МЕТОД ТА ЗАСІБ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ КОРПОРАТИВНИХ МЕРЕЖ

Доповідач: Ковальчук К. В.
Науковий керівник: к.т.н, доц.каф.ЗІ Баришев Ю. В.

Мета: покращення стану конфіденційності даних, що обробляються в корпоративній мережі.

Об’єктом дослідження є процес автентифікації користувачів.

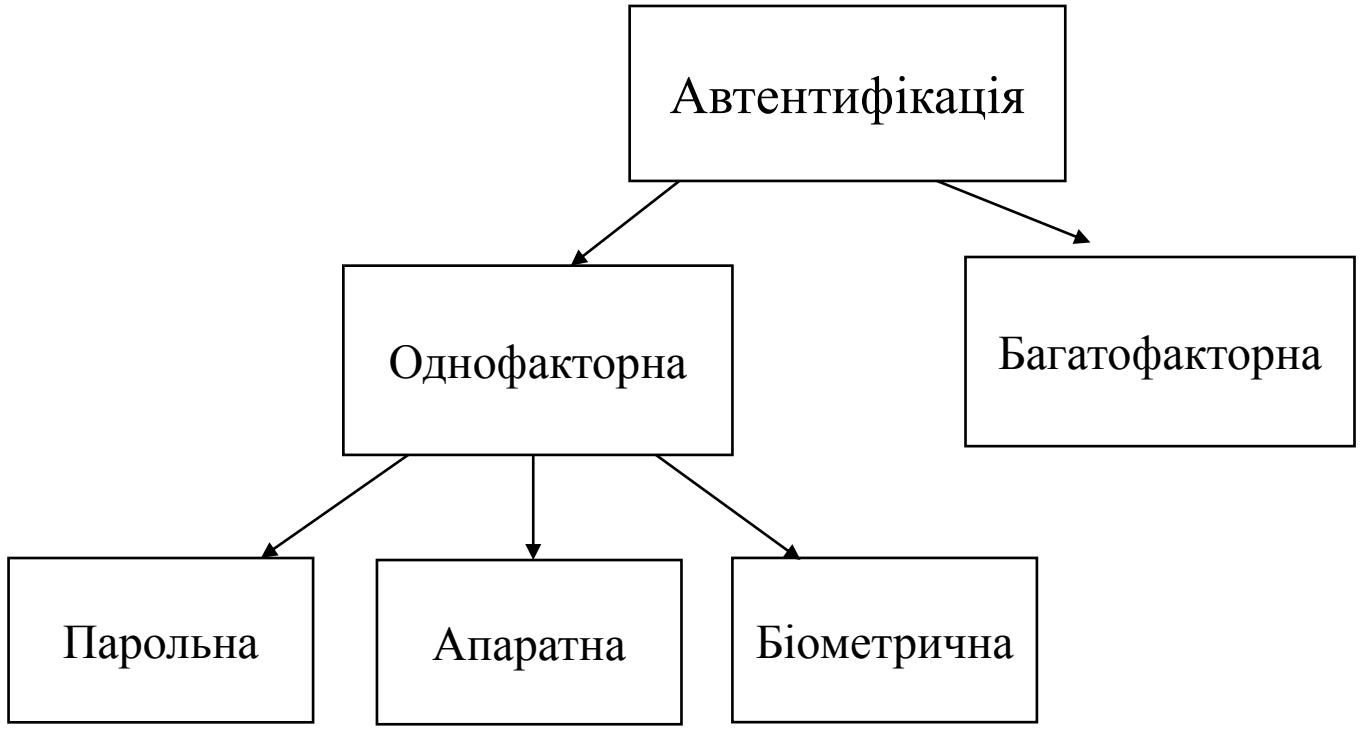
Предметом дослідження є механізми багатофакторної автентифікації з прив’язкою до робочих станцій.

Задачі:

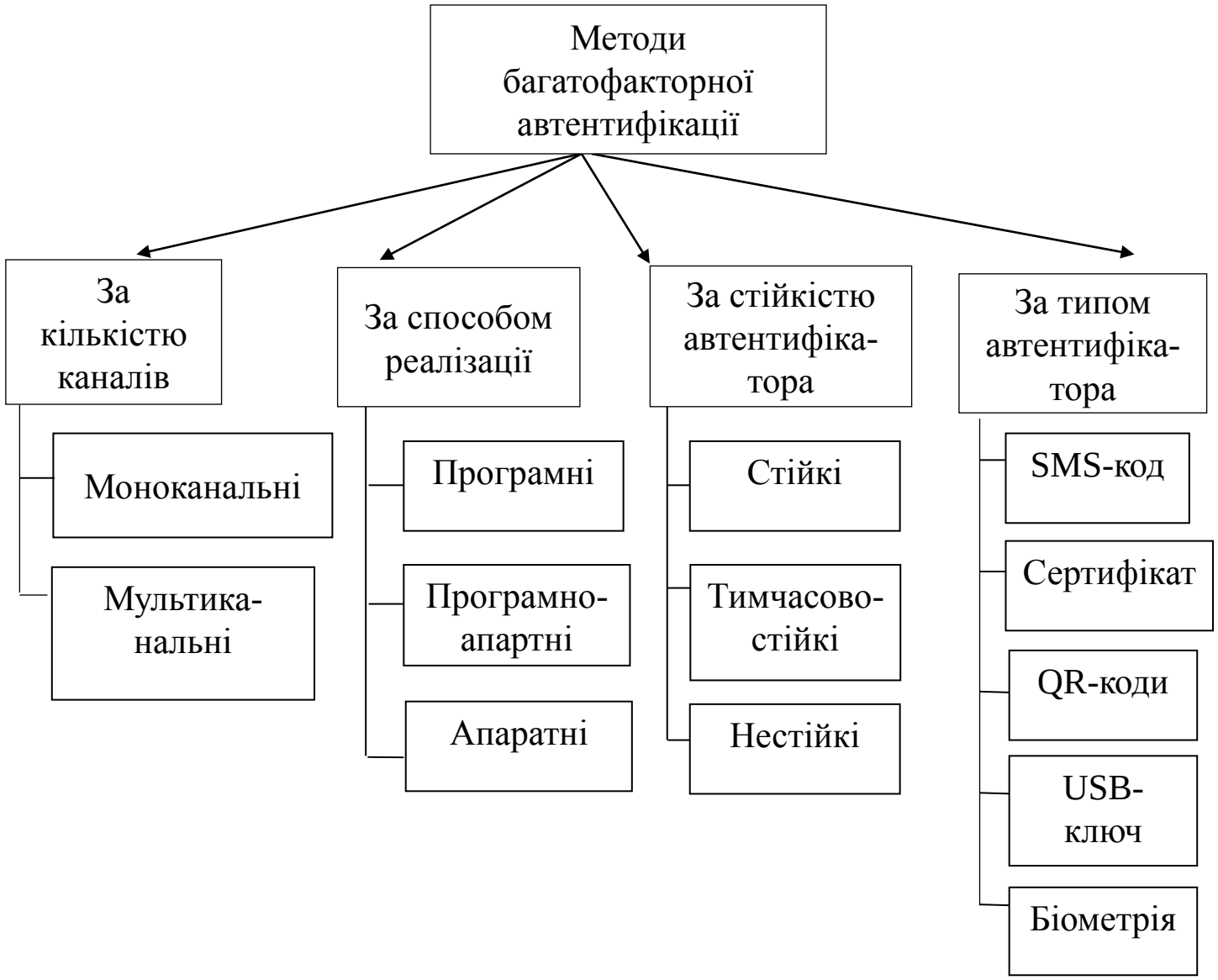
- здійснити аналіз засобів автентифікації;
- проаналізувати підходи до автентифікації користувачів та відомі методи і засоби автентифікації та атаки на них;
- визначити вимоги до автентифікації користувачів корпоративних мереж;
- виконати математичний опис процесу автентифікації;
- розробити метод автентифікації користувачів корпоративних мереж;
- реалізувати засіб розмежування прав доступу.

ПІДХОДИ ДО АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ

Методи автентифікації умовно можна поділити на: однофакторні (слабкі, з точки зору безпеки) та багатофакторні (сильні) .



КЛАСИФІКАЦІЯ МЕТОДІВ БАГАТОФАКТОРОНОЇ АВТЕНИТФІКАЦІЇ



ТЕХНОЛОГІЇ ВІДДАЛЕНОГО ДОСТУПУ

Параметри	Програмний засіб					
	Radmin	Ammyy Admin	UltraVNC	Team Viewer	Anyplace Control	Any Desk
Вид автентифікації	Однофакторна	Двохфакторна	Однофакторна	Двохфакторна	Одно-факторна	підключення до ПК без підтвердження на іншому боці
Одночасне керування декількома ПК	+	+	+	+	+	+
Можливість передачі даних між ПК	+	+	+	+	+	обмін даними, що містяться в буфері обміну
Вартість ПЗ	Безкоштовно	Demo-версія	Безкоштовно	Безкоштовно	$24.95	Безкоштовно

У сучасних серверних платформах реалізована підтримка наступних протоколів:

- протокол RADIUS (Remote Authentication Dial-In User Service);
- протокол EAP (Extensible Authentication Protocol);
- протокол CHAP (Challenge Handshake Authentication Protocol);
- протокол SPAP (Shiva Password Authentication Protocol);
- протокол SOAP (Simple Object Access Protocol);
- протокол PAP (Password Authentication Protocol)
- протокол SSL 3.0
- протокол S/MIME
- протокол Kerberos 5.0

