**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**

**КАФЕДРА** **КОМП’ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ**

ДОПУСТИТИ ДО ЗАХИСТУ

Завідувач кафедри

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ С.В. Казмірчук

«\_\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ р.

На правах рукопису

УДК 004.056.5:510.22(043.3)

**МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА**

**ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ**

**«МАГІСТР»**

**Тема**:Системи контролю доступом ОС комп’ютерних мереж

|  |  |
| --- | --- |
| **Автор:** | В.М. Шаламай |
| **Науковий керівник:** д.т.н., проф. | Л.М. Щербак |
| **Нормоконтролер:** асист. | С.В. Єгоров |

**Київ 2020**

**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**

**Факультет:** Кібербезпеки, комп’ютерної та програмної інженерії

**Кафедра:** Комп’ютеризованих систем захисту інформації

**Освітній ступінь:** Магістр

**Спеціальність:** 125 «Кібербезпека»

**Освітньо-професійна програма:** «Безпека інформаційних і комунікаційних систем»

 ЗАТВЕРДЖУЮ

 Завідувач кафедри

 \_\_\_\_\_\_\_\_\_\_\_С.В. Казмірчук

 «\_\_\_»\_\_\_\_\_\_\_\_\_\_20\_\_\_ р.

**ЗАВДАННЯ**

**на виконання магістерської атестаційної роботи**

**магістранта Шаламая Владислав Михайловича**

1. Тема роботи «Системи контролю доступом ОС комп’ютерних мереж»

затверджена наказом ректора від 02.10.2019 р. № 2265/ст.

1. Термін виконання роботи: з 14.10.2019 р. по 06.02.2020 р.
2. Вихідні дані роботи: ОС сімейства Windows, ОС Linux, дані про систему контролю доступу для аналізу та визначення рівня захищеності системи.
3. Зміст пояснювальної записки: нормативно-правове забезпечення інформаційної безпеки України, порівняння операційних систем Microsoft Windows та Linux з точки зору інформаційної безпеки, моделювання системи обов'язкового контролю доступом для ОС сімейства Windows.
4. Перелік обов'язкового ілюстративного матеріалу: таблиці, рисунки, презентація.

**КАЛЕНДАРНИЙ ПЛАН**

**виконання магістерської роботи**

|  |  |  |  |
| --- | --- | --- | --- |
| № з/п | Завдання | Термін виконання  | Примітка |
| 1 | Проаналізувати технічні та літературні джерела | 14.10.2019 – 24.10.2019 | *Виконано* |
| 2 | Обґрунтувати вибір рішення | 25.10.2019 | *Виконано* |
| 3 | Зібрати інформацію | 25.10.2019 – 30.10.2019 | *Виконано* |
| 4 | Проаналізувати та класифікувати дані | 30.10.2019 – 05.11.2019 | *Виконано* |
| 5 | Ознайомитися з моделями безпеки операційних систем сімейства Windows та Linux | 05.11.2019 – 15.11.2019 | *Виконано* |
| 6 | Провести порівняльний аналіз операційних систем з точки зору інформаційною безпеки | 15.11.2019 – 29.11.2019 | *Виконано* |
| 7 | Розробити модель системи обов'язкового контролю доступом | 29.11.2019 – 15.12.2019 | *Виконано* |
| 8 | Розробити політику безпеки системи контролю доступом | 16.12.2019 – 26.12.2019 | *Виконано* |
| 9 | Проаналізувати існуючі аналоги | 26.12.2019 | *Виконано* |
| 10 | Оформити пояснювальну записку та презентацію | 27.12.2019 – 15.01.2020 | *Виконано* |
| 12 | Отримати рецензію | 25.01.2020 | *Виконано* |
| 13 | Підготоватися до захисту | 25.01.202006.02.2020 | *Виконано* |

Магістрант В. Шаламай

(підпис, дата)

Науковий керівник Л. Щербак

(підпис, дата)

**УДК**

**РЕФЕРАТ**

Пояснювальна записка до дипломної роботи «Системи контролю доступом ОС комп’ютерних мереж»: 70 с., 27 рис., 3 табл., 39 літературних джерел.

ОПЕРАЦІЙНА СИСТЕМА, МОДЕЛЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, СИСТЕМА КОНТРОЛЮ ДОСТУПУ, НЕСАНКЦІОНОВАНИЙ ДОСТУП, АВТЕНТИФІКАЦІЯ, МІТКА, КОРИСТУВАЧ.

Об’єкт дослідження: ОС сімейства Windows та Linux.

Предмет дослідження: системи контролю доступом ОС сімейства Windows та Linux.

Мета дипломної роботи: провести аналіз та порівняти моделі безпеки ОС сімейства Windows та Linux, змоделювати систему обов’язкового контролю доступом для ОС сімейства Windows та виробити відповідні рекомендації щодо використання ОС.

Методи дослідження: аналіз, порівняння.

Технічні та програмні засоби: ОС сімейства Windows та Linux, SELinux.

Отримані результати: модель системи обов’язкового контролю доступом.

Рекомендації: використовувати дистрибутиви Linux з реалізованою системою обов'язкового контролю доступом: SUSE Linux, Ubuntu або доповнення SELinux, використання ОС з системою дискреційного контролю доступом тільки тоді, коли всі права на ресурси повинні належати користувачеві.

Галузь застосування матеріалів дипломної роботи: галузь інформаційних технологій.

Прогнозовані припущення про розвиток об'єкту та предмету дослідження: розроблену модель можливо урахувати під час розробки національної операційної системи.

**ЗМІСТ**

[Перелік умовних позанченнь та скорочень 8](#_heading=h.2et92p0)

[Вступ 10](#_heading=h.tyjcwt)

[Розділ 1. Нормативно-правове забезпечення інформаційної безпеки України 13](#_heading=h.3dy6vkm)

[1.1. Поняття інформаційної безпеки 13](#_heading=h.1t3h5sf)

[1.1.1. Рівні інформаційної безпеки 15](#_heading=h.4d34og8)

[1.1.2. Види інформаційної безпеки 15](#_heading=h.2s8eyo1)

[1.2. Елементи формування основ організації ІБ 16](#_heading=h.17dp8vu)

[1.2.1. Елементи системи ІБ 17](#_heading=h.3rdcrjn)

[1.3. Нормативно-правова база 17](#_heading=h.26in1rg)

[1.3.1. Закон України "Про інформацію" від 02.10.92, № 2658-ХІІ 18](#_heading=h.lnxbz9)

[1.3.2. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 05.07.1994 № 80/94-ВР 18](#_heading=h.35nkun2)

[1.3.3. Закон України "Про основні засади забезпечення кібербезпеки України" від 5.10.2017 року№ 2163-VIII 19](#_heading=h.44sinio)

[1.3.4. Закон України "Про захист інформації в автоматизованих системах" від 5.07.1994 року N 81/94-ВР 20](#_heading=h.2jxsxqh)

[1.3.5. ISO/IEC 15408-1:2005 Common Criteria for IT Security Evaluation 20](#_heading=h.z337ya)

[1.3.6. ISO/IEC 17799:2005 Information technology 21](#_heading=h.3j2qqm3)

[1.3.7. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу 21](#_heading=h.1y810tw)

[1.3.8. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу 22](#_heading=h.4i7ojhp)

[1.4. Висновки до розділу 23](#_heading=h.2xcytpi)

[Розділ 2. Порівняння операційнх систем Microsoft Windows та Linux з точки зору інформаційної безпеки 24](#_heading=h.1ci93xb)

[2.1. Операційні системи 24](#_heading=h.3whwml4)

[2.2. Модель безпеки ОС 25](#_heading=h.2bn6wsx)

[2.2.1. Особливості ОС Windows 25](#_heading=h.qsh70q)

[2.2.2. Особливості ОС Linux 28](#_heading=h.3as4poj)

[2.3. Ідентифікація 29](#_heading=h.1pxezwc)

[2.4. Токен доступу 30](#_heading=h.49x2ik5)

[2.5. Список контролю доступу 33](#_heading=h.2p2csry)

[2.6. Права користувачів 35](#_heading=h.147n2zr)

[2.7. Автентифікація 36](#_heading=h.3o7alnk)

[2.8. Файлова система 39](#_heading=h.23ckvvd)

[2.9. Висновки до розділу 43](#_heading=h.ihv636)

[Розділ 3. Моделювання системи обов'язкового контролю доступом для ОС сімейства Windows 44](#_heading=h.32hioqz)

[3.1. Розробка моделі загроз та моделі порушника 44](#_heading=h.1hmsyys)

[3.1.1. Розробка моделі порушника 44](#_heading=h.41mghml)

[3.1.2. Розробка моделі загроз 47](#_heading=h.2grqrue)

[3.2. Методи керування доступом 50](#_heading=h.vx1227)

[3.2.1. Вибірковий контроль доступу 50](#_heading=h.3fwokq0)

[3.2.2. Oбов'язковий контроль доступу 51](#_heading=h.1v1yuxt)

[3.2.3. Контроль доступу на основі ролей 52](#_heading=h.4f1mdlm)

[3.3. Моделювання "Windows MAC" 52](#_heading=h.2u6wntf)

[3.3.1. Недоліки стандартної DAC 52](#_heading=h.19c6y18)

[3.3.2. Вирішення проблем стандартної DAC 53](#_heading=h.3tbugp1)

[3.3.3. Суб'єкти і об'єкти 55](#_heading=h.28h4qwu)

[3.3.4. Режими роботи "Windows MAC" 55](#_heading=h.nmf14n)

[3.3.5. Контекст безпеки "Windows MAC" 55](#_heading=h.37m2jsg)

[3.3.6. Користувач "Windows MAC" 57](#_heading=h.1mrcu09)

[3.3.7. Роль у "Windows MAC" 57](#_heading=h.46r0co2)

[3.3.8. Домени "Windows MAC" 57](#_heading=h.2lwamvv)

[3.3.9. Політика "Windows MAC" 58](#_heading=h.111kx3o)

[3.3.10. Контроль доступу в "Windows MAC" 59](#_heading=h.3l18frh)

[3.4. Демонстрація програми-аналога для Linux 59](#_heading=h.206ipza)

[3.4.1. Налаштування режимів роботи 59](#_heading=h.4k668n3)

[3.4.2. Налаштування SELinux користувачів 61](#_heading=h.2zbgiuw)

[3.4.3. Налаштування мережевих портів 64](#_heading=h.1egqt2p)

[3.5. Висновки до розділу 66](#_heading=h.3ygebqi)

[Висновок 67](#_heading=h.2dlolyb)

[Список бібліографічних посилань та використаних джерел 69](#_heading=h.sqyw64)

**ПЕРEЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ**

AD - Active Directory

AES - Advanced Encryption Standard

DAC - Discretionary Access Control

DLL - Dynamic-link library

EFS - Encrypting File System

FEK - File Encryption Key

GID - Group identifier

GINA - Graphical identification and authentication

LSA - Local Security Authority

MAC - Mandatory Access Control

MCS - Multi-Category Security

MLC - Multi-Level Security

NTFS - New Technology File System

PAM - Pluggable Authentication Modules

RBAC - Role-Based Access Control

RID - Relative identifier

SAM - Security Account Manager

SID - Security identifier

TE - Type Enforcment

UID - User identifier

ДСКД - Дискретний список контролю доступу

АС - Автоматизована система

БД - База даних

ЗКД - Записи про контроль доступу

ЗМІ - Засоби масової інформації

ІБ - Інформаційна безпека

ІС - Інформаційне середовище

КМБ - Контрольний монітор безпеки

ОС - Операційна система

ПЗ - Програмне забезпечення

ПК - Персональний комп’ютер

ПЛСБ - Підсистема локальної служби безпеки

СКД - Cписок контролю доступу

СКДС - Cписок контролю доступу до системи

**ВСТУП**

Характерною рисою сучасного інформаційного суспільства є щорічне зростання кількості користувачів комп’ютерної техніки та відповідного програмного забезпечення, зворотнім боком чого є загострення проблеми інформаційної безпеки.

У сучасному суспільстві інформація стає найбільш важливою цінністю, а індустрія отримання, обробки і захисту інформації – провідною галуззю діяльності, куди з кожним роком вкладають все більш значні капітали. Вже найближчим часом саме розвиток інформаційної сфери, рівень інформаційної безпеки будуть визначати політичну й економічну роль окремих держав на світовій арені. Тривалий час методи захисту інформації розробляли лише державні органи, а їх впровадження розглядалось як виключне право тієї чи іншої держави. Однак в останні роки з розвитком комерційної та підприємницької діяльності збільшилась кількість спроб несанкціонованого доступу до конфіденційної інформації, а проблеми її захисту стали у центрі уваги багатьох учених та фахівців різних країн. Внаслідок цього з’явилася низка відкритих публікацій про дослідження та розробки в цій галузі, значно зросла потреба у фахівцях із захисту інформації.

Внаслідок інформаційної революції основною цінністю для суспільства взагалі й окремої людини зокрема поступово стають інформаційні ресурси. Організація соціуму почала трансформуватися у напрямку перерозподілу реальної влади від традиційних структур до центрів управління інформаційними потоками. Інформатизація та комп’ютеризація докорінно змінюють обличчя суспільства.

Крім того, слід наголосити на ще один важливий аспект інформаційної безпеки – захист комп'ютерної інформації від розкрадань. Протягом останніх років спостерігається стійка тенденція до різкого збільшення загроз з точки зору кількості спроб несанкціонованого втручання в роботу інформаційних та телекомунікаційних систем та несанкціонованого доступу до інформації, яка в них циркулює, а також появи нових методів та алгоритмів щодо їх здійснення. Зазначене являє собою реальну загрозу національному інформаційному простору України та у разі неприйняття необхідних заходів може призвести у найближчому майбутньому до втрати державою контролю над частиною її інформаційного простору та, відповідно, неможливості забезпечення прав громадян у цій сфері.

Існує багато різних засобів несанкціонованого доступу до інформації. Але слід одразу ж відмітити, що ніякий окремо взятий засіб захисту не в змозі гарантувати адекватну безпеку. Надійний захист можливий лише за умови створення механізму комплексного забезпечення безпеки.

Незважаючи на те, що в державі є безліч не менш нагальних проблем, які потрібно вирішувати вже сьогодні, питання інформаційної безпеки не можна лишати поза увагою.

Актуальність роботи обумовлена розвитком інформаційних технологій, що призводить до вдосконалення методів і засобів зловмисників для здійснення атак та отримання несанкціонованого доступу до інформації..

Мета даної роботи – провести аналіз та порівняти моделі безпеки ОС сімейства Windows та Linux, змоделювати систему обов’язкового контролю доступом для ОС сімейства Windows та виробити відповідні рекомендації щодо використання ОС.

Відоповідно до мети, були поставлені наступні завдання:

1. визначення та аналіз основних положень державних нормативно-правових документів та міжнародних стандартів;
2. розгляд основних компонентів моделей безпеки ОС;
3. порівняння ОС Windows та Linux з точки зору інформаційної безпеки;
4. моделювання системи обов’язкового контролю доступом для ОС сімейства Windows.

Об’єктом досліджень є ОС сімейства Windows та Linux.

Предметом досліджень є системи контролю доступом ОС сімейства Windows та Linux.

