Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
завідуюча кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
«14» червня 2022р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

дипломної роботи
бакалавра
(назва освітнього ступеня)

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітня програма Кібербезпека
(назва освітньої програми)

на тему: «Модель дискреційного керування доступом користувачів в інформаційних системах»

Виконавець: студентка IV курсу, групи КБ-41

_____ **Ілона КОБЗОВА**
(підпис) (ім'я прізвище)

	Прізвище, ініціали	**Підпис**
Керівник	Лариса МИРУТЕНКО	

Нормоконтроль	Олександр ТОРОШАНКО	

Київ 2022

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідуюча кафедри кібербезпеки
та захисту інформації
_____ Наталія ЛУКОВА-ЧУЙКО
«01» листопада 2021 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студентці **КБ-41** **Ілони Валентинівни Кобзової**
(група) (прізвище ім'я по батькові)

Тема дипломної роботи Модель дискреційного керування доступом користувачів в інформаційних системах

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №5 від 29.10.2021 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Будова та різновиди систем контролю доступу, засоби впровадження та функціонування систем контролю доступу, модель дискреційного керування

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно ознайомитися з розмежуванням доступу користувачів як одним із засобів захисту, будовою та елементами систем розмежування доступу, проаналізувати існуючі системи керування доступом, визначити переваги та недоліки дискреційного керування доступом, побудувати інформаційну систему з елементами дискреційного розмежування доступу.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розроблена ІС з елементами дискреційного керування доступом, наведені рекомендації її доповнення іншими засобами захисту для використання в роботі підприємств малого та середньо бізнесу.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання:29 жовтня 2021 року

Завдання видав _____ (підпис) Лариса МИРУТЕНКО (ім'я, прізвище)

Завдання прийняла до виконання _____ (підпис) Ілона КОБЗОВА (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	29.10.2021 – 30.01.2022	*виконано*
2	Аналіз літературних джерел	31.01.2022 – 14.02.2022	*виконано*
3	Загальний опис використання існуючих систем контролю доступу	15.02.2022 – 14.03.2022	*виконано*
4	Дослідження дискреційної моделі	15.03.2022 – 15.04.2022	*виконано*
5	Програмна реалізація спрощеної моделі дискреційного керування доступом	15.04.2022 – 15.05.2022	*виконано*
6	Формування рекомендацій щодо поєднання дискреційного керування доступом з іншими засобами захисту	16.05.2022 – 04.06.2022	*виконано*
7	Оформлення пояснювальної записки	05.06.2022 – 06.06.2022	*виконано*
8	Підготовка до захисту	07.06.2022 – 13.06.2022	*виконано*

Завдання видав _____ (підпис) Лариса МИРУТЕНКО (ініціали, прізвище)

Завдання прийняв до виконання _____ (підпис) Ілона КОБЗОВА (ініціали, прізвище)

Термін подання дипломної роботи до ЕК 06 червня 2022 року

РЕФЕРАТ

Пояснювальна записка дипломної роботи складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел та додатків. Основний текст займає 66 сторінок, включає в себе зміст, вступ, три розділи дипломної роботи, висновки, список джерел та 1 додаток із загальною кількістю сторінок 8. У пояснювальній записці дипломної роботи міститься 18 рисунків. Список використаних джерел містить 46 найменувань і займає 5 сторінок.

Об'єктом дослідження є процес розмежування прав доступу користувачів на основі дискреційної моделі.

Мета роботи: розробка інформаційної системи з елементами дискреційного керування доступом, надання рекомендацій щодо її використання спільно з іншими засобами захисту.

Предметом дослідження є дискреційний метод керування доступом користувачів в інформаційних системах.

Методи дослідження:

- аналіз інформаційних ресурсів;
- порівняння існуючих моделей керування доступом;
- моделювання інформаційної системи;
- системний підхід.

В роботі проведено аналіз існуючих систем керування доступом користувачів в інформаційних системах та необхідність їх використання, детальніше розглянуто вибіркове керування доступом, яке вважається найбільш поширеним. Запропоновано використання таких систем для малих та середніх організацій, наведено основні кроки з підготовки до впровадження керування доступом.

Побудовано модель інформаційної системи, яка працює на принципами дискретного розмежування доступу. Вона може використовуватися для наочної демонстрації основ вибіркового керування доступом.

Додатково розроблено рекомендації щодо удосконалення надійності систем, що використовують дискреційне розмежування доступ, іншими засобами захисту інформації, які за необхідності можна застосувати при роботі з конфіденційними даними.

Результати здійснених у дипломній роботі досліджень можуть бути використані в роботі малих та середніх організацій, що планують використання або вже використовують системи дискреційного керування доступом.

Подальші дослідження будуть спрямовані на детальніше вивчення мандатних систем керування доступом, поєднання їх з дискретними системами та програмна реалізація таких засобів захисту.

Ключові слова: система контролю доступу, дискреційна модель, суб’єкти та об’єкти доступу, інформаційна система, розподіл прав та повноважень.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ІС	-	інформаційна система
ACS	-	Access Control System
IT	-	інформаційні технології
VLAN	-	Virtual Local Area Network
VPN	-	Virtual Private Network
DAC	-	Discretionary Access Control
MAC	-	Mandatory Access Control
RBAC	-	Role-Based Access Control
ACL	-	Access Control List
НСД	-	несанкціонований доступ

ЗМІСТ

ВСТУП

Актуальність обраного дослідження полягає в тому, що на сьогоднішній день в Україні та в усьому світі управління доступом користувачів є важливою складовою загальної політики чи програми безпеки інформаційної системи чи організації, яка використовується для запобігання та/або зменшення ймовірності впливу злочинної поведінки й, загалом, порушення політики безпеки організації. В ідеально безпечному середовищі доступ не може отримати жоден користувач, який не є абсолютно відомим системі, персоніфікованим і несе хоча б якусь загрозу безпеці усієї системи чи організації. На практиці, на жаль, дане твердження можна вважати утопічним, адже, за рахунок людського фактору, навіть найбезпечніший, на перший погляд, користувач може стати причиною реалізації загрози безпеці. Тому переважна більшість організацій чи установ потребує використання жорстких правил контролю за доступом користувачів системи, її співробітників для захисту особистих матеріальних та нематеріальних ресурсів.

Охоронна система традиційно є найбільш поширеним і доступним засобом контролю доступу. Однак з розвитком технологій було доведено, що вона значно менш досконала, ніж розроблені автоматизовані системи контролю доступу, а також неможлива при використанні виключно віртуальної організації роботи певної системи, де доступ до ресурсів проводиться виключно через глобальну мережу.

Внаслідок цього, постає необхідність повного розуміння, при яких розмірах системи вже необхідно використовувати системи контролю доступу, як працюють такі системи, яку модель доречно обрати для конкретної інформаційної системи, чи виправдовує інтеграція такої системи витрачені кошти, чи вписується система керування доступом у загальну політику роботи організації.

Таким чином стає більш зрозумілою необхідність використання систем контролю доступу, адже вони суттєво захищають інформаційну систему, але обов’язкових вимог стосовно їх впровадження на законодавчому рівні не визначено.

Відповідно відповідальність за використання або невикористання такого режиму в роботі інформаційної системи повністю покладається на власника системи.

При впровадженні систем керування доступом варто повністю вивчити принципи роботи та функціонування системи контролю доступу, щоб не створювати невидимі чи непрораховані вразливості в програмі безпеки, ефективно підібрати вдалу систему керування для власних потреб та забезпечити її якісне функціонування та підтримку.

Метою роботи є розробка інформаційної системи з елементами дискреційного керування доступом, надання рекомендацій щодо її використання спільно з іншими засобами захисту.

Для досягнення поставленої мети необхідно виконати наступні завдання:

1. проаналізувати існуючі системи розмежування доступу;
2. проаналізувати та детально вивчити принципи роботи, побудови та механізми дискреційної моделі контролю доступу;
3. розробити поради щодо визначення критеріїв, за якими в інформаційній системі доречно використовувати дискреційну модель;
4. розробити та реалізувати спрощений програмний застосунок для демонстрації принципів роботи дискретного контролю доступу;
5. створити рекомендації стосовно поєднання дискреційної системи керування доступом з іншими існуючими засобами захисту інформаційних систем.

Об’єктом дослідження є процес розмежування прав доступу користувачів на основі дискреційної моделі.

Предмет дослідження – дискреційний метод керування доступом користувачів в інформаційних системах.

Процес проведення дослідження буде проводитися поетапно. На першому кроці роботи буде виконаний аналіз предметної області використання систем контролю доступу, за допомогою методів порівняння проведений детальніший огляд дискреційної моделі керування. На другому етапі роботи шляхом моделювання буде створений проєкт інформаційної системи, що реалізуватиме

розглянуту технологію, а на базі системного підходу – запропоновані рекомендації щодо захисту такої інформаційної системи.

Отримані результати можна використовувати для ознайомлення невеликих та середніх організацій з системами контрою доступу, в загальному, дискреційною моделлю, зокрема, аргументування до використання розподілу прав доступу та керування ними. Можна проводити презентацію з короткими поясненнями підготовки до впровадження дискреційної моделі керування доступом, демонстрації основ роботи інформаційних систем на базі дискреційного керування та викладення можливостей з доповнення такої системи іншими потенційними функціями та заходами з інформаційного та кіберзахисту.

РОЗДІЛ 1
РОЗМЕЖУВАННЯ ДОСТУПУ. ДИСКРЕЦІЙНА МОДЕЛЬ

1.1 Розмежування доступу користувачів як один із засобів захисту в ІС

Системи розмежування доступу – такі електронні системи, що контролюють процедуру входу користувачів інформаційної або іншої корпоративної системи без додаткової безпосередньої перевірки співробітником служби безпеки для підтвердження авторизації особи, яка ініціює процедуру входу, використовуючи, в більшості випадків, особисті облікові чи персональні дані.

Системи контролю доступу (Access Control Systems) часто працюють відповідно до правил та порядку, визначених адміністратором такої системи, які керують доступом користувачів до захищених інформаційних і/або мережевих ресурсів. Зазвичай, такі правила доступу вимагають аутентифікації користувача, зокрема маркерів або біометричних даних для підтвердження особи. Також може бути передбачено обмеження доступу авторизованих користувачів до різних мережевих послуг залежно від часу доби, днів тижня тощо [1].

Система контролю доступу використовує для перевірки облікові дані, щоб надати користувачу дозвіл, що запитується. Облікові дані можуть бути, як правило, персональним ідентифікаційним номером, у вигляді інформації для введення в систему при вході або у вигляді фізичного носія (картка або жетон), або представлені біометричними даними (відбиток пальця або райдужна оболонка). Дані, визначені у системі, вводяться при спробі входу, відображаються або скануються, і після встановленого рівня перевірки доступ надається або навпаки. Найбільш безпечні системи контролю доступу на даний момент використовують саме процес біометричної аутентифікації. Вона може використовуватися як єдиний засіб перевірки, але часто використовується разом із додатковим фактором [2, 3].

Системи контролю доступу працюють як автоматизований метод, який, в загальному випадку, дозволяє особам, що мають відповідний дозвіл, входити до

периметру контрольованих, обмежених та захищених зон об’єкта з мінімальною перевіркою на порталі контролю доступу. Під порталами контролю доступу маються на увазі будь-які дверні прорізи через периметр безпеки, у яких дозволяється прохід осіб, спираючись на їхній статус співробітника, підрядника або відвідувача, який пройшов попередню перевірку, або ж у випадку використання розподілених інформаційних систем, вікна авторизації користувачів для віддаленого доступу до самої системи.

Необхідно враховувати важливість систем контролю доступу, адже вони одночасно відкривають нові вразливості загальної системи безпеки. Тому при впровадженні ACS потрібно розуміти усі ризики, відповідально підходити до управління ризиками та пропрацювати типи контрзаходів. Також варто повністю вивчити принципи роботи та функціонування системи контролю доступу, щоб не створювати невидимі чи непрораховані вразливості в програмі безпеки [1, 4].

1.2 Загальна будова та елементи системи керування доступом

Системи контролю доступу в мережах TCP/IP в загальному випадку включають чотири основні логічні елементи [5]:

- основна мережа (the core network);
- серверна мережа (the server network);
- мережа робочих станцій (the workstation network);
- мережа панелі управління доступом (the access control panel network).

Більш складні системні інтеграції можуть включати [5, 6]:

- інтегровані інтерфейси системи безпеки (Integrated security system interfaces);
- багатосайтові мережеві інтерфейси (multisite network interfaces);
- інтеграція в мережу IT бізнесу (integration to the business IT network);
- мережі VLAN.

Основна мережа (the core network), зазвичай, містить від одного і більше цифрових мережевих комутаторів для функціонування системи сигналізації або

контролю доступу. Якщо мережа включає один цифровий комутатор, тоді він використовується для підключення як основного, так і резервного хост-серверів, а також будь-яких робочих станцій (у випадку, коли немає інших пристроїв TCP/IP, таких як панелі керування доступом). Якщо ж мережа містить кілька цифрових комутаторів, як правило вони виконують наступні функції:

- основний комутатор для серверів і робочих станцій;
- розподільні комутатори (для розподілу підключень);
- граничні комутатори для панелей контролю доступом.

Основна мережа повинна включати хоча б один високоякісний цифровий комутатор для надійного функціонування системи. Він повинен підтримувати технології VLAN, VPN, а також протоколи одноадресної та багатоадресної передачі даних тощо. Варто також передбачити резервні джерела живлення на комутаторах. Високоякісні комутатори є більш дорогими, однак суттєво підвищують надійність, менш схильні до впливу навколишнього середовища (наприклад, температура повітря та вологість) і в подальшому зможуть продовжити працювати у випадку, коли система контролю доступу стане частиною більшої інтегрованої системи безпеки [6].

Комутатори для серверів і робочих станцій можуть бути представлені комутаторами 3-ого рівня, а комутатори розподілу підключень можуть бути як 2-ого, так і 3-ого рівня, залежно від потреб системи. Для якісної роботи початкова потужність комутатора повинна бути приблизно в 3–4 рази більшою за пропускну здатність початкового навантаження пристрою. Якщо ж збільшити потужність комутатора в 10 разів від початкового навантаження, можна забезпечити масштабованість системи з часом.

Сервери є ядром мережі. Обов’язково потрібно передбачити у системі як основний, так і резервний сервери, працюють вони разом, взаємодіючи через основний комутатор.

Робочі станції, у свою чергу, підключаються до серверів у вигляді послідовного зв’язку (RS-232 або USB), а також рекомендується використовувати підключення на основі TCP/IP. Вони теж будуть взаємодіяти з серверами через

основний комутатор. Розглядаючи базову будову системи керування доступом, в спрощеному випадку система знаходиться в одному приміщенні, тому панелі контролю доступу можуть підключатися до мережі через кінцеві комутатори.

Прості системи сигналізації та контролю доступу часто передають відносно мало даних у порівнянні з цифровими відеосистемами, тому доцільніше застосовувати системи сигналізації з вбудованими функціями відеонагляду, що можуть надсилати відео спільно з інформацією про тривогу). Коли проводиться підключення системи сигналізації або контролю доступу до інших систем безпеки, рекомендується зробити це за допомогою Ethernet-з’єднань (за винятком з'єднань між системами, що використовують інтерфейси сухих контактів, наприклад, інтерфейси сигналізації або керування дверима між системами).

