Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет комп’ютерної інженерії та управління
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Оцінка впливу вбудованих механізмів безпеки на продуктивність системи

(тема)

Виконав:
студент II курсу, групи КСМм-20-1
Лобода М.В.
(прізвище, ініціали)

Спеціальність
123 «Комп’ютерна інженерія»
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма
Комп’ютерні системи та мережі
(повна назва освітньої програми)

Керівник: проф. Горбачов В.О.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри ЕОМ _____ Коваленко А.А.
(підпис) (прізвище, ініціали)

2021 р.

Харківський національний університет радіоелектроніки

Факультет комп’ютерної інженерії та управління

Кафедра електронних обчислювальних машин

Рівень вищої освіти другий (магістерський)

Спеціальність 123 «Комп’ютерна інженерія»
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна або Освітньо-наукова)

Освітня програма Комп’ютерні системи та мережі
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
“ ____ ” _____ 20__ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Лободі Максиму Валерійовичу
(прізвище, ім’я, по батькові)

1. Тема роботи Оцінка впливу вбудованих механізмів безпеки на продуктивність системи

затверджена наказом по університету від “ 05 ” листопада 2021 р. № 1656 Ст

2. Термін подання студентом роботи до екзаменаційної комісії 13 грудня 2021р.

3. Вхідні дані до роботи 1) середовище розробки Delphi 7, 2) ProcessMonitor, 3) система розмежування доступу — Secret Net.

4. Перелік питань, що потрібно опрацювати в роботі
1) актуальність проблеми;
2) огляд та аналіз літературних джерел;
3) аналіз предметної області та постановка задачі;
4) реалізація та використання створеної методики на практиці;
5) висновки.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) Слайд-презентація – 15 слайдів

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Вибір технології розробки та	09.11.21-13.11.21	
	інструментальних засобів		
2	Розробка алгоритмічного забезпечення	15.11.21-23.11.21	
3	Розробка програмних модулів	24.11.21-28.11.21	
4	Відлагодження програмних модулів	29.11.21-30.11.21	
5	Оформлення матеріалів кваліфікаційної роботи	30.11.20-01.12.21	
6	Подання кваліфікаційної роботи керівникові та	01.12.20-02.12.21	
	її попередній захист		
7	Подання кваліфікаційної роботи на рецензу-	03.12.21-04.12.21	
	вання		

Дата видачі завдання «08» листопада 2021 р.

Студент _____
(підпис)

Керівник роботи _____ проф. Горбачов В.О.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 84 с., 17 рис., 3 табл., 2 дод., 9 джерел.

СИСТЕМА, БЕЗПЕКА, МОНІТОР БЕЗПЕКИ, СУБ’ЄКТ, ОБ’ЄКТ, МОДЕЛЬ, КОЕФІЦІЄНТ, ПРОДУКТИВНІСТЬ.

Метою кваліфікаційної ї роботи є оцінка впливу вбудованих механізмів безпеки на продуктивність системи. Для цього потрібно розробити методику оцінки впливу механізмів безпеки.

У ході виконання кваліфікаційної роботи будуть досліджені проблеми захисту інформації проблем проектування безпечних систем, монітор безпеки та його моделі.

ABSTRACT

Master’s thesis: 84 pages, 17 figures, 2 tables, 2 appendices, 9 sources.

SYSTEM, SECURITY, SECURITY MONITOR, SUBJECT, OBJECT, MODEL, COEFFICIENT, PRODUCTIVITY.

The purpose of certification work is to assess the impact of built-in security mechanisms on system performance. To do this, we need to develop a methodology for assessing the impact of security mechanisms.

In the course of the attestation work the problems of information protection, problems of designing safe systems, security monitor and its models will be investigated

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ 8
ВСТУП 9
1 АКТУАЛЬНІСТЬ ПРОБЛЕМИ 10
1.1 Актуальність та постановка цілей дослідження 10
1.2 Проблеми захисту інформації у сучасних ІС 10
2 ОГЛЯД ТА АНАЛІЗ ЛІТЕРАТУРНИХ ДЖЕРЕЛ 14
2.1 Концептуальні питання створення, функціонування, розвитку і використання національної системи конфіденційного зв’язку 14
2.2 Послуги і механізми захисту інформації 21
2.3 Механізми безпеки та методи їх оцінки 37
2.3.1 Механізми безпеки……..37
2.3.2 Механізм безпеки що використовується в методиці……...38
2.3.3 Сучасні методи оцінки впливу систем безпеки на продукивність комп’ютерних систем……..……39
3 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧІ 45
3.1 Аналіз проблем проектування безпечних систем 45
3.2 Моделі монітору безпеки та вимоги до методики 45
4 РЕАЛІЗАЦІЯ ТА ВИКОРИСТАННЯ СТВОРЕНОЇ МЕТОДИКИ НА ПРАКТИЦІ 63
4.1 Визначення переліку системних функцій операційної системи, що підлягають контролю та алгоритм методики 63
4.2 Визначення вагових коефіцієнтів значимості системних функцій 63
4.3 Визначення коефіцієнтів уповільнення виконання системних функцій операційної системи, що підлягають оцінці 67

4.2 Визначення певного інтегрального показника зниження продуктивності системи внаслідок впливу засобів розмежування доступу 71
ВИСНОВКИ..... 73
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ 74
ДОДАТОК А Блок-схема алгоритма работи програми 75
ДОДАТОК Б Графічний матеріал кваліфікаційної роботи 76

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

МБ – монітор безпеки

МБС – монітор безпеки суб’єкта

МБО – монітор безпеки об‘єкта

API – інтерфейс прикладного програмування

ВСТУП

Швидке зростання глобальної мережі Internet та стрімкий розвиток інформаційних технологій привели до формування інформаційного середовища, що впливає на всі сфери людської діяльності. Нові технологічні можливості полегшують поширення інформації, підвищують ефективність виробничих процесів, сприяють розширенню ділових відносин. Однак незважаючи на інтенсивний розвиток комп'ютерних засобів і інформаційних технологій, вразливість сучасних інформаційних систем і комп'ютерних мереж, на жаль, не зменшується. Тому проблеми забезпечення інформаційної безпеки привертають пильну увагу як фахівців в області комп'ютерних систем і мереж, так і численних користувачів, включаючи компанії, що працюють в сфері електронного бізнесу.

З самого початку комп'ютерної ери одним з основних завдань для розробників інформаційних технологій постало завдання забезпечення безпеки.. Почи-наючи з 70-х років минулого століття в світі стали розроблятися різні конце-пції і методи захисту інформації, що незабаром привело до створення одна-кового підходу до цієї проблеми: були розроблені перші політики безпеки.

На сьогоднішній день вже положення законів та підзаконних актів в області забезпечення безпеки інформаційних технологій визначають ряд вимог до механізмів захисту в автоматизованих системах, в тому числі до механізмів логічного розмежування доступу. Разом з тим, практичної реалізації таких вимог в сучасних системах перешкоджає та обставина, що управління налаштуваннями подібних механізмів, як правило, здійснюється без належного аналізу наслідків. Зміни в налаштування вносяться локально, модифікуються невеликі фрагменти правил логічного розмежування доступу. При цьому оцінка впливу таких змін на захищеність та продуктивніть комп'ютерної системи в цілому часто не проводиться

1.АКТУАЛЬНІСТЬ ПРОБЛЕМИ

1.1 Актуальність та постановка цілей дослідження

Метою роботи є дослідження схем розмежування доступу та його вплив напродуктивність.

Актуальність роботи полягає у тому, що для збереження важливих та конфіденційних даних, встановлюються системи безпеки, що очікувано негативно впливають на продуктивність системи, що є неменш важливим фактором в сучасності.

Таким чином, виникає необхідність в розробці методики оцінки ступеня впливу засобів розмежування доступу на продуктивність системи.

1.2 Проблеми захисту інформації у сучасних ІС

Захист інформації є однією з вічних проблем. Протягом історії людства способи розв’язання цієї проблеми визначались рівнем розвитку технологій. У сучасному інформаційному суспільстві технологія відіграє роль активатора цієї проблеми – комп’ютерні злочини стали характерною ознакою сьогодення. Комп’ютерними називають злочини, пов’язані з втручанням у роботу комп’ютера, і злочини, в яких комп’ютери використовуються як необхідні технічні засоби. Серед причин комп’ютерних злочинів і пов’язаних з ними викрадень інформації головними є такі [1]:

- швидкий перехід від традиційної паперової технології зберігання та передавання інформації до електронної за одночасного відставання технологій захисту інформації, зафіксованої на машинних носіях;
- широке використання локальних обчислювальних мереж, створення глобальних мереж і розширення доступу до інформаційних ресурсів;
- постійне ускладнення програмних засобів, що викликає зменшення їх

надійності та збільшення кількості уразливих місць. Сьогодні ніхто не може назвати точну цифру загальних збитків від комп'ютерних злочинів, але експерти погоджуються, що відповідні суми вимірюються мільярдами доларів. Серед основних статей варто виокремити такі:

- збитки, до яких призводить ситуація, коли співробітники організації не можуть виконувати свої обов'язки через непрацездатність системи (мережі);
- вартість викрадених і скомпрометованих даних;
- витрати на відновлення роботи системи, на перевірку її цілісності, на доробку
- уразливих місць тощо.

Варто також враховувати й морально-психологічні наслідки для користувачів, персоналу і власників іс та інформації. Що ж до порушення безпеки так званих «критичних» додатків у державному і військовому управлінні, атомній енергетиці, медицині, ракетно-космічній галузі та у фінансовій сфері, то воно може призвести до тяжких наслідків для навколишнього середовища, економіки і безпеки держави, здоров'я і навіть для життя людей.Економічні та юридичні питання, приватна та комерційна таємниця, національна безпека – усе це зумовлює необхідність захисту інформації та іс.

Згідно із законом України «про захист інформації в автоматизованих системах» захист інформації – це сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи ас та осіб, які користуються інформацією.

У літературі вживаються також споріднені терміни «безпека інформації» та «безпека інформаційних технологій».

Забезпечення безпеки інформаційних технологій являє собою комплексну проблему, яка охоплює правове регулювання використання it, удосконалення технологій їх розробки, розвиток системи сертифікації, забезпечення відповідних організаційнотехнічних умов експлуатації. Розв'язання цієї проблеми потребує значних витрат, тому першочерговим

завданням є співвіднесення рівня необхідної безпеки і витрат на її підтримку. Для цього необхідно визначити потенційні загрози, імовірність їх настання та можливі наслідки, вибрати адекватні засоби і побудувати надійну систему захисту. Базовими принципами інформаційної безпеки є забезпечення цілісності інформації, її конфіденційності і водночас доступності для всіх авторизованих користувачів. Із цього погляду основними випадками порушення безпеки інформації можна назвати такі [1]:

- несанкціонований доступ — доступ до інформації, що здійснюється з порушенням установлених в 1с правил розмежування доступу;
- витік інформації — результат дій порушника, унаслідок яких інформація стає відомою (доступною) суб'єктам, що не мають права доступу до неї;
- втрата інформації — дія, внаслідок якої інформація в 1с перестає існувати для фізичних або юридичних осіб, які мають право власності на неї в повному чи обмеженому обсязі;
- підробка інформації — навмисні дії, що призводять до перекручення інформації, яка має оброблятися або зберігатися в 1с;
- блокування інформації — дії, наслідком яких є припинення доступу до інформації;
- порушення роботи іс — дії або обставини, які призводять до спотворення процесу обробки інформації.

Причини настання зазначених випадків такі:

- збої обладнання (збої кабельної системи, перебої в електроживленні, збої серверів, робочих станцій, мережних карт, дискових систем тощо);
- некоректна робота програмного забезпечення (втрата або змінювання даних у разі помилок у пз, втрати даних унаслідок зараження системи комп'ютерними вірусами тощо);
- навмисні дії сторонніх осіб (несанкціоноване копіювання, знищення, підробка або блокування інформації, порушення роботи 1с, спричинення витоку інформації);

- помилки обслуговуючого персоналу та користувачів (випадкове знищення або змінювання даних; некоректне використання програмного та апаратного забезпечення, яке призводить до порушення нормальної роботи системи, виникнення вразливих місць, знищення або змінювання даних, порушення інтересів інших законних користувачів тощо; неефективно організована система захисту; втрата інформації через неправильне зберігання архівних даних тощо);

- навмисні дії обслуговуючого персоналу та користувачів (усе сказане у попередніх двох пунктах, а також ознайомлення сторонніх осіб із конфіденційною інформацією). Зауважимо, що порушенням безпеки можна вважати і дії, які не призводять безпосередньо до втрати або відпливу інформації, але передбачають втручання в роботу системи.

2 ОГЛЯД ЛІТЕРАТУРИ

2.1 Концептуальні питання створення, функціонування, розвитку і використання національної системи конфіденційного зв’язку

Концептуальні проблеми створення, функціонування, розвитку і застосування національної системи конфіденційного зв’язку Існування і прогресивний ріст України як суверенної держави залежить від здійснення цілеспрямованої політики захисту її національних інтересів. Основи такої політики визначає ідейний задум національної безпеки України.

Національна безпека України як стан захищеності життєво важливих інтересів фізичних осіб, суспільства і держави від внутрішніх і зовнішніх загроз є необхідною умовою збереження і надбання духовних і матеріальних цінностей. В умовах стрімкої інформатизації суспільства, широкого застосовування засобів обчислювальної техніки і комп’ютерних систем особливої актуальності набувають проблеми інформаційної безпеки держави, найбільш складними з яких є потреба захисту цінної конфіденційної і секретної інформації в державних і приватних підприємствах, в органах і установах державного адміністрування банківській та інших системах.

Соціально-економічні наслідки інформатизації сучасного суспільства відокремили ряд питань інформаційної безпеки, наприклад [1]:

- необхідність захисту майнових прав громадян, підприємств і держави на інформацію і обчислювальні ресурси відповідно до вимог цивільного, адміністративного і господарського права;
- необхідність забезпечення ефективного функціонування найважливіших (критичних) автоматизованих і інформаційних систем і технологій, яка обумовлена вимогами фізичної безпеки людей, екологічної обстановки, збереження духовних і матеріальних цінностей та ін.;

- необхідність захисту цивільних прав і свобод, гарантованих чинним законодавством та ін.

Серед найбільших загроз національній безпеці України в інформаційній сфері вважаються:

- незважена державна політика і відсутність необхідної інфраструктури в інформаційній сфері;

- повільне входження України в світовий інформаційний простір, недостатньо об’єктивне уявлення про Україну серед міжнародного співтовариства;

- інформаційна експансія з боку інших держав;

- витік інформації, що становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, яка є власністю держави;

- введення цензури.

Основними напрямками державної політики Національної безпеки України в інформаційній сфері є:

- застосування комплексних заходів щодо захисту інформаційного простору і вхід України до світового інформаційного простору;

- виявлення і усунення причин інформаційної дискримінації України;

- усунення негативних чинників порушення інформаційного простору, інформаційної експансії з боку інших держав;

- розроблення і впровадження необхідних засобів і режимів отримання, збереження, розповсюдження і використання суспільно значущої інформації, створення розвиненої інфраструктури в інформаційній сфері.

Державна політика національної безпеки визначається пріоритетами національних інтересів і загроз національній безпеці України. Вона здійснюється шляхом реалізації відповідних доктрин, стратегій, концепцій і програм у різних сферах національної безпеки відповідно до чинного законодавства. Основним комплексним заходом щодо захисту національного

інформаційного простору України є побудова Національної системи конфіденційного зв’язку.

Національна система конфіденційного зв’язку – це сукупність спеціальних систем (мереж) зв’язку подвійного призначення, які за допомогою криптографічних та/або технічних засобів забезпечують обмін конфіденційною інформацією на користь органів державної влади і органів місцевого самоврядування, створюють належні умови для їх взаємодії в мирний час і у разі введення особливого чи військового стану. Національна система конфіденційного зв’язку входить до складу Єдиної національної системи зв’язку України.

Складовими Національної системи конфіденційного зв’язку є:

- спеціальні системи (мережі) зв’язку;
- стаціонарні і мобільні компоненти спеціальних систем (мереж) зв’язку;
- централізовані системи захисту інформації і оперативно-технічного управління.

Спеціальна система (мережа) зв’язку – система (мережа) зв’язку, призначена для обміну інформацією з обмеженим доступом.

Спеціальна система (мережа) зв’язку подвійного призначення – спеціальна система (мережа) зв’язку, призначена для забезпечення зв’язку на користь органів державної влади і органів місцевого самоврядування з використанням частини її ресурсу для надання послуг іншим споживачам.

Суб’єктами Національної системи конфіденційного зв’язку є органи державної влади і органи місцевого самоврядування, юридичні і фізичні особи, які беруть участь у створенні, функціонуванні, розвитку і використанні цієї системи.

