УДК 004.056.52

Ю. В. Баришев, к. т. н.; В. А. Каплун; К. В. Неуйміна

ДИСКРЕЦІЙНА МОДЕЛЬ ТА МЕТОД РОЗМЕЖУВАННЯ ПРАВ ДОСТУПУ ДО РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

У роботі представлено аналіз моделей розмежування прав доступу. Запропоновано модель розмежування прав доступу, яка, використовуючи особливості процесу гешування, дозволяє обмежити перелік робочих станцій, із яких користувачеві дозволено отримувати віддалений доступ до інформаційних ресурсів. Обґрунтовано вибір факторів автентифікації для робочої станції та користувача, що дозволило розробити метод, який реалізує розмежування прав доступу відповідно до запропонованої моделі.

Ключові слова: *автентифікація, гешування, фактори автентифікації, модель розмежування прав доступу, параметри робочої станції.*

Вступ

Унаслідок наявності багатьох можливих джерел порушення безпеки інформації, які обробляють із використанням засобів обчислювальної техніки, зокрема персоналу, зловмисників, збоїв тощо [1], виникає задача забезпечення захищеності цієї інформації без істотного погіршення показників якості реалізації процесу її обробки. Одним із методів захисту, які використовують для розв'язання цієї задачі, є розмежування доступу користувачів комп'ютерної системи до наявних у системі інформаційних ресурсів [1, 2].

За умов обробки інформації з використанням робочих станцій підприємства, де працівники служби захисту інформації мають можливість створити безпечні умови обробки інформації, такий підхід цілком достатній. Однак із розвитком мобільних обчислювальних пристроїв та Інтернету речей (IoT) у легальних користувачів з'явилась можливість обробляти дані поза межами підприємства в умовах, які не сприяють збереженню конфіденційності інформації, яку обробляють. Відповідно постала актуальна задача розробки таких моделі та методу розмежування доступу, які запобігають обробці конфіденційних даних із використанням незахищених обчислювальних засобів.

Метою цього дослідження є покращення захисту конфіденційної інформації, яку надають користувачам із віддалених інформаційних ресурсів.

Для досягнення мети необхідно розв'язати такі задачі:

– аналіз відомих моделей розмежування прав доступу;

– розробка моделі розмежування прав доступу, що забезпечує використання захищених обчислювальних засобів для доступу до конфіденційної інформації;

– обґрунтування вибору факторів автентифікації користувачів для реалізації цієї моделі;

– розробка методу розмежування прав доступу до розподілених інформаційних ресурсів на основі розробленої моделі.

Аналіз відомих моделей розмежування прав доступу

Системи розмежування прав доступу здійснюють контроль за доступом суб'єктів інформаційної системи до об'єктів цієї системи. В основі будь-якої такої системи лежить модель розмежування прав доступу. Відомі моделі розмежування прав доступу поділяють на дискреційні, мандатні та рольові [1, 3, 4].

Дискреційна модель розмежування прав доступу передбачає, що права доступу суб'єктів до кожного окремого об'єкта системи можуть бути обмежені на основі деякого зовнішнього щодо системи правила [1, 3, 5].

Основним елементом дискреційного розмежування доступу є матриця доступу. Матриця

доступу – матриця D розміром $|S|\times|O|$, де S – множина суб'єктів інформаційної системи, а O – множина об'єктів цієї системи. Елемент матриці доступу $D[i, j]\subseteq R$ визначає права доступу і-го суб'єкта до *j*-го об'єкта (R – множина можливих прав доступу) [3 – 5].

Модель Харрісона – Руззо – Ульмана (модель HRU) є ще одним прикладом дискреційної моделі розмежування прав доступу. Модель HRU передбачає представлення системи розмежування прав доступу скінченним автоматом, який функціонує згідно з визначеними правилами переходу [3, 5].

Модель Take-Grant також є моделлю дискреційного розмежування прав доступу і представляє можливість аналізувати й перевіряти стан безпеки інформаційної системи. У моделі Take-Grant в якості основних елементів використовують граф доступу і його перетворення. Основним завданням моделі є визначення можливості одержання прав доступу суб'єктом системи до об'єкту, стан якого описано графом доступів. Формально опис моделі Take-Grant виглядає так [3, 5, 6]:

– множина об'єктів – O, де $o_j \in O$, $O=\{o_1,o_2,...,o_j\}$, $j\in N$;

– множина суб'єктів – S, де $s_i \in S$, $S=\{s_1,s_2,...,s_i\}$, $i\in N$;

– множина активних суб'єктів – $S\subseteq O$;

– множина прав доступу R, де $r_n \in R$, $R=\{r_1,r_2,...,r_n\}\cup\{t,g\}$, де $t(take)$ – право брати права доступу, $g(grant)$ – права надавати права доступу;

Використовуючи цю модель, можна передбачити стани, у яких буде перебувати інформаційна система залежно від розмежування прав доступу [5].