У разі підключення декількох систем до однієї загальної мережі, краще виконувати це, розміщуючи кожну систему у окремій VLAN. Вони забезпечують ізоляцію зв’язку між окремими підсистемами чи приміщеннями, таким чином покращують якість зв’язку у випадку використання однієї фізичної мережі кількома системами одночасно. Однак потрібно зазначити, що для мереж VLAN необхідно, щоб основний комутатор був саме маршрутизатором, а розподільні і граничні комутатори повинні мати можливість приймати програмування VLAN [5].

Важливе розміщення системи безпеки за фаєрволом (апаратним), щоб захистити як систему управління доступом, так і бізнес-IT-систему, а також ізолювати їх одна від одної, щоб забезпечити стійкість та надійність цих систем. Для підвищення захисту можна здійснювати маршрутизацію системи безпеки через VPN, яка, в свою чергу, вплине на повну ізоляцію та шифрування даних системи безпеки від бізнес-мережі IT і, що не менш важливо, може бути альтернативним рішенням для об’єднання багатьох систем в єдину, якщо VLAN не сумісні з протоколом чи мережевою адресою.

1.3 Об’єкти та суб’єкти систем розмежування доступу в ІС

Об’єкти та суб’єкти в інформаційних системах часто можна узагальнити, хоча залежно від окремих випадків вони є конкретними. Ми, зокрема, розглядаємо узагальнену модель дискреційного керування доступом, тому можемо пояснити, що саме розуміється під поняттям «об’єкти та суб’єкти системи розподілу доступу», описати ті з них, які зустрічаються практично у кожній інформаційній системі.

Суб’єкт інформаційного доступу – це певна абстрактна сутність, що взаємодіє з системою і при цьому має або ж не має права доступу до інформації та ресурсів в конкретній інформаційній системі, має або ж не має права додатково створювати користувачів системи, надавати чи забирати доступ у тих чи інших користувачів, передавати свої права іншим користувачам [7].

Основними суб’єктами будь-якої інформаційної системи є:

- користувачі системи;
- адміністратори системи;
- власники інформації в системі;
- власники самої системи.

Часто два останніх суб’єкта поєднує в собі одна людина. Кожен з перерахованих суб’єктів можна зафіксувати у таблиці доступу у вигляді користувача системи з деякими доступними йому повноваженнями.

Поняття об’єкту в порівнянні з суб’єктом є більш невизначеним і нечітко окресленим. Однак в будь-якій інформаційній системі ключовим об’єктом виступає інформація. У формі об’єкту доступу також можуть виступати структури для зберігання даних (наприклад, можна окреслити доступ адміністратора системи до бази даних, таким чином в цій ситуації суб’єктом доступу буде адміністратор, а об’єктом – база даних). При використанні CRM-систем для підтримування бізнес-процесів організації також окреслюються різні повноваження для окремих співробітників, тобто об’єктами доступу в такому випадку можна назвати різноманітні модулі зазначеної системи.

Розмежування доступу в інформаційних системах описує правильне керування доступом та санкціоновані взаємодії об’єктів та суб’єктів доступу. Коректна взаємодія повинна описуватися наступними кроками [8, 9]:

1) правильна передача прав взаємодії об’єкта та суб’єкта в інформаційній системі;

2) використання та надання правильних грифів секретності для об’єктів в інформаційній системі;

3) використання та надання правильних грифів секретності для суб’єктів в інформаційній системі;

4) правильна передача активів інформаційної системи від одного суб’єкта до іншого;

5) чітка процедура організації процесу передачі прав та активів одного суб’єкта іншому;

6) створення та описання чіткого процесу надання доступу та передачі прав суб’єктам інформаційної системи.

Для створення простого механізму комунікації та організації описаних вище кроків, доречно розробити механізми на рівні окремої системи керування доступом для подальшого її інтегрування та використання у великих організаціях, а також створити чіткі і зрозумілі підходи до використання та розподілу ресурсів інформаційної системи, в яку буде проходити інтеграція ACS.

1.4 Існуючі моделі керування доступом

Не всі системи контролю доступу працюють за однаковими правилами та принципами. Існує чотири типи контролю доступу, три найбільш поширені з яких наведені на рисунку 1.1. Вони використовуються для керування доступом та фіксації дії користувачів усередині системи чи підприємства [5].

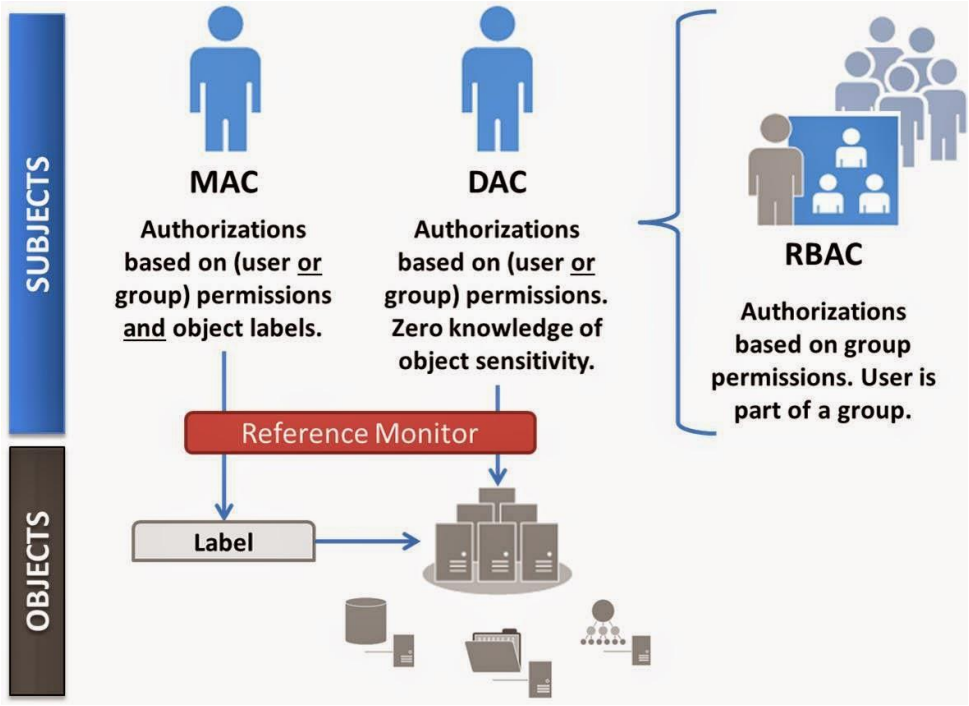

Рисунок 1.1 – Основні відмінності між поширеними моделями розмежування доступу

У кожного виду є свої плюси і мінуси, тому важливо продумати та проаналізувати власні потреби захисту та безпеки і обрати тип контролю доступу, який буде задовільняти їх найкраще.

1.4.1 Дискреційний контроль доступу

Використовуючи дискреційну систему контролю доступу (DAC) власник системи чи організації може вирішити, скільки людей мають доступ до конкретних ресурсів. Кожна точка контролю доступу, тобто кожен об’єкт, містить список авторизованих та допущених користувачів. Щоразу, коли, наприклад, вводиться PIN-код, сканується картка-ключ або відбиток пальця, система перевіряє облікові дані за раніше створеним списком і надає або забороняє доступ до об’єкту на основі раніше встановлених дозволів [10, 11].

Системи DAC вважаються найбільш гнучкими, легкими в експлуатації і пропонують фіксування найбільшої кількості дозволів у порівнянні з іншими видами контролю доступу. Дискреційні системи контролю доступу найкраще

підходять для компаній, які очікують максимальної простоти використання та гнучкості [11-13].

Детальніше про цю модель буде розглянуто в пункті 1.5.

1.4.2 Мандатний контроль доступу

Системи мандатного контролю доступу (MAC) вважаються найбільш безпечним типом контролю доступу. Усі параметри контролю доступу повинні бути заздалегідь налаштовані системним адміністратором або адміністратором з безпеки і не можуть бути модифіковані чи видалені без його попереднього дозволу.

Замість створення списку доступу для кожного окремого об’єкту чи точки входу, як запропоновано у системі DAC, MAC попередньо класифікує всіх користувачів і надає їм доступ до певних областей системи на основі програмування цієї ж системи. Наприклад, якщо організація нараховує 150 співробітників, в такому випадку знадобиться налаштувати в системі 150 різних дозволів користувачів [10, 12].

MAC використовує мітки безпеки для ідентифікації ресурсних об’єктів у системі. Існує два типи міток безпеки: класифікація (висока, середня, низька) та категорія (конкретний відділ або проект). Кожному обліковому запису користувача, в свою чергу, також призначаються мітки щодо класифікації та категорії. Відповідно користувач отримує доступ до об’єкта лише у випадку, якщо обидві мітки збігаються (рис. 1.2). Якщо ж користувач, наприклад, має високу класифікацію, але не входить до категорії об’єкта, то користувач не зможе отримати доступ до об’єкта [8].

Системи мандатного контролю доступу є найсуворішим і найбезпечнішим типом контролю доступу. Однак основним недоліком такого підходу є відсутність гнучкості. Щоб змінити, додати нові чи видалити попередні дозволи, адміністратор повинен повністю перепрограмувати доступ конкретного користувача, а не лише списки безпеки в точці входу.

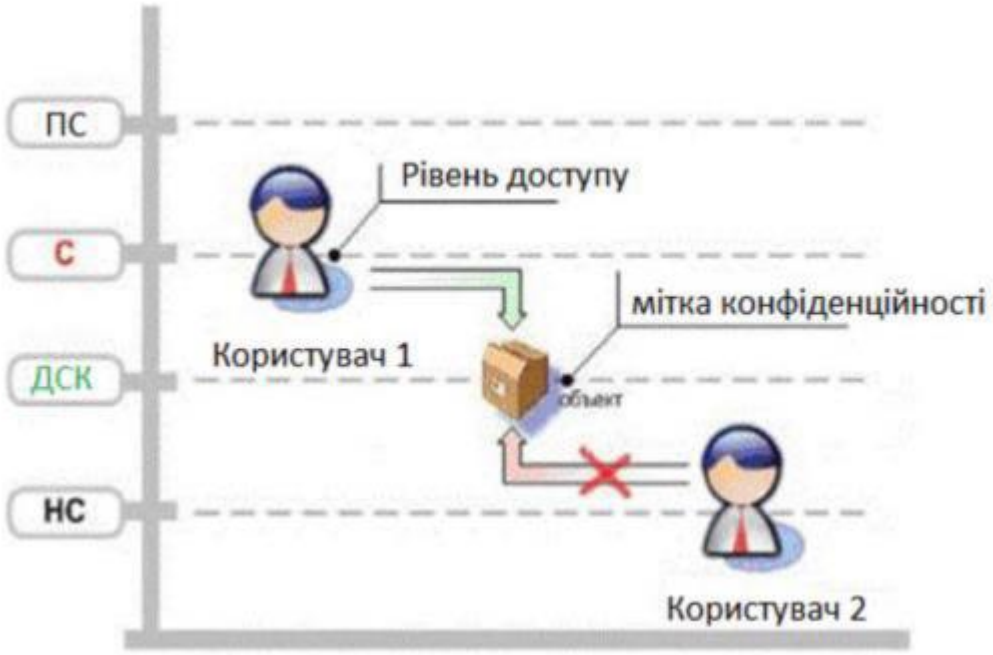

Рисунок 1.2 – Структура реалізації мандатної моделі

Спираючись на зазначені переваги та недоліки, системи MAC, в основному, використовуються компаніями та організаціями, які потребують найвищого рівня безпеки.

1.4.3 Контроль доступу на основі ролей

Контроль доступу на основі ролей (RBAC) стрімко набирає популярності завдяки простоті та зручності у використанні. Замість того, щоб призначати дозволи окремим користувачам, як реалізовано у системі MAC, дана система працює на основі призначення дозволів та повноважень для окремих посад. Це відповідно скорочує час, необхідний для налаштування або зміни доступу користувача і для адміністрування системи, в цілому [11, 12].

Наприклад, якщо на підприємстві працюють 20 розробників, 2 проєктні менеджери і 3 співробітники відділу бухгалтерії, немає необхідності створювати 25 індивідуальних профілів безпеки, достатньо створити лише три ролі: по одному для кожної зазначеної посади. Якщо відбувається зарахування нових співробітників, можна легко надати йому повноваження відповідно до посади (ролі), яку він буде

виконувати, а для розширення штату новими посадами можна створювати додаткові профілі безпеки. Також є можливість заміни існуючої ролі співробітника на іншу, наприклад, у випадку підвищення по службі.

Такий метод надає можливість застосувати в системі принцип «найменших повноважень», тобто призначати особі доступ, необхідний виключно для виконання її роботи, оскільки доступ пов'язаний безпосередньо з конкретною посадою чи обов'язками.

RBAC може бути реалізований на чотирьох рівнях відповідно до моделі RBAC NIST. Кожен наступний рівень включає властивості попереднього.

Плоский RBAC є реалізацією базових функцій та можливостей моделі RBAC. Усім користувачам призначаються ролі. Користувачі отримують необхідні дозволи, набуваючи ці ролі, яких може бути стільки, скільки потрібно компанії (рис. 1.3). Одному користувачеві можна призначити як одну, так і декілька ролей, а одну роль відповідно можна призначити одному або кільком користувачам [14].

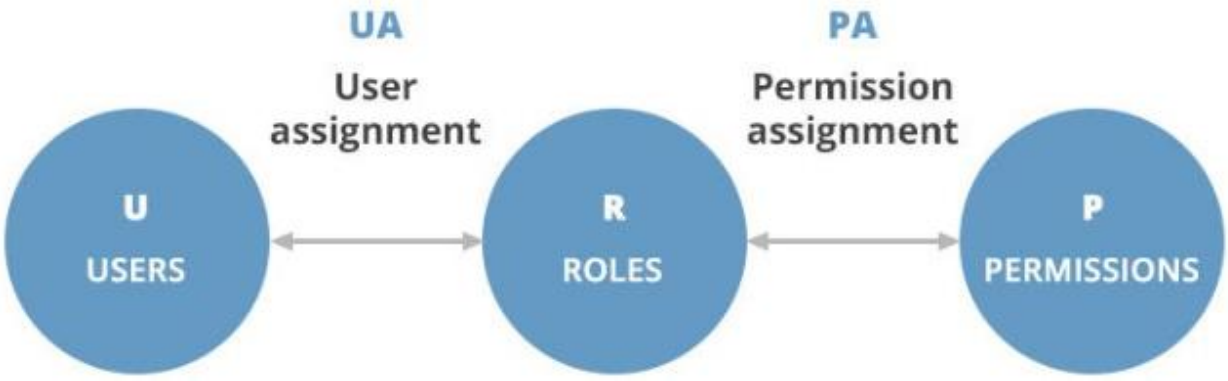

Рисунок 1.3 – Схема реалізації плоскої RBAC

Ієрархічний RBAC , як можна здогадатися з назви, реалізовує ієрархію в створеній структурі ролей. Ця ієрархія встановлює взаємозв'язки між ролями (рис. 1.4). Користувачі зі старшими ролями можуть отримувати дозволи та права всіх молодших ролей. Складність та рівень ієрархії визначається потребами компанії [14-16].