Практична значимість полягає у створенні моделі системи обов’язкового контролю доступом для операційних систем сімейства Windows для підвищення рівня захисту від несанкціонованого доступу.

Результати дослідження були апробовані на міжнародній науково-практичній конференції та опубліковані у збірнику тез:

Шаламай В.М. Порівняльний аналіз ОС Windows та Linux з точки зору інформаційної безпеки/ В.М.Шаламай// Materials of XIV Intenational Reseаrch And Practice Conference «Trends of Modern science», 30.05.-07.06.2018, - Sheffield, UK, - V.16, - p.47-50.

**РОЗДІЛ I**

**НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ**

1.1. Поняття інформаційної безпеки

Бурхливий розвиток інформаційних технологій наприкінці ХХ ст. призвів до зростання відносної важливості окремих аспектів суспільного життя. Внаслідок інформаційної революції основною цінністю для суспільства взагалі й окремої людини зокрема поступово стають інформаційні ресурси. Організація соціуму почала трансформуватися у напрямку перерозподілу реальної влади від традиційних структур до центрів управління інформаційними потоками, зросла впливовість засобів масової інформації (ЗМІ). Інформатизація та комп’ютеризація докорінно змінюють обличчя суспільства. За таких обставин забезпечення інформаційної безпеки (ІБ) поступово виходить на перший план у проблематиці національної безпеки.

Все це зумовлює необхідність формування такого аспекту інформаційної культури, як культура ІБ, культура організації ІБ. Зазначений аспект розвитку інформаційної культури набуває відображення у такій прикладній науковій дисципліні, як теорія організації ІБ.

Існує досить багато варіантів визначення поняття ІБ в науковій літературі, а також закріплено на рівні національного законодавства. Розглянемо основні з них:

ІБ – це стан захищеності інформаційного середовища (ІС) суспільства, який забезпечує його формування, використання й розвиток в інтересах громадян, організацій, держави.

Під ІС розуміють сферу діяльності суб’єктів, пов’язану із створенням, обробленням й споживанням інформації.

ІБ – це стан захищеності потреб в інформації особи, суспільства й держави, при якому забезпечується їхнє існування та прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз [1]. Стан інформованості визначає ступінь адекватності сприйняття суб’єктами навколишньої дійсності і як наслідок – обґрунтованість рішень і дій, що приймаються.

ІБ – складова національної безпеки, процес управління загрозами та небезпеками державними і недержавними інституціями, окремими громадянами, за якого забезпечується:

1. інформаційний суверенітет України;
2. вдосконалення державного регулювання розвитку ІС, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;
3. активне залучення ЗМІ до боротьби з корупцією, зловживанням службовим становищем, іншими явищами, які загрожують національній безпеці України;
4. вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

В інформаційному праві ІБ – це одна із сторін розгляду інформаційних відносин у межах інформаційного законодавства з позиції захисту життєво важливих інтересів особистості, суспільства, держави і акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами.

ІБ виступає як характеристика стабільного, стійкого стану системи, яка при впливі внутрішніх та зовнішніх загроз та небезпек зберігає суттєво важливі характеристики для власного існування.

Основні характеристики ІБ [2]:

1. доступність — можливість за прийнятний час отримати шукану інформаційну послугу будь-яким суб’єктом виконавчої влади;
2. цілісність — актуальність і несуперечливість інформації, її захищеність від руйнування і несанкціонованої зміни;
3. конфіденційність — захист від несанкціонованого ознайомлення.

Сутність і зміст ІБ проявляються по-особливому на кожному з рівнів державного управління, зокрема на:

1. стратегічному — Кабінет Міністрів України;
2. тактичному — центральні органи виконавчої влади;
3. оперативному — місцеві органи виконавчої влади, провідне місце серед яких посідають місцеві державні адміністрації.

**1.1.1. Рівні інформаційної безпеки**

Виділяють наступні рівні ІБ:

1. нормативно-правовий — закони, нормативно-правові акти тощо;
2. адміністративний — дії загального характеру, які вживаються органами державного управління;
3. процедурний — конкретні процедури забезпечення ІБ;
4. програмно-технічний — конкретні технічні заходи забезпечення ІБ.

ІБ як одна з характеристик стійкого розвитку виступає в якості базової цінності держави. Водночас, ціннісні орієнтації, що ґрунтуються на уявленнях про ІБ у різних суспільних груп і окремих осіб, почасти не співпадають. Саме у цьому знаходить свій безпосередній вираз вплив держави, яка за допомогою системи методів виражає загальні цінності у сфері ІБ.

**1.1.2. Види інформаційної безпеки**

ІБ особистості – це захищеність психіки й свідомості людини від небезпечних інформаційних впливів: маніпулювання свідомістю, дезінформування, спонукання до образ, самогубства тощо [3].

ІБ держави характеризується мірою захищеності держави (суспільства) та стійкості основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи тощо) відносно небезпечних (дестабілізуючих) інформаційних впливів, причому як з упровадження, так і добування інформації. ІБ держави визначається здатністю нейтралізувати такі впливи.

Концепція ІБ держави – це систематизована сукупність відомостей про ІБ держави та шляхи її забезпечення. В рамках цієї концепції проводиться системна класифікація дестабілізуючих факторів та інформаційних загроз безпеці особистості, суспільства, держави; обґрунтовуються основні положення з організації забезпечення ІБ держави; розробляються пропозиції щодо способів і форм забезпечення ІБ.

1.2. Елементи формування основ організації ІБ

У суспільних відносинах із застосуванням комп’ютерних інформаційних систем питання ІБ широко висвітлюється у спеціальній літературі. Сьогодні критична маса науково-практичних знань щодо розвитку суспільних інформаційних відносин у такому аспекті дає змогу сформувати на теоретичному рівні елементи загальної теорії організації ІБ в умовах формування інформаційного суспільства.

Зазначений аспект теорії має зворотний зв’язок з культурою практики: формування організаційних підходів, методів, засобів систем захисту комп’ютеризованих соціальних інформаційних систем; формування змісту навчальних дисциплін у навчальних закладах, а також формування комплексу знань фахівців, які спеціалізуються на організації захисту інформації, її безпеки у відповідних соціальних структурах (установах, організаціях, підприємствах тощо).

Аналіз наукової думки та емпіричного матеріалу дає змогу визначити такі принципові положення організації захисту інформації в умовах інформатизації у контексті ІБ:

Культура ІБ як наукове явище сьогодні формується на рівні міжгалузевого комплексного соціоінженерного інституту (наукової дисципліни), який утворився на межі поєднання технічних і гуманітарних наук: правової інформатики, інформаційного права та тектології (теорії організації соціальних систем).

За природою походження культура ІБ в умовах інформаційного суспільства має триєдиний зміст: організаційний, інженерно-технічний (у тому числі програмно-математичний) та правовий.

У перспективі сутність ІБ, у тому числі щодо захисту інформації у соціотехнічних системах, буде доповнюватися спеціальними знаннями з інших галузей, підгалузей, інституцій технічних та суспільних наук.

З погляду теорії організації і теорії систем, у науковому синтезі їх - теорії організації систем управління – формування цілеспрямованих, керованих систем (у тому числі будь-яких практичних заходів) передбачає визначення елементів системи та осмислення проблематики предметної галузі (її природу) в цілому.

**1.2.1. Елементи системи ІБ**

Провідними елементами системи ІБ, у тому числі щодо захисту інформації в автоматизованих комп’ютерних системах, є:

1. суб’єкти – держава, що здійснює свої функції через відповідні органи; громадяни, суспільні або інші організації і об’єднання, що володіють повноваженнями щодо забезпечення ІБ відповідно до законодавства;
2. об’єкти – свідомість, психіка людини; інформаційні системи різного масштабу й різного призначення. До соціальних об’єктів ІБ відносять особистість, колектив, державу, суспільство, світове товариство;
3. провідний предмет суспільних правовідносин – інформація в автоматизованих (комп’ютерних) системах (у тому числі електронних телекомунікаціях, зокрема в Інтернеті).

**1.3. Нормативно-правова база**

В сучасних умовах розвитку інформаційного суспільства активно розвивається інформаційна сфера, яка поєднує в собі інформацію, інформаційну інфраструктуру, зокрема інформаційні мережі, інформаційні відносини між суб'єктами цієї сфери, що складаються у процесі збирання, формування, розповсюдження і використання інформації. Інформаційні відносини займають чільне місце у формуванні інформаційної політики держави, в житті сучасного суспільства, а також в діловому та в особистому житті кожної людини. Це, в свою чергу, обумовлює необхідність розвитку й удосконалення правових засобів регулювання суспільних відносин у сфері інформаційної діяльності. Зрозуміло, що в демократичній правовій державі такі відносини мають базуватися на сучасній нормативно-правовій базі, що регулює діяльність в інформаційній сфері.

**1.3.1. Закон України "Про інформацію" від 02.10.92, № 2658-ХІІ**

Закон встановлює загальні правові основи одержання, використання, поширення та зберігання інформації, закріплює право особи на інформацію в усіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначає статус учасників інформаційних відносин, регулює доступ до інформації та забезпечує її охорону, захищає особу і суспільство від неправдивої інформації [4].

Закон визначає інформацію як документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому середовищі. Відповідно об’єктами інформаційних відносин є документована або публічно оголошена інформація про події та явища в галузі політики, економіки, культури, охорони здоров’я, а також у соціальній, екологічній, міжнародній та інших сферах[4].

**1.3.2. Закон України "Про захист інформації в інформаційно-****телекомунікаційних системах" від 05.07.1994 № 80/94-ВР**

Цей закон визначає загальні вимоги та організаційні засади забезпечення захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Дія цього закону не поширюється на захист інформації в системах урядового та спеціальних видів зв’язку [5].

Згідно цього закону захисту в системі підлягає:

1. відкрита інформація, яка є власністю держави і у визначенні Закону України "Про інформацію" належить до статистичної, правової, соціологічної інформації, інформації довідково-енциклопедичного характеру та використовується для забезпечення діяльності державних  органів або органів місцевого самоврядування, а також інформація про діяльність зазначених органів, яка оприлюднюється в Інтернет, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережам;
2. конфіденційна інформація, яка є власністю держави або вимога щодо захисту якої встановлена законом, у тому числі конфіденційна інформація про фізичну особу;
3. інформація, що становить державну або іншу передбачену законом таємницю[5].

**1.3.3. Закон України "Про основні засади забезпечення кібербезпеки України" від 5.10.2017 року№ 2163-VIII**

Законом визначено правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, повноваження і обов'язки державних органів, підприємств, установ, організацій, осіб та громадян, основних засад координації їх діяльності, а також базових термінів у сфері кібербезпеки [6].

Згідно закону, в Україні має бути створена Національна телекомунікаційна мережа та Державний центр кіберзахисту.

Також мають сформувати урядову команду реагування на комп'ютерні надзвичайні події CERT-UA для аналізу даних про кіберінциденти та для надання практичної допомоги щодо усунення їх наслідків.

CERT-UA має розміщувати офіційні рекомендації щодо протидії кіберзагрозам та взаємодіяти з правохоронцями по їх попередженню.

Закон визначає основні об'єкти кіберзахисту, які створюють критичну інфраструктуру країни, принципи забезпечення кібербезпеки та національну систему кібербезпеки.

Згідно закону, президент координує діяльність у сфері кібербезпеки через очолювану ним Раду національної безпеки та оборони[6].

**1.3.4. Закон України "Про захист інформації в автоматизованих системах" від 5.07.1994 року N 81/94-ВР**

Метою цього Закону є встановлення основ регулювання правових відносин щодо захисту інформації в автоматизованих системах за умови дотримання права власності громадян України і юридичних осіб на інформацію та права доступу до неї, права власника інформації на її захист, а також встановленого чинним законодавством обмеження на доступ до інформації [7].

Дія Закону поширюється на будь-яку інформацію, що обробляється в автоматизованих системах.

**1.3.5. ISO/IEC 15408-1:2005 Common Criteria for IT Security Evaluation**

Стандарт ISO/IEC 15408 "Загальні критерії оцінки безпеки інформаційних технологій" описує інфраструктуру в якій користувачі комп’ютерної системи можуть описати вимоги, розробники можуть заявити про властивості безпеки продуктів, а експерти з безпеки визначити, чи задовольняє продукт заявам. Таким чином цей стандарт дозволяє бути впевненим, що процес опису, розробки та перевірки продукту був проведений в строгому порядку. Прообразом даного документа послужили "Критерії оцінки безпеки інформаційних технологій", робота над якими почалася в 1990 році.

Стандарт містить два основних види вимог безпеки: функціональні, що висуваються до функцій безпеки і реалізує їх механізмів, і вимоги довіри, які пред’являються до технології та процесу розробки та експлуатації [8].

**1.3.6. ISO/IEC 17799:2005 Information technology**

Стандарт ISO/IEC 17799 — це модель системи менеджменту, яка визначає загальну організацію, класифікацію даних, системи доступу, напрямки планування, відповідальність співробітників, використання оцінки ризику і т.ін. в контексті ІБ. У процесі впровадження стандарту створюється так звана система менеджменту ІБ, мета якої - скорочення матеріальних втрат, зв'язаних з порушенням ІБ. Основна ідея стандарту — допомогти комерційним та державним господарським організаціям вирішити достатньо складне завдання: не тільки забезпечити надійний захист інформації, але також організувати ефективний доступ до даних та нормальну роботу з ними [9].

**1.3.7. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу**

Цей нормативний документ технічного захисту інформації визначає методологічні основи вирішення завдань захисту інформації в комп'ютерних системах і створення нормативних і методологічних документів, регламентуючих питання:

1. визначення вимог щодо захисту комп'ютерних систем від несанкціонованого доступу;
2. створення захищених комп'ютерних систем і засобів їх захисту від несанкціонованого доступу;
3. оцінки захищеності комп'ютерних систем і їх придатності для вирішення завдань споживача.

Документ призначено для постачальників (розробників), споживачів (замовників, користувачів) комп'ютерних систем, які використовуються для обробки (в тому числі збирання, зберігання, передачі і т. д.) критичної інформації (інформації, що вимагає захисту), а також для державних органів, що здійснюють функції контролю за обробкою такої інформації [10].

**1.3.8. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу**

Цей нормативний документ — встановлює критерії оцінки захищеності інформації, оброблюваної в комп'ютерних системах, від несанкціонованого доступу.

Цей документ призначено для постачальників (розробників), споживачів (замовників, користувачів) комп'ютерних систем, які використовуються для обробки (в тому числі збирання, зберігання, передачі і т. ін.) критичної інформації, а також для органів, що здійснюють функції оцінювання захищеності такої інформації та контролю за її обробкою [11].

**1.4. Висновки до розділу**

Інформаційна безпека, зокрема, кібербезпека, сьогодні стали найнагальнішими питаннями, що потребують прискіпливої уваги як окремої особи, так і суспільства та держави в цілому.

Наявність необхідної та достатньої нормативної бази і механізмів її реалізації та контролю дозволяє системі забезпечення національної безпеки України ефективно функціонувати в сучасних умовах.