Перевагою дискреційних моделей розмежування прав доступу є очевидність реалізації системи розмежування доступу, універсальність і висока гнучкість. Проте основним недоліком є необхідність "ручного" адміністрування цих систем, а отже, збільшення впливу людського фактору на надійність системи захисту інформації, що використовує таку модель розмежування прав доступу.

Мандатна модель поєднує захист і обмеження прав, які використовують щодо комп'ютерних процесів, даних і системних пристроїв, та призначена для запобігання їх небажаному використанню [1 – 3, 5, 7].

На сьогодні найпоширенішим представником мандатних моделей розмежування прав доступу є модель Белла – ЛаПадула [3, 5, 8]. Ця модель гарантує, що суб'єкт може ознайомитися з інформацією лише тоді, коли має на це достатні повноваження, і будь-який суб'єкт, крім адміністратора, ніяким чином не зможе здійснити перенесення даних з об'єкта із вищим рівнем конфіденційності до об'єкта з нижчим рівнем конфіденційності. У моделі Белла – ЛаПадула за грифами секретності розподіляють об'єкти, наявні в інформаційній системі, та за рівнями секретності (мандатами) суб'єкти, що діють у цій системі. При цьому необхідно забезпечити виконання таких правил [3, 5]:

– суб'єкту певного рівня секретності заборонено виконувати операцію "читати" для об'єктів вищого рівня секретності (правило "no read up");

– суб'єкту певного рівня секретності заборонено виконувати операцію "записувати" для нижчого рівня секретності (правило "no write down").

Якщо користувач системи, який має високий рівень допуску, запише деякі дані в об'єкт із нижчим рівнем секретності, то вони можуть стати доступними суб'єкту з нижчим рівнем, ніж дозволено політикою безпеки, рівнем допуску.

Основним недоліком цієї моделі є висока складність її практичної реалізації засобами програмування, що породжує підвищенні вимоги до ресурсів обчислювальної системи за її імплементації.

Рольова модель (Role-Based Access Control – RBAC) передбачає керування доступом як на

основі матриці прав доступу для ролей, так і за допомогою правил, які регламентують призначення ролей користувачам [3, 4, 8]. У цій моделі комп'ютерна система представляється сукупністю таких множин [3, 5, 7]: множини користувачів U ; множини ролей R; множини повноважень P; множини сеансів C роботи користувачів із системою.

Множину повноважень P загалом задають за допомогою спеціальних механізмів, що об'єднують операції доступу та об'єкти доступу.

Перевагою такої моделі є те, що вона потребує менших витрат часу на своє адміністрування. Однак ця перевага здобувається за рахунок зменшення гнучкості моделі розмежування прав доступу порівняно з дискреційною. При цьому рольова модель гнучкіша за мандатну, відповідно має вищий потенціал щодо адаптації до потреб конкретної інформаційної системи. Отже, рольову модель із практичного погляду доцільно розглядати як компромісний варіант між мандатною та дискреційною. Це зумовлює широке використання рольової моделі, зокрема в операційних системах і в системах керування базами даних [3 – 5, 9].

Отже, із виконаного аналізу моделей розмежування доступу випливає, що вони мають один спільний недолік – не забезпечують обмеження робочих станцій, із яких користувач має право отримувати доступ. Останній недолік стає вагомим у системах розмежування доступу до розподілених інформаційних ресурсів, зокрема, файлових серверів і хмарних сервісів. Під час організації доступу до розподілених інформаційних ресурсів необхідно, щоб система розмежування доступу була максимально гнучкою. Саме тому в межах цього дослідження доцільно вдосконалювати дискреційні моделі розмежування прав доступу.

Модель розмежування прав доступу з прив'язкою до робочих станцій

Підхід до автентифікації користувачів, що враховує робочі станції, із яких ініціюється ця автентифікація користувача, може бути застосований для розробки моделей розмежування прав доступу. Зокрема дискреційна модель на основі матриці доступу за використання запропонованого підходу зміниться так: замість двовимірної матриці в оригінальному підході використовуємо тривимірну матрицю $|S|\times|O|\times|PC|,$ де PC – параметри робочих станцій (використовуваний суб'єктом інструментарій для отримання доступу). Така модель розмежування прав доступу вимагає спеціального методу автентифікації користувачів, тому пропонуємо для її реалізації підхід до організації захищеного доступу користувачів до мережевих сервісів, розглянутий у роботах [10 – 12]. На рис. 1 зображено схему авторизації користувача й робочої станції [10].