Управління Національною системою конфіденційного зв’язку, її функціонування, розвиток, використання і захист інформації забезпечуються спеціально уповноваженим центральним органом виконавчої влади у сфері конфіденційного зв’язку відповідно до законодавства. Централізовані системи

захисту інформації і оперативно-технічного управління знаходяться в державній власності і не підлягають приватизації. Власниками інших компонентів Національної системи конфіденційного зв’язку можуть бути суб’єкти господарської діяльності, незалежно від форми власності.

Захист інформації в структурі Національної системи конфіденційного зв’язку забезпечується:

- дотриманням суб’єктами правового відношення норм, вимог і правил організаційного і технічного характеру щодо захисту оброблюваної інформації;

- використанням засобів обчислювальної техніки, програмного забезпечення, засобів зв’язку і автоматизованих систем у цілому, засобів захисту інформації, які відповідають установленим вимогам до захисту інформації (мають відповідний сертифікат);

- перевіркою відповідності засобів обчислювальної техніки, програмного забезпечення, засобів зв’язку і автоматизованих систем у цілому встановленим вимогам до захисту інформації (сертифікація засобів обчислювальної техніки, засобів зв’язку і автоматизованих систем);

- здійсненням контролю захисту інформації.

Таким чином, відповідно до основних нормативно-правових актів України рішення задач захисту національного інформаційного простору України покладається на Національну систему конфіденційного зв’язку, концептуальні питання створення, функціонування, розвитку і використання якої регулюються Конституцією України, законами України "Про інформацію", "Про державну таємницю", "Про захист інформації в автоматизованих системах", "Про зв’язок", "Про підприємництво", "Про ліцензування певних видів господарської діяльності", "Про Національну систему конфіденційного зв’язку". Відповідно до основних функціональних завдань використання Національної системи конфіденційного зв’язку повинне забезпечувати ефективний захист цінної конфіденційної і секретної інформації в державних і приватних підприємствах, в органах і установах

державного управління, банківській та інших системах. Проведемо аналіз можливих загроз безпеки, розглянемо їх дію на інформаційні системи й технології. Виходячи з принципів і положень державної політики забезпечення інформаційної безпеки, найбільшу небезпеку становлять загрози в політичній, економічній, оборонній і інших сферах діяльності держави (рис. 2.1).

Рисунок 2.1 – Критичні інформаційні системи і технології в різних сферах

У політичній сфері найбільш серйозній небезпеці підлягають:

- суспільна свідомість і політична орієнтація різних груп населення країни (регіонів), що безперервно формуються під впливом вітчизняних та іноземних засобів масової інформації (друк, радіо, телебачення);
- система ухвалення політичних рішень, що істотно залежить від якості і своєчасності її інформаційного забезпечення;
- право політичних організацій, партій, об’єднань і рухів на вільне вираження своїх соціально-політичних і економічних програм через засоби масової інформації;

- система регулярного інформування населення органами державної влади і управління про політичне і соціально-економічне життя через засоби масової інформації, прес-центри, центри суспільних зв’язків та ін.;

- система формування громадської думки, що включає спеціальні інститути, центри і служби виявлення, вивчення і аналізу громадської думки.

В оборонній сфері до найуразливіших ланок належать:

- інформаційні ресурси апарату Міністерства оборони, Генерального штабу, Головних штабів видів Збройних сил і родів військ, науково-дослідних установ, що містять відомості і дані про оперативні і стратегічні плани підготовки і ведення бойових дій, про склад і дислокацію військ, про мобілізаційну готовність, тактико-технічні характеристики озброєння і військової техніки;

- інформаційні ресурси підприємств оборонного комплексу, що містять відомості про науково-технічний і виробничий потенціал, про обсяги постачань і запаси стратегічних видів сировини і матеріалів, основні напрями розвитку озброєння, військової техніки, їх бойові можливості й фундаментальні і прикладні науково-дослідні роботи, що проводяться в інтересах Міністерства оборони;

- системи зв’язку і управління військами і зброєю, їх інформаційне забезпечення;

- політична стійкість військ щодо інформаційно-пропагандистської дії;

- інформаційна інфраструктура, зокрема, центри обробки та аналізу інформації Генерального штабу та інформаційні підрозділи штабів видів Збройних сил, штабів об’єднань і з’єднань видів Збройних сил і родів військ, пункти управління, вузли і лінії радіозв’язку, радіорелейного, тропосферного і супутникового, а також лінії проводового зв’язку, що розгортаються і орендуються Міністерством оборони та іншими силовими структурами.

Під загрозою в широкому розумінні зазвичай розуміють потенційно можливу подію, дію (вплив), процес або явище, які можуть призвести до нанесення збитку будь-якій зі сторін. Загрозою інтересам суб’єктів

інформаційних відносин називають потенційно можливу подію, процес або явище, яке за допомогою дії на інформацію або інші компоненти інформаційної системи може прямо чи опосередковано призвести до завдання збитку.

У процесі зберігання і обробки інформація може піддатися діям чинників випадковим або умисним. Найчастішими і найнебезпечнішими, з огляду на розмір збитків, є ненавмисні помилки користувачів, операторів, системних адміністраторів й інших осіб, що обслуговують інформаційні системи, а також помилки, що виникають при обробці і передачі інформації. Згідно зі статистикою 65 % втрат – наслідок ненавмисних помилок. Найрадикальніший спосіб боротьби з ненавмисними помилками – максимальна автоматизація і суворий контроль за правильністю виконуваних дій.

Загрози збоку навколишнього середовища відрізняються великою різноманітністю. В першу чергу це порушення інфраструктури – аварії в системі електроживлення, тимчасова відсутність зв’язку, перебої з водопостачанням, цивільні безлади та ін. Особливу небезпеку становлять стихійні лиха: пожежі, повені, землетруси, урагани. За даними статистики на ці загрози доводиться 13 % втрат, завданих інформаційним системам. На рис. 2.2 проілюстровано в загальному вигляді класифікацію загроз інформації.

Особливої небезпеки останнім часом набули умисні загрози, реалізація яких цілком досяжна для терористичних груп і організацій. Потенційною мішенню злочинних намірів можуть бути інформаційні системи Міністерства оборони й інших силових структур, системи управління атомних, хімічних та інших небезпечних виробництв, обчислювальні системи банків і великих промислових підприємств. Реалізація умисних загроз може призвести до тяжких наслідків в обороні, промисловості, економіці, банківській сфері та інших галузях господарської діяльності, екології, житті і здоров’ї населення.

Рисунок 2.2 – Основні загрози безпеки інформації

Слід зазначити, що можливості реалізації умисних загроз останнім часом різко зросли. Це пояснюється стрімким розвитком обчислювальної техніки, зокрема, "суперкомп'ютерів", широким розповсюдженням технологій розподілених обчислень.

2.2. Послуги і механізми захисту інформації

Перш ніж визначати засоби захисту інформації і будувати відповідну систему, необхідно проаналізувати основні послуги й механізми захисту інформації. Для цього розглянемо еталонну модель взаємодії відкритих систем (OSI) і класифікацію можливих атак на кожний з рівнів цієї моделі.

Еталонну модель OSI (англ. Open Systems Interconnection) було розроблену інститутом стандартизації ISO з метою розмежування функцій різних протоколів у процесі передачі інформації від одного абонента іншому. Подібних класів функцій було виділено 7. Вони одержали назву рівнів. Кожен

рівень виконує певні завдання в процесі передачі блоку інформації, причому відповідний рівень на приймальній стороні проводить перетворення, зворотні тим, які проводив той же рівень на передавальній стороні. В цілому проходження блоку даних від відправника до одержувача показане на рис. 1.3. Кожен рівень додає до пакета невеликий обсяг своєї службової інформації – префікс (на рисунку вони зображені як P1...P7). Деякі рівні в конкретній реалізації цілком можуть бути відсутніми. Дана модель дозволяє провести класифікацію мережевих атак відповідно до рівня їх дії.

Фізичний рівень відповідає за перетворення електронних сигналів у сигнали середовища передачі інформації (імпульси напруги, радіохвилі, інфрачервоні сигнали). На цьому рівні основним класом атак є "відмова в сервісі". Постановка шумів по всій смузі пропускання каналу може призвести до розриву зв’язку.

Канальний рівень керує синхронізацією двох і більшої кількості мережевих адаптерів, підключених до єдиного середовища передачі даних. Прикладом його є протокол Ethernet. Дії на цьому рівні також полягають в основному в атаці "відмова в сервісі". Проте, на відміну від попереднього рівня, тут проводиться перебій синхропосилань або самої передачі даних періодичною передачею "без дозволу або передачею не в свій час".

Мережевий рівень відповідає за систему унікальних імен і доставку пакетів за цим іменем, тобто за маршрутизацію пакетів. Відповідно й атаки на цьому рівні найчастіше спрямовані на конфіденційність і цілісність службової інформації, пов’язаної з адресацією і наявністю унікальних імен.

Транспортний рівень відповідає за доставку великих повідомлень по лініях з комутацією пакетів. Оскільки в подібних лініях розмір пакета є зазвичай невеликим числом (від 500 байт до 5 кілобайт), то для передачі великих обсягів інформації їх необхідно розбивати на передавальній стороні й збирати на приймальній. Вся річ у тому, що пакети на приймальну сторону можуть приходити й іноді приходять не в тому порядку, в якому вони були відправлені. Причина зазвичай полягає у втраті деяких пакетів через помилки

або переповненість каналів, рідше – у використанні для передачі потоку двох альтернативних шляхів у мережі.

Отже, операційна система повинна зберігати деякий буфер пакетів, чекаючи приходу тих, що затрималися в процесі передачі. А якщо зловмисник з наміром формує пакети так, щоб послідовність була великою і свідомо неповною, то тут можна чекати як постійної зайнятості буфера, так і небезпечних помилок через його переповнення.

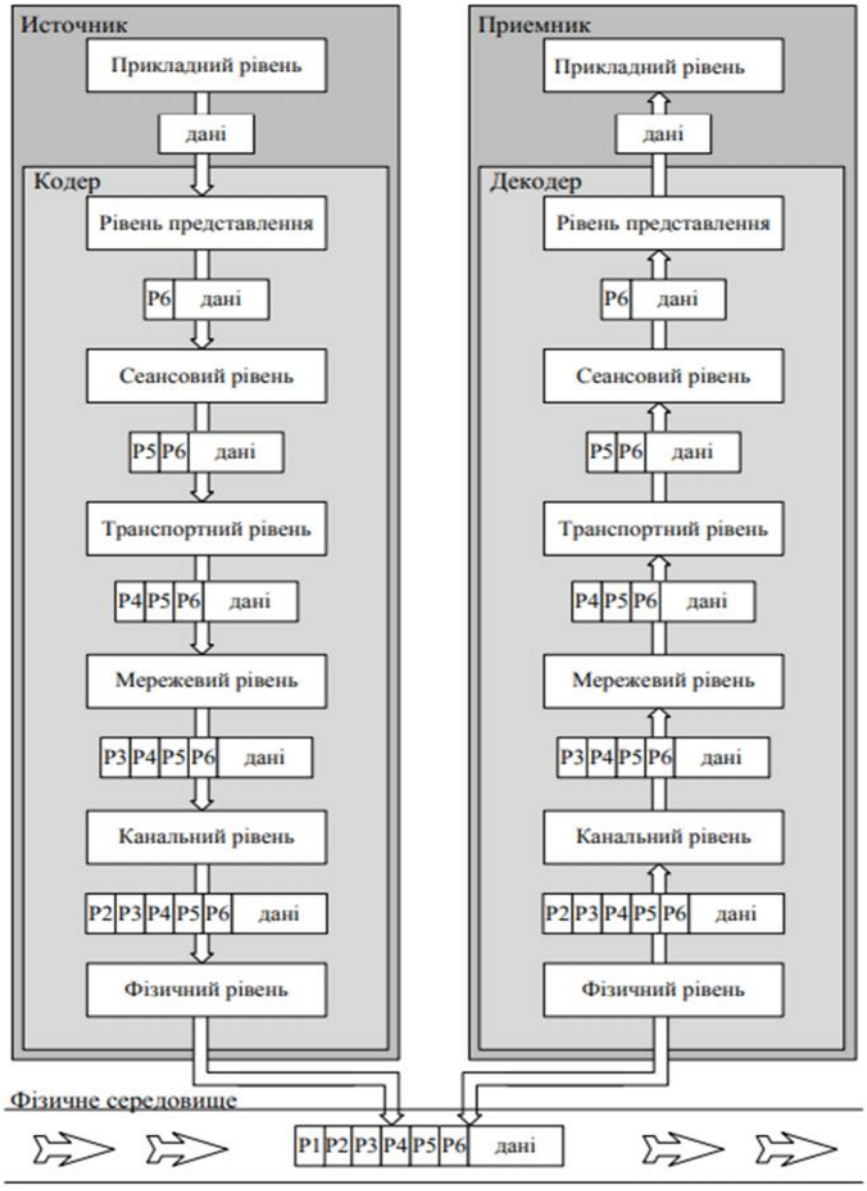

Рисунок 2.3 – Проходження блоку даних від відправника до одержувача відповідно до моделі взаємодії відкритих систем

Сеансовий рівень відповідає за процедуру встановлення початку сеансу і підтвердження (квитування) приходу кожного пакета від відправника одержувачу. У мережі Інтернет протоколом сеансового рівня є протокол TCP (він займає і 4-й, і 5-й рівні моделі OSI). Відносно сеансового рівня дуже поширена специфічна атака класу "відмова в сервісі", основана на властивостях процедури встановлення з'єднання в протоколі TCP. Вона одержала назву SYN- Flood (flood - англ. "великий потік").

Представницький рівень визначає формат, використаний для обміну даними між мережевими комп'ютерами і відповідає за перетворення протоколів, трансляцію даних, їх шифрування, зміну або перетворення вжитого набору символів (кодової таблиці) і розширення графічних команд. Представницький рівень, крім того, керує стисненням даних для зменшення переданих бітів. У зв'язку з цим особливо небезпечними є атаки, що спрямовані на спотворення даних (порушення цілісності), які часто призводять до зупинки в роботі окремих вузлів у комп'ютерних мережах.

Прикладний рівень – найвищій рівень моделі OSI. Він є вікном для доступу прикладних процесів до мережевих послуг. Цей рівень забезпечує послуги, що безпосередньо підтримують додатки користувача, такі, як програмне забезпечення для передачі файлів, доступу до баз даних, електронна пошта. Прикладний рівень керує загальним доступом до мережі і обробкою помилок. Широко використовуваним розподіленим додатком на цьому рівні є електронна пошта. У зв'язку з цим спостерігається інтерес до засобів забезпечення автентифікації і конфіденційності оброблюваних даних.

Методологічною основою розробки системи захисту інформації є стандарт ISO/IEC 15408, згідно з яким основними нормативними документами, що характеризують інформаційну систему з точки зору безпеки, є профіль захисту (protection profile) і проект забезпечення безпеки (security target). Під профілем захисту розуміють незалежну множину функціональних вимог безпеки і вимог адекватності, спрямованих на задоволення потреб

споживача. Проектом безпеки є безліч вимог безпеки й специфікацій функцій безпеки.

Відповідно до основних положень міжнародних стандартів життєвий цикл системи захисту інформації складається з п’яти етапів [1]:

- визначення політики безпеки, яка містить абстрактний ряд вимог до безпеки системи;
- аналіз вимог безпеки, включаючи аналіз ризиків, аналіз урядових, правових і стандартних вимог;
- визначення послуг безпеки, необхідних для задоволення поставлених вимог;
- побудова і впровадження системи безпеки, включаючи вибір механізмів безпеки, що забезпечують конкретні вибрані послуги безпеки;
- безперервне управління безпекою.

Послуга безпеки призначена для забезпечення захисту від ідентифікованої загрози. Існують абстрактні поняття, які можуть бути використані для характеристики вимог безпеки. Механізмом безпеки є засіб, за допомогою якого реалізується і застосовується відповідна послуга.

Стандарти ISO 7498, ISO/IEC 10181 визначають п’ять базових загальноприйнятих послуг безпеки:

- автентифікація (authentication);
- керування доступом (access control);
- конфіденційність даних (data confidentiality);
- цілісність даних (data integrity);
- невідмова (причетність) (non-repudiation).

Додатково в ISO/IEC 10181-7 розглядається перевірка безпеки (security audit).

Автентифікація – послуга, що гарантує надійність ідентифікації джерела повідомлень або електронного документа, а також оригінальність джерела.

Керування доступом – послуга, що забезпечує доступ до ресурсів лише авторизованих користувачів (процесів), що гарантує відповідні права доступу

для авторизованих користувачів і запобігає неавторизованому доступу як “внутрішніх”, так і ”зовнішніх” користувачів. Ця послуга застосовується до різних типів доступу до ресурсів, наприклад, використання комунікаційних ресурсів, читання, запис або видалення інформаційних ресурсів, використання ресурсів обчислювальних систем з обробки даних і та ін. й використовується для встановлення політики управління/обмеження доступу.