АТАКИ НА МЕРЕЖЕВІ ПРОТОКОЛИ

Протоколи	Вразливі протоколи								
	PAP	CHAP	EAP	SOAP	SPAP	SSL	Radius	S/MIME	Kerberos
фішинг	+	+							
«людина посередині»	+	+	+			+			+
атака в області соціальної інженерії	+	+	+	+	+	+	+	+	+
«людина в браузері»	+								
атака повним перебором паролів користувачів	+	+	+	+					+
витік автентифікаційних даних	+	+	+	+	+	+	+	+	+
спостереження зі спини	+	+	+	+	+	+	+	+	+

РОЗПОДІЛЕНІ СХОВИЩА ДАНИХ

Характеристика	Storj	SIA	IPFS
Децентралізація сховищ	+	+	+
Створення декількох копій файлу в незалежних сховищах	+	+	+
Децентралізація процесу перевірки і відновлення копій	–	–	+
Шифрування приватним ключем, який є лише у власника	+	–	–
Можливість безкоштовного збереження даних	–	+	+
Анонімність	+	+	+

Дискреційна модель на основі матриці доступу при використанні запропонованого підходу зміниться таким чином: замість двовимірної матриці в оригінальному підході використовується трьохвимірна матриця :

$$|S| \times |O| \times |PC|$$

Де:

S – множина суб'єктів інформаційної системи;

O – множина об'єктів цієї системи;

PC – параметри робочих станцій (використовуваний суб'єктом інтсрументарій для отримання доступу).

МЕТОД АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ

Крок 1. Введення користувачем даних з робочої станції.

Крок 2. Читання параметрів робочої станції та дописування їх (конкатенація) до автентифікаційних даних користувача.

Крок 3. Гешування отриманих даних.

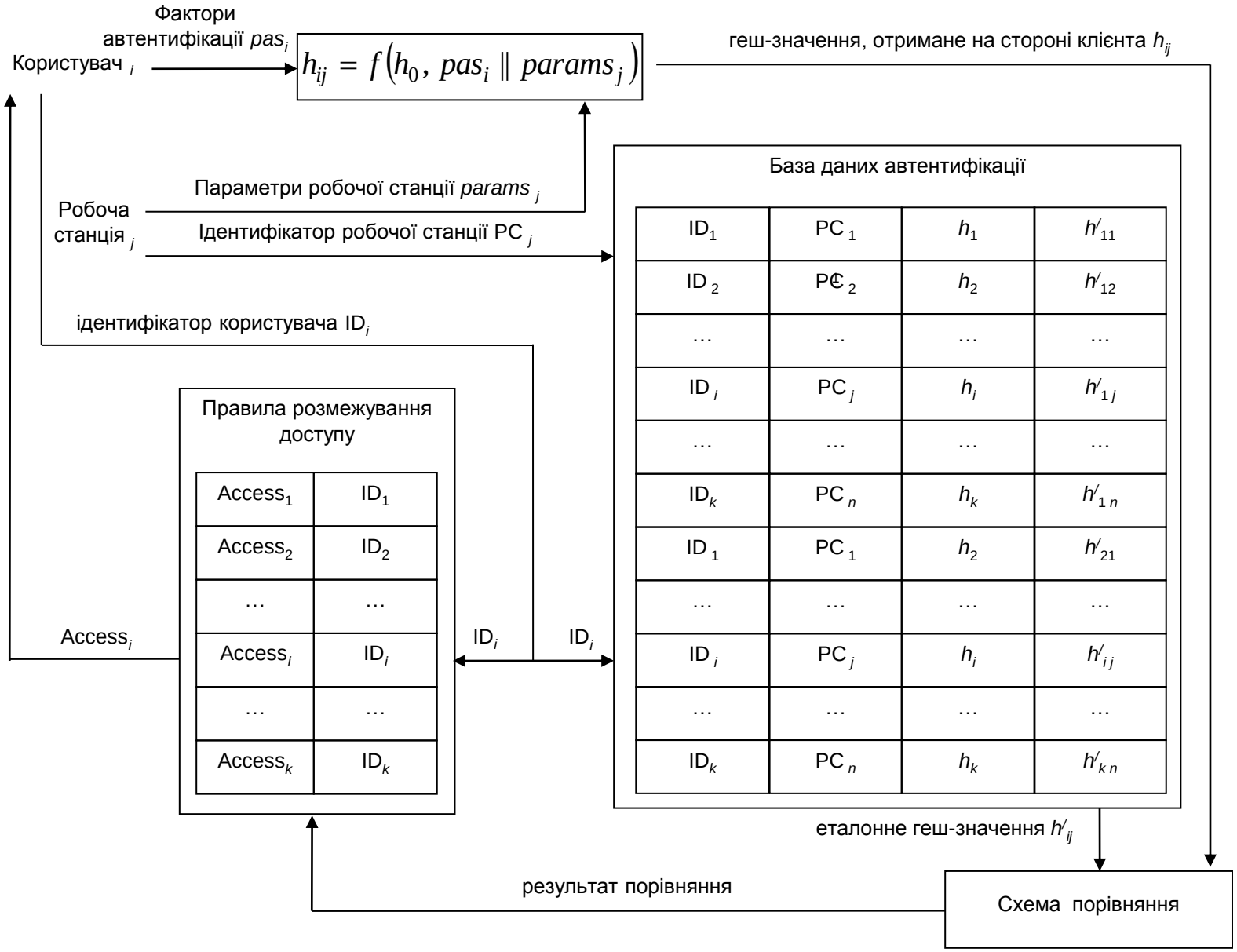
Крок 4. Надсилання геш-значення на сервер разом з ідентифікаторами користувача та робочої станції.