Нормативна база ІБ виконує, в першу чергу, три основні функції:

1. регулювання взаємовідносин між суб'єктами ІБ, визначення їх прав, обов'язків та відповідальність;
2. нормативно забезпечує дії суб'єктів ІБ на всіх рівнях, а саме - людини, суспільства, держави;
3. встановлює порядок застосування різних сил і засобів забезпечення ІБ.

Найбільш актуальним завданням у сфері забезпечення ІБ держави на сьогодні є формування відповідних положень національного інформаційного законодавства щодо правового забезпечення діяльності в інформаційній сфері відповідних суб'єктів, у першу чергу державних органів, на які державою покладено виконання пов'язаних з цим функцій.

Упорядковувати правовідносини щодо ІБ покликані закони, стандарти та нормативно – правові документи, серед яких Закон України "Про інформацію", Закон України "Про захист інформації в інформаційно-телекомунікаційних системах", Закон України "Про основні засади забезпечення кібербезпеки України", Закон України "Про захист інформації в автоматизованих системах", стандарт ISO/IEC 15408-1:2005 Common Criteria for IT Security Evaluation, стандарт ISO/IEC 17799:2005 Information technology, НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу та НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу.

**РОЗДІЛ II**

**ПОРІВНЯННЯ ОПЕРАЦІЙНИХ СИСТЕМ MICROSOFT WINDOWS ТА LINUX З ТОЧКИ ЗОРУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**

**2.1. Операційні системи**

Операційна система (ОС) - це базовий комплекс програм, що виконує управління апаратною складовою комп'ютера та забезпечує керування обчислювальним процесом і організовує взаємодію з користувачем [12]. ОС керує програмами для користувачів та надає їм відповідний інтерфейс для взаємодії з апаратним забезпеченням комп'ютера.

ОС Microsoft Windows орієнтована на архітектури ПК на базі Intel. За даними ресурсу Statcounter станом на листопад 2017 року, ОС Windows, включаючи всі наявні версії, використання становить 83,84% загальної частки ринку, що робить її домінуючою ОС у світі для ПК (рис.2.1.).



Рис. 2.1. Статистика використання ОС [13]

ОС Windows заснована корпорацією Microsoft як надбудова для MS-DOS, яка на той час була стандартною ОС.

ОС Linux - це Unix-подібна ОС, що складається з ядра ОС Linux, розробленого Лінусом Торвальдсом, а потім розширено та вдосконалено спільнотою, та GNU. Це програмний набір, складений з системних компонентів програми та інструментів для створення ОС з використанням ядра ОС Linux. З цієї причини спільний продукт ядра ОС Linux і збірки програмного забезпечення (ПЗ) GNU частіше називають GNU/Linux.

У контексті комп'ютерної безпеки практично будь-яка ОС, включаючи ОС Windows та ОС Linux, має вразливості, помилки та недоліки. Виробники ОС намагаються вирішувати наявні проблеми у своїх продуктах, щоб забезпечити максимально безпечне середовище для користувачів.

**2.2. Модель безпеки ОС**

Під безпекою ОС розуміють такий її стан, за якого унеможливлені випадкові або навмисні порушення функціонування ОС, а також унеможливлені порушення безпеки ресурсів, які перебувають під керуванням ОС.

**2.2.1. Особливості ОС Windows**

Модель безпеки (МБ) ОС Windows - це набір технологій, які забезпечують моніторинг та керування різними компонентами безпеки ОС. На рисунку 2.2 представлена МБ ОС Windows разом з її компонентами. До її складу входять наступні елементи.

Контрольний монітор безпеки (КМБ) - компонент, що працює в режимі ядра (c:\windows\system32\Ntoskrnl.exe), і забезпечує безпеку на локальному комп'ютері. Він захищає ресурси ОС, керуючись правами користувачів [14].



Рис. 2.2. Модель безпеки ОС Windows [15]

Підсистема локальної служби безпеки (ПЛСБ) - процес (c:\Windows\System32\Lsass.exe), який відповідає за автентифікацію користувача та надсилання повідомлень про аудит безпеки до журналу подій. Фактично, ПЛСБ реалізує більшість його функцій у бібліотеці динамічних посилань (c:\Windows\System32\Lsasrv.dll).

Базова політика ПЛСБ - база даних (БД), яка містить локальні параметри політики безпеки системи. Ця БД зберігається в реєстрі під назвою HKLM\SECURITY. Вона містить інформацію про домени для автентифікації, дозволи на доступ до системи та способи (інтерактивні та мережеві), права користувачів та вид аудиту безпеки.

Менеджер облікових записів безпеки (SAM) - поєднання служби та БД. Служба SAM являє собою набір підпрограм, відповідальних за управління БД, містить імена користувачів і групи, визначені на локальному комп’ютері, реалізується як бібліотека динамічних посилань (\Windows\System32\Samsrv.dll), і запускається в процесі ПЛСБ. БД SAM використовується в системах, які не функціонують як контролери доменів, і містить локальних користувачів та групи, а також їх паролі та інші атрибути. БД SAM зберігається у реєстрі під назвою HKLM\SAM [16].

Активна директорія (AD) - служба каталогів, яка містить БД для зберігання інформації про об'єкти в домені.

Домен - це сукупність комп'ютерів та пов'язаних з ними груп. AD зберігає інформацію про об'єкти в домені, включаючи користувачів, групи, комп'ютери, паролі та права. Сервер AD реалізований як "\Windows\System32\Ntdsa.dll", і запускається в процесі ПЛСБ [17].

Служба входу в мережу (Netlogon) - служба ОС Windows (\Windows\System32\Netlogon.dll), яка проводить автентифікацію при вході в обліковий запис у домені. Вона додатково перевіряє запити на вхід в систему, реєструє та виявляє контролери домену.

Пакети автентифікації - бібліотеки динамічних посилань (DLL), які працюють у контексті процесу ПЛСБ і реалізують перевірку автентичності ОС Windows. DLL для автентифікації відповідає за перевірку відповідності імені користувача та пароля, і повертає в ПЛСБ інформацію, яка деталізує ідентифікацію безпеки користувача. Пакети автентифікації ОС Windows включають Kerberos і MSV1\_0.

Процес входу в систему (Winlogon) - процес "\Windows\System32\Winlogon.exe", який відповідає за реагування на ПЛСБ та управління інтерактивними сеансами входу.

Графічна ідентифікація та автентифікація (GINA) - бібліотека, яка запускається у процесі Winlogon і яку Winlogon використовує для отримання імені користувача та пароля або PIN-коду. Стандартна бібліотека GINA розташована у "\Winnt\System32\Msgina.dll".

**2.2.2. Особливості ОС Linux**

МБ ОС Linux - це сукупність декількох активних процесів, служб-демонів та бібліотек, які забезпечують безпечну структуру для роботи ядра ОС Linux. На рисунку 2.3 представлено МБ ОС Linux разом з різними модулями [18].



Рис. 2.3 Модель безпеки ОС Linux [19]

Бібліотека модулів автентифікації з під’єднанням (PAM) забезпечує необхідний інтерфейс та функції для розробки додатків, що знаходяться під керуванням PAM. Бібліотека PAM є важливою для забезпечення автентифікації користувачів у ОС Linux.

Конфігураційний файл PAM - текстовий файл, в якому системний адміністратор може вказати, яка схема автентифікації використовується для конкретної програми. У системі ОС Linux така інформація про конфігурацію може зберігатися у файлі в каталозі "/etc/pam" або як рядок у файлі конфігурації "/etc/conf".

Модуль автентифікації - модуль, що містить кілька процедур автентифікації, які використовуються для створення облікових даних для автентифікації користувачів та надання прав користувачам, що мають автентифікацію.

Модуль управління обліковим записом керує обліковими записами користувачів і встановлює права доступу до системи. Цей модуль створює сеанс входу після успішної автентифікації та відповідає за перевірку дати закінчення дії імені користувача та / або пароля.

Модуль керування паролем обробляє та керує паролями користувачів, включаючи налаштування, скидання та зміну паролів. Іншими словами, він встановлює та змінює дані автентифікації користувача.

Модуль керування сеансом керує початком і кінцем сеансу входу. Це також стосується створення відповідних записів журналу для кожної ініціалізованої сесії.

**2.3. Ідентифікація**

Ідентифікатор - це унікальна ознака суб’єкта. Суб'єкти можуть бути користувачами, ресурсами, процесами, доменами, локальною мережею тощо.

**Особливості ОС Windows**

Ідентифікатор безпеки (SID) - це числове значення із змінною довжиною, яке складається з номера структури SID, 48-бітного ідентифікатора авторизації та змінного числа 32-бітових блоків, які складають фактичний унікальний ідентифікатор об'єкта та відносний ідентифікатор (RID)[20] (рис.2.4).



Рис. 2.4. Ідентифікатор безпеки [21]

Ідентифікатор авторизації - це номер, який визначає, хто створив або надав цей SID.

Фактичний ідентифікатор - унікальний ідентифікатор фактичного об'єкта.

RID - це відносний ідентифікатор, індекс або ідентифікатор для SID. 1128 RID означає, що в системі вже створено 1128 SID.

Кожен користувач, група та мережевий пристрій, а також сеанс входу має унікальний ідентифікатор SID. Процес Winlogon відповідає за створення унікального SID для кожного сеансу інтерактивного входу. SID для сеансу входу зазвичай є S-1-5-5-0, з випадково сформованим номером для RID.

**Особливості ОС Linux**

Користувач ідентифікується за допомогою імені користувача, коли він входить до системи. Внутрішній користувач ідентифікується за допомогою унікального номера користувача (UID), що є числовим значенням, яке вибирає системний адміністратор під час створення облікового запису. У більшості випадків вибір унікальних ідентифікаторів для кожного користувача необов’язковий. Відображення імені користувача в UID зберігається у файлі "/etc/passwd". Суперкористувач, також відомий як root, має UID = 0. Кожен користувач належить до однієї або декількох груп. Група ідентифікується з ідентифікаційним номером групи (GID) на короткий термін [22].

**Порівняння ОС Windows та ОС Linux**

Незважаючи на різницю в назвах, обидві ОС застосовують поняття ідентифікатора, щоб однозначно ідентифікувати суб’єкт з точки зору контексту безпеки. Обидві системи генерують ідентифікатори для сеансу входу, користувачів та груп. Основна різниця полягає в тому, де кожна система зберігає свої ідентифікатори. У ОС Windows SID зберігаються в реєстрі під розділом "HKLM\Security"; тоді як в ОС Linux вони зберігаються у файлі "/etc/passwd".

**2.4. Токен доступу**

Токен доступу (ТД) - це структура даних, яка ідентифікує власника. ТД є об'єктом даних, який зберігається в пам'яті і додається кожного разу, коли виникає новий процес. ОС обробляє створення та додавання ТД при виникненні нового процесу або потоку [23].

**Особливості ОС Windows**

У ОС Windows інформація в ТД включає в себе SID, SID-групи, права та дискретний список контролю доступу (ДСКД) облікового запису користувача, пов'язані з процесом або потоком. Коли користувач успішно входить в систему, процес Winlogon створює початковий ТД, що представляє користувача, і привласнює ТД до початкових процесів, які він запускає, за вмовчання, процес Userinit.exe. Оскільки похідні процеси за вмовчання успадковують копію ТД від свого творця, всі процеси в сеансі користувача виконуються за одним ТД. Іншими словами, копія ТД додається до кожного процесу та потоку, який виконує від імені користувача. На рисунку 2.5 зображено структуру даних ТД в ОС Windows.



Рис. 2.5 ТД до ОС Windows [24]

ТД до ОС Windows містить наступні елементи:

1. SID для облікового запису користувача;
2. SID для груп, членом яких є користувач;
3. SID ідентифікації, який ідентифікує поточний сеанс входу;
4. перелік прав, що належать або користувачеві, або групам користувачів;
5. SID для первинної групи;
6. стандартний ДСКД, який використовує система, коли користувач створює захищений об'єкт, не вказавши дескриптор безпеки;
7. джерело ТД;
8. інша статистика.

**Особливості ОС Linux**

У ОС Linux ТД є об'єктами даних, які зберігаються в пам'яті і додаються кожного разу, коли виникає новий процес. Компонент керування сеансом обробляє створення та додавання ТД, коли створюється новий процес або потоки. На рисунку 2.6 представлені різні елементи ТД в системах на базі ОС Linux.



Рис. 2.6 ТД до ОС Linux [25]

ТД до ОС Linux містить наступні елементи:

1. ідентифікатор користувача (User identifier, UID) для облікового запису користувача;
2. ідентифікатори груп представляють UID груп, в яких користувач є членом;
3. перелік пільг та прав користувачів;
4. UID для основної групи.

**Порівняння ОС Windows та ОС Linux**

Обидві ОС Windows та ОС Linux використовують концепцію ТД, хоча кожна з них має інший підхід до його реалізації. Різниця в тому, що, на відміну від ОС Windows, яка зберігає обмеження в ТД, ОС Linux використовує вибірковий контроль доступу (DAC) та обов'язковий контроль доступу (MAC) для накладання обмежень на певний процес.

**2.5. Список контролю доступу**

Список контролю доступу (СКД) являє собою список дозволів, що додається до об'єкта, який описує, хто може мати до нього доступ та який рівень цього доступу[26].

**Особливості ОС Windows**

У ОС Windows є два типи СКД: ДСКД та СКДС.

ДСКД (рис.2.7) - це список дозволів та заборон, тоді як СКДС (список контролю доступу до системи) визначає, які операції слід занести в журнал безпеки.



Рис. 2.7. ОС Windows ДСКД [27]

У ДСКД кожна ЗКД містить SID та маску доступу. У ДСКД можуть з'являтися чотири типи ЗКД: доступ дозволений, доступ заборонений, дозволений об'єкт і заборонений об'єкт.

На відміну від цього, СКДС містить два типи ЗКД: системний аудит ЗКД та системні аудит-об'єкти ЗКД. Ці ЗКД вказують, які операції на об'єкті повинні бути перевірені. Інформація аудиту зберігається в журналі системного аудиту. Як успішні, так і невдалі спроби можуть бути записані. На рисунку 2.8. наведено приклад перевірки доступу. Очевидно, що користувач DaveC допускається для читання та запису об'єкту, тоді як групі Writers відмовляють в читанні та запису на той самий об'єкт.



Рис.2.8 ОС Windows ДСКД [28]

**Особливості ОС Linux**

Контроль доступу до ОС Linux здійснюється через файлову систему. Кожен файл або каталог має ряд атрибутів, включаючи ім'я файлу, біти дозволів, UID та GID. UID файлу визначає його власника. Біти дозволів використовуються для визначення дозволів для читання (r), запису (w) та виконання (x) файлу для користувача, для членів групи користувачів та для всіх інших користувачів у системі. Наприклад, дозвіл типу "rwxr-x-x" вказує, що власник може читати, писати та виконувати файл; учасники групи мають право лише читати та виконувати його, а всі інші можуть виконувати лише файл. Тире "-" у наборі дозволів вказує на те, що права доступу заборонені. Більшість систем ОС Linux сьогодні також підтримують певну схему СКД.