Під конфіденційністю розуміють властивість системи, яка гарантує, що інформація не може бути доступна або розкрита для неавторизованих (неуповноважених) осіб, об’єктів або процесів.

Цілісність даних – послуга, що гарантує можливість модифікації тієї інформації, яка міститься в комп’ютерній системі і зв’язку, й пересилається по каналах, тільки суб’єктами, які мають на це право.

Під причетністю розуміють здатність запобігання можливості відмови одним з реальних учасників комунікацій від факту його повної або часткової участі в передачі даних.

Доступність визначається як додаткова послуга забезпечення захищеності інформаційних систем. Механізми забезпечення доступності запобігають атакам, що мають на меті унеможливити доступ до ресурсів або послуг інформаційної системи (або зробити їх “якість” незадовільною) для користувача. На рис. 2.5 подано розподіл послуг безпеки по рівнях моделі взаємодії відкритих систем (ВВС). Як видно з наведеного рисунка, велика частина послуг безпеки доводиться на верхні рівні моделі ВВС, переважно,на рівень прикладного процесу. Розглянемо основні системи і протоколи, що забезпечують захист інформації на різних рівнях моделі ВВС.

На прикладному рівні в теперішній час для забезпечення захисту інформації найчастіше використовуються дві системи – PGP і S/MIME.

PGP – широко розповсюджена система захисту, незалежна від будь-якої організації або органу влади. Тому вона підходить як для індивідуального користування, так і для включення в конфігурацію мережі будь-якої організації.

Зростання популярності Word Wide Web для електронної комерції і розповсюдження інформації привело до виникнення гострої необхідності в забезпеченні захисту відповідних даних у Web.

Рисунок 2.4 – Загальна класифікація послуг безпеки

Забезпечити виконання ряду послуг дозволяє застосування протоколів SSL/TLS і SET . Протокол призначений для забезпечення надійного захисту наскрізної передачі даних з використанням протоколу TCP. Протокол SET – це відкриті специфікації шифрування і захисту, розроблені з метою захисту транзакцій, що виконуються в мережі Інтернет за допомогою пластикових платіжних карток.

Незважаючи на розробку цілого ряду механізмів захисту на прикладному і сеансовому рівні, існує необхідність забезпечення безпеки на мережевому рівні. Наприклад, підприємство може захистити свою мережу TCP/IP за допомогою заборони доступу до ненадійних вузлів, шифруючи пакети даних, що передаються з мережі підприємства, і вимагаючи автентифікації пакетів, що входять у цю мережу із зовні. За допомогою реалізації захисту на мережевому рівні організація може забезпечити роботу в мережі не тільки додатків, які мають свої засоби захисту, але і додатків, що не

володіють такими засобами. Захист на рівні IP (мережевому) (рис. 2.8) охоплює 3 сфери безпеки: автентифікацію, конфіденційність, керування ключами.

Механізми безпеки є конкретними заходами для реалізації послуг безпеки. Взаємозв’язок послуг і механізмів безпеки подано на рис. 2.10.

Стандарт поділяє механізми безпеки на два класи, а саме: спеціальні механізми забезпечення безпеки, які використовуються для реалізації специфічних послуг і різняться для різних послуг, та загальні механізми, які не належать до конкретних послуг безпеки.

До спеціальних механізмів забезпечення безпеки належать такі:

- шифрування (encipherment);
- механізми цифрового підпису (digital signature mechanisms);
- механізми управління доступом (access control mechanisms);
- механізми забезпечення захисту цілісності даних (dataintegrity mechanisms), які включають криптографічні контрольні функції;
- механізми автентифікації (authentication exchange mechanisms);
- механізми заповнення трафіку (padding traffic mechanisms);
- механізми керування маршрутизацією (routing control mechanisms).

Розглянемо кожен тип механізмів детальніше. Механізми шифрування припускають використання криптографічних перетворень даних для того, щоб зробити їх нечитабельними або неосмисленими. Шифрування застосовується спільно зі зворотною функцією – розшифрування.

Шифрування використовується для забезпечення послуги конфіденційності, але може також підтримувати інші послуги забезпечення безпеки, наприклад, автентифікації і захисту цілісності даних.

