL0R1Ujvzpwg/iwES7Fv61bB
f0FaBcYFK3Ui0xZ/ANU.Kr1:18412:0:99999:7:::
```

Рис. 2.29 – Хеш-сума паролю користувача john

Виконаємо перевірку реалізації послуги безпеки НИ:

Зареєструємо носій даних автентифікації (рис. 2.30):

```
[root@trusted ~]# pamusb-conf --add-device="ROOT-TOKEN"
Please select the device you wish to add.
* Using "JetFlash Transcend 16GB (056GTYB99IOELL85)" (only option)

Which volume would you like to use for storing data ?
* Using "/dev/sdb1 (UUID: 3473-1B3C)" (only option)

Name            : ROOT-TOKEN
Vendor          : JetFlash
Model           : Transcend 16GB
Serial          : 056GTYB99IOELL85
UUID            : 3473-1B3C

Save to /etc/pamusb.conf ?
[Y/n] y
Done.
```

Рис. 2.30 – Реєстрація нового носія даних автентифікації

Назначимо користувача *john* відповідальним за носій (рис. 2.31):

```
[root@trusted ~]# pamusb-conf --add-user=john
Which device would you like to use for authentication ?
* Using "ROOT-TOKEN" (only option)

User            : john
Device          : ROOT-TOKEN

Save to /etc/pamusb.conf ?
[Y/n] y
Done.
```

Рис. 2.31 – Додавання носія користувачеві john

Ідентифікація користувача *john* за псевдонімом та множинна автентифікація (рис. 2.32):

Рис. 2.32 – Множинна автентифікація

Спроба автентифікації користувача *john* при вході в систему без носія даних автентифікації (рис. 2.33):

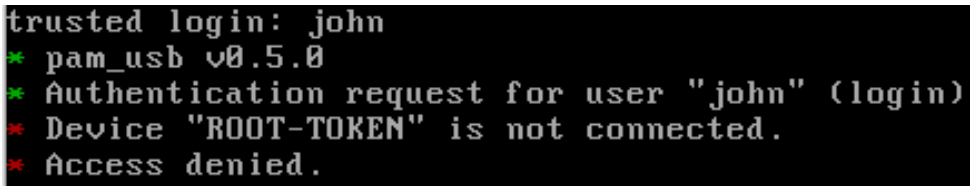


Рис. 2.33 – Помилка автентифікації

Автентифікація користувача *john* при виконанні дії з правами адміністратора (рис. 2.34):

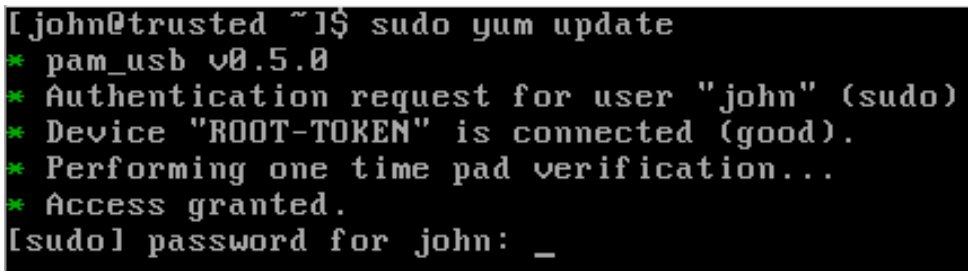


Рис. 2.34 – Множинна автентифікація при виконанні адміністративної дії

Спроба автентифікації користувача *john* при виконанні дії з правами адміністратора без носія даних автентифікації (рис. 2.35):

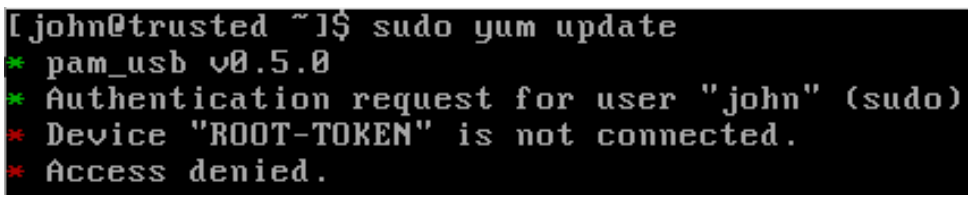


Рис. 2.35 – Помилка автентифікації

2.12 Достовірний канал

Реалізація послуги гарантує користувачеві взаємодію з системою в процесі ідентифікації та автентифікації. Політика послуги поширюється на користувачів усіх категорій.

Послугу реалізовано ядром Linux на рівні НК-1 «Однонаправлений достовірний канал».

Як і операційні системи сімейства Windows NT, ядро Linux підтримує Secure Attention Key (SAK) – спеціальну комбінацію клавіш, що повинна бути натиснута перед входом в систему. Якщо операційна система виявляє таку комбінацію, то ядро запускає перевірку входу та призупиняє усі програми, що пов’язані з входом в систему.

В операційних системах сімейства GNU/Linux такою комбінацією є «Alt+SysRq+K».

2.13 Розподіл обов’язків

Реалізація послуги дозволяє розділити повноваження користувачів. Політика послуги поширюється на користувачів усіх категорій.

Послугу реалізує система мандатного керування доступом SELinux на рівні НО-2 «Розподіл обов’язків адміністраторів».

SELinux визначає багату кількість ролей. Адміністратор має можливість зіставити кожного користувача з однією чи більше ролями. Система виділяє такі ролі (табл. 2.1):

Таблиця 2.1 – Ролі SELinux

Роль	Користувач SELinux	Роль SELinux	Користувач Linux
Системний адміністратор	sysadmin_u	sysadmin_r, logadm_r	root, sysadmin
Адміністратор безпеки	secadmin_u	secadm_r, auditadm_r	secadmin

Продовження таблиці 2.1

Роль	Користувач SELinux	Роль SELinux	Користувач Linux
Користувач з рівнем допуску s1	unclassified_u	user_r	alice