Крім того, кожен процес в ОС Linux має ідентифікатор UID, а також ефективний та дійсний GID, пов'язаний з ним. Кожного разу, коли процес намагається отримати доступ до файлу, ядро ​​використовуватиме ефективний ідентифікатор UID та GID процесу, щоб порівняти їх з ідентифікатором UID та GID, пов'язаним з файлом, та вирішити, чи надавати запит.

**Порівняння ОС Windows та ОС Linux**

Обидві ОС Windows і ОС Linux реалізують концепцію контролю доступу; однак існують деякі відмінності між ними. ОС Windows використовує права та обмеження, щоб забезпечити виконання системних політик, таких як заборона видалення чи читання системного файлу; в той час як ОС Linux використовує обов'язковий контроль доступу або MAC для обмеження доступу до системних об'єктів.

**2.6. Права користувачів**

Права користувача впливають на можливість читати та змінювати файли в системі. Права користувача, також відомі як привілеї, призначаються адміністраторами для окремих користувачів або груп як частину налаштувань безпеки ОС.

**Особливості ОС Windows**

У ОС Windows привілеєм є право облікового запису виконувати певну операцію, пов'язану з системою, наприклад, вимкнення комп'ютера або зміна системного часу чи доступу до реєстру. Права користувачів завжди перевіряються у відповідь на запити на вхід в систему. З цією метою Локальна служба безпеки (LSA) отримує права облікового запису, призначені даному користувачеві, з БД політики LSA під час спроби входу в систему.

Ще одна форма привілеїв існує в ОС Windows, вони називаються політикою обмежень ПЗ, які дозволяють адміністраторам контролювати, керувати та відключати функції встановлених програм у своїх системах.

**Особливості ОС Linux**

ОС Linux використовує MAC для забезпечення привілеїв. MAC включає в себе аспекти, які користувач не може контролювати або яких зазвичай не дозволяють контролювати. Об'єкти позначаються мітками, що відображають чутливість інформації, що міститься всередині. MAC обмежує доступ до об'єктів на основі їх чутливості [29].

**Порівняння ОС Windows та ОС Linux**

ОС Linux не реалізує концепцію привілеїв в окремому процесі, як ОС Windows, що використовує LSA, але вона використовує обов'язковий контроль доступу або MAC для обмеження доступу до системних об'єктів. Крім того, ОС Linux не реалізовує концепцію програмних обмежень; скоріше, вона використовує окремий демон для виконання певної конфігурації безпеки для певних програм.

**2.7. Автентифікація**

Автентифікація - це процес перевірки ідентичності користувача, який має доступ до системи або іншого джерела інформації. В сучасних ОС автентифікація зазвичай виконується за допомогою використання імені користувача та пароля.

**Особливості ОС Windows**

Інтерактивний вхід відбувається через взаємодію процесу входу в систему Winlogon (Winlogon.exe), ПЛСБ, одного або декількох пакетів автентифікації та SAM або AD.

Пакети автентифікації - це бібліотеки DLL, яка виконує перевірки автентичності.

Kerberos - це пакет перевірки автентичності ОС Windows для інтерактивного входу до домену, а MSV1\_0 - це пакет перевірки автентичності ОС Windows для інтерактивного входу на локальний комп'ютер.

GINA - Msgina (\Windows\System32\Msgina.dll). Msgina представляє стандартне діалогове вікно входу в систему ОС Windows. На рисунку 2.9 показані різні компоненти, що беруть участь у процесі входу в систему ОС Windows.

ОС Windows використовує протокол NTLM2 (NT LAN Manager 2) для автентифікації. Пакет автентифікації за вмовчання, що реалізує цей протокол MSV1\_0 (\Windows\System32\Msv1\_0.dll).

Перелік етапів процесу входу в ОС Windows:

1. користувач отримує доступ до клієнтського комп'ютера та надає доменне ім'я, ім'я користувача та пароль;
2. клієнт обчислює криптографічний хеш (HMAC-MD5);
3. клієнт надсилає ім'я користувача на сервер;
4. сервер створює 16-байтове випадкове число і надсилає її клієнту;
5. клієнт шифрує його і повертає результат на сервер;
6. сервер надсилає наступні три пункти на сервер SAM: ім'я користувача, виклик, надісланий клієнтові, та відповідь, отриману від клієнта;
7. сервер SAM використовує ім'я користувача для отримання хешу пароля користувача з БД SAM. Він використовує цей хеш-пароль (HMAC-MD5) для шифрування за допомогою DES із завданням;
8. сервер SAM порівнює зашифрований виклик, який він обчислив, і відповідь, обчислену клієнтом. Якщо вони однакові, автентифікація буде успішною.



Рис. 2.9 Процес входу в ОС Windows [30]

**Особливості ОС Linux**

На майже всіх дистрибутивах ОС Linux інформація користувача зберігається в "/etc/passwd", текстовому файлі, що містить ім'я користувача, його зашифрований пароль, UID, GID, необов'язкове поле коментарів (зазвичай містить такі елементи, як справжнє ім'я користувача, номер телефону тощо), їх домашній каталог та їх переважну оболонку [31]. Типовий запис у "/etc/passwd" може виглядати так:

dave: T4xcQ1Nnx7PRE: 1000: 1000: David Doe, 1-700 -: / home / dave: / bin / bash

**Тіньові паролі**. Файл "/etc/passwd", який містить інформацію про всіх користувачів, включаючи їх зашифровані паролі, доступний для читання всіма користувачами, що дозволяє будь-якому користувачеві отримати зашифрований пароль усіх користувачів. Програми розбиття паролів є широко доступними.

Інформація про групу зберігається в "/etc/group". Формат аналогічний формату "/etc/passwd"., в якому містяться поля для імені групи, пароля, числового ідентифікатора (gid) та списку членів групи, розділених комою. Вступ до "/etc/group" може виглядати так:

edu: x: 13: студент, інструктор, асистент

**Шифрування MD5**. Традиційно паролі ОС Linux були зашифровані за допомогою стандартної функції crypt(). Коли з'явився Інтернет, стали доступні інструменти для розповсюдження завдання розбиття паролів на декількох хостах. Багато нових дистрибутивів постачається з можливістю шифрування паролів з більш сильним алгоритмом хешу MD5.

Порівняння ОС Windows та ОС Linux

Очевидно, що Windows реалізує більш безпечний та елегантний механізм, ніж ОС Linux. По-перше, Windows використовує HMAC-MD5 як хеш-функцію, яка є додатком до MD5, що використовує ОС Linux. По-друге, Windows в деяких місцях виконує шифрування за допомогою Advanced Encryption Standard (AES). ОС Linux не використовує будь-який симетричний алгоритм шифрування. Нарешті, значення хешування зберігаються в Windows у файлі SAM; в той час як в ОС Linux він зберігається у файлі з ім'ям "/etc/passwd".

**2.8. Файлова система**

Комп'ютерні файлові системи використовуються на пристроях зберігання даних, таких як жорсткий диск, для підтримки фізичного розташування комп'ютерних файлів. Файлова система ефективно організовує дані та дозволяє користувачам створювати, копіювати, вставляти та видаляти файли.

**Особливості ОС Windows**

Файлова система New Technology File System (NTFS) є оригінальним форматом файлової системи Windows. NTFS містить ряд додаткових функцій, таких як безпека файлів і каталогів, квоти на диски, стиснення файлів, символьні посилання на основу каталогу, можливість відновлення та шифрування.

Шифрування файлової системи (EFS), яку користувачі можуть використовувати для убезпечення конфіденційних даних, є необхідним елементом файлової системи NTFS. Нижче наведено список кроків, пов'язаних із шифруванням файлу під EFS:

1. коли файл зашифровано, файлова система генерує ключ шифрування файлу випадкових чисел (FEK). FEK використовується для шифрування вмісту файлу за допомогою додаткового стандарту шифрування (AES);
2. FEK зберігається разом із файлом, але зашифровано за допомогою відкритого ключа користувача EFS, використовуючи RSA;
3. після того, як EFS завершить ці кроки, файл захищений. Інші користувачі не можуть розшифрувати дані без розшифрованого файлу FEK, і вони не можуть розшифрувати FEK без приватного ключа.

**Особливості ОС Linux**

Файлова система в ОС Windows має більше функцій безпеки, ніж у ОС Linux; однак, дистрибутиви ОС Linux використовують списки контролю доступу до розширеного доступу (EACL) як частину своєї файлової системи, що призводить до збільшення кількості NTFS. Цей механізм дозволяє визначати дозволи доступу для трьох класів користувачів: власника файлу, групи файлів та інших. Ці дозволи можуть бути використані для запобігання доступу певного користувача, який належить до певного класу, до даних файлу іншого користувача, якому він не має права доступу.

**Порівняння ОС Windows та ОС Linux**

На відміну від Windows, ОС Linux не забезпечує шифрування файлів як частину власної файлової системи; однак, ОС Linux за допомогою сторонніх інструментів може досягти певного рівня шифрування файлів і каталогів, таких як GnuPG за допомогою команди gpg.

Результати порівняння ОС за категоріями функцій щодо безпеки наведено у табл..2.1.

Таблиця 2.1.

Порівняння ОС Windows та ОС Linux

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Категорія** | **Технології** | **OC Windows** | **OC Linux** | **Якісніша ОС** |
| Базова безпека | Автентифікація, Контроль доступу, Шифрування, Аудит | Kerberos, PKI, Access Control lists, Microsoft Cryptoapi | Pluggable Authentication Modules, Kerberos, PKI, Winbind, LSM | Linux |
| Безпека мережі | Автентифікація на мережевому рівні | SSL, SSH, LDAP, IPSec | OpenSSL, Open SSH, OpenLDAP, IPSec | Обидві ОС |
| Безпека ПЗ | Антивірус,Firewall,Сканування ПЗ,Підтримка смарт-карт | IIS, Exchange/Outlook,PCKS 11 | OpenAV, Panda, firewall, Apache sandmail, Postfix | Linux |
| Безпека встановлення | Налаштування,Адміністрування,Пошук вразливостей | Admin GUI | Bastille, Nessus, YaST, Webmin | Обидві ОС |
| Страхування | Common Criteria Certification | Windows EAL4 | Linux EAL3 | Windows |
| Надійність обчислень | Trusted Platform Module, Тестування ПЗ | Next-Generation Secure Computing Base | Trusted Platform Module device driver open sourced by IBM | Linux |
| Відкритість стандартів | IPSec, POSIX, Common Criteria | Не відповідає всім відкритим стандартам | Відповідає всім відкритим стандартам | Linux |

Отже, як випливає з результатів аналізу, з точки зору ІБ ОС Linux перевершує ОС Windows, незважаючи на те, що в них схожа реалізація деяких функцій. Наприклад, обидві ОС реалізують концепцію контролю доступу, ОС Windows використовує права та обмеження, щоб забезпечити виконання системних політик, таких, як заборона видалення чи читання системного файлу. В той час як ОС Linux використовує обов'язковий контроль доступу або MAC для обмеження доступу до системних об'єктів, що набагато ефективніше. Загалом, ОС було порівняно за сімома параметрами і чотири із них краще реалізовані в ОС Linux, що підтверджує її статус як найбільш захищеної ОС.

**2.9. Висновки до розділу**

Модель безпеки операційної системи - це набір технологій, які забезпечують моніторинг та керування різними компонентами безпеки ОС. Основні складові моделі безпеки:

1. ідентифікація;
2. ТД;
3. права користувачів;
4. автентифікація;
5. СКД.

В цілому, моделі безпеки ОС Microsoft Windows та ОС Linux подібні, але в них відрізняються декілька атрибутів, таких як шифрування файлової системи та привілеї ПЗ, які є у ОС Windows і ОС Linux, а також тіньовий пароль, який є тільки в ОС Linux. Крім того, ОС Windows використовує такі складні функції, як аудит; в той час як ОС Linux використовує ефективні файли журналів з шифруванням. В цілому, обидві ОС забезпечують багаторівневі технології безпеки, що робить їх надійними та здатними впоратися з атаками, а також забезпечити безпечне середовище для користувачів.

**РОЗДІЛ III**

**МОДЕЛЮВАННЯ СИСТЕМИ ОБОВ’ЯЗКОВОГО КОНТРОЛЮ ДОСТУПОМ ДЛЯ ОС СІМЕЙСТВА WINDOWS**

**3.1. Розробка моделі загроз та моделі порушника**

Модель загроз -  абстрактний формалізований чи неформалізований опис методів і засобів здійснення загроз.

Модель порушника - це всебічна структурована характеристика порушника, яка використовується сумісно з моделлю загроз для розробки політики безпеки інформації.

Модель загроз і модель порушника є вихідною інформацією для розроблення політики безпеки і проектування будь-яких систем захисту.

**3.1.1. Розробка моделі порушника**

Порушник – це особа, яка помилково, внаслідок необізнаності, цілеспрямовано, за злим умислом або без нього, використовуючи різні можливості, методи та засоби здійснила спробу виконати операції, які призвели або можуть призвести до порушення властивостей інформації, що визначені політикою безпеки.

Модель порушника відображає його практичні та потенційні можливості, знання, час та місце можливої дії тощо (табл.3.1.).

Основні цілі порушника :

1. самоствердження;
2. корисливий інтерес;
3. професійний обов’язок;
4. безвідповідальність.

Перечислимо основні засоби моделі порушника за рівнем кваліфікації та обізнаності щодо автоматизованої системи (АС):

1. знає функціональні особливості системи;
2. володіє високим рівнем знань та практичними навичками роботи з технічними засобами системи та їх обслуговування;
3. володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації автоматизованих інформаційних систем;
4. знає структуру, функції й механізми дії засобів захисту, їх недоліки;
5. знає недоліки механізмів захисту, які вбудовані у системне ПЗ та його недокументовані можливості;
6. є розробником програмних та програмно-апаратних засобів захисту або системного ПЗ.

Модель порушника за показником можливостей використання засобів та методів подолання системи захисту:

1. використовує лише агентурні методи одержання відомостей;
2. використовує пасивні засоби (технічні засоби переймання без модифікації компонентів системи);
3. використовує лише штатні засоби та недоліки системи захисту;
4. застосовує методи та засоби дистанційного (з використанням штатних каналів та протоколів зв’язку) упровадження програмних закладок.

Щодо характеру дій порушника за часом дії можемо визначити такі пункти:

1. до впровадження АС або її окремих компонентів;
2. під час бездіяльності компонентів системи (в неробочій час, під час планових перерв у роботі, перерв для обслуговування і ремонту);
3. під час функціонування АС (або компонентів системи).

За місцем дії порушників можна класифікувати:

1. без доступу на контрольовану територію організації;
2. з контрольованої території без доступу у будинки та споруди;
3. усередині приміщень, але без доступу до технічних засобів АС;
4. з робочих місць користувачів (операторів) АС.

Таблиця 3.1.