Особливістю авторизації користувачів за такої моделі розмежування прав доступу є те, що для захисту автентифікаційних даних повинна використовуватись ітеративна конструкція гешування. Наприклад, до таких конструкцій належать конструкції Меркля – Дамгаарда, HAIFA та $MPH_q(2;1;1;1;0)$ [13, 14]. Конструкцію Меркля – Дамгаарда вважають класичною і формалізують так [13]:

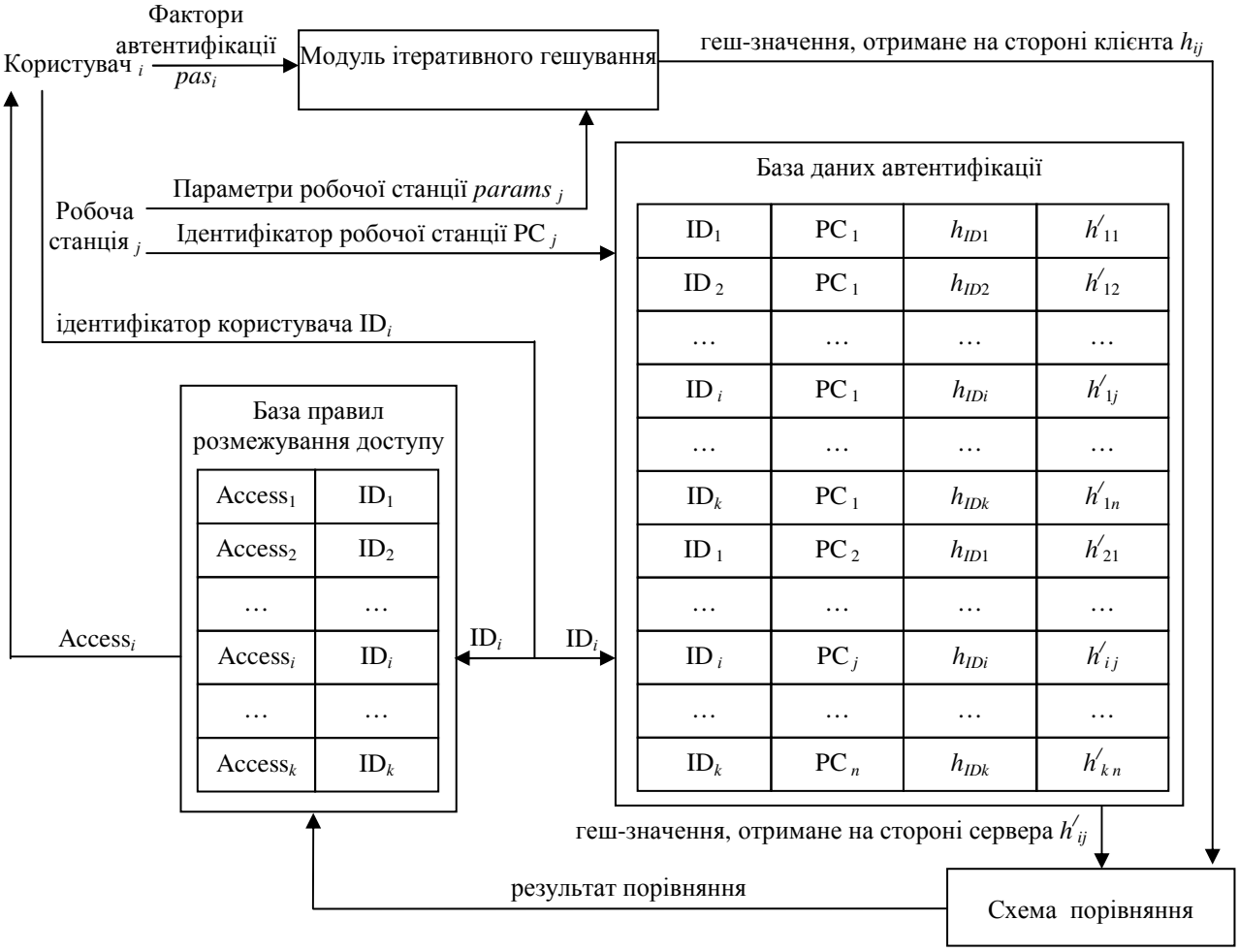
$$h_i = f(m_i, h_{i-1}), \tag{1}$$

де h_i – проміжне геш-значення, отримане на i-му кроці; m_i – i-й блок даних; $f(\cdot)$ – функція ущільнення, що забезпечує фіксовану довжину вихідного значення.