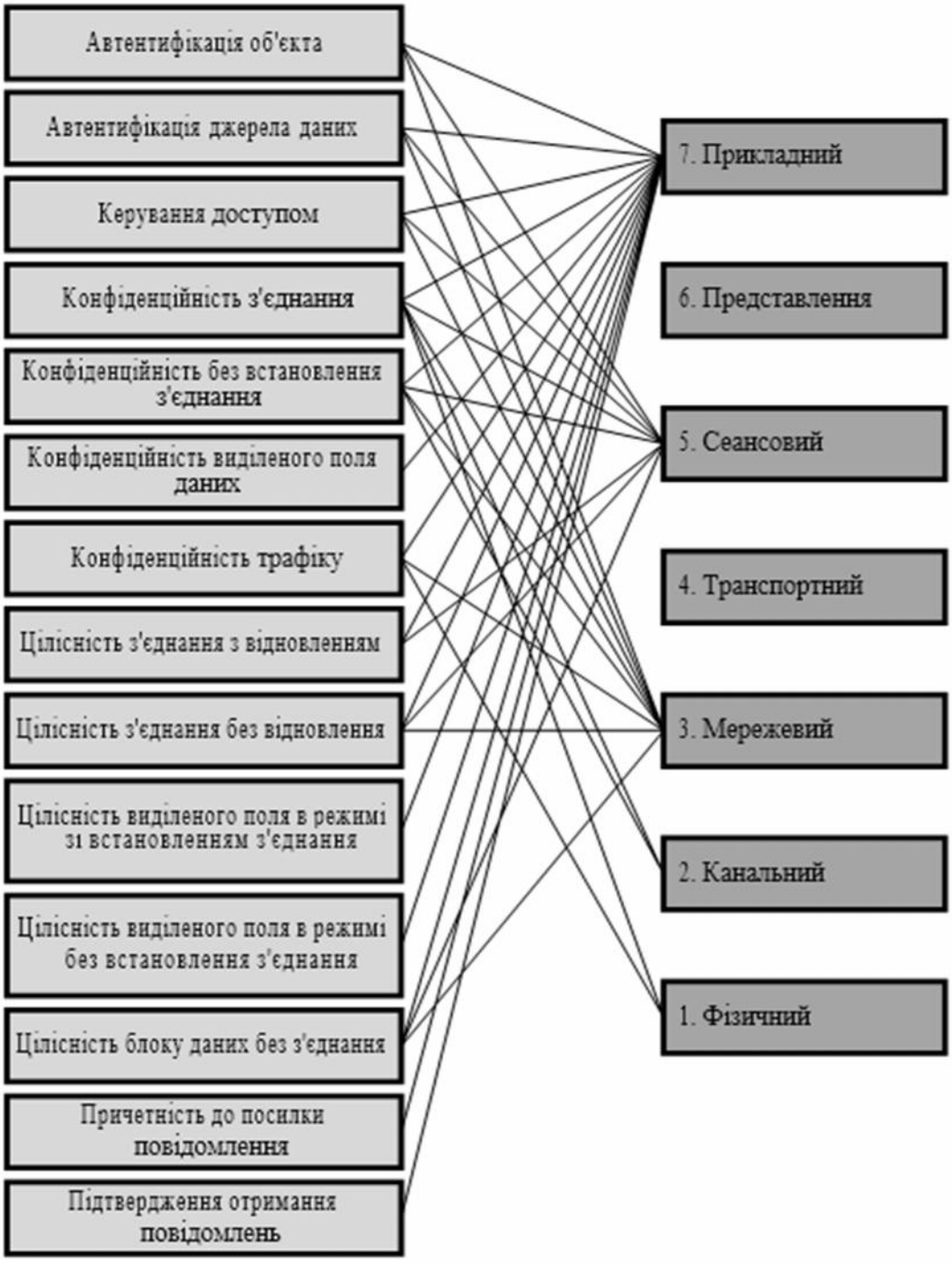

Рисунок 2.5 – Розподіл послуг безпеки по рівнях еталонної моделі ВВС

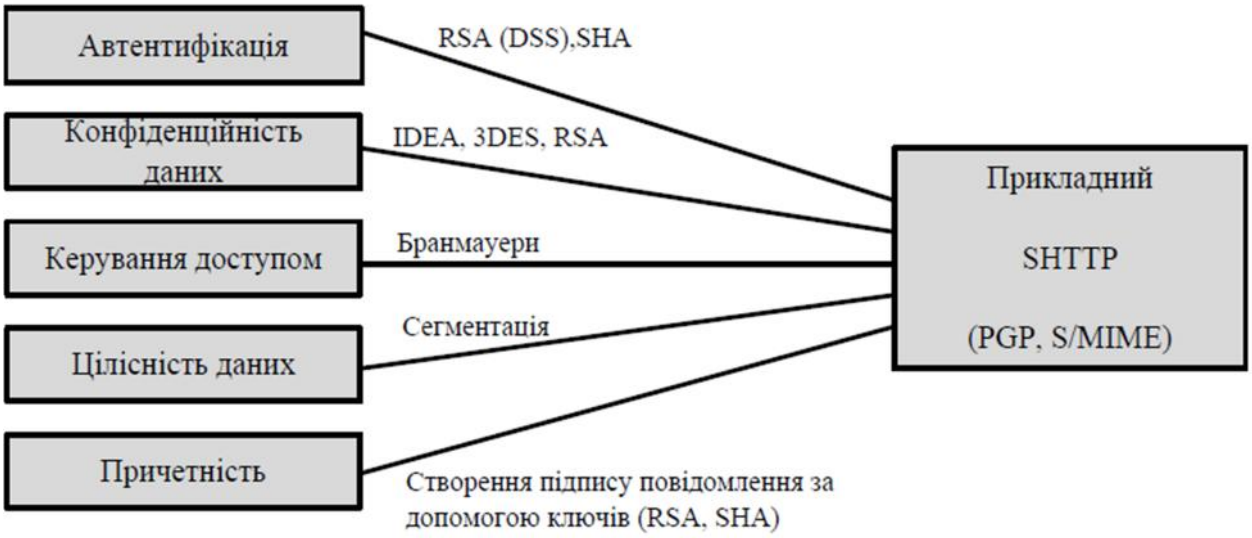

Рисунок 2.6 – Системи, що забезпечують захист інформації на прикладному Рівні

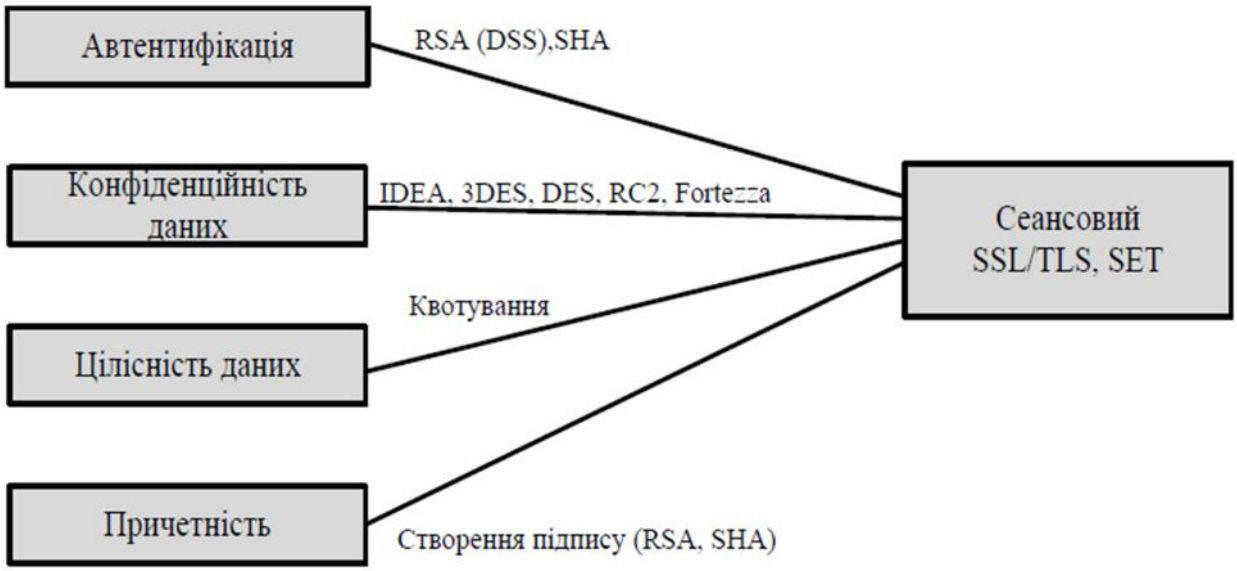

Рисунок 2.7 – Системи, що забезпечують захист інформації на сеансовому рівні

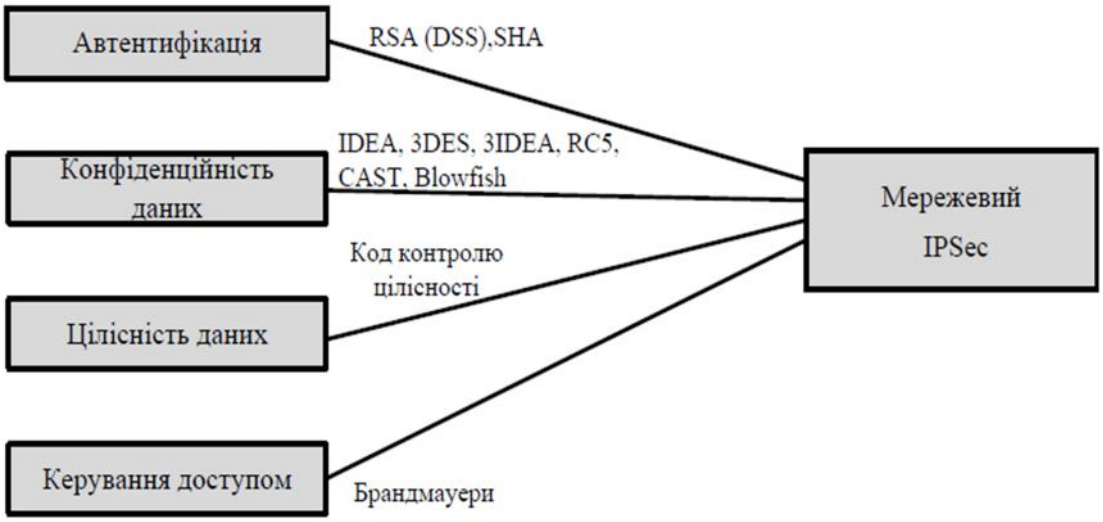

Рисунок 2.8 – Системи, що забезпечують захист інформації на мережевому рівні

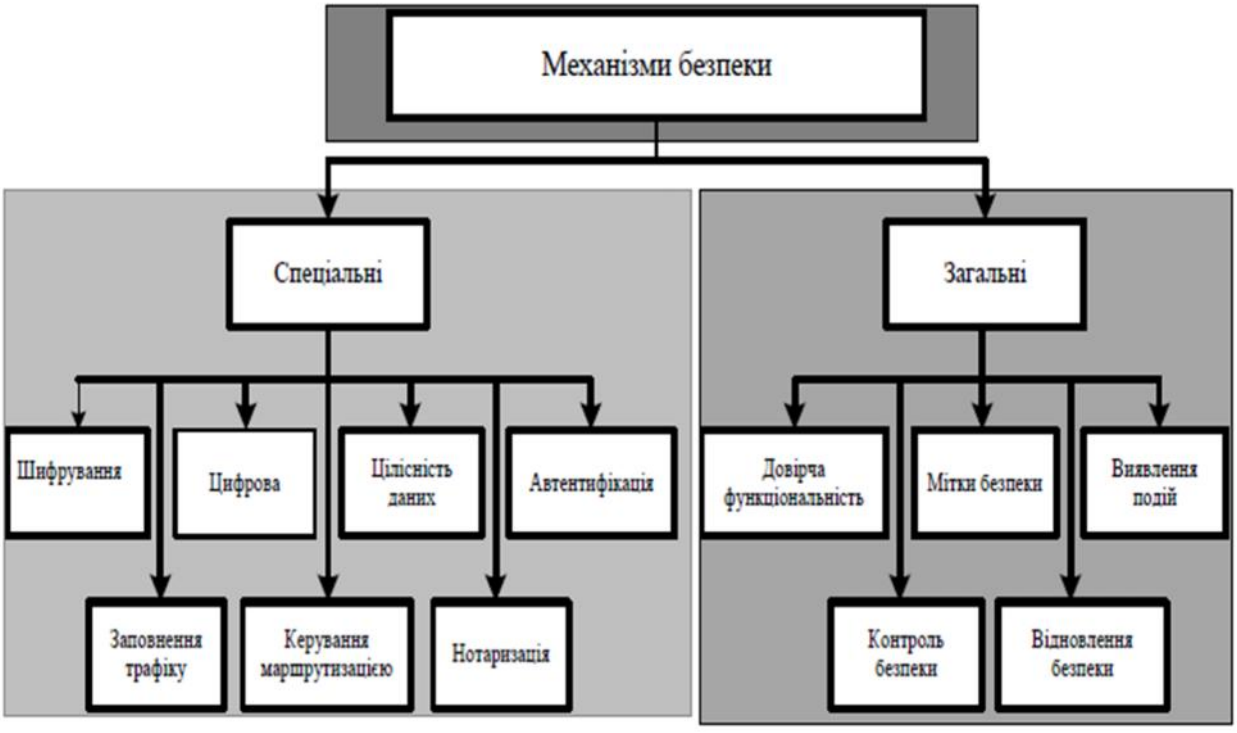

Рисунок 2.9 – Загальна характеристика механізмів

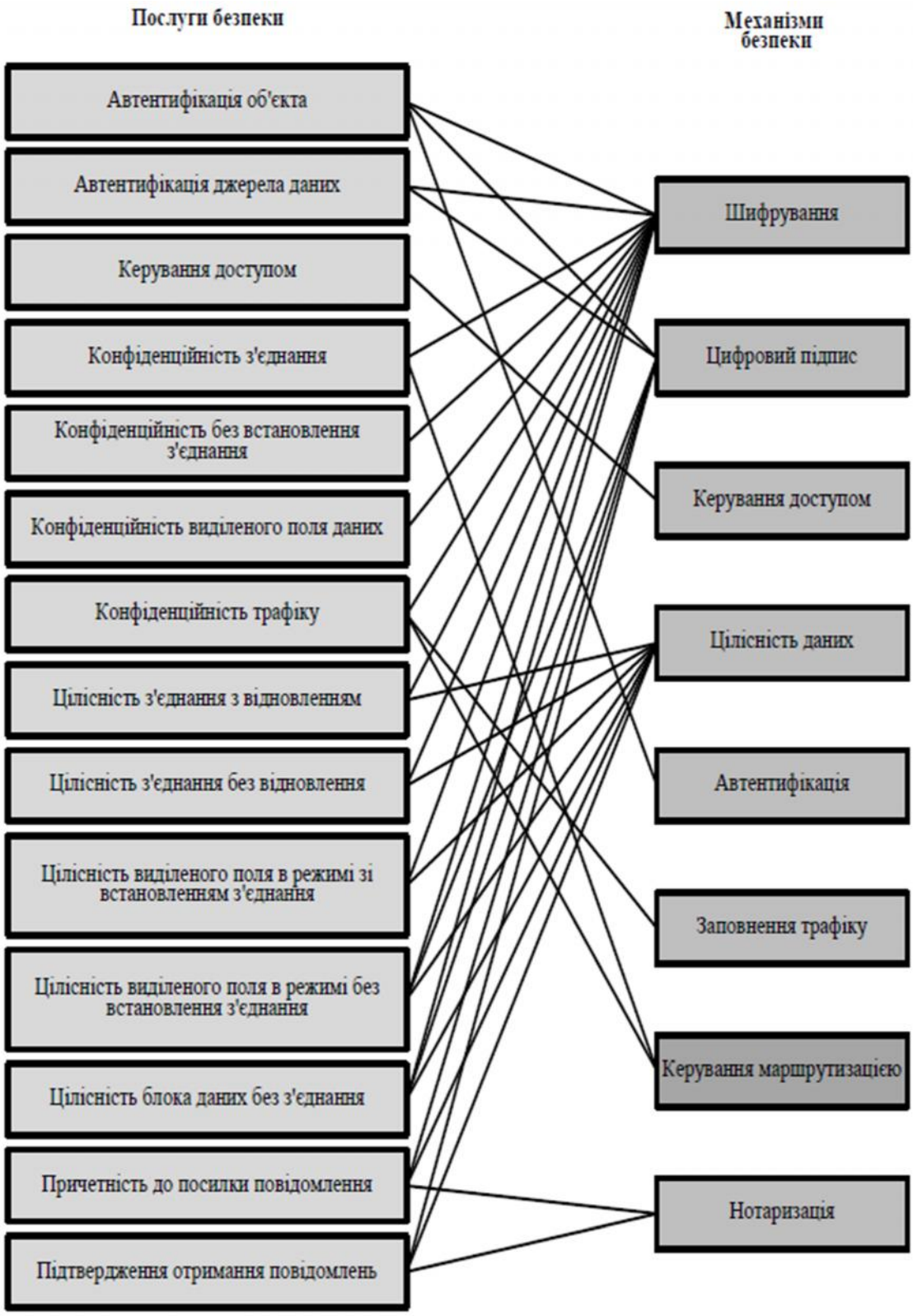

Рисунок 2.10 – Взаємозв’язок послуг і механізмів безпеки

Цифровий підпис є цифровим еквівалентом підпису (друку, штампа та ін..), наявність якого в повідомленні дозволяє з високою точністю визначити

джерело повідомлення (документа) і юридично довести, що, з певною ймовірністю, тільки він міг створити і підписати цей документ. Механізми цифрового підпису використовують "відкриті" ключі, які генеруються відправником даних і перевіряються одержувачем. Для шифрування контрольної суми підписуваного повідомлення можуть бути використані методи несиметричного шифрування. Цифровий підпис використовується для забезпечення послуг автентифікації і захисту цілісності, для яких суб’єкт верифікації підписаних даних наперед невідомий.

При певному виборі контрольованого параметра цифровий підпис також може застосовуватися в реалізації послуги підтвердження причетності.

Механізми керування доступом використовуються для забезпечення послуг керування доступом і реалізують політику керування доступом. При ухваленні рішень про надання запрошуваного типу доступу можуть використовуватися такі види й джерела інформації [2]:

- бази даних керування доступом, в яких можуть знаходитися списки керування доступом або структури аналогічного призначення;
- паролі або інша ідентифікаційна інформація;
- ідентифікаційні документи або інші посвідчення, пред’явлення яких свідчить про наявність прав доступу;
- позначки безпеки, асоційовані з суб’єктами й об’єктами доступу;
- час запрошуваного доступу;
- маршрут запрошуваного доступу;
- тривалість запитуваного доступу й інша інформація.
- механізми нотаризації (notarisation mechanisms).
- Механізми цілісності даних діляться на два типи механізмів:
- механізми захисту цілісності окремого пакета даних;
- механізми захисту цілісності послідовності пакетів даних.

Механізми другого типу, які зазвичай застосовуються спільно з механізмами захисту цілісності окремого пакета даних, можуть використовуватися для забезпечення послуг цілісності при організації зв’язку

в режимі зі встановленням з’єднання. Тут використовуються такі прийоми, як нумерація пакетів, часові штампи, криптографічне скріплення. Ці механізми дозволяють забезпечити захист від крадіжки, переупорядковування, дублювання і вставки повідомлень. У мережах, що функціонують в режимі без встановлення з’єднання, використання тимчасових штампів забезпечує також і обмежену форму захисту від дублювання.

У загальному випадку під автентифікацією розуміють встановлення достовірності повідомлення, джерела даних і приймача даних.

Автентифікація джерела даних часто забезпечується шляхом використання механізму захисту цілісності даних спільно з шифруванням або цифрового підпису. Логічна автентифікація користувача комп’ютерної системи здійснюється на основі пароля.

Автентифікація об’єкта комунікації зазвичай виконується за допомогою подвійного або потрійного підтвердження з’єднання або “рукостискання” аналогічно процедурі синхронізації пакетів у протоколах зі встановленням з’єднання. Односторонній (одноразовий) обмін забезпечує тільки одноразову автентифікацію і не може гарантувати своєчасність обміну. Двосторонній (двократний) обмін забезпечує взаємну автентифікацію джерела і приймача, але не забезпечує своєчасності обміну без застосування спеціальних засобів синхронізації. Тристоронній обмін дозволяє досягти повної взаємної автентифікації систем без додаткової синхронізації. Для забезпечення автентифікації також можуть використовуватися спеціальні механізми керування криптографічними ключами.

Механізм заповнення трафіку застосовується для забезпечення конфіденційності трафіку. Заповнення трафіку може включати генерацію випадкового трафіку, заповнення додатковою інформацією інформативних пакетів, передачу пакетів через проміжні станції в "непотрібному" напрямі. Обидва типи пакетів, як інформативний, так і випадковий, можуть доповнюватися до постійної довжини.

Механізми нотаризації привертають третю сторону, що користується

довірою двох суб’єктів, для забезпечення підтвердження комунікаційних характеристик переданих даних. Такими комунікаційними характеристиками є цілісність, час, особи відправників і одержувачів. Найчастіше механізми нотаризації застосовуються для забезпечення послуги підтвердження причетності. Для підтвердження причетності відправника даних нотаризація застосовується спільно з цифровим підписом на основі "відкритого" ключа.

Нотаризація може також застосовуватися для забезпечення надійної тимчасової позначки, що забезпечується "тимчасовим нотаріусом". Така позначка може містити підпис "нотаріуса", ідентифікатор повідомлення, імена відправника і одержувача, а також зареєстровані час і дату отримання повідомлення. При цьому "нотаріус" не має доступу до самого повідомлення, що забезпечує конфіденційність повідомлення.

Механізми керування маршрутизацією застосовуються для забезпечення конфіденційності з метою запобігання контролю за шляхом проходження даних від відправника до одержувача. Вибір шляху може здійснюватися або крайовою системою, реалізуючи маршрутизацію, яка визначається джерелом (sourse routing), або проміжною системою на основі використання "позначок безпеки", що вводяться в пакет крайовою системою.

Цей механізм вимагає забезпечення надійності (конфіденційності) проміжних систем і може мати істотні варіації при використанні різних систем. Він може також використовуватися і для забезпечення захисту цілісності даних (з функціями відновлення даних або з’єднання) за рахунок введення і використання для передачі даних альтернативних шляхів у разі виникнення атак, що призводять до переривання комунікацій.

До загальних механізмів забезпечення безпеки належать [3] :

- довірча функціональність (trusted functionality);
- позначки безпеки (security lables);
- виявлення подій (event detection)
- контроль безпеки (security audit trail);
- відновлення безпеки (security recovery).

Довірча функціональність використовується разом з іншими механізмами безпеки і є сукупністю рекомендацій і способів, які повинні реалізовуватися для забезпечення гарантії правильної і надійної роботи інших механізмів безпеки. Довірча функціональність припускає широке використання нормативної документації при розробленні програмних або апаратних засобів, що реалізовують механізми безпеки. Розроблення цих засобів повинно вестися при дотриманні відповідних організаційних вимог. Програмні і апаратні засоби повинні розроблятися, тестуватися і сертифікуватися на основі єдиних методик. Саме тут забезпечуються всі необхідні вимоги і рекомендації щодо електромагнітних випромінювань, можливостей фізичного втручання, використання безпечних каналів розповсюдження і багато іншого. Будь-які дані (записані дані, обчислювальні потужності та/або комунікаційні послуги) можуть мати асоційовані позначки безпеки, які визначають їх рівень секретності. Позначки безпеки можуть бути явно або побічно зв’язані як окремими пакетами даних, так і з послідовностями пакетів. Зазвичай позначки безпеки використовуються для реалізації методики керування доступом на основі встановлених правил, а також для керування маршрутизацією. Передані дані також можуть мати позначки безпеки, які передаються разом з ними безпечним чином. У цьому випадку для забезпечення захисту позначок застосовуються криптографічні функції, а позначки безпеки використовуються для забезпечення контролю за цілісністю повідомлень.

Механізми виявлення подій в системах захисту інформації служать для виявлення як спроб порушення безпеки, так і для реєстрації легітимної активності користувачів. Виявлення може бути локальним та/або дистанційним і реалізуватися через тривожну сигналізацію про події (event reporting (alarm)), реєстрацію подій (event logging) і відновлювальної дії (recovery actions).

Під контролем безпеки розуміють незалежний розгляд і аналіз записів безпеки з метою перевірки достатності керування системою, гарантувати

відповідність функціонування системи політиці безпеки і рекомендувати необхідні зміни в управлінні, політиці і процесах безпеки. Зазвичай розглядають дві процедури: протоколювання і аудит. Під протоколюванням розуміють збирання і накопичення інформації про події, що відбуваються в інформаційній системі. Під аудитом розуміють оперативний аналіз накопиченої інформації, що проводиться постійно або періодично.

Механізми протоколювання і аудиту служать для вирішення завдань:

- забезпечення підзвітності користувачів і адміністраторів, що є засобом заборони;

- забезпечення можливості відновлення послідовності подій, що дозволяє виявити слабкості в захисті інформації, виявити винуватця вторгнення, оцінити масштаби заподіяного збитку і повернутися до нормальної роботи;

- надання інформації для виявлення і аналізу проблем через підготовку відповідних звітів і рапортів.

Механізми відновлення безпеки виконують функцію реакції системи на порушення безпеки. Такими діями можуть бути, наприклад, негайне роз’єднання або припинення роботи, відмова суб’єкту в доступі, тимчасове позбавлення суб’єкта прав, занесення суб’єкта в "чорний список" та ін.

2.3 Механізми безпеки та методи їх оцінки

2.3.1 Механізми безпеки

В попередніх розділах були представлені та проаналізовані різноманітні механізми забезпечення безпеки, а саме:

а) До загальних механізмів забезпечення безпеки належать [3]:

1) довірча функціональність (trusted functionality);

2) позначки безпеки (security lables);

3) виявлення подій (event detection);

4) контроль безпеки (security audit trail);

5) відновлення безпеки (security recovery).

б) До спеціальних механізмів забезпечення безпеки належать такі:

1) шифрування (encipherment);

2) механізми цифрового підпису (digital signature mechanisms);

3) механізми управління доступом (access control mechanisms);

4) механізми забезпечення захисту цілісності даних (data-integrity mechanisms), які включають криптографічні контрольні функції;

5) механізми автентифікації (authentication exchange mechanisms);

6) механізми заповнення трафіку (padding traffic mechanisms);

7) механізми керування маршрутизацією (routing control mechanisms).

2.3.2 Механізм безпеки що використовується в методиці

В кваліфікаційній роботі також необхідно обрати систему безпеки, що і буде виконувати задачі механізму безпеки влив якого і буде оцінюватись в методиці. Для використання в методиці був обраний засіб розмежування доступу, а саме програмний комплекс захисту інформації Secret Net з налаштованим політиками мандатного доступу до об’єктів файлової системи. Тобто система захисту буде кожен раз перевіряти наявність необхідного рівня доступу для того щоб виконати ту чи іншу операцію з файловою системою (наприклад CreateFile). Більш детально про розмежування доступу буде написано в розділі 3.2

Secret Net – це комплексне рішення для захисту робочих станцій та серверів на рівні даних, додатків, мережі, операційної системи та периферійного обладнання. Продукт об’єднує в собі функціонал кількох засобів захисту «Коду Безпеки» (СЗІ від НСД Secret Net, міжмережевий екран TrustAccess, СЗІ Trusted Boot Loader, СКЗІ «Континент-АП»), а також включає низку нових захисних механізмів.

У рамках цього продукту вирішуються такі завдання:

а) Захист від зовнішніх загроз:

1) захист робочих станцій та серверів від вірусів та шкідливих програм;

2) захист від мережевих атак;

3) захист від підробки та перехоплення мережевого трафіку всередині локальної мережі;

4) захищений обмін даними з віддаленими робочими станціями.

б) Захист від внутрішніх загроз:

1) захист інформації від несанкціонованого доступу;

2) контроль витоків і каналів поширення інформації, що захищється;

3) захист від дій інсайдерів;

4) захист від крадіжки інформації під час втрати носіїв.

2.3.3 Сучасні методи оцінки впливу систем безпеки на продукивність комп’ютерних систем

Сучасні комп’ютери мають величезну продуктивність. Однак часто доводиться вимірювати числове значення продуктивності системи. Для того щоб можливість об’єктивно оцінити ступінь вдосконалення системи після її модернізації або порівняти продуктивність різних комп’ютерів, необхідно кількісно оцінити продуктивність. Існують спеціалізовані еталонні програми, які вимірюють продуктивність комп’ютера при виконанні на ньому певного набору завдань. Залежно від ситуації, їх можна використовувати для різних цілей:

- порівняння декількох різних систем;
- оцінка ступеня вдосконалення системи після її модернізації. Тестові програми часто використовуються для оцінки ступеня поліпшення характеристик системи після її модернізації, в тому числі модернізації системи безпеки;

- виправлення несправностей. Іноді тестові програми корисні для діагностики системи. Перевіривши і переналаштуючи ключові компоненти несподівано «уповільненого» комп'ютера і оцінивши результати маніпуляцій, виконаних за допомогою тестових програм, досвідчений фахівець зможе швидко визначити і усунути причину уповільнення роботи системи, навіть якщо причиною є система безпеки, ніж просто спостерігати за її роботою.