Крок 5. Перевірка наявності ідентифікаторів користувача та робочої станції, а також наявність дозволу у користувача здійснювати доступ до даних з цієї робочої станції.

Крок 6. Гешування параметрів робочої станції, що зберігаються у базі з використанням геш-значення автентифікаційних даних користувача як ключ.

Крок 7. Порівняння отриманого геш-значення з отриманим і надання/заборона доступу залежно від результату цього порівняння.

СХЕМА АВТОРИЗАЦІЇ КОРИСТУВАЧА



ВИБІР ФАКТОРІВ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧА

Існує декілька методів автентифікації, які відрізняються своєю складністю, надійністю, вартістю та іншими показниками:

- ✓ **парольна автентифікація;**
- ✓ **автентифікація за допомогою унікальних пасивних засобів;**
- ✓ автентифікація за допомогою унікальних активних засобів;
- ✓ біометричні методи автентифікації.

ВИБІР ФАКТОРІВ АВТЕНТИФІКАЦІЇ РОБОЧОЇ СТАНЦІЇ

Для автентифікації робочої станції пропонується використовувати комбінацію з декількох унікальних параметрів цієї станції. Прив'язка може відбуватися на основі таких характеристик комп'ютерної системи :

- ✓ **серійний номер носія постійної пам'яті;**
- ✓ **обсяг оперативної пам'яті;**
- ✓ **серійний номер, кількість ядер, частота процесора;**
- ✓ дата створення та контрольна сума BIOS;
- ✓ версії та властивості операційних систем;
- ✓ вміст системних файлів;
- ✓ продуктивність апаратури;
- ✓ наявність додаткових пристроїв.