Користувач з рівнем допуску s2	classified_u	user_r	john

Обов’язки системного адміністратора:

- інсталяція та оновлення ПЗ;
- конфігурація системи та ПЗ;
- моніторинг протоколів реєстрації системних подій.

Обов’язки адміністратора безпеки:

- керування засобами захисту;
- керування користувачами та захищеними ресурсами;
- аналіз даних аудиту безпеки.

2.14 Цілісність комплексу засобів захисту

Реалізація послуги забезпечує захист системи від зовнішніх впливів і гарантує її здатність управляти захищеними об’єктами. Політика послуги поширюється на:

- програмні засоби;
- ядро системи.

Послугу реалізує архітектура вимірювання цілісності (Integrity Measurement Architecture, IMA) на рівні НЦ-1 «КЗЗ з контролем цілісності».

IMA – це підсистема ядра Linux, яка забезпечує контроль цілісності файлової системи. Складається з двох компонентів: IMA-measurement (вимірювання) та IMA-appraisal (оцінка). Перший компонент розраховує

контрольні суми файлів, другий – порівнює ці контрольні суми з вже існуючими контрольними сумами в базі даних та забороняє доступ у разі їх невідповідності.

При розходженні поточної хеш-суми та збереженої, то система переходить у стан. в якому не можлива обробка інформації, і потребує втручання вповноваженого користувача. Адміністратор повинен відновити базу даних контрольних сум, запустивши їх повторних розрахунок, або відновити виконуваний файл з копії.

Опціонально можливе використання модулю розширеної верифікації (Extended Verification Module, EVM), який контролює цілісність атрибутів файлів, що захищаються IMA.

Підсистема IMA/EVM реалізується наступними опціями ядра Linux:

CONFIG_INTEGRITY=y

CONFIG_IMA=y

CONFIG_IMA_MEASURE_PCR_IDX=10

CONFIG_IMA_LSM_RULES=y

CONFIG_INTEGRITY_SIGNATURE=y

CONFIG_IMA_APPRAISE=y

IMA_APPRAISE_BOOTPARAM=y

CONFIG_IMA_AUDIT=y

CONFIG_INTEGRITY_ASYMMETRIC_KEYS=y

CONFIG_EVM=y

IMA увімкнено на етапі завантаження системи такими параметрами ядра: ima=on, ima_appraise=enforce, ima_policy=tcb.

Виконаємо перевірку реалізації послуги безпеки НЦ:

Розраховані хеш-суми SHA-1 (рис. 2.36):

Рис. 2.36 – Частина БД хеш-сум

Створимо тестовий скрипт, який при вдалому виконанні буде виводити на екран строку «Скрипт виконано» (рис. 2.37):

Рис. 2.37 – Виконання скрипту

Виконання скрипту можливе тому, що підсистема IMA розраховує контрольну суму файлу (рис. 2.38):

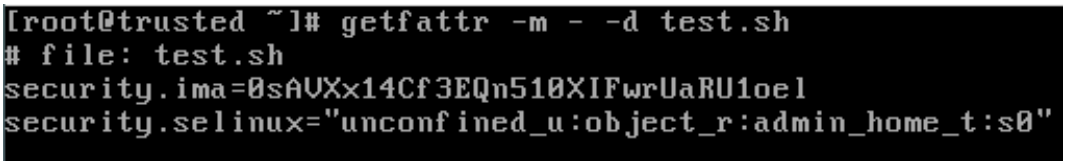


Рис. 2.38 – Хеш-сума файлу test.sh

Якщо змінити тестовий файл, то IMA-appraisal знайде розходження між збереженою контрольною сумою файлу та поточною сумою, та заборонить виконання скрипту (рис. 2.39):

Рис. 2.39 – Заборона виконання

2.15 Самотестування

Реалізація послуги надає можливість перевірити та на основі цього гарантувати правильність функціонування та цілісність функцій системи. Політика послуги поширюється на:

- програмні засоби;
- конфігураційні файли програмних засобів.

Послугу реалізовано програмним комплексом AIDE на рівні НТ-1 «Самотестування за запитом».

AIDE – це хостова система виявлення атак (Host-Based Intrusion Detection System, HIDS). Використовується для моніторингу змін у системних конфігураційних та бінарних файлах завдяки розрахунку контрольних сум для кожного об’єкту.

Виконаємо перевірку реалізації послуги безпеки НТ:

Первинна ініціалізація бази даних контрольних сум (рис. 2.40):