Однією з найбільших проблем, пов'язаних з тестовими програмами, є достовірність їх результатів. Відомий афоризм про те, що є брехня, велика брехня і статистика, повністю відноситься до тестових програм. Для того, щоб результати, отримані цими програмами, були довірені, необхідно дотримуватися певних правил:

- записати всю інформацію, пов'язану з конфігурацією системи. Тестові програми можуть давати значно різні результати при різних налаштуваннях однієї і тієї ж системи;

- щоб порівняти продуктивність системи, скористайтеся тією ж тестовою програмою. Результати будь-якої програми, включаючи тестову програму, залежать від стилю і якості написання програмного коду. Навіть дві різні версії тестової програми при перевірці однієї і тієї ж системи можуть давати різні результати. якщо ви хочете порівняти продуктивність декількох комп'ютерів, ви повинні запустити одну і ту ж версію тестової програми на кожному комп'ютері.

Одиницею вимірювання продуктивності комп'ютера є час: комп'ютер, який виконує однаковий обсяг роботи за менший час, швидше. Час виконання будь-якої програми вимірюється в секундах. Продуктивність часто вимірюється як швидкість, з якою відбувається певна кількість подій в секунду, тому менше часу передбачає більшу продуктивність.

Важливість створення тестових пакетів на основі реальних прикладних програм широкого кола користувачів і забезпечення ефективної оцінки продуктивності процесорів була реалізована більшістю найбільших виробників комп'ютерної техніки, які в 1988 році заснували некомерційну

корпорацію SPEC (Standard Performance Assessment Corporation). Основною метою цієї організації є розробка і підтримка стандартизованого набору спеціально підібраних тестових програм для оцінки продуктивності останніх поколінь високопродуктивних комп'ютерів.

Базовий набір CINT92, який вимірює продуктивність процесора в обробці цілих чисел, складається з шести програм, написаних на C і вибраних з різних областей застосування: теорія схеми, інтерпретатор Лісп, логічний дизайн, упаковка текстових файлів, електронні таблиці та компіляція програм.

Тестовий набір CFP92, який вимірює продуктивність процесора в обробці з плаваючою комою, складається з 14 програм, також обраних з різних областей застосування: розробка аналогових схем, моделювання Монте-Карло, квантова хімія, оптика, робототехніка, квантова фізика, астрофізика, прогнозування погоди та інші наукові та інженерні проблеми. Дві програми з цього набору написані на C, а решта 12 знаходяться в Fortran. П'ять програм використовують одну, квантову фізику, астрофізику, прогнозування погоди та інші наукові та інженерні проблеми, а в інших – подвійна точність.

Продуктивність процесора залежить від трьох параметрів: тактової частоти (або частоти F), середньої кількості годин на інструкцію (S) і кількості виконуваних інструкцій (N).

$$T = \frac{N * S}{F}. \quad (2.1)$$

Стандартом дефакто при порівнянні продуктивності комп'ютерів вважають результати пакету LINPACKBenchmark (далі тест LINPACK). В оперативній пам'яті пакет генерує систему лінійних алгебраїчних рівнянь (СЛАУ) із щільною матрицею коефіцієнтів, заповнену псевдовипадковими числами, і вирішує її методом LU-ня. Цей алгоритм інтенсивно використовує процесор, оперативну пам'ять та комунікаційні канали, залишаючись дуже ефективним, оскільки навантаження на процесор переважає над іншими.

Існує різноманітність програмного забезпечення, що дозволяє оцінити

працездатність комп’ютерної системи. Як правило, такий вимір проводять у два етапу. Перший – вимірювання продуктивності окремих вузлів та компонентів, включаючи процесори, оперативну пам’ять, мережу, дискові масиви. Завдання цього етапу — виявити збої в компонентах комплексу, які не обов’язково призводять до втрати працездатності: часто комп’ютер продовжує працювати зі зниженою швидкістю. Другий етап - тестування продуктивності в цілому. Для тестування процесора використовують однопроцесорну та SMP-версії тесту LINPACK, а для оперативної пам’яті - утиліту MEMTEST86, STREAM або RandomAccess.

Оскільки тест LINPACK часто використовують не за призначенням, помилково сподіваючись досягти ефективності, порівнянної з його показниками, розробники LINPACK запропонували новий пакет тестування HPCC (HPC Challenge)Benchmark Suite). Його завдання — вимірювання продуктивності різних компонентів паралельного комп’ютера, здатних обмежити виконання прикладних програм. Цей пакет складається з кількох відомих пакетів, що вимірюють аспекти продуктивності, а також надає середовище для підключенняня додаткових тестів. Зокрема, пакет HPCC включає такі відоміпрограми вимірювання продуктивності, як STREAM (швидкість оперативної пам’яті), HPL, DGEMM (множення матриць), PTRANS (транспонування матриць, FFT, RandomAccess (швидкість довільного доступу до пам’яті), bJeff (латентністьта пропускна здатність каналів). Результат виміру продуктивностів HPCC - не одне, а ряд значень продуктивності.

З рівня техніки відомий спосіб оцінки ступеня впливу засобів захисту інформації на систему, що захищається, в якому в якості показників, що характеризують вплив засобів захисту на систему, що захищається, використовуються показники, що характеризують витрата ресурсів інформаційно-обчислювальної системи.

Недоліки даного способу полягають, по-перше, у його орієнтації на оцінку ступеня впливу на продуктивність інформаційної системи антивірусних засобів, а не засобів розмежування доступу, а по-друге, оскільки

результат оцінки представляється сукупністю кількох різнорідних показників, завдання вибору оптимального (з точки зору споживання ресурсів) засоби захисту зводиться до вирішення завдання багатокритеріального вибору, що представляє певну складність і потребує значних обчислювальних ресурсів та часу.

Відомий також спосіб оцінки впливу засобів захисту на систему, що захищається, в якому використовуються показники падіння продуктивності інформаційно-обчислювальних систем при виконанні певних завдань, вироблених інформаційно-обчислювальною системою.

Недоліками зазначеного способу є: по-перше, виміряні оцінки можуть бути неоднорідні (наприклад, являти собою або оцінки збільшення часу виконання завдань, або оцінки зниження кількості операцій, що одночасно виконуються при вирішенні завдань, покладених на інформаційно-обчислювальну систему), по-друге, ці оцінки можуть мати великий розкид за кількісними показниками (наприклад, від сотих часток секунд до кількох хвилин), по-третє, завдання вибору оптимального засобу захисту зводиться до завдання багатокритеріального вибору.

В наступному розділі, як результат дослідження буде запропонована на огляд більш проста в реалізації та розумінні методика для оцінки впливу системи розмежування доступу на продуктивність системи.

3 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧІ

3.1 Аналіз проблем проектування безпечних систем

Ефективність засобів захисту від інформаційно-технічних впливів і комп’ютерних атак грає велику роль в адекватному функціонуванні системи. Крім вимог до ефективності виконання захисних функцій, до систем ставиться вимога мінімізації впливу атак на процеси функціонування системи, зокрема, на її продуктивність.

В ідеальному випадку система (або засоби) захисту не повинні впливати на продуктивність інформаційно-обчислювальної системи. Разом з тим слід зазначити, що створити якусь систему захисту (в тому числі і систему розмежування доступу в приміщення), яка не впливала б негативно на захищаємий об’єкт, практично неможливо. Виходячи з цього, одним з критеріїв вибору системи (або засобів) розмежування доступу для захисту будь-якої інформаційно-обчислювальної системи повинен бути критерій мінімуму впливу обраної системи розмежування доступу на продуктивність захищається інформаційно-обчислювальної системи.

З усіх існуючих моделей розмежування доступу найбільшого поширення набули дві основні моделі [6]:

- виборче (діскреційне) розмежування доступу;
- повноважне (мандатний) розмежування доступу.

3.2 Моделі монітору безпеки та вимоги до методики

Застосування даних моделей в информацийно-обчислювальних системах і засобах обчислювальної техніки регламентується керівними документами, при цьому в інформаційно-обчислювальних системах і засобах обчислювальної техніки повинна бути реалізована як мінімум дискреціонна

модель розмежування доступу, а в разі обробки інформції, що має конфіденційний характер, обов'язково повинна бути реалізована мандатна модель розмежування доступу. При дискреційному розмежуванні доступу певні операції над конкретним ресурсом забороняються або вирішуються суб'єктам або групам суб'єктів. Практично всі існуючі операційні системи реалізують саме таку модель доступу. Мандатне розмежування доступу полягаєв тому, що всі об'єкти доступу мають визначенні рівні секретності, а всі суб'єкти поділяються на групи, що утворюють ієрархію відповідно до рівня допуску до інформації. Для реалізації мандатної моделі розмежування доступу, як правило, необхідні додаткові програмні засоби, що вбудовуються в операційну систему. При цьому слід зазначити, що мандатна модель розмежування доступу при реалізації її в операційних системах не замінює дискреційну модель розмежування доступу, а доповнює її, вносячи додатковий рівень перевірки прав доступу суб'єктів, при їх запитах на будь-які дії з об'єктами.

Реалізація мандатного доступу в різних операційних системах (Linux, Windows), як правило, здійснюється шляхом вбудовування в операціну систему додаткових програмних компонентів, які здійснюють перехоплення API-функцій операційної системи, які призначені для здійснення будь-яких дій з об'єктами доступу [3] (файлами, ділянками пам'яті, мережевими з'єднаннями, інтерфейсами введення / виведення зовнішніх пристроїв та ін.) (рис. 3.2)

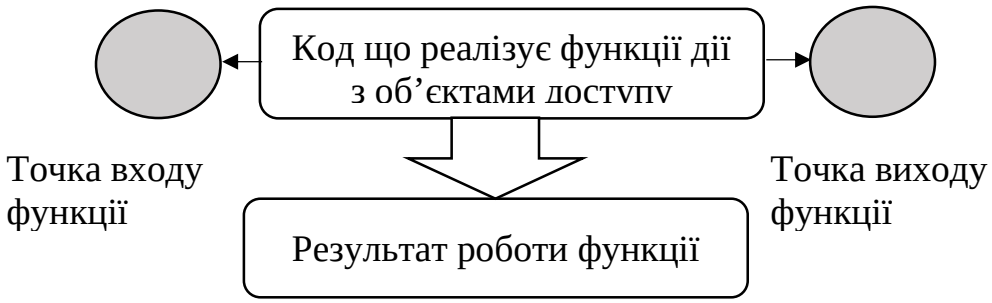

Рисунок. 3.1 – Реалізація функції дій з об'єктами доступу без її перехоплення

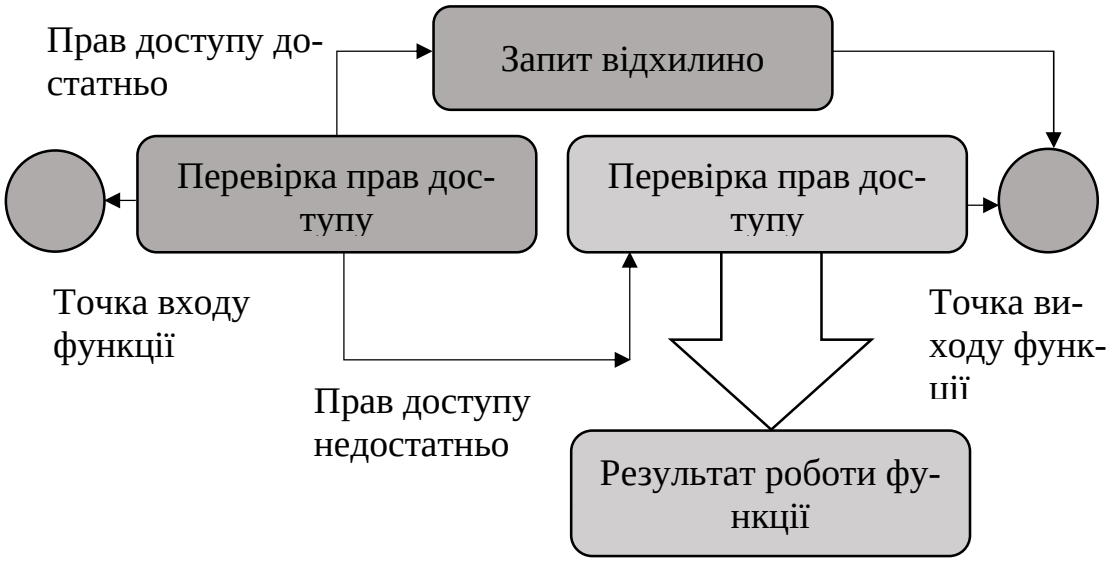

Рисунок. 3.2 – Реалізація функції дій з об’єктами доступу з перехопленням її компонентом, які виконують перевірку прав доступу

Спосіб перехоплення зазначених системних функцій залежить від типу операційної системи, для якої призначена система (або засіб) розмежування доступу. Для операційних систем сімейства Windows перехоплення функцій може бути здійснений або внесенням змін до таблиці дескрипторів системних викликів SDT, або з використанням драйвера-фільтра файлової системи. Для операційних систем сімейства Linux перехоплення зазначених функцій здійснюється із застосуванням механізму LSM. Особливості реалізації мандатної моделі розмежування доступу в інформаційно-обчислювальних системах різного призначення приводить до істотного зниження продуктивності системи, оскільки права доступу до об’єкта повинні перевірятися не тільки при відкритті об’єкта, але і при проведенні будь-якої операції з об’єктом (читання, запис, переміщення).

Виходячи з цього при побудові або при виборі засобів розмежування доступу для різних інформаційно-обчислювальних систем необхідно мати можливість оцінювати рівень впливу цих засобів на продуктивність системи для вибору найбільш прийнятного варіанту реалізації мандатної моделі розмежування доступу в інформаційно-обчислювальних системах.

Відомі методики оцінювання впливу засобів захисту на якість функціонування та на продуктивність інформаційно-обчислювальних систем або не дозволяють виробляти оцінку ступеню впливу засобів розмежування доступу, або не мають можливості виробити оцінку ступеня впливу засобів розмежування доступу на продуктивність інформаційно-обчислювальної системи в цілому. Крім цього, в більшості методик при згортку приватних показників, що характеризують ступінь впливу засобів захисту на продуктивність системи, використовується експертний метод вагових коефіцієнтів значущості того чи іншого приватного показника, що знижує об’єктивність оцінки і ускладнює проведення самої процедури оцінки.

Таким чином, виникає необхідність в розробці методики оцінки ступеня впливу засобів розмежування доступу на продуктивність системи. Методика повинна відповідати наступним вимогам [5]:

- мати можливість оцінювати вплив засобів розмежування доступу на продуктивність інформаційно-обчислювальної системи в цілому з урахуванням особливостей її функціонування і вирішення покладених на неї завдань;

- вагові коефіцієнти, необхідні для згортки приватних показників ступеня зниження продуктивності в інтегральний, повинні визначатися без використання методів експертних оцінок;

- в якості приватних показників, характеризуючи ступінь впливу засобів розмежування доступу на продуктивність системи, повинні використовуватися коефіцієнти уповільнення швидкості виконання системних функцій операційної системи, що реалізують всі керуючи засоби розмежування доступу операції з об’єктами доступу.

Методика оцінки ступеня впливу засобів розмежування доступу на продуктивність інформаційно-обчислювальної системи повинна включати в себе наступні етапи:

- визначення переліку системних функцій операційної системи, що підлягають контролю;

- визначення вагових коефіцієнтів значимості (для виконання покладених на систему завдань) системних функцій;

- визначення коефіцієнтів уповільнення виконання системних функцій операційної системи, що підлягають оцінці;

- визначення загального (інтегрального) показника зниження продуктивності системи внаслідок впливу засобів розмежування доступу системи.

Аналіз практичного досвіду щодо захисту комп'ютерної інформації, а також основних положень суб'єктно об'єктної моделі КС дозволяє сформулювати кілька аксіоматичних умов, що стосуються структури і функціонування захищених КС [4] .

Аксіома 1. У захищеної КС в будь-який момент часу будь-який суб'єкт і об'єкт повинні бути персоніфіковані (ідентифіковані) і автентифіковано.

Дана аксіома визначається самою природою і змістом процесів колективного доступу користувачів до ресурсів КС. Якщо будь-які суб'єкти (користувачі) мають можливість видати себе в КС за інших суб'єктів (користувачів) або якщо мають можливість підміняти (видавати) одні об'єкти доступу за інші, то ні про яку безпеки, захищеність мови бути не може. Таким чином, аксіома 1 висловлює необхідну умову безпеки (захищеності) інформації в КС, а процедури, механізми і системи, що здійснюють ідентифікацію та аутентифікацію користувачів, їх суб'єктів і об'єктів доступу, є вихідним і найважливішим програмно технічним кордоном захисту інформації в КС.