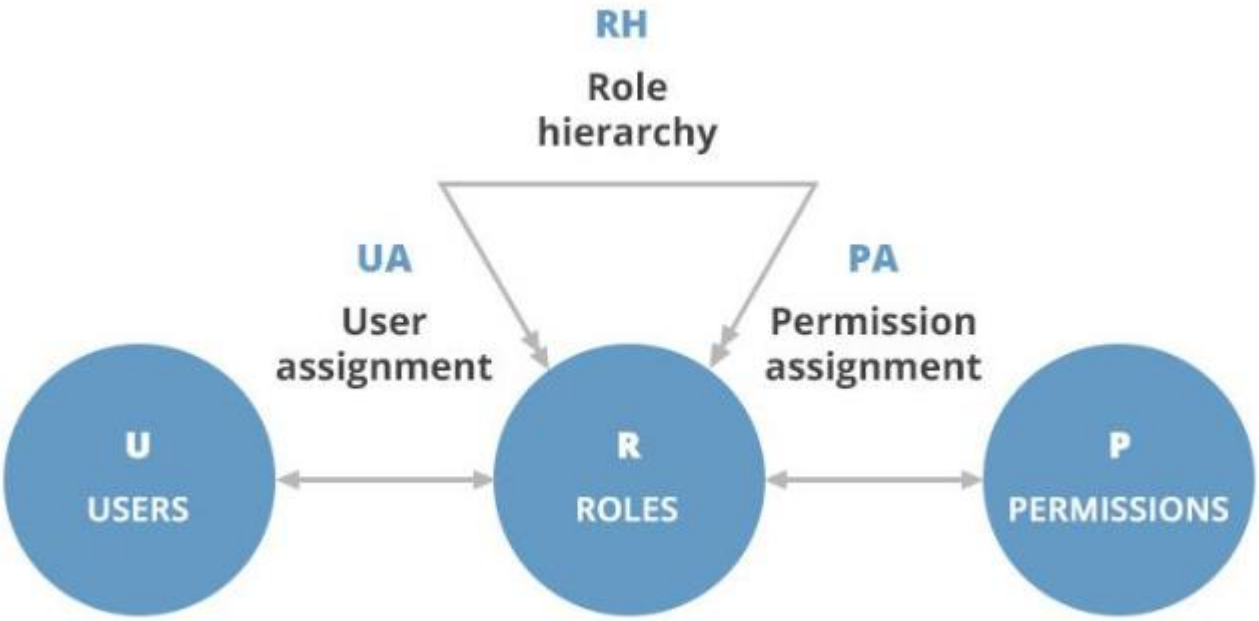

Рисунок 1.4 – Структура ієрархічної RBAC

Обмежений RBAC додає до створеної системи безпеки також розділення обов'язків (SOD) (рис. 1.5). SOD – це поширена практика безпеки, коли один обов’язок розподіляється між кількома працівниками, що досить корисно для використання в середньому бізнесі та великих підприємствах [14, 15].

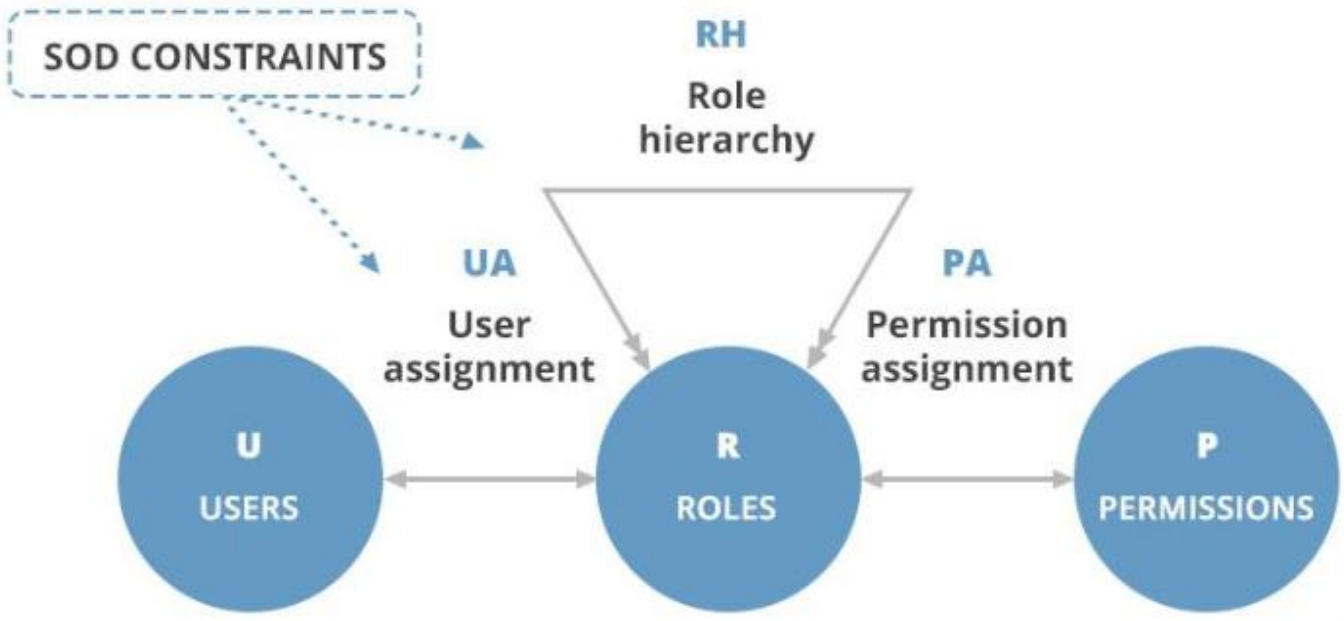

Рисунок 1.5 – Схема організації обмеженої RBAC

Симетричний RBAC виконує перевірку ролі дозволів, а також ролі користувачів (рис. 1.6). Він спершу ідентифікує дозволи, призначені наявним ролям, і потім навпаки [14].

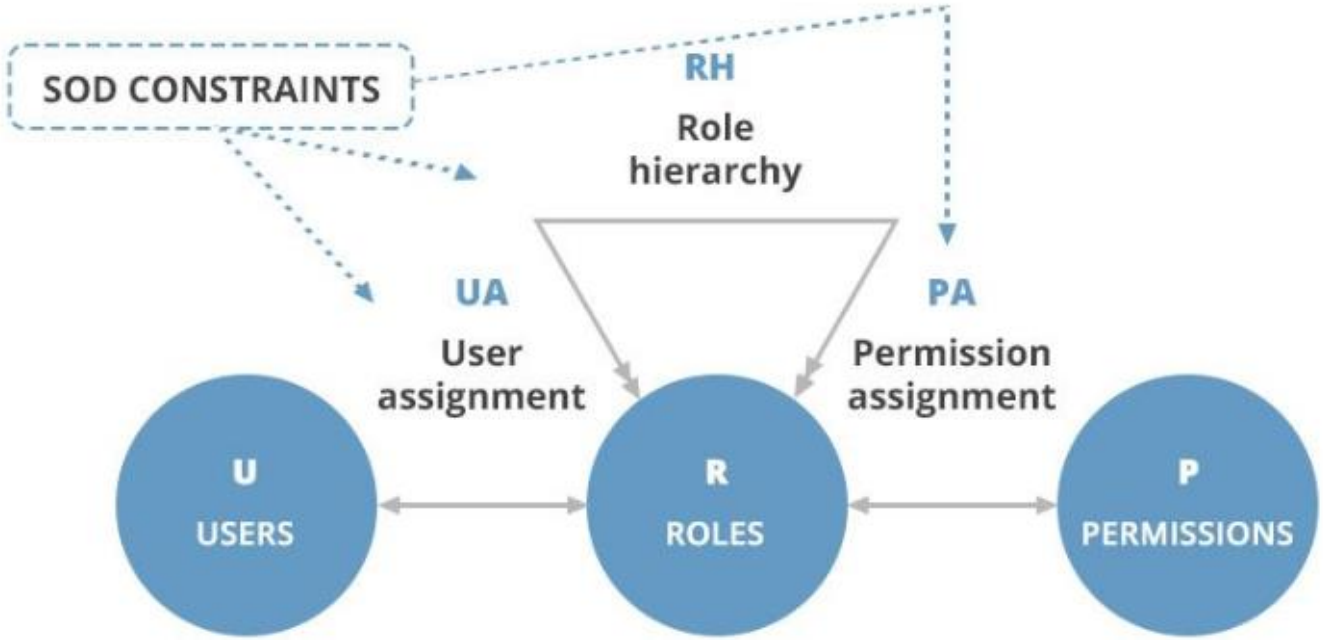

Рисунок 1.6 – Структурна схема симетричного RBAC

1.4.4 Контроль доступу на основі правил

Контроль доступу на основі правил (Rule-Based Access Control) рідко класифікується, як окрема модель керування доступом користувачів до системи, а, зазвичай, використовується як доповнення до інших типів контролю доступу. На підвищення рівня безпеки, застосовуючи будь-яку з трьох попередніх моделей керування доступом, контроль доступу на основі правил може змінювати та доповнювати дозволи на основі певного набору правил, створених адміністратором. Зокрема, зручно доповнювати таким чином мандатне керування доступом, щоб відкинути необхідність щоразу перепрограмовувати дозволи профілів декількох користувачів. Однак зазначимо, що за допомогою контролю доступу на основі правил можна додати лише «м’які» правила, що не суперечать основній моделі контролю [10].

До прикладу, якщо організація працює виключно до 21:00, а після завершення робочого дня суворо заборонено будь-якому користувачу мати доступ до системи, то завдяки контролю доступу на основі правил можна встановити додаткове правило для заборони доступу будь-яких входів у систему з 21:00 до 7:00 наступного ранку.

1.5 Дискреційне управління доступом

Дискреційний контроль доступу (DAC) на даний момент є найпоширенішою моделлю контролю доступу в інформаційних системах. Він є основою майже всіх користувацьких операційних систем (включаючи Windows, macOS), часто використовується і для хмарних сервісів (Google Drive). Незалежно від того, знайомий користувач з цією моделлю чи ні, існує дуже висока ймовірність, що він працював або стикався з однією з форм дискреційного контролю доступу у повсякденному комп’ютерному житті або на роботі. Розглянемо детальніше принцип роботи DAC [17].

Модель дискреційного контролю доступу набула особливої популярності через гнучкість, яку вона пропонує. Однак не рекомендується застосовувати дискреційний контроль доступу для роботи великих масштабних організацій, адже можна стикнутися з некерованістю системи, враховуючи що в зазначених умовах власниками об’єктів можуть виступати сотні або й тисячі окремих співробітників [18].

DAC, як було зазначено вище, характеризується розмежуванням доступу між наявними в системі суб’єктами та об’єктами. Суб’єкт з певним правом доступу може передавати це право будь-якому іншому суб'єкту, тобто делегувати свої права доступу. Для кожної пари (суб’єкт – об’єкт) задається явне і конкретне перерахування допустимих типів доступу (читання, писання, виконання тощо), які є узгодженими для даного суб’єкта до даного об’єкта. Кожен об’єкт системи має свого власника, який є прив'язаним до нього. Саме власник має всі повноваження

стосовно встановлення прав доступу до даного об’єкта для всіх інших користувачів (рис. 1.7) [17-19].

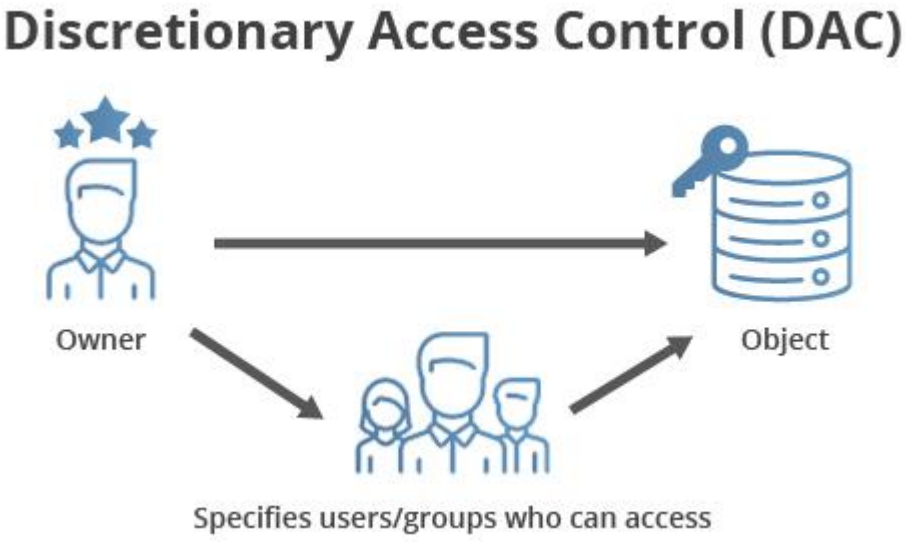

Рисунок 1.7 – Взаємодія суб’єктів та об’єктів в дискреційній моделі

Уся система загалом має єдиний привілейований суб’єкт, який уповноважений визначати та призначати права власності для всіх інших суб’єктів системи. Можлива побудова змішаної системи керування, коли одночасно в системі присутні власники конкретних об’єктів, а також привілейовані суб’єкти, що можуть змінювати права для будь-якого об’єкта без виключень або взагалі змінювати власників об’єктів. Саме такий варіант реалізований в багатьох операційних системах.

Дискреційна політика безпеки передбачає, що права доступу користувачів до окремих об’єктів можуть бути обмежені, базуючись на зовнішньому (по відношенню до системи) правилі. DAC обов’язково вимагає ідентифікації всіх суб’єктів та об’єктів системи.

Механізм, що реалізовує політику DAC, повинен відповідати на наступне питання: «Чи має суб’єкт *S* право *R* відносно об’єкта *O*?". Візуально інформація для відповіді на це питання може бути представлена у вигляді математичного відношення *D* щодо суб’єктів, об’єктів та прав: тобто якщо (*S,O,R*) належать в *D*, то суб’єкт *s* дійсно має право *r* до об’єкта *o*; в протилежному випадку суб’єкт s не має такого повноваження [17].

Основний механізм керування доступом у дискреційній моделі – матриця доступу. Матриця доступу – матриця D розміром $|S|$ на $|O|$, де рядки відповідають суб'єктам системи, а стовпці – об'єктам. Кожен елемент матриці доступу $D|s,o|$ описує права доступу відповідного суб'єкта s до об'єкта o і належить множині прав доступу та повноважень. Здебільшого суб'єкти s є активними сутностями, наприклад користувачі або процеси в системі, а об'єкти o є пасивними сутностями (інформація або ресурси), що власне й потребують захисту. Не виключено, що у деяких операціях доступу суб'єкти s можуть виступати також як пасивні сутності, до яких ініціюють доступ інші активні суб'єкти, тому множини S та O знаходяться у відповідності S до O. Підмножина об'єктів, до яких суб'єкт має певні права доступу, називається доменом цього суб'єкта. На рисунку 1.8 наведена матриця доступу, що ілюструє основні принципи вибіркового керування [8].