```
[root@trusted ~]# aide --init

AIDE, version 0.15.1

### AIDE database at /var/lib/aide/aide.db.new.gz initialized.
```

Рис. 2.40 – Ініціалізація бази даних

За запитом адміністратора виконується тестування – розраховується нова контрольна сума для кожного об’єкту та звіряється з вже існуючою (рис. 2.41):

```
[root@trusted ~]# aide --check

AIDE, version 0.15.1

### All files match AIDE database. Looks okay!
```

Рис. 2.41 – Перевірка цілісності

Якщо були внесені зміни до конфігураційних файлів або встановлено/видалено програмний засіб, тест не буде пройдено. AIDE покаже зміни в системі (для прикладу було видалено текстовий редактор *nano* та його конфігураційні файли) (рис. 2.42):

```
[root@trusted ~]# aide --check
AIDE 0.15.1 found differences between database and filesystem!!
Start timestamp: 2020-05-13 12:20:23

Summary:
  Total number of files:        63753
  Added files:                  0
  Removed files:                94
  Changed files:                3


---------------------------------------------------
Removed files:
---------------------------------------------------

removed: /bin/nano
```

Рис. 2.42 – Повторна перевірка цілісності

2.16 Інсталяція та налаштування системи

Для встановлення та подальшого налаштування було обрано операційну систему CentOS 7. Варіант інсталяції – мінімальний набір ПЗ, без політики безпеки.

На даному етапі необхідно задати пароль автентифікації системного адміністратора та створити шифрований розділ для зберігання ІзОД (рис. 2.43):

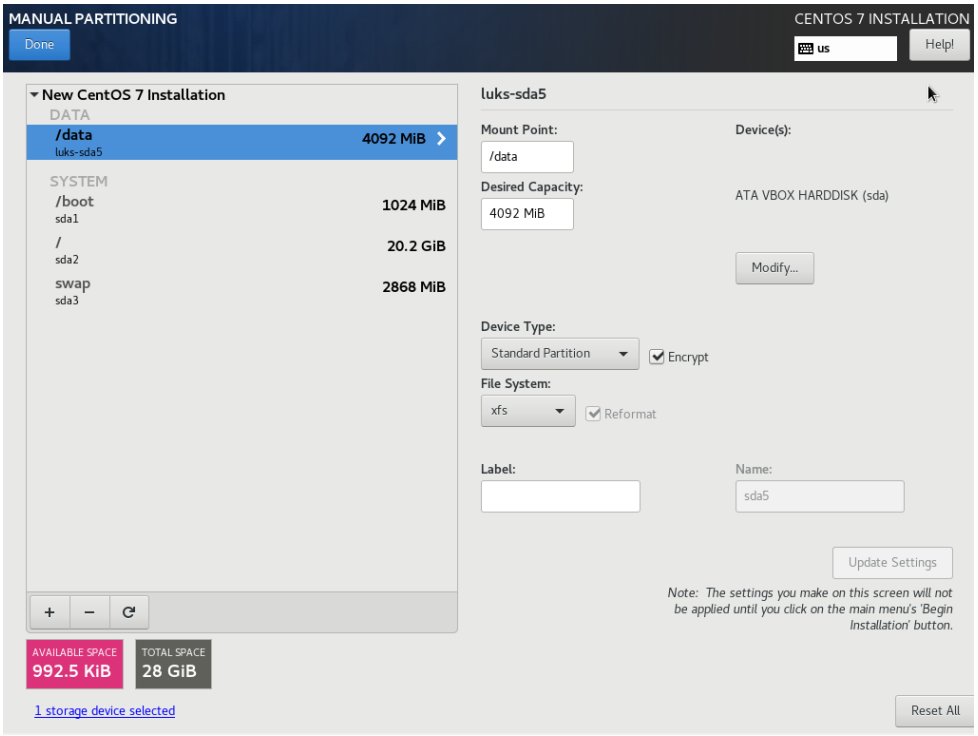


Рис. 2.43 – Розмітка файлової системи

Для використання політики MLS необхідно встановити програмний пакет *selinux-policy-mls* та в конфігураційному файлі */etc/selinux/config* встановити значення параметру SELINUXTYPE=mls. Необхідно створити файл */.autorelabel* та перезавантажити систему, щоб провести встановлення контекстів безпеки політики MLS.

Щоб увімкнути очищення сторінок оперативної пам’яті, необхідно додати до конфігурації ядра наступні параметри: *page_poisoning=on*, *slub_debug=PF*.

Для множинної автентифікації необхідно встановити *pamusb*, додати новий носій даних автентифікації (рис. 2.30) та користувача (рис. 2.31).

Для увімкнення підсистеми контролю цілісності додати до конфігурації ядра: *ima=on, ima_appraise=enforce, ima_policy=tcb*.

2.17 Висновки спеціальної частини

У спеціальній частині виконано аналіз механізмів безпеки операційної системи RedHat Enterprise Linux 7, наведено послуги безпеки згідно з НД ТЗІ 2.5-004 та виконано їх тестування згідно з НД ТЗІ 2.7-009-09.

Отримані результати були використані для створення КЗЗ на базі механізмів операційної системи RedHat Enterprise Linux 7 з функціональним профілем КА-3, КО-1, КВ-2, ЦА-3, ЦО-1, ЦВ-2, ДР-1, ДЗ-1, ДВ-1, НР-4, НИ-3, НК-1, НО-2, НЦ-1, НТ-1.

Застосування розробленого КЗЗ можливе в освітньому процесі підготовці бакалаврів з «Кібербезпеки», що забезпечить фахові компетенції відповідно до Стандарту вищої освіти спеціальності «Кібербезпека» [18]. Компетенції зазначені у таблиці 2.2:

Таблиця 2.2 – Фахові компетенції та результати навчання

Фахові компетентності	Результати навчання
КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.	- забезпечувати процеси захисту інформаційно-телекомунікаційних (автоматизованих) систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту; - забезпечувати функціонування спеціального програмного забезпечення, щодо захисту даних від руйнуючих програмних впливів, руйнуючих кодів в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - виконувати розробку експлуатаційної документації на комплексів засобів захисту.

КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.	- обирати основні методи та засоби захисту інформації відповідно до вимог сучасних стандартів інформаційної та/або кібербезпеки, та критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії захисту інформації; - вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації, користувачів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - проектувати та реалізувати комплексні системи захисту інформації в автоматизованих системах організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації; - вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - визначати рівень захищеності інформаційних ресурсів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; -використовувати інструментальні засоби оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах.
КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-	- вирішувати задачі супроводу та впровадження комплексних систем захисту інформації, а також протидії несанкціонованому

правових, організаційних та технічних засобів і методів, процедур, практичних прийомів.	доступу до ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - здійснювати оцінку рівня захищеності інформації що обробляється в інформаційно-телекомунікаційних системах використовувати інструментальні засоби оцінювання наявності потенційних вразливостей; - вирішувати задачі управління комплексною системою захисту інформації в інформаційних та інформаційно-телекомунікаційних (автоматизованих); - вирішувати задачі експертизи, випробування комплексних систем захисту інформації.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Постановка задачі

Мета економічного розділу – техніко-економічний аналіз ефективності та обґрунтування доцільності створення комплексу засобів захисту на базі механізмів операційних систем сімейства RedHat Enterprise Linux.

Економічно доцільним слід вважати, якщо витрати на створення КЗЗ не перевищують збитків від реалізації загрози порушення безпеки.

3.2 Визначення витрат на створення КЗЗ

По-перше, необхідно визначити трудомісткість створення комплексу засобів захисту.

Трудомісткість створення КЗЗ визначається тривалістю виконання кожної операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного спеціаліста з інформаційної безпеки):

$$t = t_a + t_{тз} + t_{озб} + t_в + t_{вз} + t_{овр} + t_д \text{ годин,} \qquad (3.1)$$

де t_a – тривалість процесу аналізу загроз;

$t_{тз}$ – тривалість складання технічного завдання на створення КЗЗ;

$t_{озб}$ – тривалість вибору основних рішень з забезпечення безпеки інформації;

$t_в$ – тривалість аналізу документації до операційної системи та систем захисту;

$t_{вз}$ – тривалість процесу налаштування системи та механізмів забезпечення безпеки інформації;

$t_{овр}$ – тривалість тестування функціональних послуг;

$t_Д$ – тривалість документального оформлення.

Таким чином трудомісткість створення КЗЗ дорівнює:

$$t=5+5+15+30+10+30+10$$

$$t = 105 \text{ год.}$$

Розрахуємо витрати на створення КЗЗ. Розрахунок проводиться за формулою 3.2:

$$K_{рп} = З_{зп} + З_{мч} \text{ грн,} \qquad (3.2)$$

де $K_{рп}$ – витрати на створення КЗЗ;

$З_{зп}$ – заробітна плата спеціаліста з інформаційної безпеки;

$З_{мч}$ – вартість витрат машинного часу, що необхідні для створення КЗЗ.

Витрати на заробітну плату спеціаліста ІБ розраховуються за формулою 3.3:

$$З_{зп} = t \cdot З_{іб}, грн, \qquad (3.3)$$

де t – загальна тривалість створення КЗЗ, годин;

$З_{іб}$ – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

Средньогодинна заробітна плата спеціаліста з інформаційної безпеки становить – 90 грн/год.

Відповідно до формули 3.3, витрати на заробітну плату спеціаліста ІБ становлять:

$$З_{зп} = 105 \text{ год} \cdot 90 \text{ грн/год,}$$

$$З_{зп} = 9450 \text{ грн.}$$

Витрати машинного часу визначаються за формулою 3.4:

$$З_{мч} = t \cdot С_{мч} \text{ грн,} \qquad (3.4)$$

де t – трудомісткість створення КЗЗ на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою 3.5:

$$С_{мч} = P \cdot t_{нал} \cdot С_е + \frac{Ф_{зал} \cdot Н_а}{F_р} + \frac{К_{лпз} \cdot Н_{апз}}{F_р} \text{ грн,} \qquad (3.5)$$

де P – встановлена потужність ПК, кВт;

$С_е$ – тариф на електричну енергію, грн/кВт·година;

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн.;

$Н_а$ – річна норма амортизації на ПК, частки одиниці;

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.;

$F_р$ – річний фонд робочого часу (за 40-годинного робочого тижня $F_р$ = 1920).

Залишкова вартість ПК визначається виходячи з фактичного терміну його експлуатації як різниця між первісною вартістю та зносом за час використання.

$$С_{мч} = 0{,}5 \cdot 1 \cdot 1{,}68 + (7100*0{,}3)/1920 + (1500*0{,}1)/1920 \text{ грн,}$$

$$С_{мч} = 2{,}02 \text{ грн.}$$

Отже, витрати на створення КЗЗ за формулою 3.2 становлять:

$$K_{рп} = 9662{,}1 \text{ грн.}$$

В результаті розрахунків, вартість створення КЗЗ становить – 9662,1 гривень.

Повна вартість капітальних витрат розраховується за формулою 3.6:

$$K = K_{рп} + K_{аз} \text{ грн,} \qquad (3.6)$$

де $К_{рп}$ – вартість створення КЗЗ, тис. грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення, тис. грн.

Необхідно придбати наступне апаратне забезпечення:

- Процесор Intel Pentium G5400 (1600 грн);
- Оперативна пам’ять 2x8 GB (1000 грн);
- Жорсткий диск 2x500 GB (2000 грн);
- Материнська плата Gigabyte H310M (1400 грн);
- Корпус (700 грн).

Відповідно до цього, вартість апаратного забезпечення становить 6700 грн.

Таким чином, згідно з формулою 3.6:

$$K = 16362{,}1 \text{ грн.}$$

3.3 Розрахунок експлуатаційних витрат

Річні поточні витрати на функціонування КЗЗ розраховуються за формулою 3.7:

$$C = C_в + C_к + C_{ак} \text{ грн,} \qquad (3.7)$$

де $C_в$ – вартість оновлення та модернізації системи ($C_в$ = 1500 грн.);

$C_к$ – витрати на керування системою в цілому;

$C_{ак}$ – витрати, викликані активністю користувачів ($C_{ак}$ = 8000 грн.).

Витрати на керування КЗЗ розраховується за формулою 3.8:

$$C_к = C_н + C_а + C_з + C_{єв} + C_{ел} + C_о + C_{тос} \text{ грн}, \quad (3.8)$$

Витрати на навчання персоналу та користувачів складають $C_н$ = 0 грн.

Річний фонд амортизаційних відрахувань становить $C_а$ = 1340 грн.

Річний фонд заробітної плати інженерно-технічного персоналу:

$$C_з = З_{осн} + З_{дод} \text{ грн}, \quad (3.9)$$

Основна заробітна плата одного спеціаліста з інформаційної безпеки складає 14400 грн на місяць. Додаткова заробітна плата – 10% від основної. Виконання роботи щодо налаштування КЗЗ потребує залучення спеціаліста на 0,5 ставки.

Отже, за формулою 3.9:

$$C_з = (14400*12 + 14400*12*0,1)*0,5 = 95040 \text{ грн.}$$

Ставка ЄСВ складає 22%:

$$C_{єв} = 95040 * 0,22 = 20908,8 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою, розраховується за формулою 3.10:

$$C_{ел} = P \cdot F_р \cdot Ц_е \text{ грн}, \quad (3.10)$$

де P – потужність апаратури;

$F_р$ – річний фонд робочого часу;

$Ц_е$ – тариф на електроенергію.

Отже, за формулою 3.10:

$$C_{ел} = 0,5 * 1920 * 1,68 = 1612,8 \text{ грн.}$$

Витрати на залучення сторонніх організацій становлять 0 грн.

Витрати на адміністрування та сервіс становлять 2% від вартості капітальних витрат:

$$C_{тос} = 16362,1 * 0,02 = 327,24 \text{ грн.}$$

Витрати на керування КЗЗ за формулою 3.8:

$$C_к = 0 + 1340 + 95040 + 20908,8 + 1612,8 + 0 + 327,24$$
$$C_к = 119228,84 \text{ грн.}$$

Річні поточні витрати за формулою 3.7:

$$C = 1500 + 119228,84 + 8000$$
$$C = 128728,84 \text{ грн.}$$

3.4 Оцінка величини збитку у разі реалізації загроз

Мета оцінки – визначення обсягів матеріальних збитків, що розраховуються виходячи з ймовірності реалізації загрози та можливих матеріальних втрат від неї.

Упущена вигода розраховується за формулою 3.11:

$$U = П_п + П_в + V \text{ грн,} \qquad (3.11)$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників, грн;

$П_в$ – вартість відновлення працездатності (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла, грн.

У свою чергу, для розрахунку $П_п$, $П_в$ *і* V, використовуються формули 3.12, 3.13, 3.14 відповідно:

$$П_п = \frac{\sum Зс \cdot Чс}{F} \cdot t_п \text{ грн}, \qquad (3.12)$$

де F – місячний фонд робочого часу;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн/місяць;

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин;

$Ч_с$ – чисельність співробітників атакованого вузла.

$$П_в = П_{ви} + П_{пв} + П_{зч} \text{ грн}, \qquad (3.13)$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

$$V = \frac{О}{Fг} \cdot (t_П + t_В + t_{ВИ}) \text{ грн}, \qquad (3.14)$$

де $F_г$ – річний фонд часу роботи організації;

O – обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн у місяць;

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин.

У свою чергу, $П_{ви}$ і $П_{пв}$ розраховуються за формулами 3.15 і 3.16 відповідно:

$$П_{ви} = \frac{\sum Зс \cdot Чс}{F} \cdot t_{ви} \text{ грн,} \qquad (3.15)$$

де F – місячний фонд робочого часу;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн/місяць;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин;

$Ч_с$ – чисельність співробітників атакованого вузла.

$$П_{пв} = \frac{\sum Зо \cdot Чо}{F} \cdot t_в \text{ грн,} \qquad (3.16)$$

де F – місячний фонд робочого часу;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), грн на місяць;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин;

$Чо$ – чисельність обслуговуючого персоналу.

Вихідні дані для розрахунків наведені у таблиці 3.1:

Таблиця 3.1 – Вихідні дані для розрахунку збитків від реалізації загроз

Умовні позначення	Величина
$t_п$	8 год
$t_в$	3 год
$t_{ви}$	6 год
$З_о$	14400 грн
$Ч_о$	2 особи
$Ч_с$	5 осіб
$О$	1500000 грн
$П_{зч}$	2000 грн
i	1 шт
n	15 шт
F	176 год
$F_г$	2080 год

Результати розрахунків наведено у таблиці 3.2:

Таблиця 3.2 – Результати розрахунків

Умовні позначення	Результат, грн
$П_п$	1818,18
$П_{ви}$	1363,63
$П_{пв}$	490,9
$П_в$	3854,53
V	12259,6
U	17932,31

Загальний збиток атаки на вузол розраховується за формулою 3.17:

$$B = \sum i \times \sum n \times U \qquad (3.17)$$

Таким чином, загальний збиток дорівнює:

$$B = 1 * 15 * 17932,31 = 268984,65 \text{ грн.}$$

3.5 Загальний ефект від впровадження КЗЗ

Загальний ефект впровадження КЗЗ визначається з урахуванням ризиків порушення інформаційної безпеки за формуло 3.18:

$$E = B \cdot R - C \text{ грн}, \quad (3.18)$$