Аксіома 2. У захищеної КС повинна бути присутня активна компонента (суб'єкт, процес і та.ін.) з відповідним об'єктом (-ами) - джерелом, яка здійснює управління доступом і контроль доступу суб'єктів до об'єктів. У літературі для даної активної компоненти утвердився термін «монітор безпеки». Поняття монітора безпеки дозволяє висловити схемотехнічний аспект захисту інформації в КС у вигляді схеми, представленої на рис.3.3

У структурі більшості типів програмних засобів, на основі яких будуються інформаційні системи (ОС, СУБД), можна виділити ядро (ядро ОС, машина даних СУБД), в свою чергу, розділяється на компоненту подання інформації (файлова система ОС, модель даних СУБД) і на компоненту доступу до даних (система вводу-виведення ОС, процесор запитів СУБД), а також над будову (утиліти, сервіс, інтерфейсні компоненти). Початкові суб'єкти при здійсненні процесів доступу звертаються за сервісом, функціями до ядра системи (рис. 3.3.а.)

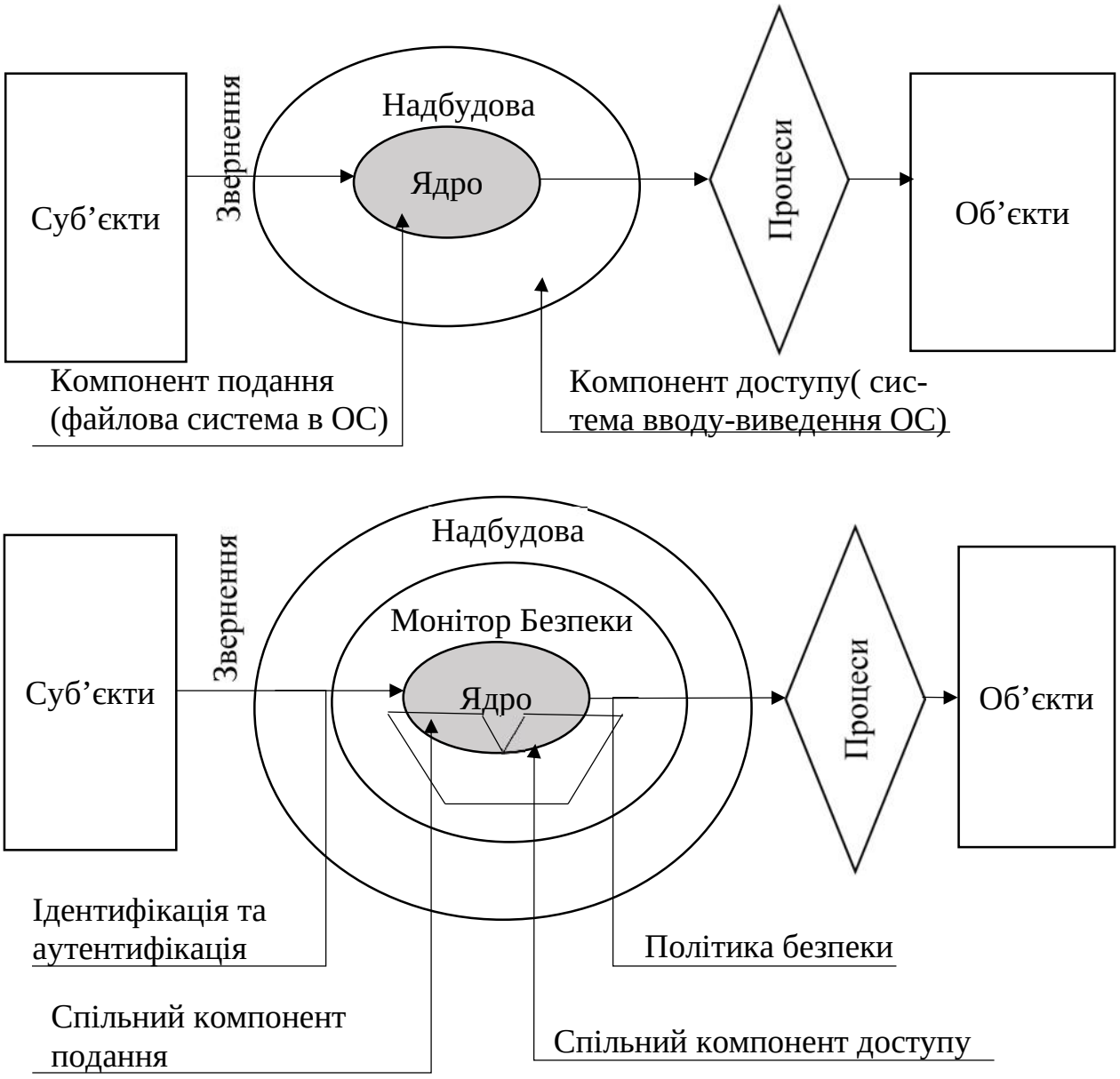

Рисунок. 3.3 – Системотехнічний аспект: незахищеною КС та захищеної КС

У захищеної системи з’являється додаткова компонента, що забезпечує процеси захисту інформації, перш за все, процедури ідентифікації / аутентифікації, а також управління доступом на основі тієї чи іншої політики безпеки (розмежування доступу) – рис. 3.3.б. З огляду на те, що як саме ядро КС (компонент уявлення та компонент доступу), так і процеси розмежування доступу нерозривно пов’язані з поданням інформації та маніпулюванням з нею, то монітор безпеки повинен бути інтегрований безпосередньо в ядро системи. Іноді кажуть, що монітор безпеки повинен бути реалізований на нульовому рівні (на рівні ядра) системи. В цьому відношенні зауважимо, що більш правильний підхід полягає в такій розробці компонентів ядра КС, які б спочатку будувалися на основі певної моделі безпеки (моделі розмежування) доступу. У практичному плані, в тому числі і з урахуванням вітчизняних і міжнародних нормативних вимог по сертифікації захищених систем, до реалізації монітора безпеки пред’являються такі обов’язкові вимоги [4]:

- повнота. Монітор безпеки повинен викликатися (активізуватися) при кожному зверненні за доступом будь-якого суб’єкта до будь-якого об’єкту, і не повинно бути ніяких способів його обходу;
- ізольованість. Монітор безпеки повинен бути захищений від відстеження і перехоплення своєї роботи;
- верифіковані. Монітор безпеки повинен бути перевірятися (само- або зовні тестованим) на предмет виконання своїх функцій;
- безперервність. Монітор безпеки повинен функціонувати при будь-яких штатних і позаштатних, в тому числі і аварійних ситуаціях. Таким чином, саме монітор безпеки в захищеній системі є суб’єктом здійснення прийнятої політики безпеки, реалізуючи через алгоритми своєї роботи відповідні моделі безпеки. В цьому відношенні велике значення має наступне аксіоматичне положення.

Аксіома 3. Для реалізації прийнятої політики безпеки, управління і контролю доступу суб’єктів до об’єктам необхідна (повинна існувати)

інформація і об’єкт (и), що її містить (ять) (крім інформації для ідентифікації і аутентифікації користувачів).

З аксіоми 3 випливає, що монітор безпеки, в свою чергу, як і будь-яка активна сутність в КС, є суб’єктом з відповідним об’єктом-джерелом і асоційованими об’єктами. Звідси випливають такі важливі слідства.

Слідство 1 (з аксіоми 3). У захищеної КС існують особлива категорія суб’єктів (активних сутностей), що не ініціалізують і якими не керують користувачі системи т.ін. системні процеси (суб’єкти), присутні (функціонуючі) в систем і від самого початку. До числа подібних системних суб’єктів відноситься вихідний системний процес, який ініціалізує первинні суб’єкти користувачів, а також монітор безпеки, який керує доступами суб’єктів користувачів до об’єктів системи. Відповідно, для забезпечення захищеності в КС властивості системних суб’єктів повинні бути незмінними, від чого напряму залежать гарантії безпеки.

Слідство 2 (з аксіоми 3). Асоційований з монітором безпеки об’єкт, що містить інформацію по системі розмежування доступу, є найбільш критичним з точки зору безпеки інформаційних ресурсом в захищеній КС.

Дійсно, можливість не санкціоновано змінювати, видаляти даний об’єкт може повністю зруйнувати або дискредитувати всю систему безпеки КС. Тому способи і особливості реалізації даного об’єкта мають визначальне значення для захищеності інформації в КС.

Інформація в асоційованим з монітором безпеки об’єкті повинна стосуватися конкретних зареєстрованих в системі користувачів і конкретних об’єктів системи. Отже, для планування і управління системою розмежування доступу конкретного колективу користувачів КС повинна бути передбачена процедура доступу до даного об’єкта з боку зовнішнього фактора, т. е. через суб’єкт (и) користувача. Звідси випливає ще один наслідок.

Слідство 3 (з аксіоми 3). У захищеній системі може існувати довірений користувач (адміністратор системи), суб’єкти якого мають доступ до асоційованого з монітором безпеки об’єкту-даними для управління політикою

розмежування доступу.

Зауважимо також, що суб’єкти, які ініціюються адміністратором системи, не є елементами або процесами монітора безпеки, а лише забезпечують монітор безпеки конкретною інформацією для управління і контролю доступом суб’єктів до об’єктів системи.

Принципи, способи подання та реалізація асоційованих з монітором безпеки об’єктів визначаються типом політики безпеки і особливостями конкретної КС.

Незважаючи на те, що до теперішнього часу розроблено і опробовано в практичній реалізації велика кількість різних моделей безпеки КС, всі вони висловлюють кілька вихідних політик безпеки. В спрощеної трактуванні політику безпеки розуміють, як загальний принцип (методологію, правило, схему) безпечної роботи (доступу) колективу користувачів з загальними інформаційними ресурсами, при цьому згідно визначенню найважливіше значення має критерій безпеки доступів суб’єктів до об’єктів, правило поділу інформаційних потоків, породжуваних доступами суб’єктів до об’єктів, на небезпечні і безпечні. Методологічною основою для формування політик безпеки в захищених КС послужили реальні організаційно-технологічні схеми забезпечення безпеки інформації поза (до) комп’ютерних сфер. Багато підходів до захисту комп’ютерної інформації були «Підглянуті», зокрема, в сфері роботи з «паперовими» конфіденційними документами, простіше кажучи, в сфері діловодства.

Політика дискреційного (виборчого) доступу. Безліч безпечних (дозволених) доступів PL задається для іменованих користувачів (суб’єктів) і об’єктів явним чином в вигляді дискретного набору трійок «Користувач (суб’єкт) -поток (операція)-об’єкт».

Принцип дискреційної політики розмежування доступу можна охарактеризувати схемою «кожен-з кожним», іншими словами для будь-якої зі всіляких комбінацій «Користувач (суб’єкт) - ресурс (об’єкт)» має бути явно задано («прописано») дозвіл / заборона доступу і вид відповідної дозволеної /

забороненої операції (Read,Write т.ін.). Таким чином, при дискреційної політики розмежування доступу здійснюється самим детальним чином - до рівня окремо взятого суб’єкта, окремо взятого об’єкта доступу і окремо взятої операції.

Політика мандатної (Повноважного) доступу. Безліч безпечних (дозволених) доступів PL задається неявним чином через введення для користувачів-суб’єктів деякої дискретної характеристики довіри (рівня допуску), а для об’єктів деякої дискретної характеристики конфіденційності (грифа секретності), і наділення на цій основі користувачів-суб’єктів якимись повноваження породжувати певні потоки в залежності від співвідношення «рівень допуску-потік (операція) - рівень конфіденційності ».

Таким чином, на відміну від дискреційної політики, при мандатної політики розмежування доступу проводиться менш детально - до рівня групи користувачів з певним рівнем допуску та групи об’єктів з певним рівнем конфіденційності. Зауважимо також, що зменшення гранулювання доступу створює умови для спрощення і поліпшення управління доступом через істотного зменшення кількості суб’єктів управління і контролю. Політика тематичного доступу. Безліч безпечних доступів задається неявним чином через введення для користувачів-суб’єктів деякої тематичної характеристики – дозволених тематичних інформаційних рубрик, а для об’єктів аналогічної характеристики у вигляді набору тематичних рубрик, інформація за якими міститься в об’єкті, і на ділення на цієї основі суб’єктів-користувачів повноваженнями породжувати певні потоки в залежності від співвідношення «набір тематичних рубрик суб’єкта-набір тематичних рубрик об’єкта ». Як і при мандатному доступі, тематичний принцип визначає доступ суб’єкта до об’єкта неявно, через співвідношення пропонованих спеціальних характеристик суб’єкта і об’єкта і, відповідно, в порівнянні з дискреційним принципом істотно спрощує управління доступом [4].

Політика рольового доступу. Безліч безпечних (Дозволених) доступів задається через введення в системі додаткових абстрактних сутностей - ролей,

виступаючих якимись «типовими» (рольовими) суб'єктами доступу, з якими асоціюються конкретні користувачі (В ролі яких здійснюють доступ), і наділення рольових суб'єктів доступу на основі дискреційного або мандатної принципу правами доступу до об'єктів системи. Рольова політика розмежовує доступ не на рівні користувачів-суб'єктів, а на рівні ролей, які є групами однотипного доступу до об'єктів системи, і на цій основі розвиває ту чи іншу базову політику безпеки(Дискреционную або мандатну). Тому в більшості джерел рольової принцип розмежування доступ не виділяється в окрему політику, а розглядається в якихось доповнень до моделей дискреційного або мандатної доступу. слід також відзначити, що в практиці функціонування захищених комп'ютерних систем широко використовується тимчасові і маршрутні (в розподілених КС) обмеження доступу, що дозволяє, в принципі, говорити про тимчасової і маршрутної політиці безпеки, які, доповнюють відмічені базові політики безпеки.

Кожна політика безпеки вимагає певної інформації для розмежування доступу в конкретній системі, локалізуємої в об'єкті, асоційоване з монітором безпеки. Для моделей дискреційного доступу ця інформація представляє список дозволених трійок «Суб'єкт (користувач) -операція-об'єкт». Для керування доступом в системах з мандатних доступом необхідна інформація за рівнями допуску суб'єктів і грифам конфіденційності об'єктів. У системах рольового доступу крім інформації, яка регламентує доступ ролей до об'єктів (на основі дискреційного або мандатного принципу), необхідна інформація по асоціації користувачів-суб'єктів з ролями. При тематичному доступі необхідна інформація за тематичними рубриками користувачів-суб'єктів і об'єктів. Конкретна модель безпеки деталізує і формалізує (у вигляді аналітичних співвідношень, алгоритмів, і т. д.) загальний принцип розмежування доступу на основі одніє з розглянутих політик, а іноді деякої їх сукупності. У конкретної КС розробники будують і реалізують оригінальні програмно-технічні рішення, втілюють моделі безпеки, в тому числі структуру, функції, програмно технічне втілення монітора безпеки.

Правила розмежування доступу, становлять основу політики безпеки, повинні включати і правила породження (Ініціалізації) користувачами суб'єктів доступу.

У технологічному плані виконання данної вимоги призводить до необхідності розщеплення монітора безпеки на два окремих суб'єкта:

- монітор безпеки об'єктів;
- монітор безпеки суб'єктів.

Вводяться відповідні визначення [4].

Визначення 1. Монітором безпеки об'єктів (МБО) називається суб'єкт, що активізується при виникненні потоку між будь-якими об'єктами, породжується будь-яким суб'єктом, і дозволяє тільки ті потоки, які належать множині.

Визначення 2. Монітором безпеки суб'єктів (МБС) називається суб'єкт, що активізується при будь-якому породженні суб'єктів, і дозволяє породження суб'єктів з фіксованого підмножини пар активізують суб'єктів і об'єктів-джерел.

Визначення 2, по суті, вводить до складу політики безпеки КС в якості додаткової складової частини спеціальну політику породження користувачами суб'єктів доступ. Відповідно, як і у будь-якого суб'єкта, у МБС повинен бути об'єкт-джерело, функціонально асоційований об'єкт (виконуваний код в оперативній пам'яті) і асоційований об'єкт-дані, що містить необхідну інформацію по політиці породження користувачами суб'єктів доступу в системі - рис.3.4. Другим аспектом, поміченим в плані гарантій виконання політики безпеки, є незмінність властивостей суб'єктів доступу в процесі функціонування КС. Багато відомих атаки на захищені КС якраз і здійснюються за сценарієм підміни коду програм, запускаються на виконання регламентованих функцій(Т. Е. Фактично підміни властивостей суб'єктів). Дана вимога має відношення до будь-яким суб'єктам доступу будь-яких користувачів, але особливо для системних суб'єктів, і, в зокрема, для монітора безпеки.