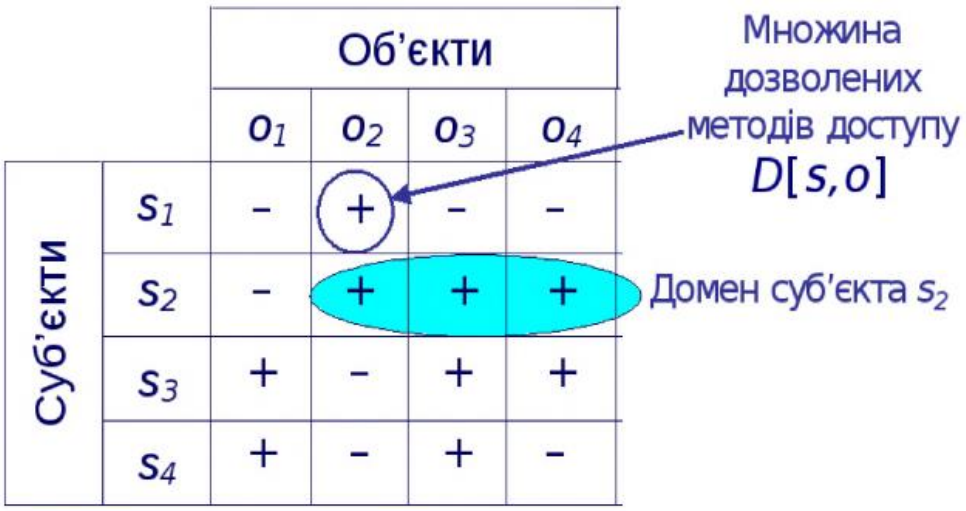

Рисунок 1.8 – Матриця доступу дискреційної моделі

Матриця доступу дуже громіздка і неефективна з точки зору використання пам'яті. Натомість у реальних функціонуючих інформаційних системах створюються списки доступу або списки повноважень.

Список доступу – спеціально складений список, що асоціюється з кожним захищеним об'єктом в системі і зберігає ідентифікатори суб'єктів разом з їхніми

правами стосовно даного об’єкту (тобто список доступу описує окремий стовпчик матриці доступу).

У свою чергу список повноважень навпаки – асоціюється з кожним суб’єктом в системі і містить в собі ідентифікатори об’єктів разом з повноваженнями цього суб’єкта стосовно цих об’єктів (таким чином список повноважень відповідає окремому рядкові матриці доступу).

Застосовуючи таку модель керування доступом політика безпеки інформації повинна містити матрицю доступу, яка описує правила розмежування доступу, а також чітко визначені обмеження, що накладаються на можливість та способи внесення змін до цієї матриці.

Звідси слідує, що при довірчому керуванні доступом всі повноваження на зміну прав доступу до об’єкта надаються його власнику. Це означає, що список прав доступу суб’єкта *s* до об’єкта *o* містить і право власника, а суб’єкт-власник *s* отримує повний контроль над стовпчиком матриці доступу, що відповідає об’єкту *o*.

Висновки за розділом 1

Отже, у першому розділі було розглянуто основні методи розмежування доступу в інформаційних системах, доцільність їх застосування, побудову, основні принципи функціонування та детально описано дискреційну модель керування доступом, яка є найбільш поширеною на сьогоднішній день. Аналізуючи дану інформацію, було поставлено завдання дослідити доцільність впровадження дискреційної моделі керування доступом в різних інформаційних системах.

В результаті проведеної роботи, було виявлено, що механізм реалізації такого типу керування доступом користувачів є доречним для не надто масштабних ІС та може бути представлений у вигляді практичної моделі.

Також, було проаналізовано підходи реалізації такого розмежування та конкретної фізичної побудови системи керування доступом, що в наступних розділах дасть можливість розробити загальні рекомендації стосовно впровадження дискретної моделі керування доступом в інформаційних системах.

Було виявлено, що існує багато практики використання розглянутого механізму керування доступом, тобто підтверджена актуальність обраного дослідження. У наступному розділі буде розглянуто переваги та недоліки обраної моделі, а також порівняння її з іншими типами систем керування доступом, що в подальшому може використовуватися при виборі моделі керування доступом, яка буде відповідати потребам конкретної організації чи системи.

РОЗДІЛ 2
ДИСКРЕЦІЙНА МОДЕЛЬ ЯК ОСНОВНА РЕАЛІЗАЦІЯ ПОЛІТИКИ РОЗМЕЖУВАННЯ ДОСТУПУ

2.1 Переваги та недоліки дискреційного керування доступом

При підвищенні рівня захищеності інформаційної системи шляхом інтеграції в неї системи контролю доступу, постає питання коректності вибору типу такої системи. Важливо розуміти, що не існує єдиного підходу впровадження і використання ACS для всіх. Вибір залежить від багатьох факторів, необхідно орієнтуватися на власні унікальні потреби та вимоги. Хоча звертатися за досвідом власників інших інформаційних систем цілком правильно в процесі аналізу особистих ресурсів.

Як зазначалося вище, дискреційний контроль доступу – це система, в якій користувач, що вже має доступ до певних даних, може надати цей доступ іншому користувачеві на основі особистого рішення. Перший список контролю доступу (ACL) створюється адміністратором системи, він також може бути перевірений, переглянутий та оновлений в будь-який час.

Така організація робочого процесу робить потік даних значно зручнішим, ніж в інших системах керування доступом. Однак постає проблема, яка полягає в тому, що потік інформації не може контролюватися безперервно, а це створює додаткові дірки в системі безпеки. Враховуючи зазначений фактор, зазначена система не забезпечує надійності в ході циркулювання потоків інформації, що автоматично робить її непридатною для організацій, які обробляють конфіденційну інформацію та вимагають високого рівня безпеки своїх даних, зокрема без використання додаткових засобів протидії НСД, наприклад, у таких галузях, як медицина, фінанси, військові, державні установи тощо.

Розглядаючи переваги DAC, наведемо нижче наступні функції та можливості дискреційного контролю доступу [20-22]:

- гнучкість (дискреційні системи контролю доступу надають можливість користувачам налаштовувати кожну політику доступу окремо. DAC пропонує такий підхід до аутентифікації та авторизації, де власник ресурсів має можливість налаштувати політику дозволів відповідно до кожного користувача індивідуально, тобто призначення прав доступу виконується найбільш ефективним для конкретної мережі та цілей);
- простота керування (кінцеві системи підключені до центрального пристрою, з нього користувачі створюють політики безпеки для визначення входу, а також легко контролюють усі точки доступу);
- резервне копіювання (DAC дозволяє організаціям створювати резервні копії налаштованих політик безпеки та даних, щоб забезпечити ефективні точки входу та доступу в будь-який момент, коли це необхідно).
- зручність використання (складність в такій системі контролю доступу зведена до мінімуму для досягнення кращого управління ресурсами мережі. Так як організація чи установа не може вручну контролювати кожну спробу доступу до своєї мережі, що зумовлене додатковими втратами часу та коштів для бізнесу чи організації загалом, розглянутий контроль доступу автоматизує систему охоронного спостереження. Точки входу та доступу контролюються з централізованої платформи для перевірки та автентифікації осіб, які намагаються отримати доступ до важливих файлів).
- швидка аутентифікація (в порівнянні з ручним керуванням, автентифікація в дискреційній системі виконується за лічені секунди).
- мінімізація вартості (цей тип контролю доступу також є економічно вигідним, оскільки зменшується кількість ресурсів, що використовуються для контролю за мережею організації).

На противагу зазначеним перевагам варто зазначити ряд суттєвих недоліків, які в деяких випадках можуть бути критично важливими [23-27]:

- відносно низька захищеність системи (доступ до ресурсів може бути переданий від однієї особи до іншої, за рахунок цього дані не надто захищені в DAC, тому з’являється необхідність, щоб служба безпеки періодично переглядала та

контролювала усі списки доступу для зниження ризику витоку інформації за межі контрольованої зони);

- складність керування усіма наявними списками доступів при масштабуванні інформаційної системи (при наявності великої кількості користувачів в системі важко відслідковувати усі призначення та передачі прав).

2.2 Порівняння дискреційної та мандатної моделей керування доступом

Контроль доступу визначає, які користувачі, програми та пристрої, вони ж суб'єкти, можуть переглядати, модифікувати, додавати та вилучати ресурси, вони ж об'єкти, в середовищі організації. Контроль доступу є однією з ключових практик захисту від НСД, крадіжки важливих даних, неправильного використання, зловживання посадовими обов'язками та інших аналогічних загроз.

Можна виокремити два рівні контролю доступу: фізичний і логічний (рис. 2.1). В обох випадках він допомагає пом'якшити як внутрішні, так і зовнішні загрози, а також наслідки від їх потенційного впливу. Саме тому IT-стандарти, такі як NIST , HIPAA , PCI DSS та інші, рекомендують забезпечення суворих заходів фізичного та логічного контролю доступу [20].

Рисунок 2.1 – Рівні керування доступом

Так як було наведено вище, існує декілька логічних моделей контролю доступу: обов'язкова або мандатна, дискреційна або вибіркова, на основі ролей, на

основі правил, атрибутів тощо. Процес вибору та розгортання моделі контролю доступу виглядає по-різному для кожної організації і прямо залежить від характеру даних, що потребують захисту, IT-вимог, галузевих стандартів, рекомендацій, кількості працівників, тобто користувачів інформаційної системи, бюджету організації в загальному, та для потреб кіберзахисту зокрема.

З'ясуємо, коли використовується мандатна та дискреційна моделі контролю доступу.

MAC по праву вважається найбезпечнішою з усіх існуючих моделей контролю доступу. Правила, за якими здійснюється вхід та будь-які дії з об'єктами, визначаються вручну системним адміністраторам або службою безпеки і суворо дотримуються користувачами, операційною системою та ядром безпеки. Усі інші користувачі не можуть змінювати встановлені атрибути безпеки навіть для тих даних, які вони самі ж створили.

Базуючись на MAC, процес отримання доступу виглядає так [20]:

1. Адміністратор налаштовує політики доступу та визначає атрибути безпеки: рівні конфіденційності, дозволи доступу до різних проектів і типи ресурсів.

2. Адміністратор призначає кожному суб'єкту (користувачу або ресурсу, який отримує доступ до даних) та об'єкту (файлу, базі даних, порту тощо) набір атрибутів.

3. Коли суб'єкт намагається отримати доступ до об'єкта, операційна система перевіряє атрибути безпеки суб'єкта та вирішує, чи можна надати доступ.

Таким чином мандатне керування надає багато переваг для системи в розрізі кібербезпеки, але має ряд недоліків в побудові та адмініструванні, які теж слід враховувати.

Застосування: MAC, наприклад, використовується урядом США для захисту секретної інформації та підтримки багаторівневої політики безпеки, державними організаціями, військовими та правоохоронними установами.

Доречно інтегрувати MAC в інформаційні системи установ, які визначають пріоритетом безпеку даних, а не операційну гнучкість чи фінансування. Реалізація

MAC в приватній організації зустрічається рідко, в особливості через складність впровадження, використання і масштабування [21].

На противагу MAC, дискреційний контроль доступу – це модель контролю доступу на основі ідентифікації, яка дозволяє користувачам здійснювати власноруч певний контроль над окремими даними. Власник даних або інший користувач, наділений повноваженнями керувати даними від власника, може самостійно, без відома та погодження системного адміністратора визначити дозволи доступу для інших суб’єктів.

Покроково отримання доступу до ресурсу на основі моделі DAC працює так [20-22]:

1. Користувач А створює файл і стає його власником або отримує права доступу до існуючого файлу від власника чи адміністратора.
2. Користувач Б запитує доступ до даного файлу.
3. Користувач А надає або забороняє доступ на власний розсуд. Однак в разі позитивного рішення, він все одно не може надати права доступу, які перевищують його власні права на даних файл.
4. Якщо протиріччя між списком керування доступом, створеним адміністратором, і рішенням, прийнятим користувачем А, відсутні, доступ надається.

DAC є досить популярною та поширеною моделлю, оскільки надає велику ряд переваг для користувачів і не спричиняє адміністративних серйозних витрат, однак як і MAC, має ряд істотних обмежень, які варто приймати до уваги.

На рисунку 2.2 наведене порівняння DAC та MAC, базуючись на основних функціях, що повинні бути доступні в системах розмежування доступу [20].

Characteristic	MAC	DAC
Access control enforced by	Administrators and operating system	Administrators and users
Flexibility	—	✓
Scalability	—	✓
Simplicity	—	✓
Maintenance	Hard	Easy
Implementation cost	High	Low
Granularity	High (admins adjust clearances for each user and object manually)	High (users can assign access rights for any other user or group)
Easy to use	—	✓
Security level	High	Low
Useful for	Government, military, law enforcement	Small and medium-sized companies

Рисунок 2.2 – Порівняння моделей MAC та DAC

Підсумовуючи, можна зазначити такі ключові аспекти: MAC і DAC – це дві абсолютно протилежні моделі керування доступом. В мандатній моделі доступ обов'язково контролюється адміністраторами і вимагає багато часу та зусиль для підтримки, але в свою чергу забезпечує високий рівень захисту даних. DAC значно простіша у впровадженні та підтримці, оскільки користувачі можуть керувати доступом до даних, якими вони володіють, але така модель недостатньо вдала для захисту важливих конфіденційних даних.

2.3 Порівняння дискреційної та рольової моделей керування доступом

Ще однією широко розповсюдженою моделлю керування доступом вважається система на основі ролей.

Контроль доступу на основі ролей (RBAC) — це метод контролю доступу, заснований на визначенні ролей співробітників і надання їм відповідних привілеїв в організації відносно визначеної ролі.

Ідея цієї моделі дуже проста та лаконічна: кожному користувачу інформаційної системи призначається своя роль. Кожна роль заздалегідь має набір дозволів та обмежень. Конкретний співробітник може отримати доступ до обраних об’єктів і виконувати певні дії з ними лише за умови, що його роль у системі має на це відповідні права (рис. 2.3).

Основними складовими рольового підходу до контролю доступу є користувачі (фізичні особи з доступом до системи), ролі (зазвичай, називаються відповідними посадовими функціями та вказують на рівень повноважень), дозволи (еквіваленти прав доступу), сесії (поодинокі зіставлення між користувачем і набором ролей, яких він набуває в процесі обмеженого робочого часу), об’єкти (системні ресурси, на доступ до якого запитується дозвіл від користувачів системи), операції (будь-які конкретні дії в визначеній захищеній мережі) [14].

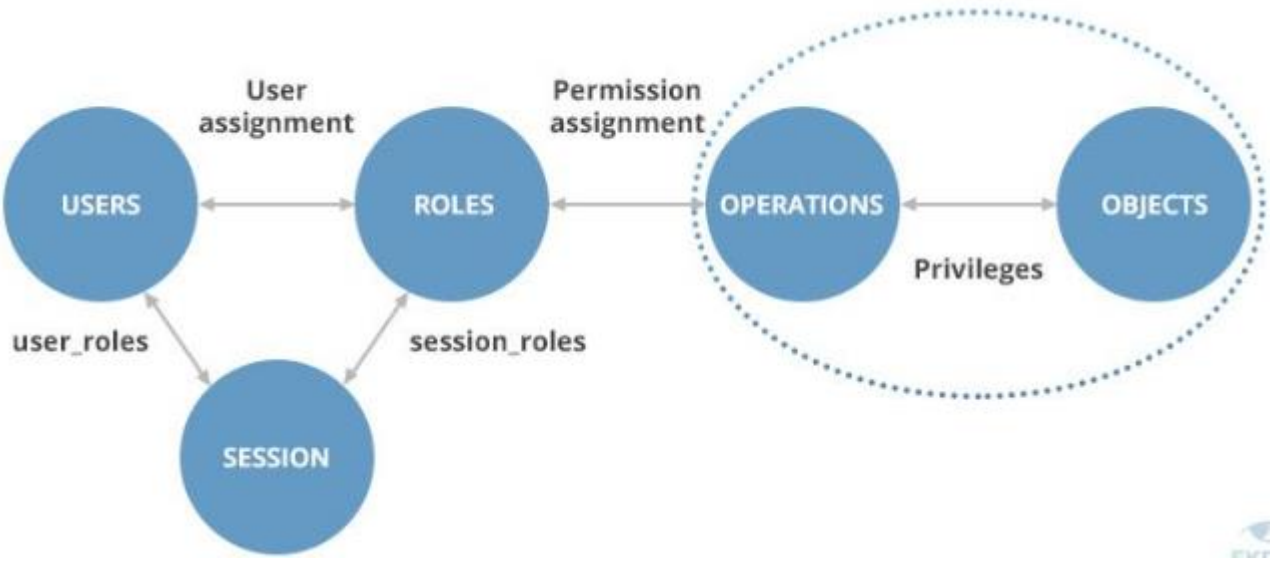

Рисунок 2.3 – Взаємодія складових RBAC

Визначення ролі може виявитися досить непростим завданням. Потрібно врахувати всі дозволи, що на разі або найближчим часом можуть виявитися необхідні користувачеві для виконання своїх професійних обов’язків, і положення

самої ролі у обраній структурі чи ієрархії. Важливо, що якщо для ролі буде призначено занадто багато дозволів, це порушить принцип найменших привілеїв і в подальшому може призвести до неправильного використання чи зловживання привілеями.