Модель порушника

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№** | **Порушник** | **Класифікація по відношенню до об’єкта** | **Мотиви порушника** | **Рівень кваліфікації** | **Можливість використання методів для подолання системи захисту** | **Рівень порушника** |
| 1 | АС | Внутрішні | Корисливий інтерес | Знає структуру, функції і механізм дії засобів захисту | Застосовує методи та засоби активного впливу | 4 |
| 2 | ОП | Внутрішні | Корисливий інтерес | Має достатній рівень знань і досвід роботи з технічними засобами системи, знає функціональні особливості АС | Застосовує методи та засоби активного впливу, використовує тільки штатні засоби та недоліки системи захисту | 3 |
| 3 | ВК | Внутрішні | Безвідповідальність, корисливий інтерес  | Знає функціональні особливості АС, основні закономірності формування в ній масивів даних і потоків запитів до них | Використовує тільки штатні засоби та недоліки системи захисту для її подолання. | 2 |
| 4 | КС | Внутрішні | Самоствердження, корисливий інтерес | Уміє користуватися штатними засобами | Використовує тільки штатні засоби та недоліки системи захисту для її подолання | 1 |
| 5 | Навмисний зловмисник | Зовнішні | Корисливий інтерес | Має високий рівень знань в області програмування | Застосовує модифікацію та підключення додаткових технічних засобів | 3 |

**3.1.2. Розробка моделі загроз**

При обробці персональних даних в АС, що мають підключення до мереж зв'язку загального користування і (чи) мережам міжнародного інформаційного обміну, можлива реалізація наступних загроз:

1. загрози витоку інформації по технічних каналах;
2. загрози до персональних даних, що обробляються на автоматизованому робочому місці і в мережі;
3. аналізу мережевого трафіку з перехопленням інформації по мережі інформації;
4. загрози виявлення паролів;
5. загрози віддаленого запуску додатків;
6. загрози впровадження по мережі шкідливих програм;
7. загрози DoS -атак.

Джерела загроз:

1. персонал;
2. сторонні особи;
3. недостатність, чи погана якість апаратних та програмних засобів;
4. стихійні лиха.

Ненавмисні загрози:

1. стихійні явища (пожежа, аварії);
2. збої та відмови системи електроживлення;
3. збої та відмови обчислювальної техніки;
4. збої, відмови та пошкодження  носіїв інформації;
5. збої та відмови ПЗ.

Загрози інформаційним ресурсам можна в загальному випадку класифікувати (табл.3.2.):

1. загрози конфіденційності:
2. розкрадання (копіювання) інформації і засобів її обробки (носіїв);
3. втрата (ненавмисна втрата, витік) інформації і засобів її обробки (носіїв);
4. загрози доступності:
	1. блокування інформації;
	2. знищення інформації і засобів її обробки (носіїв);
5. загрози цілісності:
	1. модифікація (спотворення) інформації;
	2. заперечення достовірності інформації;
	3. нав'язування помилкової інформації, обман.

При цьому:

Розкрадання і знищення інформації розуміється аналогічно по застосуванню до матеріальних цінних ресурсів. Знищення комп'ютерної інформації - стирання інформації в пам'яті ЕОМ.

Копіювання інформації - повторення і стійке збереження інформації на машинному або іншому носієві.

Ушкодження - зміна властивостей носія інформації, при якому істотно погіршується його стан, втрачається значна частина його корисних властивостей і він ставати повністю або частково непридатним для цільового використання.

Модифікація інформації - внесення будь-яких змін, окрім пов'язаних з адаптацією програми для ЕОМ або баз даних (БД) для комп'ютерної інформації.

Блокування інформації - несанкціоноване утруднення доступу користувачів до інформації, не пов'язане з її знищенням.

Обман (заперечення достовірності, нав'язування помилкової інформації) - умисне спотворення або приховання істини з метою ввести в оману особу, у веденні якої знаходиться майно, і таким чином добитися від добровільної передачі майна.

Таблиця 3.2.

Модель загроз

|  |  |
| --- | --- |
| **Потенційні загрози інформації** | **Потенційні загрози інформації** |
| **К** | **Ц** | **Д** | **С** |
| Загрози об’єктивної природи |
| Збої та відмови обчислювальної техніки |  | + | + |  |
| Збої, відмови та пошкодження носіїв інформації |  | + | + |  |
| Збої та відмови ПЗ |  | + | + |  |
| Загрози суб’єктивної природи |
| Помилки адміністраторів (неправильна настройка та адміністрування системи захисту, операційної системи; неправомірне відключення засобів захисту). | + | + | + |  |
| Несанкціоноване перехоплення інформації | + | + | + | + |
| Несанкціоноване підключення до технічних засобів | + |  |  |  |
| Порушення нормальних режимів роботи |  | + | + | + |
| Ураження ПЗ комп’ютерними вірусами | + | + | + | + |
| Втрата засобів розмежування доступу (паролів) (розголошення), магнітних носіїв інформації та резервних копій | + | + | + | + |
| Несанкціоноване внесення змін до технічних засобів, в ПЗ, в компоненти інформаційного забезпечення, тощо |  | + | + | + |
| Використання недозволеного ПЗ або модифікація компонентів ПЗ |  | + | + | + |
| Пошкодження носіїв інформації |  |  | + |  |
| Зовнішні загрози | + | + | + | + |
| Несанкціоноване перехоплення інформації шляхом витоку інформації за рахунок побічного електромагнітного випромінювання та наводок | + |  |  |  |

**3.2. Методи керування доступом**

Більшість ОС мають засоби і методи управління доступом, які в свою чергу визначають, чи може якийсь об'єкт на рівні ОС (користувач або програма) отримати доступ до певного ресурсу. Використовуються такі методи управління доступом.

DAC. Даний метод реалізує обмеження доступу до об'єктів на основі груп, до яких вони належать. В ОС, в основі цього методу лежить стандартна модель контролю доступу до файлів. Права доступу визначені для наступних категорій: користувач (власник файлу), група (всі користувачі, які є членами групи), інші (всі користувачі, які не є ні власниками файлу, ні членами групи). Причому до кожної з груп надаються такі права: права на запис, на читання і на виконання [31].

MAC. Cуть цього методу полягає у встановленні певних прав доступу суб'єкта до певних об'єктів. В ОС реалізовано наступне: програма має тільки ті можливості, які необхідні їй для виконання своїх завдань, і не більше того. Даний метод має перевагу в порівнянні з попереднім; якщо в програмі буде виявлена уразливість, то можливості її доступу будуть обмежені.

Контроль доступу на основі ролей (RBAC). Права доступу реалізовані у вигляді ролей, які видаються системою безпеки. Ролі - певні повноваження на виконання конкретних дій групою суб'єктів над об'єктами в системі. Дана політика є поліпшенням DAC.

**3.2.1. Вибірковий контроль доступу**

DAC — управління доступом суб'єктів до об'єктів на основі списків управління доступом або матриці доступу.

Приклад: суб'єкт доступу "Користувач № 1" має право доступу тільки до об'єкта доступу № 3, тому його запит до об'єкта доступу № 2 відхиляється. Суб'єкт "Користувач № 2" має право доступу як до об'єкта доступу № 1, так і до об'єкта доступу № 2, тому його запити до даних об'єктів не відхиляються.

Для кожної пари (суб'єкт - об'єкт) має бути задане явне і недвозначне перерахування припустимих типів доступу (читати, писати і т.д.), Тобто тих типів доступу, які є санкціонованими для даного суб'єкта (індивіда або групи індивідів) до даного ресурсу (об'єкту).

DAC є основною реалізацією розмежувальної політики доступу до ресурсів при обробці конфіденційних відомостей, відповідно до вимог до системи захисту інформації.

**3.2.2. Oбов'язковий контроль доступу**

MAC — розмежування доступу суб'єктів до об'єктів, засноване на призначенні мітки конфіденційності для інформації, що міститься в об'єктах, і видачу офіційних дозволів (допуску) суб'єктам на звернення до інформації такого рівня конфіденційності. Це спосіб поєднує захист і обмеження прав, що застосовується відносно до комп'ютерних процесів, даних і системних пристроїв, і призначений для запобігання їх небажаного використання.

Приклад: суб'єкт "Користувач № 2", який має допуск рівня "не таємно", не може отримати доступ до об'єкта, що має мітку "для службового користування". У той же час, суб'єкт "Користувач № 1" з допуском рівня "секретно" право доступу до об'єкта з міткою "для службового користування" має.

При цьому дана модель доступу не використовується ізольовано, зазвичай на практиці вона доповнюється елементами інших моделей доступу.

Для файлових систем, MAC може розширювати або заміняти DAC і концепцію користувачів і груп.

Найважливіша перевага полягає в тому, що користувач не може повністю контролювати доступ до ресурсів, які він створює.

Політика безпеки системи, встановлена адміністратором, повністю визначає доступ, і зазвичай користувачеві не дозволяється встановлювати більш вільний доступ до його ресурсів ніж той, який встановлений адміністратором користувачеві.

**3.2.3. Контроль доступу на основі ролей**

RBAC — розширення політики виборчого управління доступом; при цьому права доступу суб'єктів системи на об'єкти групуються з урахуванням специфіки їх застосування, утворюючи ролі [32].

Формування ролей покликане визначити чіткі і зрозумілі для користувачів комп'ютерної системи правила розмежування доступу. RBAC  дозволяє реалізувати гнучкі, що змінюються динамічно в процесі функціонування комп'ютерної системи, правила розмежування доступу.

Так як привілеї не призначаються користувачам безпосередньо і купуються ними тільки через свою роль (або ролі), управління індивідуальними правами користувача по суті зводиться до призначення йому ролей. Це спрощує такі операції, як додавання користувача або зміна підрозділу користувачем.

**3.3. Моделювання "Windows MAC"**

Основна мета "Windows MAC" – це розмежування доступу суб'єктів до об'єктів, засноване на призначенні мітки конфіденційності для інформації, що міститься в об'єктах. Цей спосіб поєднує захист і обмеження прав.

**3.3.1. Недоліки стандартної DAC**

Для того, щоб зрозуміти, в чому полягає практична цінність MAC, розглянемо кілька прикладів, коли стандартна система контролю доступу недостатня. Якщо MAC відключена, то доступна тільки класична система контролю доступу, яка включає в себе DAC або списки контролю доступу. Тобто мова йде про маніпулювання правами на запис, читання і виконання на рівні користувачів і груп користувачів, чого в деяких випадках може бути недостатньо.

Приклад: адміністратор не може в повній мірі контролювати дії користувача. Користувач цілком здатний дати всім іншим користувачам права на читання власних конфіденційних файлів, таких як ключі SSH.

Процеси можуть змінювати налаштування безпеки. Файли, що містять в собі пошту користувача повинні бути доступні для читання тільки одному конкретному користувачеві, але поштовий клієнт цілком може змінити права доступу так, що ці файли будуть доступні для читання всім.

Процеси успадковують права користувача, який їх запустив. Інфікована трояном версія браузера Firefox в стані читати SSH-ключі користувача, хоча не має для того жодних підстав.

В цілому, в традиційній моделі DAC добре реалізовані тільки два рівня доступу - користувач і привілейований користувач. Немає простого методу, який дозволив би встановлювати для кожного користувача необхідний мінімум привілеїв.

Звичайно, є безліч методів обходу цих проблем в рамках класичної моделі безпеки, але жоден з них не є універсальним.

**3.3.2. Вирішення проблем стандартної DAC**

"Windows MAC" (рис.3.1) має слідувати моделі мінімально необхідних привілеїв для кожного сервісу, користувача і програм. За вмовчання буде встановлено "режим заборони", коли кожен елемент системи має тільки ті права, які необхідні йому для функціонування. Якщо ж користувач, програма або сервіс намагаються змінити файл або отримати доступ до ресурсу, який не потрібен для вирішення їх завдань, то їм буде відмовлено в доступі, а така спроба буде зареєстрована в журналі [33].



Рис. 3.1.Система обов’язкового контролю доступом [34]

"Windows MAC" має бути реалізованою на рівні ядра, так що прикладні програми можуть зовсім нічого не знати про версії цієї системи примусового контролю доступу, особливості її роботи і т.д. У разі коректного налаштування, "Windows MAC" ніяк не вплине на функціонування сторонніх програм і сервісів. Хоча, якщо додаток здатний перехоплювати повідомлення про помилки цієї системи контролю доступу, зручність користування таким додатком істотно зростає. Адже в разі спроби отримати доступ до захищеного ресурсу або файлу, "Windows MAC" передасть в основний додаток помилку з сімейства "access denied". Але лише деякі додатки будуть використовувати одержувані від "Windows MAC" коди повернення системних викликів.

Ось кілька прикладів використання "Windows MAC", які дозволяють побачити, яким чином можна збільшити ступінь безпеки всієї системи: створення та налаштування списку програм, які можуть читати ssh-ключі, запобігання несанкціонованого доступу до даних через mail-клієнт, налаштування браузера таким чином, щоб він міг читати в домашній папці користувача тільки необхідні для функціонування файли і папки.

**3.3.3. Суб'єкти і об'єкти**

Суб'єкти - це користувачі, які виконують будь-які операції на комп'ютері. Однак користувачі завжди діють через ті чи інші прикладні програми. Тому, під суб'єктами найчастіше маються на увазі саме програми (процеси). Інакше кажучи, суб'єкти - це ті, хто виконує якісь дії.

Об'єкти - це те, над чим дії виконуються. Найчастіше під об'єктами маються на увазі файли даних. Але це можуть бути і пристрої, і навіть програми.

**3.3.4. Режими роботи "Windows MAC"**

"Windows MAC" повинен мати три основних режими роботи, при цьому за вмовчання має бути встановлено режим Enforcing. Це досить жорсткий режим, і в разі необхідності він може бути змінений на більш зручний для кінцевого користувача [35].

**Enforcing**: Режим за вмовчання. При виборі цього режиму всі дії, які якимось чином порушують поточну політику безпеки, будуть блокуватися, а спроба порушення буде зафіксована в журналі.

**Permissive:** У разі використання цього режиму, інформація про всі дії, які порушують поточну політику безпеки, будуть зафіксовані в журналі, але самі дії не будуть заблоковані.

**Disabled:** Повне відключення системи примусового контролю доступу.

**3.3.5. Контекст безпеки "Windows MAC"**

Це набір даних, який складається з:

1. типу користувача;
2. ролі;
3. типу даних або домена процесу;
4. рівнів і категорій.

Контекст безпеки (рис.3.2) записується в атрибути файлу (в файловій системі) і створюється при встановленні "Windows MAC". Уже присвоєний контекст безпеки може бути згодом змінений.



Рис. 3.2.Контекст безпеки [36]

Якщо файлова система не підтримує запис міток "Windows MAC", тоді мітки записуються окремо від файлів, при цьому зв'язок між файлами і мітками відбувається по коліях файлів.

Мітка файлу може виявитися невірною навіть в разі, якщо файлова система підтримує запис таких міток, але до файлу були неправильно застосовані операції копіювання або переміщення всередині файлової системи. Наприклад при копіюванні в іншу папку файл може отримати мітку, встановлену для цієї папки, замість тієї мітки, яка у нього була раніше.

**3.3.6. Користувач "Windows MAC"**

Це описовий тип користувача, а не якийсь конкретний користувач з логіном і паролем. Принципово це те ж саме, що і група користувачів в системі безпеки DAC. При додаванні в систему кожного нового користувача він за вмовчання (або явно) зіставляється з будь-яким типом користувача "Windows MAC" і надалі матиме ті дозволи або заборони, які вказані для його типу користувача [37].