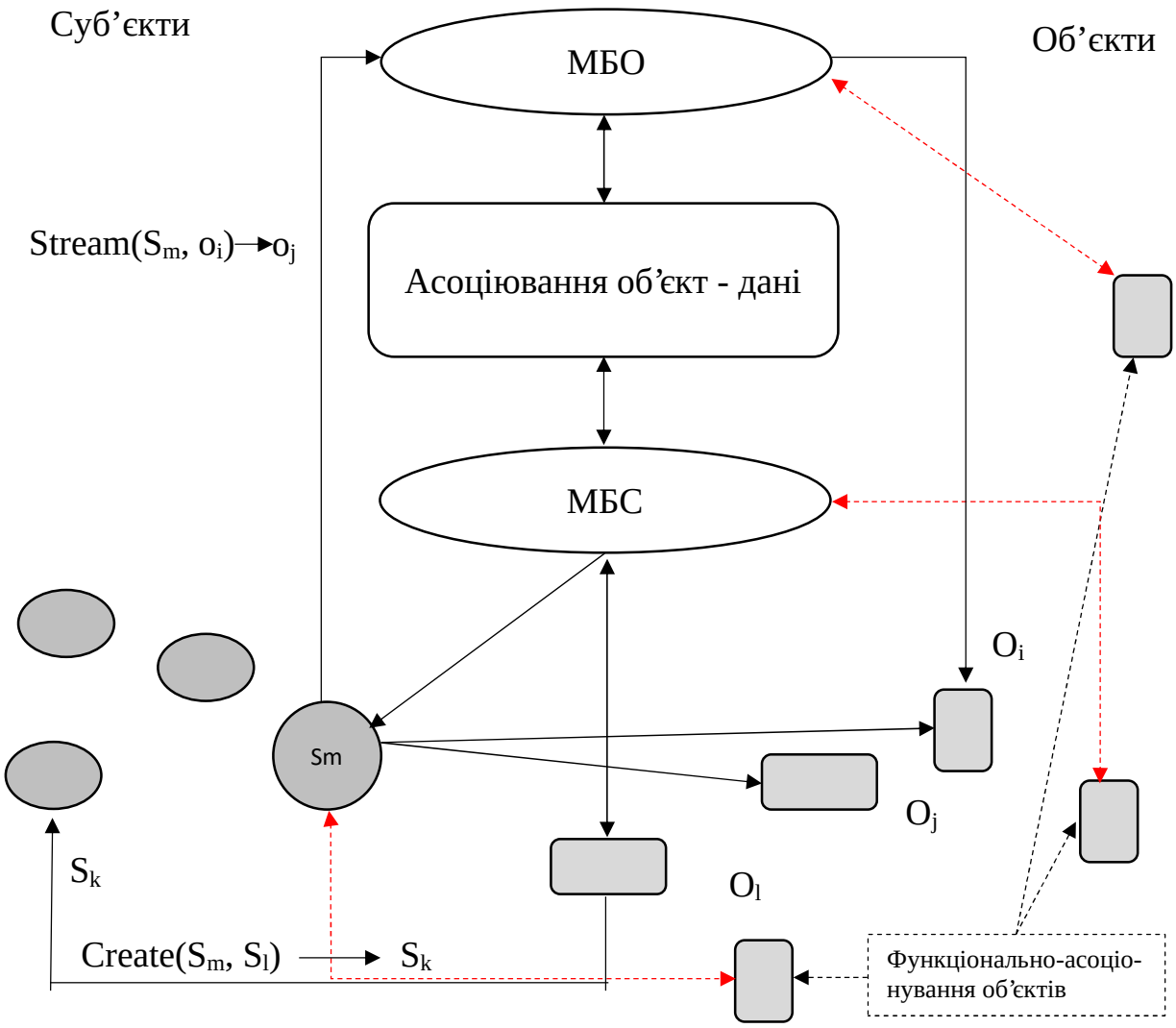

Рисунок. 3.4 – Породження потоків (Stream) і суб'єктів (Create) з урахуванням МБО і МБС

Для розгляду умов незмінності суб'єктів, вводяться такі визначення [4] .

Визначення 3. Об'єкти Oi і Oj тотожні в момент часу t (Oi[t] ≡Oj[t]), якщо вони збігаються як слова, записані в одній мові. Тотожність об'єктів за визначенням 3 ґрунтується не на фізичній тотожності, а на тотожності до рівня послідовності символів з алфавіту мови уявлення. Для ілюстрації поняття тотожності наведемо приклад еквівалентності (Тотожності) двох файлів на основі побайтного порівняння, один з яких розміщений на диску, інший в оперативній пам'яті, і знаходяться, відповідно, в різній реалізації по фізичним процесам функціонування носіїв (т. о. є фізично не тотожними).введене

поняття тотожності об’єктів дозволяє перейти до розгляду поняття тотожності і незмінності суб’єктів доступу.

Визначення 4. суб’єкти Si і Sj тотожні в момент часу t, якщо попарно тотожні все асоційовані з ними об’єкти. Визначення 4 і 5 неявно вимагають наявності в КС спеціального механізму сортування однотипних об’єктів і їх попарного порівняння, і, крім того, обумовлюють наступне важливе слідство.

Слідство 1 (з визначень 3 і 4). Породжені суб’єкти тотожні, якщо тотожні все породжуючи суб’єкти та об’єкти-джерела. Обґрунтованість даного слідства випливає з тотожності функціонально-асоційованих об’єктів в породжуючих суб’єктах, які відповідають за породження нового суб’єкта, а також з тотожності аргументів операції породження, т. е. асоційованих об’єктів-даних і об’єктів-джерел, які визначають властивості породжуваних суб’єктів. Очевидно, що суб’єкти, які здійснюють доступ до об’єктам системи, в тому числі і до об’єктів, асоційованим з іншими суб’єктами, можуть тим самим впливати на них і змінювати їх властивості. Тому вводиться наступне визначення.

Визначення 5. Суб’єкти Si і Sj називаються не впливаючими один на одного (або коректними що до один одного), якщо в будь-який момент часу відсутній потік (Змінює стан об’єкта) між будь-якими об’єктами Oik і Ojl, асоційованими, відповідно з суб’єктами Si і Sj. Причому об’єкти Oik не асоційовані з суб’єктом Sj, а об’єкти Ojl не асоційовані з суб’єктом Si.

Відзначимо, що термін «зміна стану об’єкта» в визначенні 5 трактується як нетотожність (в сенсі визначення 3) об’єкта з самим собою в різні моменти часу. Аналіз поняття асоційованих з суб’єктом об’єктів дозволяє ввести ще жорсткіше визначення щодо впливу одних суб’єктів на інших.

Визначення 6. суб’єкти Si і Sj називаються зовсім не впливаючими один на одного (або абсолютно коректними відносно один одного), якщо в умовах визначення 5 множини асоційованих об’єктів зазначених суб’єктів не мають перетину.

На підставі даного визначення можна, сформулювати достатню умова гарантованого виконання політики безпеки.

Затвердження 1 (достатня умова гарантій безпеки 1). Монітор безпеки об’єктів дозволяє породження потоків тільки з множини PL, якщо все існуючі в системі суб’єкти абсолютно коректні щодо нього і один одного.

Затвердження 1 для забезпечення гарантій безпеки накладає надзвичайно жорсткі умови, практично не здійсненні на практиці, або істотно знижують функціональні можливості КС (відсутність загальних об’єктів-джерел для запуску програм різними користувачами, відсутність загальних ділянок пам’яті, буферів для обміну даними і т. ін.). Для дослідження підходів, в більшій мірі можливих при практичній реалізації, вводяться поняття замкнутості і ізольованості підмножини суб’єктів системи.

Визначення 7. КС називається замкнутої по породженню суб’єктів, якщо в ній діє МБС ,що дозволяє породження тільки фіксованого кінцевої підмножини суб’єктів для будь-яких об’єктів-джерел, розглянутих для фіксованої декомпозиції КС на суб’єкти і об’єкти.

Еквівалентним поняттям для замкнутої по породженню суб’єктів системи є поняття «Ізольованою програмного середовища» (ІПС). Механізм замкнутого програмного середовища скорочує безліч можливих суб’єктів до деякої множини фіксованої потужності, але при цьому не гарантує відсутність некоректних суб’єктів всередині замкнутого середовища.

Визначення 8. Множина суб’єктів КС називається ізольованими (абсолютно ізольованими), якщо в ній діє МБС і суб’єкти з породжуємої множини коректні (абсолютно коректні) відносно один одного і МБС .

З даного визначення випливають такі слідства.

Слідство 1. (З визначення 8).

Будь-яка підмножина суб’єктів ізольованої(абсолютно ізольованої) КС, що включає МБС, також становить ізольовану (абсолютно ізольовану) середу.

Слідство 2. (З визначення 8). Доповнення ізольованого (абсолютно ізольованою) середовища суб’єктом, коректним (абсолютно коректним) щодо

будь-якого з числа вхідних в ізольовану (абсолютно ізольовану)середу, залишає її ізольованою(абсолютно ізольованою) На цій основі можна сформулювати іншу умову достатності гарантій виконання політики безпеки.

Затвердження 2. (Достатня умова гарантій безпеки 2). Якщо в абсолютно ізольованій КС є МБО і породжаємі суб'єкти абсолютно коректні стосовно МБО , а також існує МБС ,який абсолютно коректний щодо МБО , то в КС реалізується тільки доступ, описаний політикою розмежування доступу .

На відміну від першої умови достатності гарантій виконання політики безпеки, друга умова менш жорстка, так як накладає умови абсолютної коректності не на всі множини можливих суб'єктів, а лише на фіксовану їх підмножину, що утворюють замкнуте (ізольоване) програмне середовище (ІПС).

І все ж, вимога абсолютної коректності, хоча і для фіксованої підмножини суб'єктів, є також надзвичайно жорстким і важко здійсненним на практиці без істотного зниження функціональних можливостей КС. Подальший аналіз підходів до гарантій безпеки, точніше, до можливостей реалізації ІПС, показав необхідність включення вимог щодо незмінності властивостей суб'єктів, заснованих на деяких додаткових процедурах, пов'язаних з породженням суб'єктів.

Визначення 9. Операція породження суб'єктів Create (Sk, Om) → Sl називається породженням з контролем незмінності об'єкта, якщо для будь-якого моменту часу t>t0, в який активізована операція породження об'єкта Create , породження об'єкта можливо толькі при тотожності об'єкта-джерела щодо моменту t0, при Om[t] ≡Om[t0].

З визначення 10 випливає наступний важливий наслідок, який має безпосереднє відношення до незмінності властивостей суб'єктів доступу, як найважливішої умови забезпечення політики безпеки в системі.

Слідство 3. (З визначення 9). В умовах визначення 10 породжені суб'єкти Sl[t1] і Sl[t2] тотожні, якщо t1>t0 і t2>t0. При t1 =t2 породжується один і той же об'єкт.

Введення поняття породження суб’єктів з контролем незмінності об’єктів дозволяє сформулювати і довести таку достатню умова для забезпечення ІПС, яке може бути практично реалізовано в реальних КС.

Затвердження 3. (Базова теорема ІПС). Якщо в ізольованій КС, в якій діє породження суб’єктів з контролем незмінності об’єкта, в момент часу t0 через будь-який суб’єкт до будь-якого об’єкту існують тільки потоки, що не суперечать умові коректності (абсолютної коректності), то в будь-який момент часу tk>t0 КС також залишається ізольованою (абсолютно ізольованою).

Затвердження 3 має найважливіше значення з точки зору достатніх умов для забезпечення гарантій виконання політики безпеки в захищених КС. Разом з тим, при практичній реалізації умов затвердження 3 також виникає кілька серйозних проблем. Одна з них, якщо так можна висловитися, співзвучна з відомою проблемою «Ахіллесовою п’яти». А саме, з вихідним станом КС, в якому повинні бути тільки потоки, що гарантують коректність вихідних суб’єктів.

Проблеми та шляхи забезпечення первинної коректності (ізольованості) КС ґрунтуються на певних принципах і процедурах завантаження(ступінчастої ініціалізації) КС в початковий момент часу.

Друга проблема пов’язана з зниженням продуктивності (швидкодії) КС у зв’язку з здійсненням процедур контролю незмінності об’єктів-джерел при породженні суб’єктів.

Від себе також зазначимо, не применшуючи достоїнств і теоретичного значення розглянутої моделі гарантій виконання політики безпеки, що її авторами упущений ще один важливий в практичному плані аспект. Зокрема, як уже зазначалося в слідстві 1 з аксіоми 3, для управління конкретними параметрами системи розмежування доступу можуть (повинні) існувати суб’єкти довірених користувачів (адміністраторів), що мають доступ до асоційованого з МБО об’єкту – даними. Однак розглянуті вище умови гарантій безпеки ґрунтуються на понятті коректності (не впливу) щодо МБО і МБС всіх суб’єктів доступу. Згідно визначенню 6 коректність суб’єктів забезпечується їх

неможливістю змінювати стан всіх асоційованих з іншими суб’єктами об’єктів, в тому числі і об’єктів-даних, асоційованих з МБО , містять конкретну інформацію по політиці розмежування доступу. Отже, повна і сувора реалізація умов ІПС з-за неможливості згодом змінювати асоційовані з МБО об’єкти потребують початкового вбудовування в систему конкретні параметрів розмежування доступу(по конкретним, відповідно, від самого початку зареєстрованим в системі користувачам, і конкретним, спочатку створеним в системі об’єктів доступу), що позбавляє таку систему будь-якої універсальності і гнучкості.

Проте, теоретична значимість розглянутої моделі безсумнівна, так як створює інваріантну основу по відношенню до будь-яких політикам і моделям розмежування доступу для гарантій виконання політики безпеки в захищених КС.

4 РЕАЛІЗАЦІЯ ТА ВИКОРИСТАННЯ СТВОРЕНОЇ МЕТОДИКИ НА ПРАТИЦІ

4.1 Визначення переліку системних функцій операційної системи, що підлягають контролю.

На даному етапі виявляються контрольовані засобами розмежування доступу системні функції.

Загальну схему методики оцінки ступеня впливу засобів розмежування доступу на продуктивність інформаційно-обчислювальної системи з усіма етапами можна побачити на рис. 4.1.

Як правило, в більшості випадків засобами розмежування доступу контролюються системні функції, які виконують наступне [6]:

- всі файлові операції (відкриття файлу, читання з файлу, запис в файл, видалення файлу, переміщення файлу, зміна атрибутів файлу, а також аналогічні операції з каталогами);
- операції з пам’яттю
- операції мережевого обміну;
- операції обміну з зовнішніми пристроями.

Етап 1. Для прикладу, контролю будуть підлягать такі функції:

- CreateFile
- CopyFile
- DeleteFile
- MoveFile
- ReadFile
- WriteFile

4.2 Визначення вагових коефіцієнтів значущості системних функцій.

Як було відзначено, при визначенні вагових коефіцієнтів значимості системних функцій необхідно уникати використання експертних методів оцінювання. У зв’язку з цим пропонується оцінювати значимість системної

функції на основі частоти її виклику при функціонуванні інформаційно-обчислювальної системи. Для цього необхідно відстежувати і підраховувати всі виклики системних функцій при штатному функціонуванні інформаційно-обчислювальної системи за певний проміжок часу.

Рисунок. 4.1 – Загальна схема методики оцінки

Для відстеження викликів системних функцій можливе використання існуючих програмних засобів (зокрема, ProcessMonitor, API-Monitor для

операційних систем сімейства Windowsабо утиліта ptrace (strace) зі складу систем Linux) (рис. 4.2).