СТРУКТУРА ПРОГРАМНОГО ЗАСОБУ

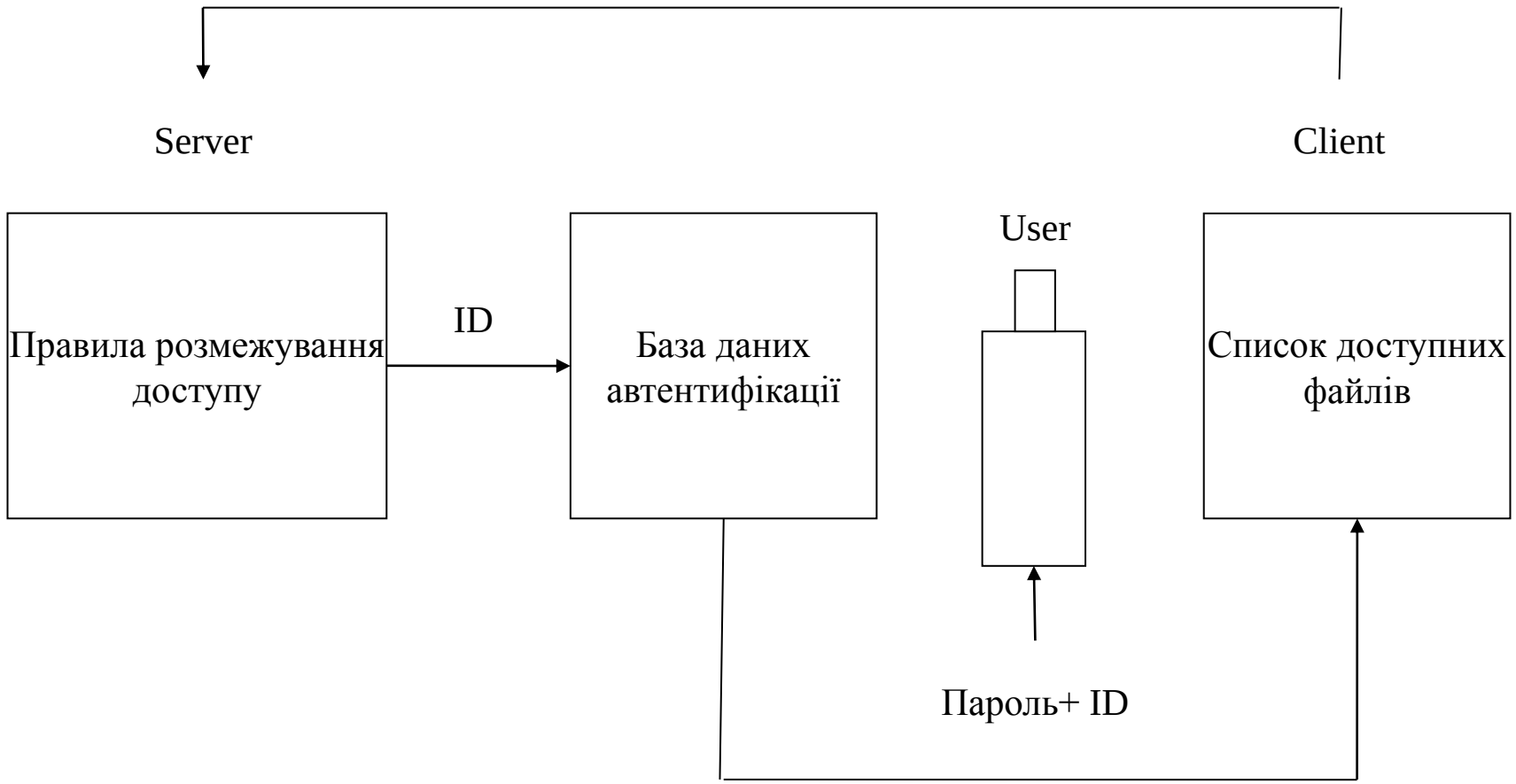


СХЕМА МОДУЛІВ ПРОГРАМНОГО ЗАСОБУ

СХЕМА ЗАСОБУ, ЩО РЕАЛІЗУЄ НАДАННЯ ДОСТУПУ ДО РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ НА СТОРОНІ СЕРВЕРА

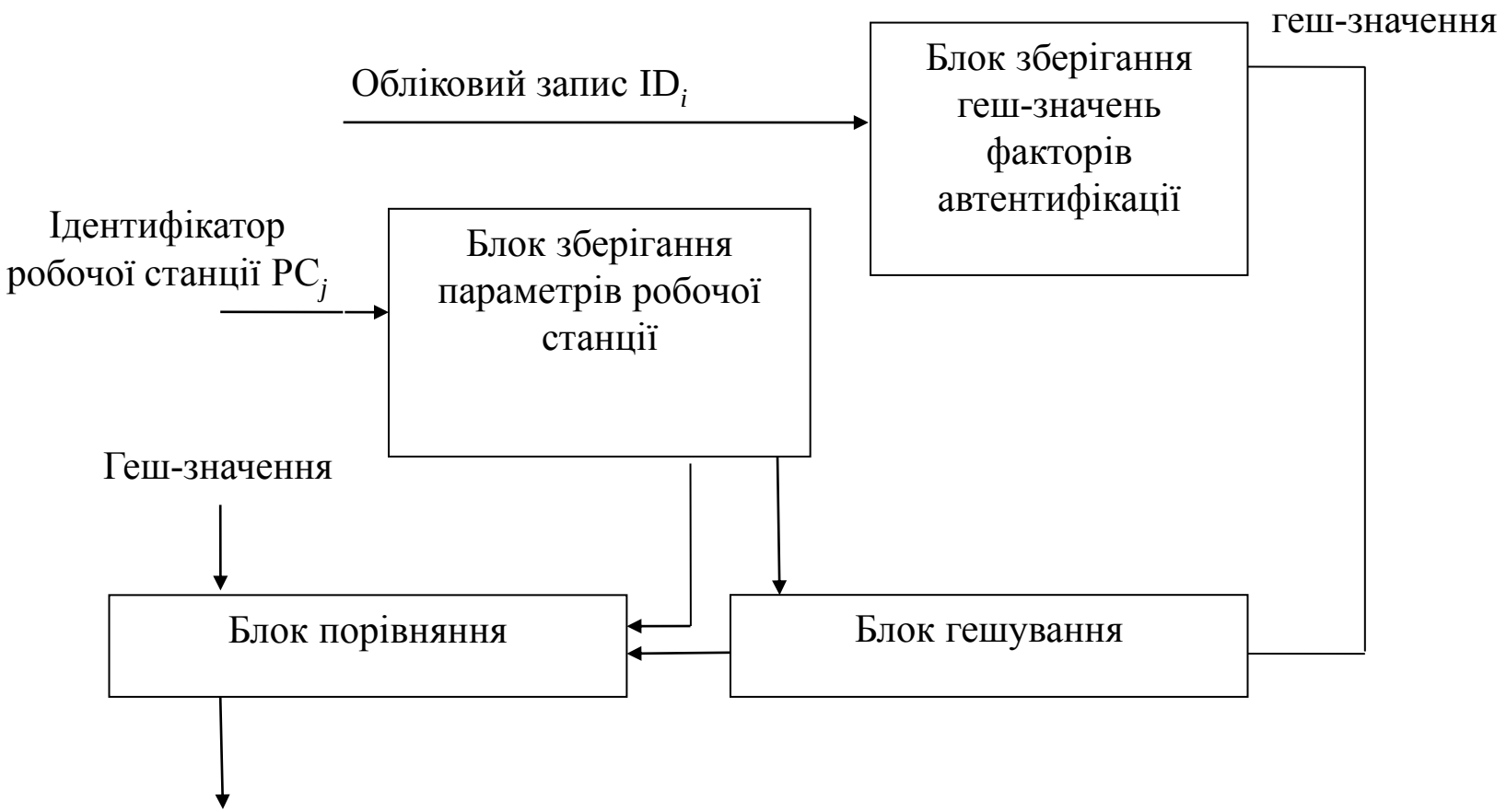