Застосування: RBAC найчастіше впроваджується в інформаційних системах малих і середніх підприємств. Такі організації часто провадять елементарні робочі процеси, що застосовують обмежену кількість ролей і передбачають лаконічну ієрархію, що надає можливість ефективно визначати й описати ролі окремих користувачів [28].

Перевагою такої системи є те, що після налаштування всіх необхідних ролей ця система керування не потребує особливого обслуговування чи безперервної підтримки системного адміністратора. Недоліком можна вважати, що створити якісну рольову систему для масштабного підприємства може бути складно (наприклад, організація з тисячами співробітників може потребувати розробки системи з кількома тисячами ролей). Таке явище відоме як «рольовий вибух», і це неминуче для великої компанії при впровадженні RBAC.

Детально про DAC було розглянуто вище. Не дивлячись на подібність в організації згаданих моделей керування доступом, можемо зазначити основні відмінності в реалізації DAC та RBAC [28-29]:

- DAC заснований на особистих дозволах, RBAC — на дозволах на рівні окремої групи чи ролі;
- DAC встановлюється і налаштовується власником даних, RBAC — власником системи чи адміністратором (найчастіше розробник визначає доступ, наданий кожній ролі, а операційний адміністратор розставляє користувачів у ці ролі);
- ролі RBAC адмініструються централізовано (хто з якими ролями пов’язаний), тоді як в DAC адмініструється «на ресурсі» (кожним ресурсом відбувається керування окремо);

• визначення дозволів для ролі часто є статичне в RBAC, користувачам надаються лише необхідні ролі, тоді як в DAC дозволи на ресурс часто модифікуються за необхідності в процесі роботи.

На рисунку 2.4 можна спостерігати наявність або відсутність певних можливостей системи в залежності від обраного типу керування доступом.

Attribute/ Access Control Type	DAC	MAC	RBAC
Ease of Usage orConvenience	High	Varies	High
Performance	Low	Varies with Security Levels	High
Reusability	Yes	No	Yes
Single Point Failure	Authorization failure	Less	Less
Authentication Failure	less	varies	Based on role

Рисунок 2.4 – Порівняння основних можливостей DAC, MAC та RBAC

2.4 Комбінування існуючих моделей керування доступом для підвищення захищеності ІС

Часто виникає ситуація, коли враховуючи структуру організації, важко виділити одну модель керування доступом, яка задовольняла б усі вимоги та критерії. В такому випадку можна намагатися виділити більш важливі потреби, які обов’язково повинна покривати обрана модель або ж звернутися до поєднання декількох розглянутих вище моделей.

Багаторівнева безпека — це політика безпеки інформаційної системи, установи, організації, яка дозволяє підприємствам використовувати ієрархічну систему безпеки. По суті, такі системи мають сувору багаторівневу політику безпеки, з деталізацією окремих рівнів, в яку дуже важко проникнути. Багаторівнева організація безпеки також дозволяє компаніям інтегрувати більше одного методу контролю доступу для підвищення надійності та безпеки шляхом поєднання переваг кількох моделей контролю доступу.

Наприклад, базова модель MAC забезпечує високий і детальний рівень безпеки, однак її важко налаштувати та обслуговувати. Тому часто зустрічається поєднання MAC з іншими моделями контролю доступу. Її комбінація з моделлю на основі ролей прискорює конфігурацію профілів користувачів. Тобто замість визначення прав доступу для кожного окремого користувача, адміністратор може створювати ролі користувачів. Адміністратор може налаштувати ролі для цих груп замість того, щоб налаштовувати окремі профілі користувачів з нуля. Але так як ролі додаються до MAC, зберігається перевага забезпечення високого рівня захисту.

Профіль безпеки — це поширений спосіб групування дозволів і доступів до певної ролі в організації. Використання профілю безпеки зустрічається і в мандатному контролі доступу, і в контролі доступу на основі ролей. MAC і RBAC дозволяють системним адміністраторам або фахівцям служби безпеки розділяти користувачів на основі профілів безпеки.

Також існують комбіновані реалізації DAC та RBAC. Найвдалішим та найпоширенішим прикладом такого поєднання є Active Directory, що працює з ролями і дозволами. Варто відзначити, що RBAC і ACL можуть замінювати один одного: можна налаштувати дозволи RBAC, щоб охопити політику, встановлену DAC, і навпаки. Крім того, існує досить багато окремих реалізацій RBAC, які надають користувачам дискреційні повноваження, запозичені в DAC.

Ще однією популярною комбінацією є поєднання моделей MAC і DAC. MAC можна використовувати для забезпечення надійного захисту конфіденційних даних, тоді як DAC дозволяє колегам обмінюватися інформацією в корпоративній файловій системі в значно спрощеному режимі.

Відомі також різні комбінації з моделлю на основі ролей. Компанії часто починають із впровадження плоскої RBAC. Цю модель досить просто налаштувати та обслуговувати на початку. Враховуючи ріст та розвиток організацій, нерідко виникає необхідність використання більш складної та надійної системи контролю доступу. RBAC можна використовувати разом з моделлю на основі правил, при цьому RBAC буде відповідати за більш «грубу» роботу, а правила доповнюватимуть її додатковою тонкою фільтрацією.

Відомий такий тип комбінування моделей як RBAC-A (модель на основі ролей та атрибутів). Зокрема виділяють три підходи до реалізації RBAC-A , які визначають зв'язок між ролями та атрибутами: орієнтований на атрибути, рольовий центр, де атрибути додаються для обмежень певних ролей, що не передбачено в класичній RBAC (у такій моделі атрибути можуть зменшити дозволи, доступні для користувача, такий чином підсиливши безпеку даних), та динамічні ролі (для визначення ролі суб'єкта використовуються різні атрибути, такі як час доби) [14].

На сьогоднішній день також існує новий метод під назвою контроль доступу наступного покоління (NGAC) , який розробляється в NIST. Він заснований на моделі на основі атрибутів, але реалізує більш тонкий підхід до політики безпеки. Наприклад, NGAC підтримує кілька типів політик одночасно, включаючи ті, які застосовуються як у локальному середовищі, так і в мережі [30-32].

Висновки за розділом 2

В даному розділі було розглянуто основні переваги та недоліки дискреційної моделі контролю доступу в інформаційних системах. Було проведено аналіз та порівнянні DAC з іншими існуючими моделями, можна зробити наступні висновки:

1. Системи на базі дискретного керування надзвичайно гнучкі та дозволяють використовувати найбільшу кількість дозволів у порівнянні з іншими типами контролю доступу. Однак в парі з зазначеною перевагою йде недолік в організації безпеки даних та ресурсів. Такі системи не є безпечними.

2. Крім того, оскільки системи DAC дозволяють власникам бізнесу напряму, а не фахівцям з безпеки чи технічним спеціалістам, контролювати права доступу та дозволи для користувачів інформаційної системи, вони повинні володіти знаннями та глибоким розумінням політик безпеки, що не завжди враховується.

3. В найбільш вдалих випадках рекомендується використовувати все-таки поєднання одразу декількох моделей. Так, потрібно бути готовим до додаткових витрат при інтегруванні таких систем керування, однак таким чином можна перекрити недоліки однієї моделі перевагами іншої.

4. Один з важливих аспектів, який необхідно врахувати при виборі системи контролю доступу, — це те, які політики, моделі та механізми контролю доступу насамперед доцільно застосувати в конкретних умовах. Ці три компоненти допомагають визначити вимоги до апаратного та програмного забезпечення. Потрібно дізнатися про будь-які вимоги до сумісності та підключення обраної системи. Важливо знати, як буде відбуватися структурування доступу і на основі яких моделей це можна реалізувати.

5. Перш ніж остаточно визначитися з вибором конкретної системи контролю доступу необхідно оцінити усі можливі витрати. Поширеною помилкою є врахування лише початкових затрат. Але обслуговування системи, оновлення, регулярна експлуатація, навчання та придбання можуть вимагати й додаткових витрат, що в подальшому може викликати додаткові труднощі в організації.

У наступному розділі буде розроблено рекомендації стосовно впровадження в інформаційну систему системи контролю доступу, зокрема на основі дискреційної моделі та продемонстровано спрощену модель дискреційного керування доступом. Також буде розроблено рекомендації щодо поєднання вибіркової системи керування доступом з іншими засобами захисту для підвищення надійності та стійкості інформаційної системи.

РОЗДІЛ 3
ПОБУДОВА ДИСКРЕЦІЙНОЇ МОДЕЛІ РОЗМЕЖУВАННЯ ДОСТУПУ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

3.1 Первинний аналіз та підготовка ІС до впровадження дискреційного керування доступом

Для якісного та надійного захисту даних, а також покращеного рівня безпеки усієї інформаційної системи додавання ефективних та вдалих політик контролю доступу грає часто вирішальне значення. Незалежно від того, яку модель керування планується використовувати, розпочинати необхідно з чітко визначених правил за узгодженим алгоритмом. Обрана система та політика безпеки повинні охоплювати кожного співробітника, усі активні ролі, програмне та апаратне забезпечення, ресурси інформаційної системи, бази даних, фізичну будову системи, цілі та майбутній розвиток самої системи та усієї організації [33, 34].

Дотримання принципу найменших привілеїв при використанні дискреційної моделі є досить вдалим рішенням, яке суттєво зменшує ризик кібератак, тому варто серйозно підходити до опису усіх активів перед впровадження контролю доступу, не створюючи дірки в системі безпеки.

Щоб забезпечити чітку підзвітність та відповідність аудиту безпеки, прозорість дій користувачів та журналювання подій, в моделі DAC кожен юзер повинен мати власний персоніфікований обліковий запис. Таке рішення вирішує проблему використання спільних облікових записів і пов’язаних з ними додаткових ризиків безпеки.

Фактори, які обов’язково слід враховувати, включають в себе характер обраної інформаційної системи, кількість користувачів у системі та вже налаштовані процедури та засоби безпеки в організації.

При впровадженні дискреційної моделі контролю доступу в інформаційній системі рекомендуємо першочергово відповісти для себе на наступні запитання:

Хто буде керувати системою?

Перед безпосередньою інтеграцією системи дискреційного контролю доступу до наявної інформаційної системи, керівники або власники ІС повинні вирішити, хто буде керувати системою контролю доступу, допомагати впроваджувати оперативну політику, проводити адміністрування. Ця відповідальність має покладатися на особу або відділ безпеки, що буде охоплювати контроль усіх аспектів системи, включаючи протоколи, яких слід дотримуватися під час прийому на роботу, створення нових облікових записів користувачів, звільнення співробітників та вилучення їхніх прав доступу, а також активації та деактивації неактуальних прав доступу користувачів, ведення та контроль за матрицями доступу або списками повноважень.

Як зазначалося раніше, в DAC права на окремий об’єкт може контролювати власник цього ж об’єкту, але для зниження ймовірності реалізації загрози витоку даних, рекомендуємо створити відділ для контролю та адміністрування системи розмежування доступу або делегувати ці обов’язки вже існуючому відділу інформаційної безпеки чи окремому співробітнику (наприклад, системному адміністратору).

Скільки модулів інформаційної системи або ж зон на території організації потребують контролю доступу?

Необхідно визначити контрольовані зони, які потребують організації розмежування доступу, або ж у разі використання розподіленої інформаційної системи, окремі ресурси в системі, доступ до яких має бути обмеженим, оскільки це прямо впливає на розмір і складність системи. Деякі області можуть бути більш небезпечними, ніж інші, і потребують додаткової безпеки, що може не покриватися можливостями DAC. В такому випадку необхідно буде розглянути варіант комбінування дискреційної моделі, наприклад, з мандатною.

Цей крок важливо пропрацювати до інтеграції дискреційної моделі контролю доступу, адже таким чином можна уникнути додаткових витрат та проблем при проектуванні та впровадженні системи керування доступом.

Скільки користувачів у системі, чи буде збільшуватися їх кількість в подальшому?

Кількість користувачів є одним з найважливіших аспектів, які слід врахувати, оскільки саме він, частіше за все, задає основу для типу системи разом із необхідним рівнем безпеки. Як було описано в попередніх розділах, для невеликих або середніх організацій з обмеженою кількістю співробітників або користувачів система DAC є ефективним варіантом, тоді як великі організації можуть отримати більше переваг від системи RBAC.

Якщо ж власника інформаційної системи цілком задовольняють можливості дискреційної моделі керування, варто також проаналізувати необхідність майбутнього масштабування системи чи розширення штату, враховуючи перспективи розвитку, та закласти додаткові ризики до бюджету в такому випадку. Завжди необхідно думати наперед. Вибираючи систему контролю доступу, краще подумати про майбутнє зростання та перспективи у вашій сфері на найближчі декілька років.

Який необхідний рівень безпеки?

Визначення рівня безпеки є ще однією ключовою частиною вибору правильної моделі контролю доступу, оскільки всі вони відрізняються за рівнем контролю, управління та суворістю. Система MAC найкраще підходить для власності з високим рівнем ризику та високої безпеки через її суворі процеси.

Якщо власник інформаційної системи все-таки зупиняється на DAC через інші її переваги, можна вирішити питання підвищення рівня захищеності за допомогою додаткових засобів та методів захисту. Або, знову ж таки, розглянути варіант комбінування обраної моделі з іншими.

Зокрема дискреційний контроль доступу також можна інтегрувати з такими системами безпеки, як охоронна сигналізація, системи відеоспостереження та пожежна сигналізація , щоб забезпечити більш комплексне рішення безпеки для фізичного периметру.

Який метод аутентифікації буде найдоцільнішим у використовуваній системі?

Існує багато різних методів аутентифікації, для систем контролю доступу в тому числі (наприклад, карти доступу, брелки, токени, біометричні дані, постійні або тимчасові паролі, мобільний контроль доступу). Вибір того, який з них підходить для ваших потреб найбільше, залежить від очікуваного рівня безпеки, розміру власності, виділеного бюджету, кількості користувачів тощо.

Тому обов'язково перед впровадженням дискреційної моделі рекомендується вибрати один або декілька методів аутентифікації, що безпосередньо вплине на процес інтеграції та будови точок входу або доступу.

Які функції та інтеграції потрібні в конкретній інформаційній системі?

Системи дискреційного контролю доступу мають ряд функціональних можливостей, таких як звіти про доступ, сповіщення в реальному часі, віддалений моніторинг подій та багато інших. Потрібно завчасно визначитися, які саме функції вимагає інформаційна система і спроєктувати індивідуальне рішення для власних потреб на основі існуючої моделі.