де B – загальний збиток від атаки на вузол корпоративної мережі, грн;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

C – щорічні витрати на експлуатацію системи інформаційної безпеки, грн.

Економічний ефект становить:

$$E = 268984{,}65 * 0{,}6 - 128728{,}84 = 32661{,}95 \text{ грн.}$$

3.6 Визначення та аналіз показників економічної ефективності

Коефіцієнт повернення інвестицій ROSI показує, скільки додаткового прибутку приносить одна одиниця капітальних інвестицій. Розраховується за формулою 3.19:

$$ROSI = E / K, \quad (3.19)$$

де E – загальний ефект від впровадження системи інформаційної безпеки, грн;

K – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Таким чином:

$$ROSI = 1{,}99$$

Проект вважається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції. Розраховується за формулою 3.20:

$$ROSI > (N_{деп} - N_{інф}) / 100 \quad (3.20)$$

де $N_{деп} = 20$ – річна депозитна ставка або прибутковість альтернативного варіанту вкладення коштів, %;

$N_{інф} = 5$ – річний рівень інфляції, %.

Оскільки 1,99 > 0,15, проект є економічно доцільним.

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупаються за рахунок загального ефекту від впровадження системи інформаційної безпеки, розраховується за формулою 3.21:

$$T_o = K / E = 1 / ROSI \quad (3.21)$$

Маємо:

$$T_o = 0{,}5 \text{ року.}$$

3.7 Висновки економічного розділу

У цьому розділі були проведені розрахунки:

- Капітальних витрат на створення КЗЗ (16362,1 грн);
- Річних поточних витрат (128728,84 грн).
- Економічного ефекту (32661,95 грн);
- Коефіцієнту ефективності, який перевищує річний рівень прибутковості альтернативного варіанта (1,99 > 0,15);
- Терміну окупності капітальних інвестицій (0,5 року).

Отже, впровадження та використання обраних проектних рішень повністю доцільне.

ВИСНОВКИ

У першому розділі кваліфікаційної роботи описано актуальність питання, класифікацію АС, типову АС класу «1», системи керування доступом та керування доступом в GNU/Linux. Порівняно операційні системи сімейств Windows NT та GNU/Linux. Проведено аналіз профілів захищеності КЗЗ.

Таким чином визначено доцільність створення КЗЗ для захисту інформації в автоматизованих системах класу «1» на основі механізмів безпеки операційних систем сімейства RHEL.

У спеціальній частині виконано аналіз механізмів безпеки операційної системи RedHat Enterprise Linux 7, наведено послуги безпеки згідно з НД ТЗІ 2.5-004 [12] та виконано їх тестування згідно з НД ТЗІ 2.7-009-09 [11].

Отримані результати були використані для створення КЗЗ на базі механізмів операційної системи RedHat Enterprise Linux 7.

В третьому розділі було проведено розрахунки капітальних та річних витрат на КЗЗ. В ході розрахунків з’ясовано, що створення КЗЗ вигідне.

Отже, створення КЗЗ повністю доцільне та сприяє підвищенню рівню захисту інформації в АС класу «1».

ПЕРЕЛІК ПОСИЛАНЬ

1 НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні профілі захищеності оброблюваної інформації від несанкціонованого доступу" [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=110187&cat_id=89734&ctime=1344501089407.

2 Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсівта інформації, вимога щодо захисту якої встановлена законом [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: http://195.78.68.84/dsszzi/control/uk/publish/article?showHidden=1&art_id=288071&cat_id=44795.

3 NetMarketShare [Електронний ресурс] – Режим доступу до ресурсу: https://netmarketshare.com/windows-market-share.