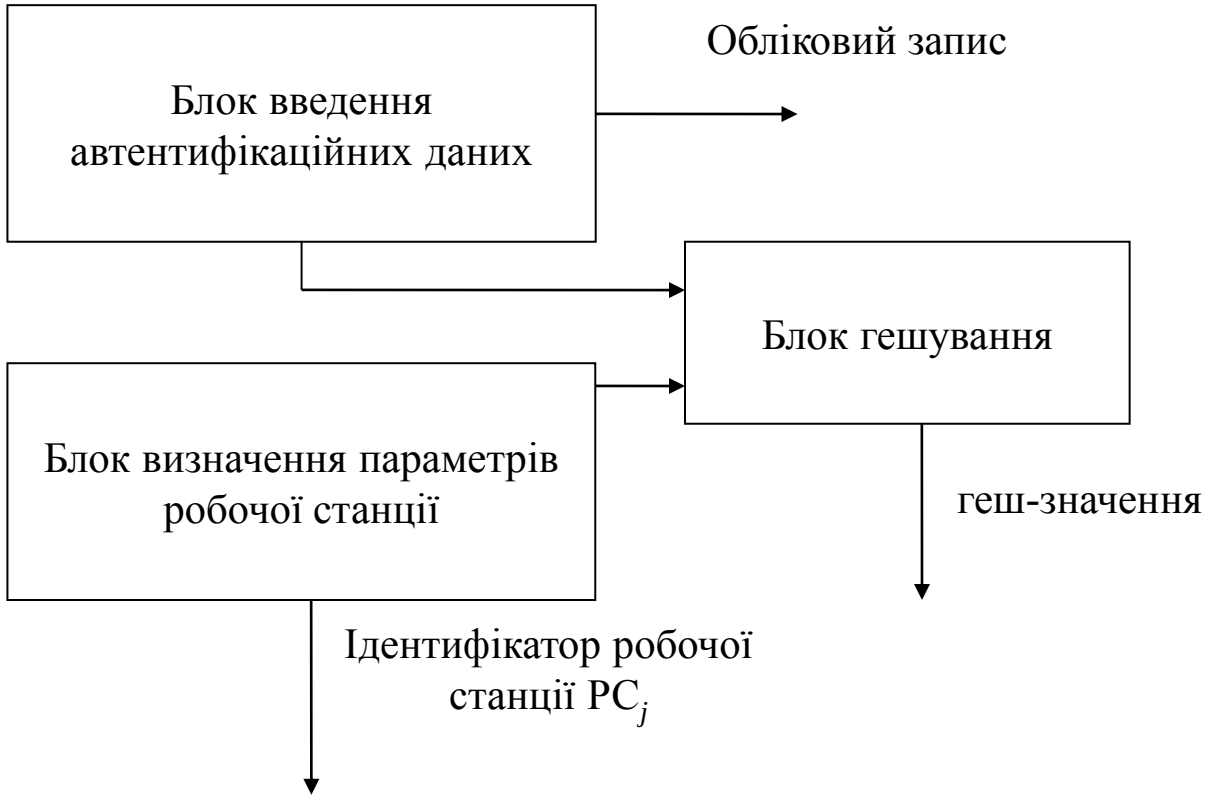
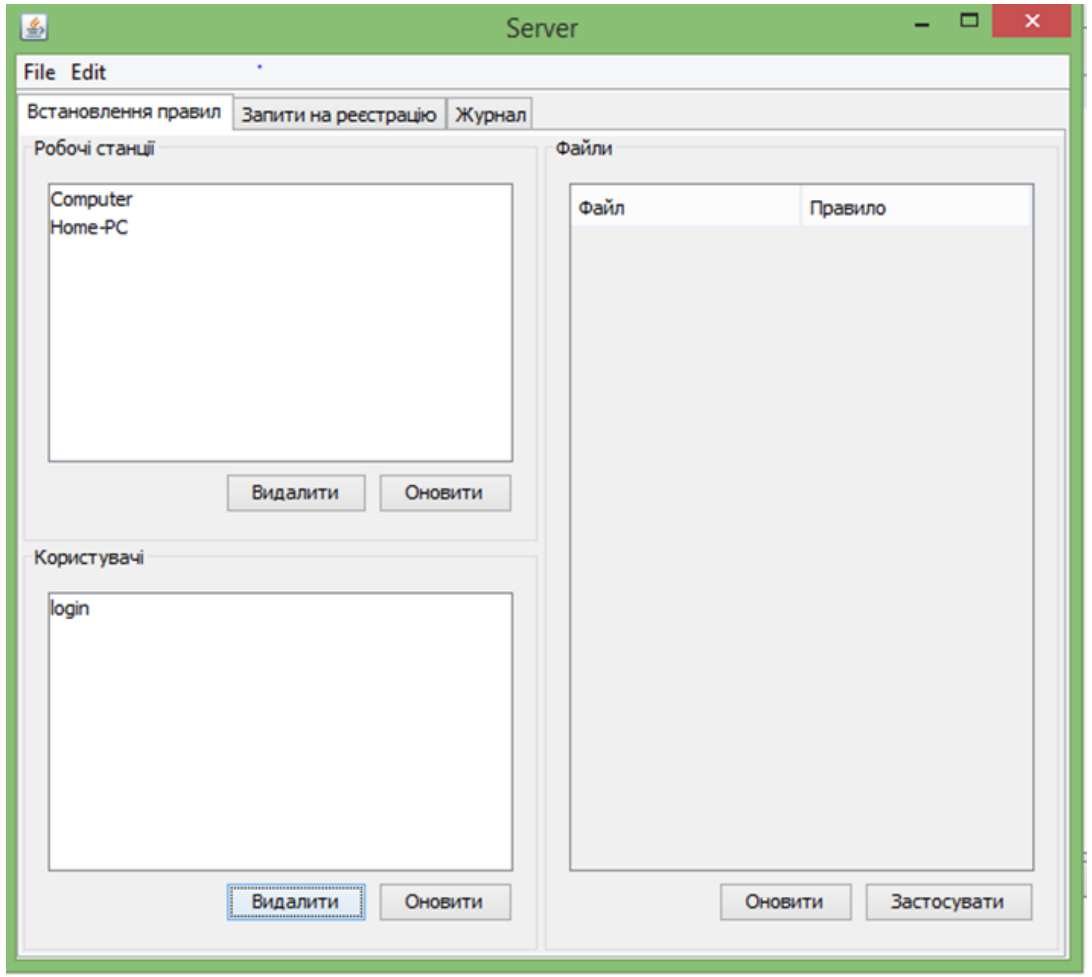
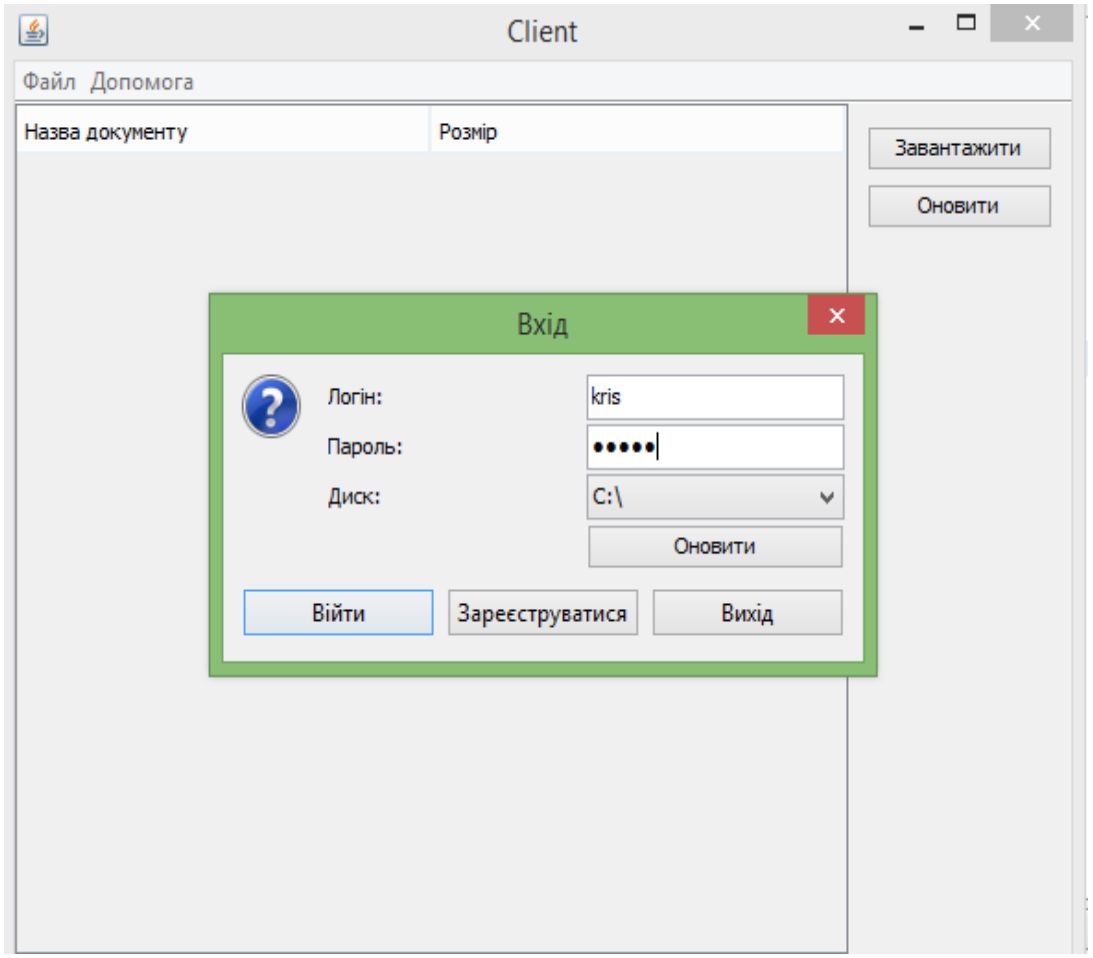