Тоді ваговий коефіцієнт значущості і-й системної функції буде визначатися як

$$w_i = \frac{x_i}{X} \qquad (4.1)$$

де хі – кількість викликів і-й системної функції за контрольований проміжок часу ($i = \overline{1; N}$; N -число системних функцій, що підлягають оцінці);

X - загальна кількість всіх системних викликів за керуємий проміжок часу, визначається як

$$X = \sum_{i=1}^{N} x_i. \qquad (4.2)$$

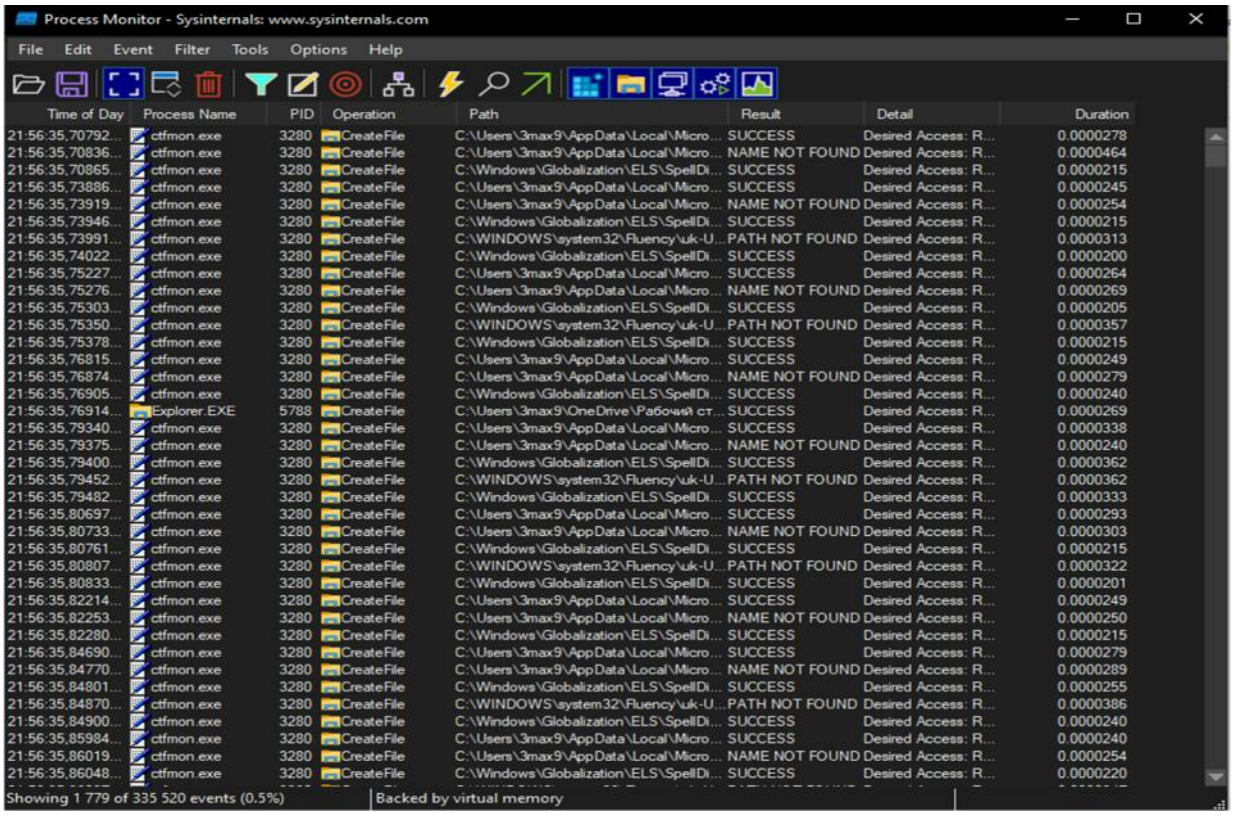

Рисунок. 4.2 – Програма Process Monitor із комплекту утиліт Sysinternals (показано фіксацію числа викликів API-функції CreateFile)

Етап 2. Визначемо кількість викликі функцій визначених на Етапі 1 (CreateFile, CopyFile, DeleteFile, MoveFile, ReadFile, WriteFile) та загальну кількість викликів всі фукцій що підлягають контролю за контрольний проміжок часу — 7 хвилин (x_i, X), за допомогою програма Process Monitor із комплекту утиліт Sysinternals після чого буде необхідно визначині коефіцієнти значущості для кожної функції (w_i):

x_{Create}=452 викликів, $X = \sum_{i=1}^{N} x_i = 2215$ викликів;

x_{Copy}=84 викликів, $X = \sum_{i=1}^{N} x_i = 2210$ викликів;

x_{Delete}=84 викликів, $X = \sum_{i=1}^{N} x_i = 2181$ виклик;

x_{Move}=19 викликів, $X = \sum_{i=1}^{N} x_i = 2111$ викликів;

x_{Read}=895 викликів, $X = \sum_{i=1}^{N} x_i = 2209$ викликів;

x_{Write}=734 викликів, $X = \sum_{i=1}^{N} x_i = 2210$ виклик.

Далі необхідно визначити коефіцієнти значущості для кожної функції:

$$w_{i} = \frac{x_i}{X} = \frac{4}{2} = 0.204;$$

$$w_{i} = \frac{x_i}{X} = \frac{8}{2} = 0.038;$$

$$w_{i} = \frac{x_i}{X} = \frac{2}{2} = 0.011;$$

$$w_{i} = \frac{x_i}{X} = \frac{1}{2} = 0.009;$$

$$w_{i} = \frac{x_i}{X} = \frac{8}{2} = 0.405;$$

$$w_{i} = \frac{x_i}{X} = \frac{7}{2} = 0.332.$$

Загальні результати наведені у таблиці 4.1.

Таблиця 4.1 – Результати оцінки вагових коефіцієнтів значимості системних функцій

Назва API-функцій	Кількість викликів API-функцій	Загальна кількість викликів всі фукцій що підлягають контролю	Вагових коефіцієнт значості
CreateFile	452	2215	0.204
CopyFile	84	2210	0.038
DeleteFile	24	2181	0.011
MoveFile	19	2111	0.009
ReadFile	895	2209	0.405
WriteFile	734	2210	0.332

4.3 Визначення коефіцієнтів уповільнення виконання системних функцій операційної системи, що підлягають оцінці.

Даний коефіцієнт розраховується як відношення середнього часу виконання оцінюваної системної функції без контролю засобами розмежування доступу до середнього часу виконання оцінюваної системної функції під контролем засобів розмежування доступу:$k_i = \frac{\overline{t_i^*}}{\overline{t_i}}$, де $\overline{t_i}$- середній час виконання і-ї системної функції без контролю її засобами розмежування доступу; $\overline{t_i^*}$-середній час виконання і -ї системної функції під контролем її засобами розмежування доступу. Для оцінки середнього часу виконання системної функції можливі два способи:

- фіксувати час виконання кожного виклику системної функції і визначати середній час виконання наступним чином: $\bar{t} = \frac{\sum_{k=1}^{N} t_k}{n}$, де n - число викликів загальної функції; t_k - час виконання функції в ході k-го виклику[6];

- справити потрібне кількість викликів загальної функції, зафіксувати загальний час виконання всіх викликів функції, після чого середній час визначити наступним чином: $\bar{t} = \frac{T}{n}$, де n - число викликів системної функції; T

– загальний час виконання всіх викликів системної функції[6].

Для оцінки часу виконання була розроблена програма оцінки часу виконання API-функцій (Рис. 4.3). Для фіксації часу виконання API-функцій використовується підрахунок тактів процесора за допомогою API-функцій Windows QueryPerformanceCounter і QueryPerformanceFrequency. Перша API-функція повертає кількість імпульсів лічильника, друга повертає поточну частоту роботи лічильника (число імпульсів за одну секунду). Розділивши значення, отримане з за допомогою функції QueryPerformanceCounter, на значення, отримане за допомогою функції і QueryPerformanceFrequency, отримаємо час роботи обчислювальної системи з моменту початку роботи до моменту виклику функції QueryPerformanceCounter. Таким чином, різниця виміряних значень часу я покаже шуканий час виконання цієї API-функції.

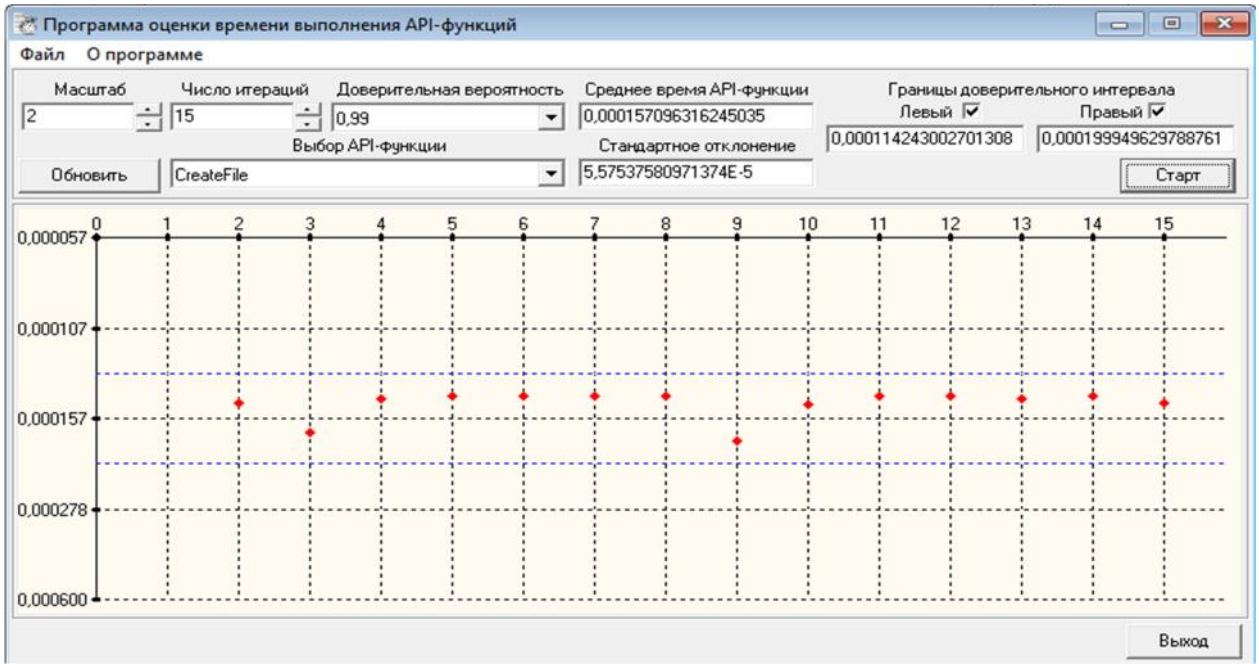

Рисунок. 4.3 – Програма оцінки часу виконання с API-функцій (показана оцінка часу виконання API-функції CreateFile)

Загальний алгоритм роботи програми наведено у Додатку А. У програмі організується цикл необхідного числа повторень виклику оцінюваної API-функції із виміром час виконання кожної ітерації та наступним розрахунком

середнього часу виконання обраної функції за формулою $\bar{t} = \frac{\sum_{k=1}^{N} t_k}{n}$. Також у програмі реалізовано оцінку довірчого інтервалу середнього значення часу виконання API-функції та графічне подання результатів вимірів тимчасових проміжків. Програма розроблена в середовищі Delphi 7.

Етап 3. Для вибраних API-функцій були зроблено оцінки часу виконання функцій без контролю їх засобами розмежування доступу та під контролем засобів розмежування доступу – по 30 викликів кожної функції з фіксаціїцією часу виконання кожного виклику. Засобом розмежування доступу виступав програмний комплекс захисту інформації Secret Net з налаштованим політиками мандатного доступу до об’єктам файлової системи.

Результати вимірювань середнього часу виконання системних функцій, а також розраховані коефіцієнти уповільнень роботи системних функцій наведено у таблиці 4.2.

Таблиця 4.2 – Результати вимірів часу роботи API-функцій

Назва API-функцій	Час роботи функції без контролю t_i (сек.)	Час роботи функції під контролем t_i^* (сек.)
Createfile	0,000816	0,001225
Copyfile	0,002614	0,003219
Deletefile	0,000429	0,000952
Movefile	0,000440	0,000973
Readfile	0,000082	0,000145
Writefile	0,000207	0,000371

Етап 4. За допомогою отриманих результатів необхідно визначити коефіцієнти уповільнення за допомогою формули:

$$k_i = \frac{\bar{t}_i^*}{\bar{t}_i} \qquad (4.3)$$

де $\overline{t_i}$ – середній час виконання і-ї системної функції без контролю її засобами розмежування доступу;

$\overline{t_i^*}$ – середній час виконання і-ї системної функції під контролем її засобами розмежування доступу:

$$k_C = \frac{\overline{t_i^*}}{\overline{t_i}} = \frac{0.001225}{0.000816} = 1.502 \qquad k_M = \frac{\overline{t_i^*}}{\overline{t_i}} = \frac{0.000973}{0.000440} = 2.211$$

$$k_C = \frac{\overline{t_i^*}}{\overline{t_i}} = \frac{0.0}{0.0} = 1.231 \qquad k_R = \frac{\overline{t_i^*}}{\overline{t_i}} = \frac{0.0}{0.0} = 1.768$$

$$k_D = \frac{\overline{t_i^*}}{\overline{t_i}} = \frac{0.000952}{0.000429} = 2.219 \qquad k_W = \frac{\overline{t_i^*}}{\overline{t_i}} = \frac{0.0}{0.0} = 1.792$$

Загальні результати етапу 3 та 4 наведені у таблиці 4.3

Таблиця 4.3 – Результати вимірів часу роботи API-функцій та оцінки коефіцієнта уповільненняроботи функцій

Назва API-функцій	Час роботи функції без контролю t_i (сек.)	Час роботи функції під контролем t_i^* (сек.)	Коефіцієнт уповільнення роботи функцій k_i
Createfile	0,000816	0,001225	1,502
Copyfile	0,002614	0,003219	1,231
Deletefile	0,000429	0,000952	2,219
Movefile	0,000440	0,000973	2,211
Readfile	0,000082	0,000145	1,768
Writefile	0,000207	0,000371	1,792

4.4 Визначення певного інтегрального показника зниження продуктивності системи внаслідок впливу засобів розмежування доступу.

Даний показник визначається як адитивна згортка коефіцієнтів уповільнення роботи кожної системної функції з урахуванням вагового коефіцієнта значущості цієї функції: $K = \sum_{i=1}^{N} k_i w_i$.

Етап 5. З урахуванням даних, отриманих на етапах 2 та 3 та 4, загальний коефіцієнт уповільнення роботи системи при введенні до її складу засобів розмежування доступу:

$$K = \sum_{i=1}^{6} k_i w_i = 1.502 * 0.204 + 1.231 * 0.038 + 2.219 * 0.011 + 2.211 * 0.009 + 1.768 * 0.405 + 1.792 * 0.332 = 1.707$$

Таким чином, запропонована методика та її програмна реалізація дозволяють оцінити вплив системи розмежування доступу до об’єктів доступу на продуктивність інформаційно-обчислювальної системи, при цьому при оцінці вагових коефіцієнтів значимості приватних показників використовувати розрахунковий метод без використання експертних оцінок.

ВИСНОВОК

В процесі написання дипломної роботи на тему: «Оцінка впливу вбудованих механізмів безпеки на продуктивність системи».Були підняті та проаналізовані такі питання:

- аналіз проблем проектування безпечних систем;
- моделі монітора безпеки;
- оцінка впливу на ситему монітора безпеки.

Результатом роботи є створена методика оцінки впливу системи розмежування доступу на продуктивність системи та програмний застосунок, для розрахування часу виконання API-функцій, що використовується у методиці.

В результаті використання методики були отримані результати вимірювань, які були занесені в таблиці 4.1, 4.2 та 4.3 і був розрахований загальний коефіцієнт уповільнення роботи системи K = 1.707.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпаю. - Київ.: ДУТ, 2015. - 288 с.

2. Галатенко, В. А. Основы информационной безопасности/ В.А. Галатенко. – М.: Изд-во "Интернет-университет информационных технологий – ИНТУИТ.ру", 2003. –280 с.: ил.

3. Дроботун Є.Б., Козлов Д.В. Оцінка ступеня впливу антивірусних засобів на якість функціонування інформаційно-обчислювальних систем / Дроботун Є.Б., Козлов Д.В. // Програмні продукти та системи. – 2016. – № 4. – С. 129-134.

4. Дроботун, Є.Б Оцінка ступеня впливу засобів розмежування доступу на продуктивність інформаційно-обчислювальної системи / Дроботун Є.Б // Програмні продукти та системи – 2018. – № 1. – С 128-132.

5. Куліков, С. С. Моделі безпеки комп'ютерних систем / С. С. Куликов. - Воронеж: ФДБОУ ВПО "Воронезький державний технічний університет", 2015. – 179 с.

6. Лобода, М.В. Розмежування доступу та оцінка його впливу на продуктивність систем / М.В.Лобода, проф. Горбачов В.О. // Міжнародна НТК "Проблеми інформатизації" , 19 листопада 2021. – Т. 3. – Харків – с. 98-99

7. Семенов, С.Г. Захист інформації в комп'ютерних системах та мережах. / С.Г.Семенов, А.О.Подорожняк, О.І.Баленко, С.Ю.Гавриленко – Харків.: НТУ «ХПІ», 2014.– 251 с.

8. Стельмашонок О.В, Захист інформації у комп'ютерних системах / О.В. Стельмашонок, канд. фіз.-мат. наук І.М. Васильєва. – СПб. : Вид-во СПб ГЕУ, 2017. – 163 с.

9. Шаньгін В. Ф, Інформаційна безпека комп'ютерних систем та мереж / Шаньгін В. Ф. – М.: ВД «ФОРУМ»: ІНФРА-М, 2011. – 416 с.