Зібравши відповіді на перераховані запитання, обов'язково необхідно задокументувати усю отриману інформацію, повторно узгодити прийняті рішення з керівництвом та технічним відділом, скласти план та закласти бюджет. Після цього рекомендується переходити до впровадження дискреційної моделі керування доступом.

3.2 Практична реалізація спрощеної моделі ІС з використанням дискреційного розмежування контролю доступу користувачів

При програмній реалізації спрощеної дискреційної моделі керування доступом для наочності були створені 4 окремі суб'єкти доступу, які виступають у ролі користувачів системи, тобто фізичні особи, матриця доступу (рис. 3.1), зображена за допомогою елементу DataGridView, що демонструється при першочерговому запуску програмного додатку, у ролі об'єктів виступають окремі Windows Forms додатки, написані мовою програмування C++.

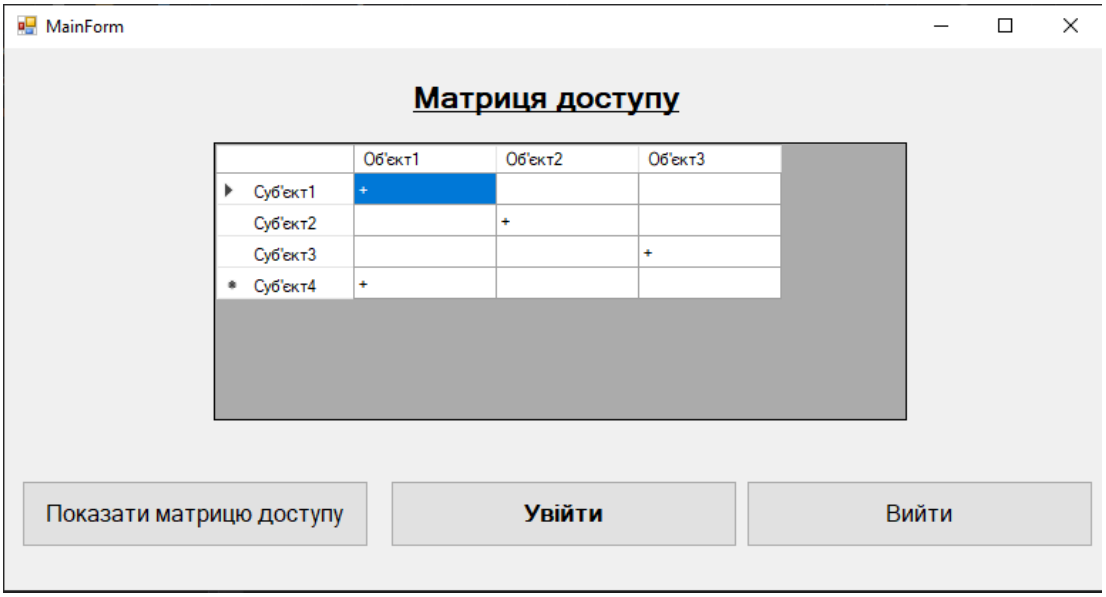

Рисунок 3.1 – Матриця доступу розробленої дискреційної моделі

Обраний механізм вибіркового керування доступом можемо проілюструвати на рисунку 3.2. Необхідно ретельно підходити до вибору сервісу авторизації. Так як в даному випадку реалізовано спрощену модель, вхід відбувається при введенні вбудованого ідентифікатора, тоді як більш просунуті системи додають окремий сервіс авторизації, що взаємодіє з системою, а також з базою даних, що містить матрицю або списки доступу.

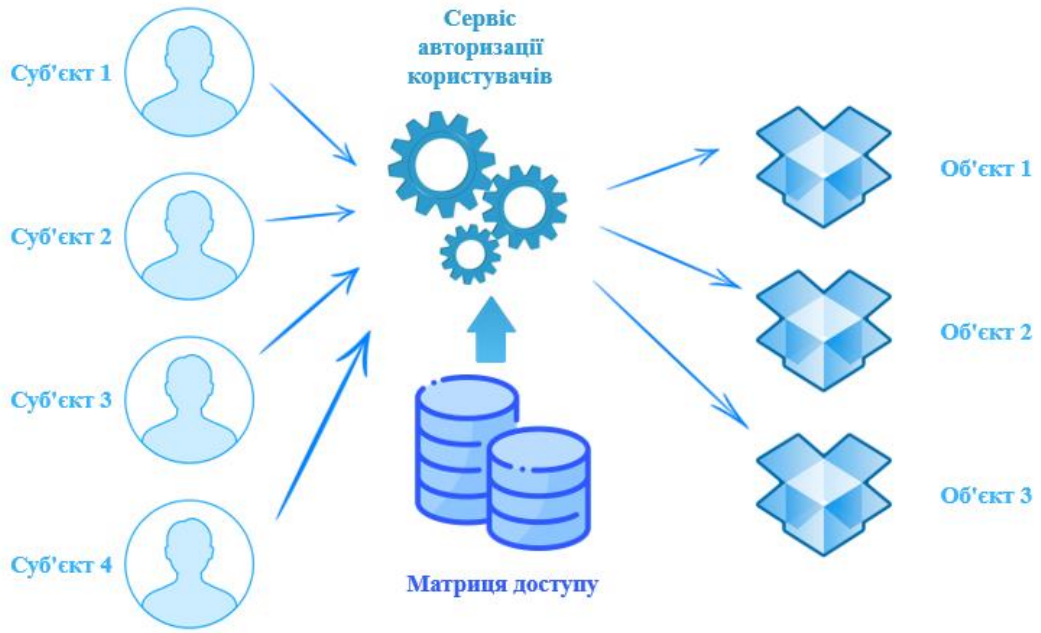

Рисунок 3.2 – Механізм дискретного керування в запропонованій моделі

Розподіл доступу до створених об’єктів відбувається за допомогою методу класу з механізмом створення окремого файлу та підключення його до проекту.

На усіх об’єктах доступу використовується операційне меню та реалізовано управління з вкладками.

В процесі вибіркового контролю доступу в запропонованій інформаційній системі користувачу пропонується ввести особистий ідентифікатор доступу, в залежності від якого і буде надаватися доступ до об’єкта (рис. 3.3-3.6). Базуючись на загальному вигляді інформаційної системи, було визначено такі основні суб’єктні посади користувачів: керівник всієї системи/організації, його заступник, керівник служби охорони, клієнтський адміністратор. Зазначимо, що ідентифікатори для суб’єктів визначені завчасно:

Суб’єкт 1 – Керівник організації – Ідентифікатор: 5943674842651258.

Суб’єкт 2 – Керівник служби охорони організації – Ідентифікатор: 6248512365852351.

Суб’єкт 3 – Клієнтський адміністратор організації – Ідентифікатор: 1269852466985205.

Суб’єкт 4 – Заступник керівника організації – Ідентифікатор: 9853612542380060.

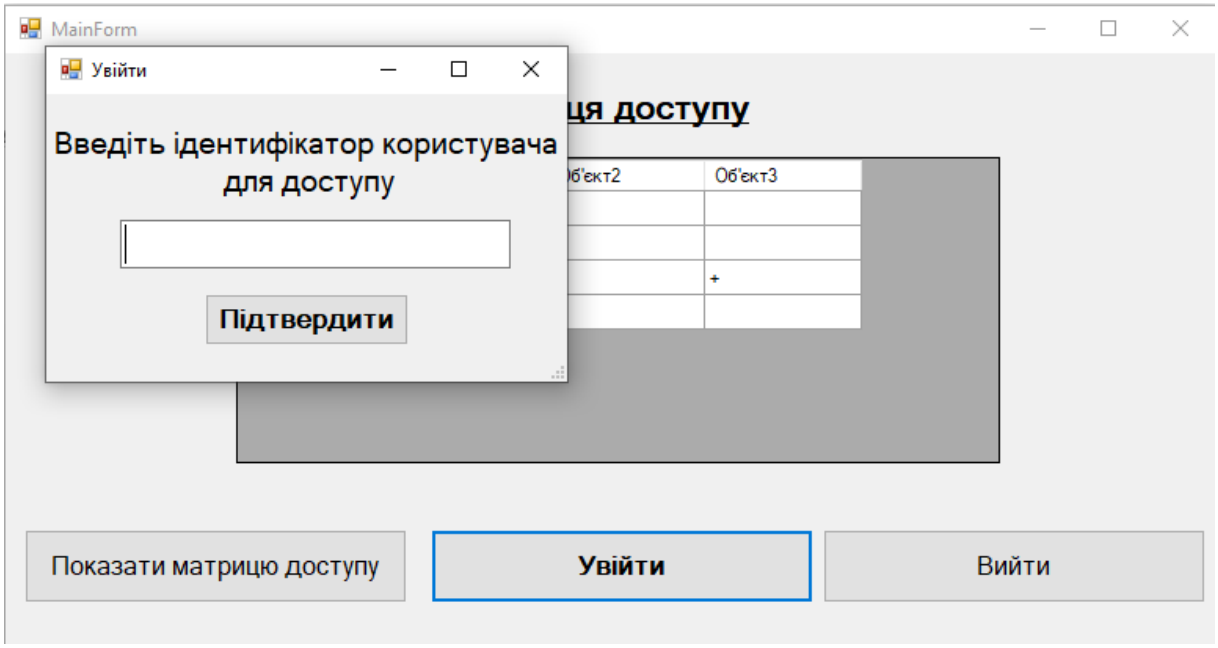

Рисунок 3.3 – Ініціація входу в інформаційну систему

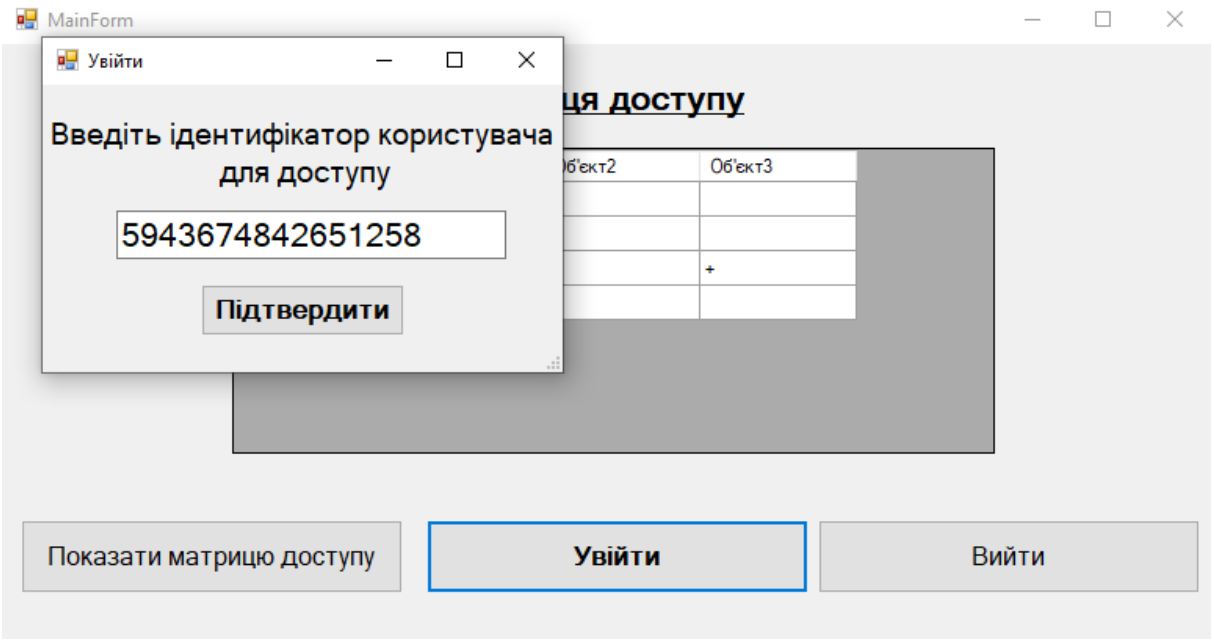

Рисунок 3.4 – Демонстрація введення ідентифікатора суб’єкта 1

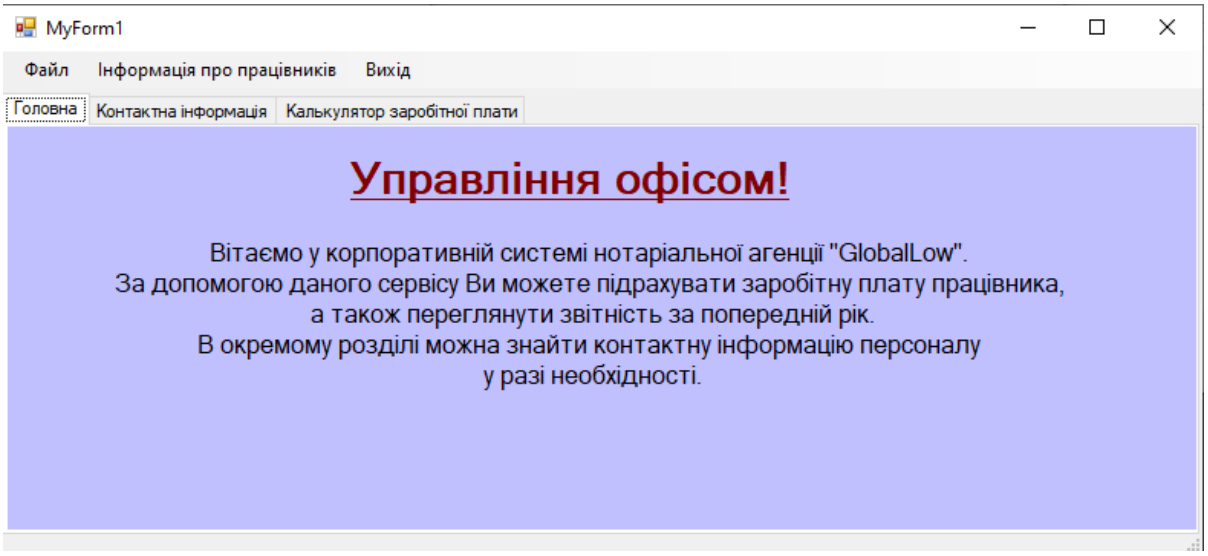

Рисунок 3.5 – Отримання доступу суб’єктом 1 до об’єкту 1

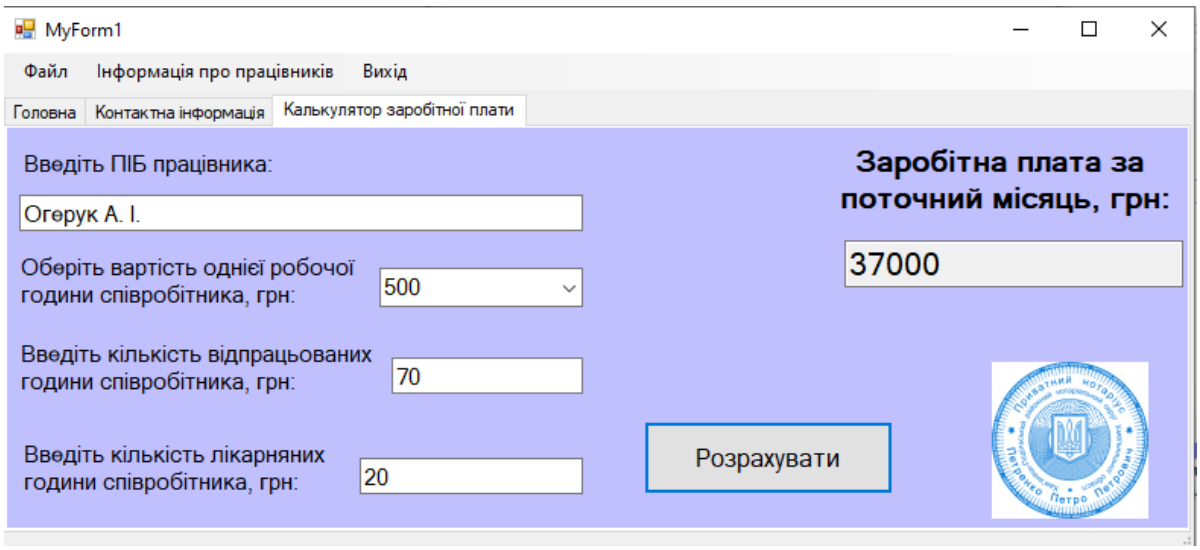

Рисунок 3.6 – Доступ суб’єкту 1 до усіх функцій, передбачених в об’єкті 1

Також варто відмітити, що дане визначення суб’єктів не демонструє рольову політику доступу, хоча суб’єкти визначені відносно їхньої ролі в організації. Дане позначення було обране для зручності розуміння роботи системи, так як присвоєння суб’єктам звичайних імен не демонструвало б взаємозв’язку з об’єктом, до якого надається доступ. Це продемонстровано також за рахунок різних профілів керівника та його заступника (суб’єкти 1 і 4). Хоча вони мають однакові права доступу і аналогічну роль в управлінні, у кожного з них є свій профіль та ідентифікатор для входу, так як у DAC кожен користувач має мати власний обліковий запис.