**3.3.7. Роль у "Windows MAC"**

Роль – це перелік дозволених дій. В системі має бути можливим перехід з однієї ролі в іншу для зміни повноважень. При цьому ідентичність користувача не змінюється. Ролі не поєднуються, вони замінюють одна одну.

Політика безпеки визначає допустимі переходи з однієї ролі в іншу. Тобто неможливо перейти з будь-якої ролі в будь-яку роль. Оскільки ролі завжди пов'язані з типами (доменами), то часто говорять не про зміну ролей, а про зміну домену.

**3.3.8. Домени "Windows MAC"**

Домени об'єднують суб'єкти та об'єкти в групи, всередині цих груп визначають дозволені дії суб'єктів над об'єктами. Для суб'єктів замість терміна "тип" використовується термін "домен".

У "Windows MAC", в загальних політиках, використовується механізм примусового присвоєння типів. Тобто кожен об'єкт і суб'єкт повинен бути обов'язково приведеним до якого-небудь типу (або домену) [38].

**3.3.9. Політика "Windows MAC"**

Політика "Windows MAC" - це сукупність усіх описаних в системі співвідношень користувач - роль - тип (домен) - рівень і категорія (рис.3.3).



Рис. 3.3.Політика MAC [39]

Політика targeted - всі процеси не внесені в спеціальні обмежені домени, працюють в необмеженому домені unconfined\_t. Таким чином здійснюється можливість виконання процесів, які ще не описані в політиці. Але такі процеси фактично виконуються майже з адміністративними правами. У цьому слабке місце політики targeted.

Політика strict - всі процеси працюють в спеціальних обмежених доменах, в необмеженому домені unconfined\_t ніхто не працює. Політика strict використовується вузькоспеціально, оскільки потрібне її налаштування для кожного конкретного випадку. Адже процеси не описані в цій політиці просто не будуть працювати. Але зате ця політика забезпечує повний захист в рамках тих можливостей, які є в "Windows MAC".

**3.3.10. Контроль доступу в "Windows MAC"**

"Windows MAC" надає наступні моделі управління доступом:

Type Enforcement (TE): основний механізм контролю доступу, який використовується в цільових політиках. Дозволяє детально, на найнижчому рівні управляти дозволами. Найгнучкіший, але і найбільш трудомісткий для системного адміністратора механізм.

Role-Based Access Control (RBAC): в цій моделі права доступу реалізуються в якості ролей. Роль - сукупність прав доступу на об’єкти комп’ютерної системи. RBAC є подальшим розвитком TE.

Multi-Level Security (MLS): багаторівнева модель безпеки, в якій всім об'єктам системи присвоюється певний рівень доступу. Дозвіл або заборона доступу визначається тільки співвідношенням цих рівнів.

Всі процеси і файли в рамках "Windows MAC" мають контекст безпеки.

**3.4. Демонстрація програми-аналога для Linux**

SELinux – реалізація системи обов'язкового керування доступом, яка може працювати паралельно з класичним дискреційним керуванням доступом. Входить в стандартне ядро Linux.

**3.4.1. Налаштування режимів роботи**

Отримати інформацію про поточний стан можна за допомогою команд getenforce (рис.3.4) або sestatus (рис.3.5).



Рис. 3.4. Команда getenforce.



Рис. 3.5.Команда setstatus.

**Вискористання setenforce команди.** Щоб перейти від режиму enforcing до режиму permissive і навпаки, можна скористатися командою setenforce. Ця команда приймає "Enforcing, Permissive", 1 або 0 як аргумент.

Використання команди setenforce (рис.3.6) є корисним для тимчасового переходу з режиму або до режиму виконання. Наприклад, якщо система завантажується у дозволеному режимі, і адміністратор вважає, що система готова працювати в режимі примусового завантаження, адміністратор може використовувати setenforce 1 після завантаження, щоб увімкнути режим примусового виконання.



Рис. 3.6. Команда setenforce.

**SElinux configuration file.** (рис.3.7)Значення за вмовчання (enforcing or permissive) зберігається при завантаженні системи в файлі "/etc/selinux/config" через параметр "SELINUX".



Рис. 3.7. SELinux configuration file.

Також можна отримати огляд поточних дозволених доменів (рис.3.8), використовуючи semanage permissive -l.



Рис. 3.8.Поточні дозволені домени.

**3.4.2. Налаштування SELinux користувачів**

SELinux користувач - частина контексту (рис.3.9). Якщо повернутися до поточного контексту користувача, то можна побачити, що друге поле - це роль, а третє - домен.

****

Рис. 3.9.SELinux користувач.

Ролі, призначені для певного користувача SELinux, можна побачити за допомогою команди  semanage user -l.

Але на відміну від ролей та їх впливу на домени, можна змінити, які ролі призначаються для яких користувачів SELinux (рис.3.10). Також можна побачити різницю між користувачем SElinux та роллю SElinux.



Рис. 3.10. Ролі користувачів.

**Різниця між Linux користувачем і SELinux користувачем.** Можна побачити відображення облікових записів Linux (рис.3.11) для користувачів SELinux semanage login -l.



Рис. 3.11. Облікові записи Linux.

В наведеному вище прикладі:

1. root-користувач, звязаний з root-користувачем SELinux;
2. swift-користувач, звязаний з swift-користувачем SELinux;
3. спеціальний system\_u обліковий запис (запис для системних демонів);
4. спеціальний \_\_default\_\_ обліковий запис, який звязує всі інші облікові записи.

Обліковий запис \_\_default\_\_  вказує на те, що створені користувачі Linux мають звязатися з user\_u SELinux користувачем.

Назви груп мають обовязково починатися з символу "%"(рис.3.12). Це необхідно для того, щоб система відрізняла імена користувачів від імен груп.



Рис. 3.12. Групи SELinux.

Відповідно до наведеного вище прикладу, всі користувачі групи "%operators" буть зв’язані з staff\_u  користувачем SELinux.

**Маніпуляція інформацією про користувача SELinux.** Як зазначено вище, можна змінювати налаштування користувачів Linux. Це можна здійснити за допомогою зміни налаштувань SELinux або за допомогою зміни налаштувань ролі SELinux.

**Управління зв’язками користувачів.** Перш за все, для керування зв’язками користувачів використовуємо набір команд semanage login.

Наприклад, команда для створення зв’язку з групою "%operators" (рис.3.13).



Рис. 3.13. Зв’язок користувача з групою.

Для видалення звя’зку використовують параметр –d замість –a. Також зв’язок можна змінити за допомогою параметра –m.

Однак, якщо змінити зв’язок для користувача, який вже володіє файлами у файловій системі, дуже важливо повністю перезавантажити контекст цих файлів (рис.3.14) (наприклад, використовуючи -F з командою restorecon) або встановити нового власника SELinux і роль, використовуючи chcon.



Рис. 3.14. Оновлення власника і ролі.

Якщо цього не зробити, то це може спричинити порушення дозволів пізніше.

**Управління зв'язками користувача з роллю.** Подібно до попереднього прикладу, використовуємо semanage user для зміни зв’язків користувача з роллю.

Наприклад, щоб створити нового користувача SELinux, який називається infra\_u, та надати йому права staff\_r та sysadm\_r, потрібно скористатися наступною командою (рис.3.15):



Рис. 3.15. Створення користувача.

**3.4.3. Налаштування мережевих портів**

В основному SELinux призначений для управління доступом до файлів і каталогів, але існує безліч інших ресурсів, якими він керує. Деякі з них пов'язані з мережевими ресурсами, такими як мережеві порти. Це стає актуальним, коли потрібно змінити порт за вмовчання, який використовує демон.

Приклад: SSH демон (рис.3.16).



Рис. 3.16. SSH демон.

За допомогою команди semanage можна позначити маркер порту на іншому порті (рис.3.17). Приклад для ssh\_port\_t порту 1122.



Рис. 3.17. Маркер порту.

В межах SELinux, порти позначені, як і інші ресурси (рис.3.18).



Рис. 3.18. Порти SELinux.

У третьому стовпці вказано номер порту або діапазон портів. Якщо це діапазон, він має нижчий пріоритет, ніж певний номер порту.

Отже, для підвищення рівня ІБ необхідно використовувати дистрибутиви Linux з реалізованою системою MAC: SUSE Linux, Ubuntu. В системах з реалізованою системою DAC, необхідно підвищувати рівень інформаційної безпеки за допомогою доповнення SELinux. Використовувати ОС з системою DAC необхідно тільки тоді, коли всі права на ресурси повинні належати користувачеві.

**3.1. Розробка моделі загроз та моделі порушника**

Модель загроз -  абстрактний формалізований чи неформалізований опис методів і засобів здійснення загроз.

Модель порушника - це всебічна структурована характеристика порушника, яка використовується сумісно з моделлю загроз для розробки політики безпеки інформації.

Модель загроз і модель порушника є вихідною інформацією для розроблення політики безпеки і проектування будь-яких систем захисту.

**3.5.1. Розробка моделі порушника**

Порушник – це особа, яка помилково, внаслідок необізнаності, цілеспрямовано, за злим умислом або без нього, використовуючи різні можливості, методи та засоби здійснила спробу виконати операції, які призвели або можуть призвести до порушення властивостей інформації, що визначені політикою безпеки.

Модель порушника відображає його практичні та потенційні можливості, знання, час та місце можливої дії тощо (табл.3.1.).

Основні цілі порушника :

1. самоствердження;
2. корисливий інтерес;
3. професійний обов’язок;
4. безвідповідальність.

Перечислимо основні засоби моделі порушника за рівнем кваліфікації та обізнаності щодо автоматизованої системи (АС):

1. знає функціональні особливості системи;
2. володіє високим рівнем знань та практичними навичками роботи з технічними засобами системи та їх обслуговування;
3. володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації автоматизованих інформаційних систем;
4. знає структуру, функції й механізми дії засобів захисту, їх недоліки;
5. знає недоліки механізмів захисту, які вбудовані у системне ПЗ та його недокументовані можливості;
6. є розробником програмних та програмно-апаратних засобів захисту або системного ПЗ.

Модель порушника за показником можливостей використання засобів та методів подолання системи захисту:

1. використовує лише агентурні методи одержання відомостей;
2. використовує пасивні засоби (технічні засоби переймання без модифікації компонентів системи);
3. використовує лише штатні засоби та недоліки системи захисту;
4. застосовує методи та засоби дистанційного (з використанням штатних каналів та протоколів зв’язку) упровадження програмних закладок.

Щодо характеру дій порушника за часом дії можемо визначити такі пункти:

1. до впровадження АС або її окремих компонентів;
2. під час бездіяльності компонентів системи (в неробочій час, під час планових перерв у роботі, перерв для обслуговування і ремонту);
3. під час функціонування АС (або компонентів системи).

За місцем дії порушників можна класифікувати:

1. без доступу на контрольовану територію організації;
2. з контрольованої території без доступу у будинки та споруди;
3. усередині приміщень, але без доступу до технічних засобів АС;
4. з робочих місць користувачів (операторів) АС.

Таблиця 3.1.

Модель порушника

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№** | **Порушник** | **Класифікація по відношенню до об’єкта** | **Мотиви порушника** | **Рівень кваліфікації** | **Можливість використання методів для подолання системи захисту** | **Рівень порушника** |
| 1 | АС | Внутрішні | Корисливий інтерес | Знає структуру, функції і механізм дії засобів захисту | Застосовує методи та засоби активного впливу | 4 |
| 2 | ОП | Внутрішні | Корисливий інтерес | Має достатній рівень знань і досвід роботи з технічними засобами системи, знає функціональні особливості АС | Застосовує методи та засоби активного впливу, використовує тільки штатні засоби та недоліки системи захисту | 3 |
| 3 | ВК | Внутрішні | Безвідповідальність, корисливий інтерес  | Знає функціональні особливості АС, основні закономірності формування в ній масивів даних і потоків запитів до них | Використовує тільки штатні засоби та недоліки системи захисту для її подолання. | 2 |
| 4 | КС | Внутрішні | Самоствердження, корисливий інтерес | Уміє користуватися штатними засобами | Використовує тільки штатні засоби та недоліки системи захисту для її подолання | 1 |
| 5 | Навмисний зловмисник | Зовнішні | Корисливий інтерес | Має високий рівень знань в області програмування | Застосовує модифікацію та підключення додаткових технічних засобів | 3 |

**3.5.2. Розробка моделі загроз**

При обробці персональних даних в АС, що мають підключення до мереж зв'язку загального користування і (чи) мережам міжнародного інформаційного обміну, можлива реалізація наступних загроз:

1. загрози витоку інформації по технічних каналах;
2. загрози до персональних даних, що обробляються на автоматизованому робочому місці і в мережі;
3. аналізу мережевого трафіку з перехопленням інформації по мережі інформації;
4. загрози виявлення паролів;
5. загрози віддаленого запуску додатків;
6. загрози впровадження по мережі шкідливих програм;
7. загрози DoS -атак.

Джерела загроз:

1. персонал;
2. сторонні особи;
3. недостатність, чи погана якість апаратних та програмних засобів;
4. стихійні лиха.

Ненавмисні загрози:

1. стихійні явища (пожежа, аварії);
2. збої та відмови системи електроживлення;
3. збої та відмови обчислювальної техніки;
4. збої, відмови та пошкодження  носіїв інформації;
5. збої та відмови ПЗ.

Загрози інформаційним ресурсам можна в загальному випадку класифікувати (табл.3.2.):

1. загрози конфіденційності:
2. розкрадання (копіювання) інформації і засобів її обробки (носіїв);
3. втрата (ненавмисна втрата, витік) інформації і засобів її обробки (носіїв);
4. загрози доступності:
	1. блокування інформації;
	2. знищення інформації і засобів її обробки (носіїв);
5. загрози цілісності:
	1. модифікація (спотворення) інформації;
	2. заперечення достовірності інформації;
	3. нав'язування помилкової інформації, обман.

При цьому:

Розкрадання і знищення інформації розуміється аналогічно по застосуванню до матеріальних цінних ресурсів. Знищення комп'ютерної інформації - стирання інформації в пам'яті ЕОМ.

Копіювання інформації - повторення і стійке збереження інформації на машинному або іншому носієві.

Ушкодження - зміна властивостей носія інформації, при якому істотно погіршується його стан, втрачається значна частина його корисних властивостей і він ставати повністю або частково непридатним для цільового використання.

Модифікація інформації - внесення будь-яких змін, окрім пов'язаних з адаптацією програми для ЕОМ або баз даних (БД) для комп'ютерної інформації.

Блокування інформації - несанкціоноване утруднення доступу користувачів до інформації, не пов'язане з її знищенням.

Обман (заперечення достовірності, нав'язування помилкової інформації) - умисне спотворення або приховання істини з метою ввести в оману особу, у веденні якої знаходиться майно, і таким чином добитися від добровільної передачі майна.

Таблиця 3.2.