4 Microsoft Windows 10 Vulnerability Statistics [Електронний ресурс] – Режим доступу до ресурсу: https://www.cvedetails.com/product/32238/Microsoft-Windows-10.html?vendor_id=26.

5 RedHat Enterprise Linux Vulnerability Statistics [Електронний ресурс] – Режим доступу до ресурсу: https://www.cvedetails.com/product/78/Redhat-Enterprise-Linux.html?vendor_id=25.

6 Committee on National Security Systems (CNSS) Glossary [Електронний ресурс]. – 2015. – Режим доступу до ресурсу: https://www.cnss.gov/CNSS/openDoc.cfm?9t6Hf3KkM/sXpJWgWXdGvA==.

7 DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA [Електронний ресурс]. – 1985. – Режим доступу до ресурсу:

https://web.archive.org/web/20060527214348/http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html#HDR2.1.1.1.

8 Role-Based Access Controls [Електронний ресурс]. – 1992. – Режим доступу до ресурсу: https://csrc.nist.gov/CSRC/media/Publications/conference-paper/1992/10/13/role-based-access-controls/documents/ferraiolo-kuhn-92.pdf.

9 RedHat Enterprise Linux 7 SELINUX USER`S AND ADMINISTRATOR'S GUIDE [Електронний ресурс] – Режим доступу до ресурсу: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/index.

10 Vermeulen S. SELinux System Administration / Sven Vermeulen., 2016. – 290 с. – (Packt Publishing Ltd.).

11 НД ТЗІ 2.7-009-09 "Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу" [Електронний ресурс]. – 2009. – Режим доступу до ресурсу: https://tzi.com.ua/downloads/2.7-009-09.pdf.

12 НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу" [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-004-99.pdf.

13 Національний стандарт ДСТУ 3396.0-96 "Захист інформації. Технічний захист інформації. Основні положення" [Електронний ресурс]. – 1996. – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38883&cat_id=38836.

14 Національний стандарт ДСТУ 3396.2-97 "Захист інформації. Технічний захист інформації. Терміни та визначення" [Електронний ресурс]. – 1997. – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38934&cat_id=38836.

15 Нормативний документ системи технічного захисту інформації НД ТЗІ 1.1-003-99 "Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу" [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: https://tzi.com.ua/downloads/1.1-003-99.pdf.

16 Закон України "Про інформацію" [Електронний ресурс]. – 1992. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2657-12.

17 Закон України "Про державну таємницю" [Електронний ресурс]. – 1994. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/3855-12.

18 Стандарт вищої освіти України: перший (бакалаврський) рівень,галузь знань 12–Інформаційні технології, спеціальність 125 – Кібербезпека [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://mon.gov.ua/storage/app/media/vishcha-osvita/zatverdzeni%20standarty/12/21/125-kierbezpeka-bakalavr.pdf.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	1 Розділ	12	
6	А4	2 Розділ	25	
7	А4	3 Розділ	12	
8	А4	Висновки	1	
9	А4	Список літератури	3	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	
14	А4	Додаток Д	1	
15	А4	Додаток Е	1	

ДОДАТОК Б. Перелік документів на оптичному носії

ДИПЛОМ_ГерасимовМО_125_16_3.docx

ДИПЛОМ_ГерасимовМО_125_16_3.pdf

ПРЕЗЕНТАЦІЯ_ГерасимовМО_125_16_3.docx

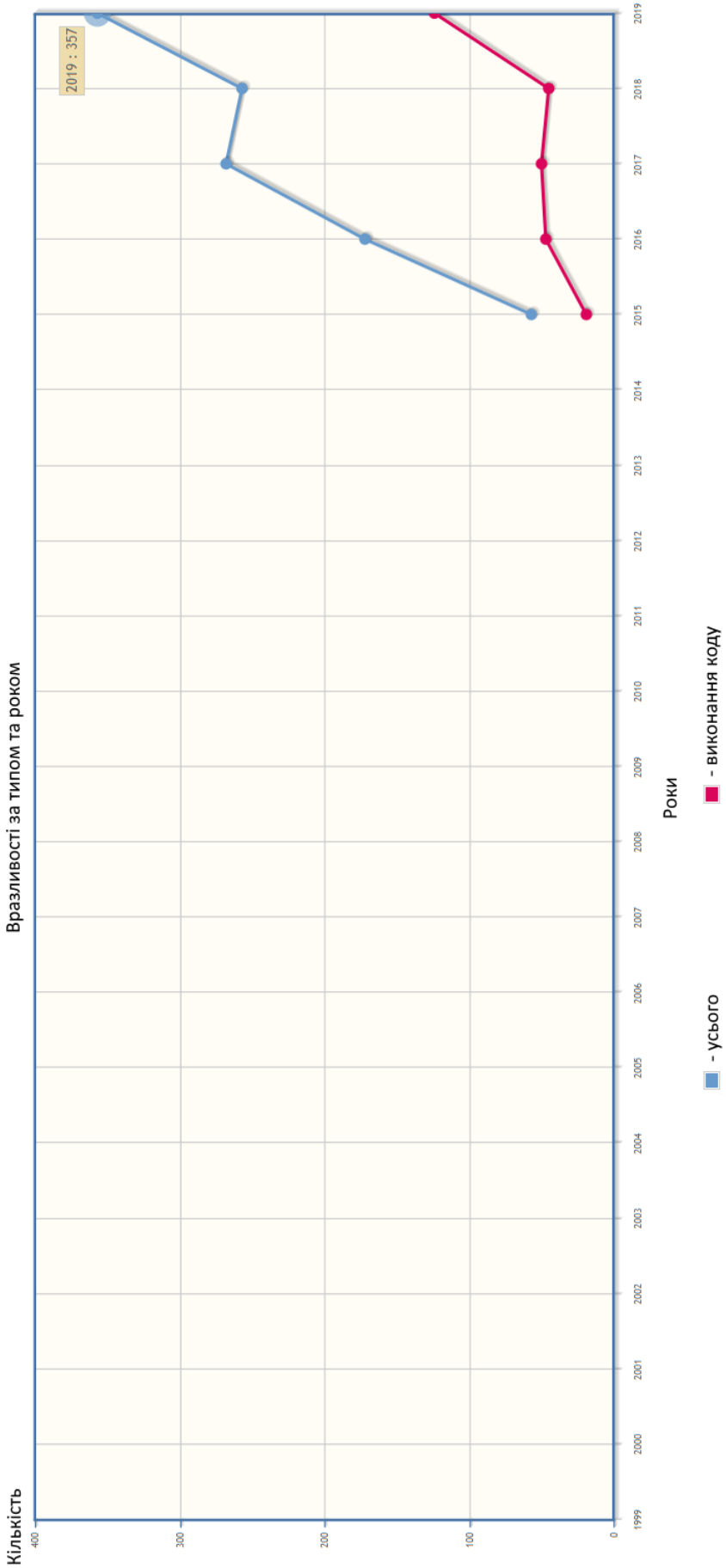
ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____
(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК

ДОДАТОК Д. ГРАФІК ВРАЗЛИВОСТЕЙ WINDOWS 10



ДОДАТОК Е. ГРАФІК ВРАЗЛИВОСТЕЙ RHEL