3.3 Поєднання дискреційного розмежування доступу з іншими засобами захисту інформації для підвищення стійкості ІС

Безперечно керування доступом функціонує, як один з засобів безпеки, контролює допуск осіб до певного об’єкту чи території, веде електронний облік відвідувачів та зберігає зібрану інформацію, додатково допомагає забезпечувати трудову дисципліну користувачів інформаційної системи, моніторить прихід/вхід в систему, а також вихід працівників, запобігає проникненню осіб, для яких доступ заборонено або обмежено [35].

Так як необхідно розуміти важливість використання систем контролю доступу до об’єктів, що потребують захисту, так само варто не переоцінювати їх можливості та критично підходити до оцінки рівня захищеності системи. Для побудови надійного захисту інформаційної системи цього недостатньо, потрібно звертатися до додаткових засобів захисту, а найкращим рішенням буде загалом побудова комплексної системи захисту інформації для цілого об’єкту з використання, в тому числі, систем контролю доступу.

Комплексна система захисту інформації – сукупність організаційних і інженерно-технічних заходів, які спрямовані на забезпечення захисту інформації від розголошення, витоку і несанкціонованого доступу [36].

Відповідно до чинного законодавства України і вимог окремих нормативних документів Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» [37] та Закону України «Про захист персональних даних» [38] обов'язковому захисту інформації підлягає: інформація, що є власністю держави, або інформація з обмеженим доступом, вимоги по захисту якої встановлені законом, в тому числі персональні дані громадян.

Якщо ж відповідно до законодавства у вашій системі не циркулює інформація, що визначена як така, що повинна бути захищена в обов’язковому порядку, і побудова КСЗІ не несе в собі серйозної практичної цінності, в такому випадку рекомендуємо створити власний комплекс з декількох засобів та заходів захисту інформації в інформаційній системі.

При використанні лише дискреційного керування доступом в системі невеликого розміру основну загрозу становить витік важливих даних, що спричинене забезпеченням гнучкості системи. Тому основною порадою для уникнення даних ризиків є використання DAC спільно з системою протидії витоку даних, тобто DLP-систем. Таким чином можна забезпечити наступні заходи [39]:

✓ контроль передачі інформації через Інтернет з використанням E-Mail, HTTP, HTTPS, FTP, Skype, ICQ та інших додатків та протоколів;

✓ контроль збереження інформації на зовнішні носії – CD, DVD, flash, мобільні телефони тощо;

✓ захист інформації від витоку шляхом контролю виведення даних на друк;

✓ блокування спроб пересилання/збереження конфіденційних даних, інформування адміністраторів ІБ про інциденти, створення тіньових копій, використання карантинної папки;

✓ пошук конфіденційної інформації на робочих станціях та файлових серверах за ключовими словами, мітками документів, атрибутами файлів та цифровими відбитками;

✓ запобігання витоку інформації шляхом контролю життєвого циклу та руху конфіденційних відомостей.

Як результат, ми отримаємо надійний контроль вибіркового контролю доступу, недоліки якого будуть перекриті використанням системи протидії витоку даних.

При використанні DAC важливо впевнитися, чи всі функції з захисту, які ви очікуєте, входять в пропозиції компанії-розробника. Якщо пакет запропонованих послуг досить вузький, необхідно додатково передбачити інтегрування до інформаційної системи засоби для резервного копіювання усіх даних, логування подій, не лише пов’язаних з контролем доступу, але й ведення будь-яких дій в системі, забезпечувати своєчасне та регулярне навчання персоналу з основ інформаційної та кібербезпеки для уникнення ненавмисних інцидентів, спричинених внутрішніми користувачами системи та проведення як зовнішніх, так і внутрішніх аудитів усієї інформаційної системи, системи захисту, та зокрема системи контролю доступу [40-42].

При встановленні дискреційної системи керування ще на етапі замовлення системи рекомендується визначитися з усіма тонкощами реалізації контролю та управління доступом користувачів до інформаційної системи, зрозуміти, як має проходити ідентифікація та автентифікація користувачів, як часто потрібно буде повторно оновлювати та перевіряти права окремих суб’єктів. Враховуючи сучасні тенденції доречним є використання обов’язкової двофакторної автентифікації, використовуючи, наприклад, окрім стандартних паролів чи токенів, другий фактор у вигляді біометричних даних, OTP (One Time Password) тощо [43, 44].

Якщо планується використання дискреційної моделі керування, але інформаційна система організації перевищує рекомендовані розміри та обмеження в кількості користувачів, теж є додатковий вихід. Можна розділити усю інформаційну систему на окремі підрозділи або створити різні віртуальні локальні мережі, і в кожному з них забезпечити функціонування окремої системи контролю доступу, визначити адміністраторів цих систем, які окремо будуть слідкувати за дотриманням всіх визначених пунктів політики безпеки у своєму підрозділі. Завдяки таким діям можна уникнути нагромадження матриць доступу або списків повноважень при збільшенні кількості користувачів в інформаційній системі [45].

Рекомендуємо не намагатися включити усі описані вище функції в саму систему дискретного керування доступом та вимагати від розробника додавання великої кількості можливостей безпосередньо на базі ресурсів системи контролю. Таким чином буде збільшуватися навантаження на ресурси системи керування доступом, що може спричините її регулярне виведення з ладу. Краще розглянути комбінування дискретної моделі контролю доступу з додатковими засобами, заходами та методами захисту, до того ж наведені вище рекомендації не є вичерпними. Можна обирати будь-які поєднання систем з забезпечення захисту інформаційної системи, опираючись на власні конкретні вимоги, але при цьому необхідно серйозно підходити до опису загальної політики безпеки та впевнитися, що обрані системи захисту доповнюють одна одну, а не створюють додаткові ризики та перевитрати.

Висновки за розділом 3

В ході даного розділу було викладено практичні напрацювання, що покроково супроводжують інтеграцію та підтримку системи дискреційного керування доступом в інформаційних системах. В першому пункті було описано рекомендації стосовно того, як краще підходити до вибору та підготовки до впровадження системи дискретного управління доступом, наведено опис вимог, які необхідно підготувати, перш ніж переходити до безпосереднього встановлення такої системи.

В другому пункті вже було змодельовано потенційну інформаційну систему, в якій для керування правами доступу за основу вибрана дискреційна модель. Програмний застосунок виконано у спрощеному вигляді для демонстрації саме процесу отримання доступу суб’єктів до конкретних об’єктів за алгоритмом дискреційної моделі.

В третьому ж пункті було наведено перелік рекомендацій щодо використання додаткових засобів захисту інформації спільно з дискреційним керуванням доступу для підвищення надійності та захищеності усієї інформаційної системи.

Отримані результати можуть бути корисними для невеликих або середніх організацій, що планують використовувати дискреційну систему керування доступом для підготовки наявної інформаційної системи до її впровадження.

ВИСНОВКИ

В ході проведеного дослідження було проаналізовано існуючі системи розмежування доступом. Було визначено, що система контролю доступу – сукупність програмно-апаратних, технічних засобів безпеки, які мають на меті обмеження та реєстрацію входу-виходу суб'єктів до заданих об’єктів через «точки входу»: двері, ворота, КПП, системи автентифікації тощо. Основне завдання таких систем – управління та контроль доступу до визначених ресурсів, а також ідентифікація осіб, що має відповідний доступ.

Також було проаналізовано та детально вивчено принципи роботи, побудову та механізми дискреційної моделі контролю доступу. Для підприємств малого та середнього бізнесу саме такі системи вважаються найбільш поширеними, враховуючи їх гнучкість, легкість впровадження та використання, нескладні принципи роботи.

При подальшому вивченні обраної теми було наведено критерії та вимоги, які необхідно скласти для правильного вибору системи керування доступом та її ефективного використанні. Ці вимоги включають призначення осіб, відповідальних за підтримку системи, визначення усіх наявних та потенційних точок входу, точне розуміння кількості потенційних користувачів системи, майбутня необхідність її масштабування, додаткові функції та інтеграції, які обов’язково хочеться бачити реалізованими в системі керування доступом, а також головне – рівень безпеки інформаційної системи.

Було розроблено та реалізовано спрощений програмний застосунок моделі інформаційної системи, робота якої побудована на принципах дискреційного розподілу прав доступу.

На завершення проведеного дослідження було створено загальні рекомендації стосовно поєднання дискреційної системи керування доступом з іншими існуючими засобами захисту інформаційних систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Foundational Security and Access Control Concepts [Electronic resource]: Thomas L. Norman CPP/PSP, Electronic Access Control (Second Edition), 2017 – Access: https://www.sciencedirect.com/topics/computer-science/access-control-system.

2. Central Alarm Stations and Dispatch Operations [Electronic resource]: Sean Smith, Rich Abrams, The Professional Protection Officer, 2010 – Access: https://www.sciencedirect.com/topics/computer-science/access-control-system.

3. Property Management [Electronic resource]: Lawrence J. Fennelly CPOI, CSSI, CHL-III, CSSP-1, Marianna A. Perry M.S., CPP, CSSP-1, Physical Security: 150 Things You Should Know (Second Edition), 2017 – Access: https://www.sciencedirect.com/topics/computer-science/access-control-system.

4. Central Alarm Stations and Dispatch Operations [Electronic resource]: Sean Smith, Rich Abrams, in The Professional Protection Officer, 2010 – Access: https://www.sciencedirect.com/topics/computer-science/access-control-system.

5. Access Control System Servers and Workstations [Electronic resource]: Thomas L. Norman CPP/PSP, Electronic Access Control (Second Edition), 2017 – Access: https://www.sciencedirect.com/topics/computer-science/access-control-system.

6. Domain 5: Identity and Access Management (Controlling Access and Managing Identity) [Electronic resource]: Eric Conrad, Joshua Feldman, in CISSP Study Guide (Third Edition), 2016 – Access: https://www.sciencedirect.com/topics/computer-science/access-control-system.

7. Марченко П.А., Методи розмежування доступу в розподілених системах кешування даних, Київ, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», 2018.

8. Розмежування доступу [Електронний ресурс]: StudFiles – Режим доступу: https://studfile.net/preview/5206324/page:3/.

9. Об`єкти та процедури їх системою контролю і управління доступом [Електронний ресурс] – Режим доступу: https://ua-

referat.com/%D0%9E%D0%B1%60%D1%94%D0%BA%D1%82%D0%B8_%D1%82%D0%B0_%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D0%B4%D1%83%D1%80%D0%B8_%D1%97%D1%85_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%BE%D1%8E_%D0%BA%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D1%8E_%D1%96_%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D1%96%D0%BD%D0%BD%D1%8F_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%BE%D0%BC.

10. 4 Types of Access Control [Electronic resource]: Four Walls Security Blog – Access: https://www.fourwallssecurity.com.au/blog/4-types-of-access-control.

11. С.Г. Семенов, В.М. Зміївська, А.В. Голубенко, Порівняльні дослідження технологій розмежування доступу для захисту даних в комп'ютерній системі, Харків, Національний технічний університет «Харківський політехнічний інститут», 2014.

12. Bell D.E. Unified Exposition and Multics Interpretation MITRE Corporation [Electronic resource]: Secure Computer System – Access: http://csrc.nist.gov/publications/history/bell76.pdf.

13. K. Biba, Biba K. Integrity Considerations for Secure Computer Systems, Technical Report MTR-3153, MITRE Corporation, Bedford, MA, 1977.

14. Role-based Access Control vs Attribute-based Access Control: How to Choose [Electronic resource]: Ekran – Access: https://www.ekransystem.com/en/blog/rbac-vs-abac.

15. Види політик безпеки [Електронний ресурс]: Helpiks.org – Режим доступу: https://helpiks.org/6-26932.html.

16. Що таке управління доступом на основі ролей в Azure (RBAC)? [Електронний ресурс]: Microsoft – Режим доступу: https://docs.microsoft.com/ru-ru/azure/role-based-access-control/overview.

17. Authorization and Access Control [Electronic resource]: Jason Andress, The Basics of Information Security (Second Edition), 2014– Access: https://www.sciencedirect.com/topics/computer-science/discretionary-access-control.

18. An analysis of security access control on healthcare records in the cloud [Electronic resource]: P. Chinnasamy, K. Shankar, Intelligent Data Security Solutions for e-Health Applications, 2020 – Access: https://www.sciencedirect.com/topics/computer-science/discretionary-access-control.

19. Introduction to General Security Concepts [Electronic resource]: Derrick Rountree, Security for Microsoft Windows System Administrators, 2011 – Access: https://www.sciencedirect.com/topics/computer-science/discretionary-access-control.

20. Mandatory Access Control vs Discretionary Access Control: Which to Choose? [Electronic resource]: Ekran – Access: https://www.ekransystem.com/en/blog/mac-vs-dac.

21. Discretionary Access Control [Electronic resource] – Access: https://www.cs.cornell.edu/courses/cs5430/2015sp/notes/dac.php.

22. Discretionary Access Control [Electronic resource]: Techopedia – Access: https://www.techopedia.com/definition/229/discretionary-access-control-dac.

23. What is Discretionary Access Control? [Electronic resource]: KISI blog – Access: https://www.getkisi.com/blog/discretionary-access-control-explained.

24. Discretionary Access Control (DAC) [Electronic resource]: Calder Security – Access: https://www.caldersecurity.co.uk/discretionary-access-control-dac/.

25. Discretionary Access Control: Uses, Advantages, Disadvantages & More [Electronic resource]: Secure Pass – Access: https://thesecurepass.com/blog/discretionary-access-control-system.

26. Discretionary Access Control [Electronic resource]: Firewall Times – Access: https://firewalltimes.com/discretionary-access-control/.