Модель загроз

|  |  |
| --- | --- |
| **Потенційні загрози інформації** | **Потенційні загрози інформації** |
| **К** | **Ц** | **Д** | **С** |
| Загрози об’єктивної природи |
| Збої та відмови обчислювальної техніки |  | + | + |  |
| Збої, відмови та пошкодження носіїв інформації |  | + | + |  |
| Збої та відмови ПЗ |  | + | + |  |
| Загрози суб’єктивної природи |
| Помилки адміністраторів (неправильна настройка та адміністрування системи захисту, операційної системи; неправомірне відключення засобів захисту). | + | + | + |  |
| Несанкціоноване перехоплення інформації | + | + | + | + |
| Несанкціоноване підключення до технічних засобів | + |  |  |  |
| Порушення нормальних режимів роботи |  | + | + | + |
| Ураження ПЗ комп’ютерними вірусами | + | + | + | + |
| Втрата засобів розмежування доступу (паролів) (розголошення), магнітних носіїв інформації та резервних копій | + | + | + | + |
| Несанкціоноване внесення змін до технічних засобів, в ПЗ, в компоненти інформаційного забезпечення, тощо |  | + | + | + |
| Використання недозволеного ПЗ або модифікація компонентів ПЗ |  | + | + | + |
| Пошкодження носіїв інформації |  |  | + |  |
| Зовнішні загрози | + | + | + | + |
| Несанкціоноване перехоплення інформації шляхом витоку інформації за рахунок побічного електромагнітного випромінювання та наводок | + |  |  |  |

**3.2. Методи керування доступом**

Більшість ОС мають засоби і методи управління доступом, які в свою чергу визначають, чи може якийсь об'єкт на рівні ОС (користувач або програма) отримати доступ до певного ресурсу. Використовуються такі методи управління доступом.

DAC. Даний метод реалізує обмеження доступу до об'єктів на основі груп, до яких вони належать. В ОС, в основі цього методу лежить стандартна модель контролю доступу до файлів. Права доступу визначені для наступних категорій: користувач (власник файлу), група (всі користувачі, які є членами групи), інші (всі користувачі, які не є ні власниками файлу, ні членами групи). Причому до кожної з груп надаються такі права: права на запис, на читання і на виконання [31].

MAC. Cуть цього методу полягає у встановленні певних прав доступу суб'єкта до певних об'єктів. В ОС реалізовано наступне: програма має тільки ті можливості, які необхідні їй для виконання своїх завдань, і не більше того. Даний метод має перевагу в порівнянні з попереднім; якщо в програмі буде виявлена уразливість, то можливості її доступу будуть обмежені.

Контроль доступу на основі ролей (RBAC). Права доступу реалізовані у вигляді ролей, які видаються системою безпеки. Ролі - певні повноваження на виконання конкретних дій групою суб'єктів над об'єктами в системі. Дана політика є поліпшенням DAC.

**3.6.1. Вибірковий контроль доступу**

DAC — управління доступом суб'єктів до об'єктів на основі списків управління доступом або матриці доступу.

Приклад: суб'єкт доступу "Користувач № 1" має право доступу тільки до об'єкта доступу № 3, тому його запит до об'єкта доступу № 2 відхиляється. Суб'єкт "Користувач № 2" має право доступу як до об'єкта доступу № 1, так і до об'єкта доступу № 2, тому його запити до даних об'єктів не відхиляються.

Для кожної пари (суб'єкт - об'єкт) має бути задане явне і недвозначне перерахування припустимих типів доступу (читати, писати і т.д.), Тобто тих типів доступу, які є санкціонованими для даного суб'єкта (індивіда або групи індивідів) до даного ресурсу (об'єкту).

DAC є основною реалізацією розмежувальної політики доступу до ресурсів при обробці конфіденційних відомостей, відповідно до вимог до системи захисту інформації.

**3.6.2. Oбов'язковий контроль доступу**

MAC — розмежування доступу суб'єктів до об'єктів, засноване на призначенні мітки конфіденційності для інформації, що міститься в об'єктах, і видачу офіційних дозволів (допуску) суб'єктам на звернення до інформації такого рівня конфіденційності. Це спосіб поєднує захист і обмеження прав, що застосовується відносно до комп'ютерних процесів, даних і системних пристроїв, і призначений для запобігання їх небажаного використання.

Приклад: суб'єкт "Користувач № 2", який має допуск рівня "не таємно", не може отримати доступ до об'єкта, що має мітку "для службового користування". У той же час, суб'єкт "Користувач № 1" з допуском рівня "секретно" право доступу до об'єкта з міткою "для службового користування" має.

При цьому дана модель доступу не використовується ізольовано, зазвичай на практиці вона доповнюється елементами інших моделей доступу.

Для файлових систем, MAC може розширювати або заміняти DAC і концепцію користувачів і груп.

Найважливіша перевага полягає в тому, що користувач не може повністю контролювати доступ до ресурсів, які він створює.

Політика безпеки системи, встановлена адміністратором, повністю визначає доступ, і зазвичай користувачеві не дозволяється встановлювати більш вільний доступ до його ресурсів ніж той, який встановлений адміністратором користувачеві.

**3.6.3. Контроль доступу на основі ролей**

RBAC — розширення політики виборчого управління доступом; при цьому права доступу суб'єктів системи на об'єкти групуються з урахуванням специфіки їх застосування, утворюючи ролі [32].

Формування ролей покликане визначити чіткі і зрозумілі для користувачів комп'ютерної системи правила розмежування доступу. RBAC  дозволяє реалізувати гнучкі, що змінюються динамічно в процесі функціонування комп'ютерної системи, правила розмежування доступу.

Так як привілеї не призначаються користувачам безпосередньо і купуються ними тільки через свою роль (або ролі), управління індивідуальними правами користувача по суті зводиться до призначення йому ролей. Це спрощує такі операції, як додавання користувача або зміна підрозділу користувачем.

**3.7. Моделювання "Windows MAC"**

Основна мета "Windows MAC" – це розмежування доступу суб'єктів до об'єктів, засноване на призначенні мітки конфіденційності для інформації, що міститься в об'єктах. Цей спосіб поєднує захист і обмеження прав.

**3.7.1. Недоліки стандартної DAC**

Для того, щоб зрозуміти, в чому полягає практична цінність MAC, розглянемо кілька прикладів, коли стандартна система контролю доступу недостатня. Якщо MAC відключена, то доступна тільки класична система контролю доступу, яка включає в себе DAC або списки контролю доступу. Тобто мова йде про маніпулювання правами на запис, читання і виконання на рівні користувачів і груп користувачів, чого в деяких випадках може бути недостатньо.

Приклад: адміністратор не може в повній мірі контролювати дії користувача. Користувач цілком здатний дати всім іншим користувачам права на читання власних конфіденційних файлів, таких як ключі SSH.

Процеси можуть змінювати налаштування безпеки. Файли, що містять в собі пошту користувача повинні бути доступні для читання тільки одному конкретному користувачеві, але поштовий клієнт цілком може змінити права доступу так, що ці файли будуть доступні для читання всім.

Процеси успадковують права користувача, який їх запустив. Інфікована трояном версія браузера Firefox в стані читати SSH-ключі користувача, хоча не має для того жодних підстав.

В цілому, в традиційній моделі DAC добре реалізовані тільки два рівня доступу - користувач і привілейований користувач. Немає простого методу, який дозволив би встановлювати для кожного користувача необхідний мінімум привілеїв.

Звичайно, є безліч методів обходу цих проблем в рамках класичної моделі безпеки, але жоден з них не є універсальним.

**3.3.2. Вирішення проблем стандартної DAC**

"Windows MAC" (рис.3.1) має слідувати моделі мінімально необхідних привілеїв для кожного сервісу, користувача і програм. За вмовчання буде встановлено "режим заборони", коли кожен елемент системи має тільки ті права, які необхідні йому для функціонування. Якщо ж користувач, програма або сервіс намагаються змінити файл або отримати доступ до ресурсу, який не потрібен для вирішення їх завдань, то їм буде відмовлено в доступі, а така спроба буде зареєстрована в журналі [33].



Рис. 3.1.Система обов’язкового контролю доступом [34]

"Windows MAC" має бути реалізованою на рівні ядра, так що прикладні програми можуть зовсім нічого не знати про версії цієї системи примусового контролю доступу, особливості її роботи і т.д. У разі коректного налаштування, "Windows MAC" ніяк не вплине на функціонування сторонніх програм і сервісів. Хоча, якщо додаток здатний перехоплювати повідомлення про помилки цієї системи контролю доступу, зручність користування таким додатком істотно зростає. Адже в разі спроби отримати доступ до захищеного ресурсу або файлу, "Windows MAC" передасть в основний додаток помилку з сімейства "access denied". Але лише деякі додатки будуть використовувати одержувані від "Windows MAC" коди повернення системних викликів.

Ось кілька прикладів використання "Windows MAC", які дозволяють побачити, яким чином можна збільшити ступінь безпеки всієї системи: створення та налаштування списку програм, які можуть читати ssh-ключі, запобігання несанкціонованого доступу до даних через mail-клієнт, налаштування браузера таким чином, щоб він міг читати в домашній папці користувача тільки необхідні для функціонування файли і папки.

**3.7.3. Суб'єкти і об'єкти**

Суб'єкти - це користувачі, які виконують будь-які операції на комп'ютері. Однак користувачі завжди діють через ті чи інші прикладні програми. Тому, під суб'єктами найчастіше маються на увазі саме програми (процеси). Інакше кажучи, суб'єкти - це ті, хто виконує якісь дії.

Об'єкти - це те, над чим дії виконуються. Найчастіше під об'єктами маються на увазі файли даних. Але це можуть бути і пристрої, і навіть програми.

**3.7.4. Режими роботи "Windows MAC"**

"Windows MAC" повинен мати три основних режими роботи, при цьому за вмовчання має бути встановлено режим Enforcing. Це досить жорсткий режим, і в разі необхідності він може бути змінений на більш зручний для кінцевого користувача [35].

**Enforcing**: Режим за вмовчання. При виборі цього режиму всі дії, які якимось чином порушують поточну політику безпеки, будуть блокуватися, а спроба порушення буде зафіксована в журналі.

**Permissive:** У разі використання цього режиму, інформація про всі дії, які порушують поточну політику безпеки, будуть зафіксовані в журналі, але самі дії не будуть заблоковані.

**Disabled:** Повне відключення системи примусового контролю доступу.

**3.7.5. Контекст безпеки "Windows MAC"**

Це набір даних, який складається з:

1. типу користувача;
2. ролі;
3. типу даних або домена процесу;
4. рівнів і категорій.

Контекст безпеки (рис.3.2) записується в атрибути файлу (в файловій системі) і створюється при встановленні "Windows MAC". Уже присвоєний контекст безпеки може бути згодом змінений.



Рис. 3.2.Контекст безпеки [36]

Якщо файлова система не підтримує запис міток "Windows MAC", тоді мітки записуються окремо від файлів, при цьому зв'язок між файлами і мітками відбувається по коліях файлів.

Мітка файлу може виявитися невірною навіть в разі, якщо файлова система підтримує запис таких міток, але до файлу були неправильно застосовані операції копіювання або переміщення всередині файлової системи. Наприклад при копіюванні в іншу папку файл може отримати мітку, встановлену для цієї папки, замість тієї мітки, яка у нього була раніше.

**3.7.6. Користувач "Windows MAC"**

Це описовий тип користувача, а не якийсь конкретний користувач з логіном і паролем. Принципово це те ж саме, що і група користувачів в системі безпеки DAC. При додаванні в систему кожного нового користувача він за вмовчання (або явно) зіставляється з будь-яким типом користувача "Windows MAC" і надалі матиме ті дозволи або заборони, які вказані для його типу користувача [37].

**3.7.7. Роль у "Windows MAC"**

Роль – це перелік дозволених дій. В системі має бути можливим перехід з однієї ролі в іншу для зміни повноважень. При цьому ідентичність користувача не змінюється. Ролі не поєднуються, вони замінюють одна одну.

Політика безпеки визначає допустимі переходи з однієї ролі в іншу. Тобто неможливо перейти з будь-якої ролі в будь-яку роль. Оскільки ролі завжди пов'язані з типами (доменами), то часто говорять не про зміну ролей, а про зміну домену.

**3.7.8. Домени "Windows MAC"**

Домени об'єднують суб'єкти та об'єкти в групи, всередині цих груп визначають дозволені дії суб'єктів над об'єктами. Для суб'єктів замість терміна "тип" використовується термін "домен".

У "Windows MAC", в загальних політиках, використовується механізм примусового присвоєння типів. Тобто кожен об'єкт і суб'єкт повинен бути обов'язково приведеним до якого-небудь типу (або домену) [38].

**3.7.9. Політика "Windows MAC"**

Політика "Windows MAC" - це сукупність усіх описаних в системі співвідношень користувач - роль - тип (домен) - рівень і категорія (рис.3.3).



Рис. 3.3.Політика MAC [39]

Політика targeted - всі процеси не внесені в спеціальні обмежені домени, працюють в необмеженому домені unconfined\_t. Таким чином здійснюється можливість виконання процесів, які ще не описані в політиці. Але такі процеси фактично виконуються майже з адміністративними правами. У цьому слабке місце політики targeted.

Політика strict - всі процеси працюють в спеціальних обмежених доменах, в необмеженому домені unconfined\_t ніхто не працює. Політика strict використовується вузькоспеціально, оскільки потрібне її налаштування для кожного конкретного випадку. Адже процеси не описані в цій політиці просто не будуть працювати. Але зате ця політика забезпечує повний захист в рамках тих можливостей, які є в "Windows MAC".

**3.7.10. Контроль доступу в "Windows MAC"**

"Windows MAC" надає наступні моделі управління доступом:

Type Enforcement (TE): основний механізм контролю доступу, який використовується в цільових політиках. Дозволяє детально, на найнижчому рівні управляти дозволами. Найгнучкіший, але і найбільш трудомісткий для системного адміністратора механізм.

Role-Based Access Control (RBAC): в цій моделі права доступу реалізуються в якості ролей. Роль - сукупність прав доступу на об’єкти комп’ютерної системи. RBAC є подальшим розвитком TE.

Multi-Level Security (MLS): багаторівнева модель безпеки, в якій всім об'єктам системи присвоюється певний рівень доступу. Дозвіл або заборона доступу визначається тільки співвідношенням цих рівнів.

Всі процеси і файли в рамках "Windows MAC" мають контекст безпеки.

**3.8. Демонстрація програми-аналога для Linux**

SELinux – реалізація системи обов'язкового керування доступом, яка може працювати паралельно з класичним дискреційним керуванням доступом. Входить в стандартне ядро Linux.

**3.8.1. Налаштування режимів роботи**

Отримати інформацію про поточний стан можна за допомогою команд getenforce (рис.3.4) або sestatus (рис.3.5).



Рис. 3.4. Команда getenforce.



Рис. 3.5.Команда setstatus.

**Вискористання setenforce команди.** Щоб перейти від режиму enforcing до режиму permissive і навпаки, можна скористатися командою setenforce. Ця команда приймає "Enforcing, Permissive", 1 або 0 як аргумент.

Використання команди setenforce (рис.3.6) є корисним для тимчасового переходу з режиму або до режиму виконання. Наприклад, якщо система завантажується у дозволеному режимі, і адміністратор вважає, що система готова працювати в режимі примусового завантаження, адміністратор може використовувати setenforce 1 після завантаження, щоб увімкнути режим примусового виконання.



Рис. 3.6. Команда setenforce.