СХЕМА ЗАСОБУ, ЩО РЕАЛІЗУЄ НАДАННЯ ДОСТУПУ ДО РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ НА СТОРОНІ КЛІЄНТА



Програмний застосунок:





Абсолютна ефективність вкладених інвестицій рівна 320186,203 грн.,

- вкласти кошти у розробку програмного засобу є вигідніше, ніж покласти кошти на депозит, оскільки відносна ефективність наукової розробки становить 32,5%, що є вищим за мінімальну ставку дисконтування (25%), т
- термін окупності вкладених у реалізацію наукового проекту інвестицій складе 3 роки, що є менше 5-ти і вказує на швидку окупність вкладених інвестицій.

Крім того, розраховано, що наукова розробка приноситиме підприємству додатковий прибуток протягом 3-х років за рахунок покращення її якості порівняно з існуючими аналогами.

Наукова новизна одержаних результатів:

- Удосконалено метод автентифікації користувачів корпоративних мереж, який на відміну від існуючих здійснює прив’язку до параметрів робочої станції, що забезпечує обмеження допустимих робочих станцій, з яких користувач може отримати доступ до критичних даних;
- Здобула подальший розвиток модель дискреційного розмежування доступу користувачів, яка на відміну від відомих враховує ідентифікатори робочих станцій, з яких користувач може отримати доступ до критичних даних, що дозволяє збільшити гнучкість при розрозбці політики розмежування прав доступу.

Практичне значення магістерської кваліфікаційної роботи:

- Методика розробки моделей розмежування прав доступу, які враховують робочі станції як складову суб’єктів інформаційного обміну.
- Засіб розмежування прав доступу до файлів, що може бути використаний як елемент програмного забезпечення корпоративних мереж.

Результати Магістерської кваліфікаційної роботи апробовано на 3-ох конференціях:

- V Міжнародна науково-практична конференція «Методи та засоби кодування, захисту й ущільнення інформації»;
- Міжнародна науково-практична конференція «Інформаційні технології та комп’ютерне моделювання»;
- XLV Науково-технічна конференція підрозділів ВНТУ;
- XLVI Науково-технічна конференція підрозділів ВНТУ.

ЗА РЕЗУЛЬТАТАМИ МАГІСТЕРСЬКОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ ОПУБЛІКОВАНО:

- свідоцтво про реєстрацію авторського права на твір (комп'ютерну програму) № 69991 від 26.10.2016;
- патент на корисну модель «Спосіб автенифікації користувачів» (рішення №6112/ЗУ/17 від 14.03.2017);
- опубліковано статтю у фаховому журналі.

ДЯКУЮ ЗА УВАГУ!