27. Do you need a DAC? [Electronic resource]: SoundGuys – Access: https://www.soundguys.com/do-you-need-a-dac-13488/.

28. Comparing Access Control: RBAC, MAC, DAC, RuBAC, ABAC [Electronic resource]: TechGenix – Access: https://techgenix.com/5-access-control-types-comparison/.

29. Access Control Models [Electronic resource]: UHWO Cyber Security – Access: https://westoahu.hawaii.edu/cyber/best-practices/best-practices-weekly-summaries/access-control/.

30. Why You Should Choose NGAC as Your Access Control Model [Electronic resource]: TheNewStack – Access: https://thenewstack.io/why-you-should-choose-ngac-as-your-access-control-model/.

31. Unpacking Next Generation Access Control (NGAC) [Electronic resource]: Tetrate – Access: https://www.tetrate.io/blog/unpacking-next-generation-access-control-ngac-and-tetrate-q/.

32. Alex Chiquito, Access Control Model for Time Series Databases using NGAC, Alex Chiquito, Ulf Bodin and Olov Schelen, Dept. of Computer Science, Electrical and Space Engineering Lulea University of Technology, Lulea, Sweden, 2020.

33. Захист комп'ютера від комп'ютерних атак [Електронний ресурс]: Studwood.net – Режим доступу: https://studwood.net/1586271/informatika/zaschita_kompyutera_kompyuternyh_atak .

34. Антонюк А. О., Політика безпеки інформації в захищених автоматизованих системах.

35. Системи контролю і управління доступом від А до Я [Електронний ресурс]: Deps – Режим доступу: https://deps.ua/ua/knowegable-base/reference-information/7824.html.

36. Що таке комплексна система захисту інформації (КСЗІ) [Електронний ресурс]: AlterSign – Режим доступу: http://altersign.com.ua/korysna-informacija/pobudova-kszi/shcho-take-kompleksna-systema-zahystu-informaciji-kszi.

37. Про захист інформації в інформаційно-комунікаційних системах [Електронний ресурс]: Закон України № 1089-IX від 16.12.2020. – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

38. Про захист персональних даних [Електронний ресурс]: Закон України № 5491-VI від 20.11.2012. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

39. Використання DLP-систем [Електронний ресурс]: TechExpert – Режим доступу: https://techexpert.ua/ru/our-services/implementation-of-dlp-systems/.

40. Захист даних за допомогою процесів резервного копіювання та відновлення [Електронний ресурс]: Microsoft – Режим доступу:

https://support.microsoft.com/uk-ua/office/%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82-%D0%B4%D0%B0%D0%BD%D0%B8%D1%85-%D0%B7%D0%B0-%D0%B4%D0%BE%D0%BF%D0%BE%D0%BC%D0%BE%D0%B3%D0%BE%D1%.

41. Що корисного можна знайти у системних логах [Електронний ресурс]: Велика база знань – Режим доступу: https://sfp.org.ua/shho-korisnogo-mozhna-znajti-u-sistemnix-logax/.

42. Аудит безпеки інформаційної безпеки [Електронний ресурс]: ТЗІ – Режим доступу: https://tzi.com.ua/audbezib.html.

43. Двофакторна аутентифікація для бізнесу: як захистити облікові записи співробітників [Електронний ресурс]: Eset – Режим доступу: https://eset.ua/ua/blog/view/22/dvukhfaktornaya-autentifikatsiya-chto-eto-i-kak-rabotayet.

44. OTP — Авторизація за допомогою одноразових паролів [Електронний ресурс]: MetaTrader5 – Режим доступу: https://www.metatrader5.com/ru/terminal/help/start_advanced/otp.

45. Virtual Local Area Networks (VLANs) [Electronic resource]: Practical Networing – Access: https://www.practicalnetworking.net/stand-alone/vlans/.

46. VLAN (virtual LAN) [Electronic resource]: Tech Target – Access: https://www.techtarget.com/searchnetworking/definition/virtual-LAN.

ДОДАТОК А

Лістинг MainForm.h:

```
public:
        MyForm^ form_access;

 private: System::Void dataGridView1_CellContentClick(System::Object^ sender, System::Windows::Forms::DataGridViewCellEventArgs^ e) {

 }
 private: System::Void button1_Click(System::Object^ sender, System::EventArgs^ e) {
        dataGridView1->ColumnCount = 3;
        dataGridView1->RowCount = 4;

        dataGridView1->Columns[0]->Name = "Об'єкт1";
        dataGridView1->Columns[1]->Name = "Об'єкт2";
        dataGridView1->Columns[2]->Name = "Об'єкт3";

        dataGridView1->Rows[0]->HeaderCell->Value = "Суб'єкт1";
        dataGridView1->Rows[1]->HeaderCell->Value = "Суб'єкт2";
        dataGridView1->Rows[2]->HeaderCell->Value = "Суб'єкт3";
        dataGridView1->Rows[3]->HeaderCell->Value = "Суб'єкт4";

        dataGridView1->Rows[0]->Cells[0]->Value = "+";
        dataGridView1->Rows[1]->Cells[1]->Value = "+";
        dataGridView1->Rows[2]->Cells[2]->Value = "+";
        dataGridView1->Rows[3]->Cells[0]->Value = "+";
 }
private: System::Void button3_Click(System::Object^ sender, System::EventArgs^ e)
{
  Application::Exit();
}
private: System::Void button2_Click(System::Object^ sender, System::EventArgs^ e)
{
 try {
        MyForm^ form_access = gcnew MyForm();
        form_access->ShowDialog();
 }
 catch (TimeoutException^ ex)
 {
        MessageBox::Show("Закінчився час виконання програми! Спробуйте повторно. ", "Помилка!", MessageBoxButtons::OK, MessageBoxIcon::Error);
```

```
    }

}
};
}
```

Лістинг MyForm.h:

```
public:
        MyForm1^ form1;
        MyForm2^ form2;
        MyForm3^ form3;

 private: System::Void button1_Click(System::Object^ sender, System::EventArgs^
e) {
        try {
                String^ x;

                MyForm1^ form1 = gcnew MyForm1();
                MyForm2^ form2 = gcnew MyForm2();
                MyForm3^ form3 = gcnew MyForm3();

                x = System::Convert::ToString(textBox1->Text);

                if (x == "5943674842651258") {
                        form1->ShowDialog();
                }
                else if (x == "6248512365852351") {
                        form2->ShowDialog();
                }
                else if (x == "1269852466985205") {
                        form3->ShowDialog();
                }
                else if (x == "9853612542380060") {
                        form1->ShowDialog();
                }
                else MessageBox::Show("Невизначений ідентифікатор!", "Помилка
введення. Спробуйте ще раз.", MessageBoxButtons::OK, MessageBoxIcon::Warning);
        }
        catch (UnauthorizedAccessException^ ex)
        {
                MessageBox::Show("Помилка авторизації! ", "Помилка!",
MessageBoxButtons::OK, MessageBoxIcon::Error);
        }
 }
 };
}
```

Лістинг MyForm1.h:

```
private: System::Void вихідToolStripMenuItem_Click(System::Object^ sender, System::EventArgs^ e) {
            Application::Exit();
 }
private: System::Void огерукAIToolStripMenuItem_Click(System::Object^ sender, System::EventArgs^ e) {
  label3->ForeColor = Color::Red;
  label4->ForeColor = Color::Black;
  label5->ForeColor = Color::Black;
  label6->ForeColor = Color::Black;
  label7->ForeColor = Color::Black;
}
private: System::Void зубчикВГToolStripMenuItem_Click(System::Object^ sender, System::EventArgs^ e) {
  label3->ForeColor = Color::Black;
  label4->ForeColor = Color::Red;
  label5->ForeColor = Color::Black;
  label6->ForeColor = Color::Black;
  label7->ForeColor = Color::Black;
}
private: System::Void вакулаНАToolStripMenuItem_Click(System::Object^ sender, System::EventArgs^ e) {
  label3->ForeColor = Color::Black;
  label4->ForeColor = Color::Black;
  label5->ForeColor = Color::Red;
  label6->ForeColor = Color::Black;
  label7->ForeColor = Color::Black;
}
private: System::Void кушнерукБЮToolStripMenuItem_Click(System::Object^ sender, System::EventArgs^ e) {
  label3->ForeColor = Color::Black;
  label4->ForeColor = Color::Black;
  label5->ForeColor = Color::Black;
  label6->ForeColor = Color::Red;
  label7->ForeColor = Color::Black;
}
private: System::Void костюкКРToolStripMenuItem_Click(System::Object^ sender, System::EventArgs^ e) {
  label3->ForeColor = Color::Black;
  label4->ForeColor = Color::Black;
  label5->ForeColor = Color::Black;
  label6->ForeColor = Color::Black;
  label7->ForeColor = Color::Red;
}
```

```
    private: System::Void button1_Click(System::Object^ sender, System::EventArgs^
e) {
            try {
                double x, y, z, sal;
                x = System::Convert::ToDouble(comboBox1->Text);
                y = System::Convert::ToDouble(textBox1->Text);
                z = System::Convert::ToDouble(textBox2->Text);

                money ob;
                sal = ob.salary(x, y, z);
                textBox3->Text = System::Convert::ToString(sal);
            }
            catch (Exception^ ex)
            {
                MessageBox::Show("Помилка при виконанні програми! ",
"Помилка!", MessageBoxButtons::OK, MessageBoxIcon::Error);
            }
            catch (FormatException^ ex)
            {
                MessageBox::Show("Помилка введених даних! Спробуйте ще раз.
", "Помилка!", MessageBoxButtons::OK, MessageBoxIcon::Error);
            }

    }

    private: System::Void зберегтиToolStripMenuItem_Click(System::Object^ sender,
System::EventArgs^ e) {
    try {
            saveFileDialog1->ShowDialog();
            if                  (saveFileDialog1->ShowDialog()                  ==
System::Windows::Forms::DialogResult::OK)
            {
                File::WriteAllText(saveFileDialog1->FileName, "Заробітна плата " +
textBox4->Text + ":\n" + textBox3->Text + " грн.");
            }
    }
    catch (InsufficientMemoryException^ ex)
    {
        MessageBox::Show("Переповнення пам'яті. Спробуйте ще раз. ",
"Помилка!", MessageBoxButtons::OK, MessageBoxIcon::Error);
    }

    }
```

Лістинг MyForm2.h:

```
    private: System::Void виглядToolStripMenuItem_Click(System::Object^ sender,
System::EventArgs^ e) {
     }
    private: System::Void label1_Click(System::Object^ sender, System::EventArgs^ e)
{
    }
    private: System::Void вихідToolStripMenuItem_Click(System::Object^ sender,
System::EventArgs^ e) {
     Application::Exit();
    }
    private: System::Void колірТекстуToolStripMenuItem_Click(System::Object^
sender, System::EventArgs^ e) {
     label3->ForeColor = Color::Red;
     label4->ForeColor = Color::Black;
     label5->ForeColor = Color::Black;
     label6->ForeColor = Color::Black;
     label7->ForeColor = Color::Black;
    }
    private: System::Void
заступникКерівникаToolStripMenuItem_Click(System::Object^ sender,
System::EventArgs^ e) {
     label3->ForeColor = Color::Black;
     label4->ForeColor = Color::Red;
     label5->ForeColor = Color::Black;
     label6->ForeColor = Color::Black;
     label7->ForeColor = Color::Black;
    }
    private: System::Void
провідний АдвокатToolStripMenuItem_Click(System::Object^ sender,
System::EventArgs^ e) {
     label3->ForeColor = Color::Black;
     label4->ForeColor = Color::Black;
     label5->ForeColor = Color::Red;
     label6->ForeColor = Color::Black;
     label7->ForeColor = Color::Black;
    }
    private: System::Void асистентАдвокатаToolStripMenuItem_Click(System::Object^
sender, System::EventArgs^ e) {
     label3->ForeColor = Color::Black;
     label4->ForeColor = Color::Black;
     label5->ForeColor = Color::Black;
     label6->ForeColor = Color::Red;
     label7->ForeColor = Color::Black;
    }
```

```
    private: System::Void адміністраторToolStripMenuItem_Click(System::Object^ sender, System::EventArgs^ e) {
        label3->ForeColor = Color::Black;
        label4->ForeColor = Color::Black;
        label5->ForeColor = Color::Black;
        label6->ForeColor = Color::Black;
        label7->ForeColor = Color::Red;
    }

    private: System::Void зберегтиToolStripMenuItem_Click(System::Object^ sender, System::EventArgs^ e) {
        saveFileDialog1->ShowDialog();
        if (saveFileDialog1->ShowDialog() == System::Windows::Forms::DialogResult::OK)
        {
            File::WriteAllText(saveFileDialog1->FileName, "Графік працівників: " + label3->Text + "\n" +  label4->Text + "\n" + label5->Text + "\n" + label6->Text + "\n" + label7->Text);
        }
    }
    };
    }
```

Лістинг MyForm3.h:

```
    private: System::Void label4_Click(System::Object^ sender, System::EventArgs^ e) {
        }
    private: System::Void вихідToolStripMenuItem_Click(System::Object^ sender, System::EventArgs^ e) {
        Application::Exit();
    }
    private: System::Void зберегтиToolStripMenuItem_Click(System::Object^ sender, System::EventArgs^ e) {
        saveFileDialog1->ShowDialog();
        if (saveFileDialog1->ShowDialog() == System::Windows::Forms::DialogResult::OK)
        {
            File::WriteAllText(saveFileDialog1->FileName, "Прайс послуг: " + label13->Text + "\n" + label14->Text + "\n" + label15->Text + "\n" + label16->Text + "\n" + label17->Text);
        }
    }
    private: System::Void понеділокToolStripMenuItem_Click(System::Object^ sender, System::EventArgs^ e) {
        textBox1->BackColor = Color::Yellow;
        textBox2->BackColor = Color::White;
```

```
  textBox3->BackColor = Color::White;
  textBox4->BackColor = Color::White;
  textBox5->BackColor = Color::White;
 }
 private: System::Void вівторокToolStripMenuItem_Click(System::Object^ sender, System::EventArgs^ e) {
  textBox1->BackColor = Color::White;
  textBox2->BackColor = Color::Yellow;
  textBox3->BackColor = Color::White;
  textBox4->BackColor = Color::White;
  textBox5->BackColor = Color::White;
 }
 private: System::Void середаToolStripMenuItem_Click(System::Object^ sender, System::EventArgs^ e) {
  textBox1->BackColor = Color::White;
  textBox2->BackColor = Color::White;
  textBox3->BackColor = Color::Yellow;
  textBox4->BackColor = Color::White;
  textBox5->BackColor = Color::White;
 }
 private: System::Void четверToolStripMenuItem_Click(System::Object^ sender, System::EventArgs^ e) {
  textBox1->BackColor = Color::White;
  textBox2->BackColor = Color::White;
  textBox3->BackColor = Color::White;
  textBox4->BackColor = Color::Yellow;
  textBox5->BackColor = Color::White;
 }
 private: System::Void пятницяToolStripMenuItem_Click(System::Object^ sender, System::EventArgs^ e) {
  textBox1->BackColor = Color::White;
  textBox2->BackColor = Color::White;
  textBox3->BackColor = Color::White;
  textBox4->BackColor = Color::White;
  textBox5->BackColor = Color::Yellow;
 }
 };
 }
```

Лістинг Header.h:

```
#pragma once

class  money {
public:
  double sum;
  double salary(double x, double y, double z);
```

```
};
```

Лістинг dopFile.cpp:

```
#include "Header.h"

double money::salary (double x, double y, double z){
  sum = (x * y) + 100 * z;
  return sum;
  }
```