**SElinux configuration file.** (рис.3.7)Значення за вмовчання (enforcing or permissive) зберігається при завантаженні системи в файлі "/etc/selinux/config" через параметр "SELINUX".



Рис. 3.7. SELinux configuration file.

Також можна отримати огляд поточних дозволених доменів (рис.3.8), використовуючи semanage permissive -l.



Рис. 3.8.Поточні дозволені домени.

**3.8.2. Налаштування SELinux користувачів**

SELinux користувач - частина контексту (рис.3.9). Якщо повернутися до поточного контексту користувача, то можна побачити, що друге поле - це роль, а третє - домен.

****

Рис. 3.9.SELinux користувач.

Ролі, призначені для певного користувача SELinux, можна побачити за допомогою команди  semanage user -l.

Але на відміну від ролей та їх впливу на домени, можна змінити, які ролі призначаються для яких користувачів SELinux (рис.3.10). Також можна побачити різницю між користувачем SElinux та роллю SElinux.



Рис. 3.10. Ролі користувачів.

**Різниця між Linux користувачем і SELinux користувачем.** Можна побачити відображення облікових записів Linux (рис.3.11) для користувачів SELinux semanage login -l.



Рис. 3.11. Облікові записи Linux.

В наведеному вище прикладі:

1. root-користувач, звязаний з root-користувачем SELinux;
2. swift-користувач, звязаний з swift-користувачем SELinux;
3. спеціальний system\_u обліковий запис (запис для системних демонів);
4. спеціальний \_\_default\_\_ обліковий запис, який звязує всі інші облікові записи.

Обліковий запис \_\_default\_\_  вказує на те, що створені користувачі Linux мають звязатися з user\_u SELinux користувачем.

Назви груп мають обовязково починатися з символу "%"(рис.3.12). Це необхідно для того, щоб система відрізняла імена користувачів від імен груп.



Рис. 3.12. Групи SELinux.

Відповідно до наведеного вище прикладу, всі користувачі групи "%operators" буть зв’язані з staff\_u  користувачем SELinux.

**Маніпуляція інформацією про користувача SELinux.** Як зазначено вище, можна змінювати налаштування користувачів Linux. Це можна здійснити за допомогою зміни налаштувань SELinux або за допомогою зміни налаштувань ролі SELinux.

**Управління зв’язками користувачів.** Перш за все, для керування зв’язками користувачів використовуємо набір команд semanage login.

Наприклад, команда для створення зв’язку з групою "%operators" (рис.3.13).



Рис. 3.13. Зв’язок користувача з групою.

Для видалення звя’зку використовують параметр –d замість –a. Також зв’язок можна змінити за допомогою параметра –m.

Однак, якщо змінити зв’язок для користувача, який вже володіє файлами у файловій системі, дуже важливо повністю перезавантажити контекст цих файлів (рис.3.14) (наприклад, використовуючи -F з командою restorecon) або встановити нового власника SELinux і роль, використовуючи chcon.



Рис. 3.14. Оновлення власника і ролі.

Якщо цього не зробити, то це може спричинити порушення дозволів пізніше.

**Управління зв'язками користувача з роллю.** Подібно до попереднього прикладу, використовуємо semanage user для зміни зв’язків користувача з роллю.

Наприклад, щоб створити нового користувача SELinux, який називається infra\_u, та надати йому права staff\_r та sysadm\_r, потрібно скористатися наступною командою (рис.3.15):



Рис. 3.15. Створення користувача.

**3.8.3. Налаштування мережевих портів**

В основному SELinux призначений для управління доступом до файлів і каталогів, але існує безліч інших ресурсів, якими він керує. Деякі з них пов'язані з мережевими ресурсами, такими як мережеві порти. Це стає актуальним, коли потрібно змінити порт за вмовчання, який використовує демон.

Приклад: SSH демон (рис.3.16).



Рис. 3.16. SSH демон.

За допомогою команди semanage можна позначити маркер порту на іншому порті (рис.3.17). Приклад для ssh\_port\_t порту 1122.



Рис. 3.17. Маркер порту.

В межах SELinux, порти позначені, як і інші ресурси (рис.3.18).



Рис. 3.18. Порти SELinux.

У третьому стовпці вказано номер порту або діапазон портів. Якщо це діапазон, він має нижчий пріоритет, ніж певний номер порту.

Отже, для підвищення рівня ІБ необхідно використовувати дистрибутиви Linux з реалізованою системою MAC: SUSE Linux, Ubuntu. В системах з реалізованою системою DAC, необхідно підвищувати рівень інформаційної безпеки за допомогою доповнення SELinux. Використовувати ОС з системою DAC необхідно тільки тоді, коли всі права на ресурси повинні належати користувачеві.

**3.9. Висновки до розділу**

Більшість ОС мають засоби і методи управління доступом, які в свою чергу визначають, чи може якийсь об'єкт на рівні ОС (користувач або програма) отримати доступ до певного ресурсу.

Використовуються такі методи управління доступом:

1. DAC;
2. MAC;
3. контроль доступу на основі ролей (RBAC).

В цілому, в традиційній моделі DAC, добре реалізовані тільки два рівня доступу - користувач і привілейований користувач. Немає простого методу, який дозволив би встановлювати для кожного користувача необхідний мінімум привілеїв.

Є безліч методів обходу цих проблем в рамках класичної моделі безпеки, але жоден з них не є універсальним.

В рамках даної роботи було змодельовано систему обов’язкового контролю доступу, яка б значно підвищила ефективність захисту ОС сімейства Windows. Основа цієї системи - розмежування доступу суб'єктів до об'єктів, засноване на призначенні мітки конфіденційності для інформації, що міститься в об'єктах, і видачу офіційних дозволів (допусків) суб'єктам на звернення до інформації такого рівня конфіденційності. Ця система поєднує захист і обмеження прав, що застосовується відносно до комп'ютерних процесів, даних і системних пристроїв.

Рекомендовано надавати перевагу ОС з реалізованою системю MAC, оскільки це значно підвищить рівень ІБ. Але коли всі права на ресурси повинні належати користувачеві, можливе використання ОС з реалізованою системою DAC.

**ВИСНОВОК**

Інформаційна безпека, зокрема, кібербезпека, сьогодні стали найнагальнішими питаннями, що потребують прискіпливої уваги як окремої особи, так і суспільства та держави в цілому.

Наявність необхідної та достатньої нормативної бази і механізмів її реалізації та контролю дозволяє системі забезпечення національної безпеки України ефективно функціонувати в сучасних умовах.

В рамках даної роботи, було розглянуто моделі безпеки ОС сімейства Widows та Linux – набір технологій, які забезпечують моніторинг та керування різними компонентами безпеки ОС. Зокрема такі складові як:

1. ідентифікація;
2. ТД;
3. права користувачів;
4. автентифікація;
5. СКД.

В цілому, моделі безпеки ОС Microsoft Windows та ОС Linux подібні, але в них відрізняються декілька атрибутів, таких як шифрування файлової системи та привілеї ПЗ, які є у ОС Windows і ОС Linux, а також тіньовий пароль, який є тільки в ОС Linux. Крім того, ОС Windows використовує такі складні функції, як аудит; в той час як ОС Linux використовує ефективні файли журналів з шифруванням. В цілому, обидві ОС забезпечують багаторівневі технології безпеки, що робить їх надійними та здатними впоратися з атаками, а також забезпечити безпечне середовище для користувачів.

В традиційній моделі DAC, добре реалізовані тільки два рівня доступу - користувач і привілейований користувач. Немає простого методу, який дозволив би встановлювати для кожного користувача необхідний мінімум привілеїв.

Є безліч методів обходу цих проблем в рамках класичної моделі безпеки, але жоден з них не є універсальним.

В рамках даної роботи було змодельовано систему обов’язкового контролю доступу, яка б значно підвищила ефективність захисту ОС сімейства Windows. Основа цієї системи - розмежування доступу суб'єктів до об'єктів, засноване на призначенні мітки конфіденційності для інформації, що міститься в об'єктах, і видачу офіційних дозволів суб'єктам на звернення до інформації такого рівня конфіденційності. Ця система поєднує захист і обмеження прав, що застосовується відносно до комп'ютерних процесів, даних і системних пристроїв.

В результаті даної роботи було надані наступні рекомендації:

1. використовувати дистрибутиви Linux з реалізованою системою обов'язкового контролю доступом: SUSE Linux, Ubuntu;
2. використовувати доповнення SELinux для дистрибутивів Linux з реалізованою системою дискреційного контролю доступом;
3. використовувати ОС з системою дискреційного конртролю доступом тільки тоді, коли всі права на ресурси повинні належати користувачеві.

Отже, під час даної роботи було проаналізовано основні положення державних нормативно-правових документів та міжнародних стандартів, розглянуто основні компоненти моделей безпеки ОС, порівняно ОС сімейства Windows та Linux з точки зору інформаційної безпеки, змодельовано систему обов’язкового контролю доступом для ОС сімейства Windows.

**СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ ВИКОРИСТАНИХ ДЖЕРЕЛ**

1. Інформаційна безпека – [Електронний ресурс] – Режим доступу до ресурсу: <http://jure.in.ua/tema-9-informatsijna-bezpeka/>.

2. Інформаційна безпека як складова національної безпеки України – [Електронний ресурс] – Режим доступу до ресурсу: <http://www.rusnauka.com/16_ADEN_2010/Informatica/68028.doc.htm>.

3. Інформаційна безпека – [Електронний ресурс] – Режим доступу до ресурсу: <http://nbuviap.gov.ua/index.php?option=com_content&view=category&layout=blog&id=125&Itemid=459>.

4. Закон України "Про інформацію" – [Електронний ресурс] – Режим доступу до ресурсу: <http://zakon5.rada.gov.ua/laws/show/2657-12>.

5. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" – [Електронний ресурс] – Режим доступу до ресурсу: <http://zakon5.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80>.

6. Закон України "Про основні засади забезпечення кібербезпеки України" – [Електронний ресурс] – Режим доступу до ресурсу: <http://zakon5.rada.gov.ua/laws/show/2163-19>.

7. Закон України "Про захист інформації в автоматизованих системах" – [Електронний ресурс] – Режим доступу до ресурсу: <http://zakon5.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80>.

8. ISO/IEC 15408-1:2005 – [Електронний ресурс] – Режим доступу до ресурсу: <https://www.iso.org/standard/50341.html>.

9. ISO/IEC 17799:2005 – [Електронний ресурс] – Режим доступу до ресурсу: <https://www.iso.org/standard/39612.html>.

10. НД ТЗІ 1.1-002-99 – [Електронний ресурс] – Режим доступу до ресурсу: <https://tzi.com.ua/nd-tz-1.1-002-99.html>.

11. НД ТЗІ 2.5-004-99 – [Електронний ресурс] – Режим доступу до ресурсу: <https://tzi.ua/ua/nd_tz_2.5-004-99.html>.

12. Stallings W. Operating Systems: Internals and Design Principles. – Prentice Hall, 2011. – 19 с.

13. Operation System Market Share Worldwide – [Електронний ресурс] – Режим доступу до ресурсу: <http://gs.statcounter.com/>.

14. Carpenter T. Operating System Market Share. Net Applications. – Academic Press, 2012. – 145 с.

15. Модель безпеки ОС Windows – [Електронний ресурс] – Режим доступу до ресурсу: <https://www.microsoftpressstore.com/articles/article.aspx?p=2228450&seqNum=2>.

16. Carpenter T. Microsoft Windows Operating System Essentials. – Sybex, 2012. – 34 с.

17. Linux Foundation, What Is Linux: An Overview of the Linux Operating System. – BantamzPress, 2009. – 128 с.

18. A. Chou, J. Yang, B. Chelf, S. Hallem, D. Engler An empirical study of operating system errors. – In Proc. 18th ACM Symposium on Operating Systems Principles, 2001. – 19 с.

19. Модель безпеки ОС Linux – [Електронний ресурс] - Режим доступу до ресурсу: <https://www.ibm.com/developerworks/library/l-selinux/>.

20. Jacobs C. Trusted Operating Systems. – Technical report, 2001. – 17 с.

21. Ідентифікатор безпеки – [Електронний ресурс] – Режим доступу до ресурсу: <http://www.c-jump.com/CIS24/Slides/Registry/Registry.html>.

22. Mark E. Russinovich, David A. Solomon Windows Internals: Including Windows Server 2008 and Windows Vista. – Microsoft Press, 2009. – 179 c.

23. Access Tokens – [Електронний ресурс] - [https://msdn.microsoft.com/ru-ru/library/windows/desktop/aa374909(v=vs.85).aspx](https://msdn.microsoft.com/ru-ru/library/windows/desktop/aa374909%28v%3Dvs.85%29.aspx).

24. Токен доступу до ОС Windows – [Електронний ресурс] – Режим доступу до ресурсу: <https://www.slideshare.net/rbattistoni/windows-hips-ldf>.

25. Токен доступу до ОС Linux – [Електронний ресурс] – Режим доступу до ресурсу: <https://www.ibm.com/developerworks/library/l-selinux/>.

26. MSDN, Security Account Manager (SAM). – Quarto Group, 2012. – 179 c.

27. Дискреційна система контролю доступу – [Електронний ресурс] – Режим доступу до ресурсу: <https://technet.microsoft.com/en-us/library/bb463216.aspx>.

28. ДСКД ОС Windows – [Електронний ресурс] – Режим доступу до ресурсу: <https://technet.microsoft.com/en-us/library/bb463216.aspx>.

29. Riemer S., Kezema C. Windows Server 2008 Active Directory Resource Kit. – Microsoft Press, 2010. – 190 c.

30. Процес входу в ОС Windows – [Електронний ресурс] – Режим доступу до ресурсу: [https://technet.microsoft.com/en-us/library/dn751049(v=ws.11).aspx](https://technet.microsoft.com/en-us/library/dn751049%28v%3Dws.11%29.aspx).

31. Brown K. Customizing GINA Part 1, Developer tutorial for writing a custom GINA. – Reed Books, 2010. – 80 c.

32. Open Source Project, Security-Enhanced Linux. – Linux Foundation, 2016. – 156 c.

33. Open Source Project, What Is Linux: An Overview of the Linux OperatingSystem. – Linux Foundation, 2009. – 120 c.

34. Джонс Т. Анатомия SELinux Архитектура и реализация. – DeveloperWorks, 2008. – 290 c.

35. Security-Enhanced Linux – [Елктронний ресурс] – Режим доступу до ресурсу: <https://access.redhat.com/documentation/enus/red_hat_enterprise_linux/6/html/security-enhanced_linux/index>.

36. SELinux users and administrators guide – [Електронний ресурс] – Режим доступу до ресурсу: <https://access.redhat.com/documentation/enus/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/index>.

37. SELinux – описание и особенности работы с системой. – [Елктронний ресурс] – Режим доступу до ресурсу: <https://habr.com/company/blog/209644/>.

38. Система обов’язкового контролю доступом – [Електронний ресурс] – Режим доступу до ресурсу: <https://habr.com/company/kingservers/blog/209644/>.

39. Контекст безпеки - [Електронний ресурс] – Режим доступу до ресурсу: <https://habr.com/company/kingservers/blog/209644/>.