Удосконаленим варіантом конструкції Меркля – Дамгаарда, що дозволяє підвищити криптографічну стійкість до загальних атак за рахунок збільшення кількості обчислень, є конструкція HAIFA [13]:

$$h_i = f(m_i, h_{i-1}, \#bits_i, r), \tag{2}$$

де $\#bits_i$ – кількість уже загешованих бітів повідомлення; r – псевдовипадкове число (криптографічна сіль).



ID_1	PC_1	h_{ID1}	h'_{11}
ID_2	PC_1	h_{ID2}	h'_{12}
…	…	…	…
ID_i	PC_1	h_{IDi}	h'_{1j}
…	…	…	…
ID_k	PC_1	h_{IDk}	h'_{1n}
ID_1	PC_2	h_{ID1}	h'_{21}
…	…	…	…
ID_i	PC_j	h_{IDi}	h'_{ij}
…	…	…	…
ID_k	PC_n	h_{IDk}	h'_{kn}

Access$_1$	ID_1
Access$_2$	ID_2
…	…
Access$_i$	ID_i
…	…
Access$_k$	ID_k

Рис. 1. Схема авторизації користувача

Оскільки додаткові аргументи у функції ущільнення в конструкції (2) порівняно з конструкцією (1) призводять до збільшення навантаження на сервер, який виконує автентифікацію, пропонуємо використовувати геш-функції, що ґрунтуються на конструкціях багатоканального гешування $MPH_q(2;1;1;0)$ [14]:

$$\begin{cases} h_i^{(1)} = f^{(1)}\left(h_{i-1}^{(1)}, h_{i-1}^{(2)}, m_i, r_i^{(1)}, \#bits_i\right); \\ h_i^{(2)} = f^{(2)}\left(h_{i-1}^{(2)}, h_{i-1}^{(3)}, m_i, r_i^{(2)}, \#bits_i\right); \\ \ldots \\ h_i^{(q)} = f^{(q)}\left(h_{i-1}^{(q)}, h_{i-1}^{(1)}, m_i, r_i^{(q)}, \#bits_i\right). \end{cases} \tag{3}$$

Головною властивістю розглянутих вище конструкцій є те, що для гешування $(i+1)$-го блока даних достатньо знати проміжне геш-значення h_i, незалежно від того, як воно було отримане. Останнє робить можливим зберігання на стороні сервера результату гешування параметрів факторів автентифікації *i*-го користувача h_{IDi}, а не власне значення цих параметрів. Це забезпечує виконання такої рівності:

$$f\left(h_0, pas_i \,\|\, params_j\right) = f\left(f\left(h_0, pas_i\right), params_j\right), \tag{4}$$

де $h_{IDi} = f\left(h_0, pas_i\right)$.

Властивість, аналогічну (4), забезпечуватимуть розглянуті конструкції гешування за подальшого збільшення довжини повідомлення, якщо це збільшення буде кратним довжині блоку даних m_i.

Для зменшення навантаженості сервера пропонуємо виконувати процес гешування параметрів робочих станцій одразу після додавання відповідного правила до бази даних автентифікації і зберігання цього значення h_{ij} в базі, як це наведено на рис. 1. За рахунок властивості гешування, зумовленої використанням конструкцій (1) – (3), відбувається водночас автентифікація і користувача, і робочої станції перед наданням доступу до інформаційного ресурсу.

Таким чином розділяють властивості суб'єкта, за якими відбувається його автентифікація, на фактори, які автентифікують користувача, та фактори, які автентифікують його обчислювальні засоби. Для розробки методу необхідно визначити потенційні фактори автентифікації.

Обґрунтування вибору факторів автентифікації

Методи автентифікації умовно можна поділити на однофакторні та багатофакторні [1, 2, 4, 15], де під факторами розуміють властивість суб'єкта, за якою відбувається його автентифікація. При цьому однофакторні простіші для реалізації, однак забезпечують гірший рівень безпеки, що зумовлено меншою складністю їх підробки.

Парольна автентифікація є найпоширенішим простим і звичним методом, у якому як фактор автентифікації використовують знання користувачем певного секретного слова – паролю [1, 4, 5, 15]. Використання цього фактора автентифікації не висуває додаткових вимог до апаратної та програмної частини інформаційних ресурсів, однак часто виявляється нестійким унаслідок значного впливу людського фактора.

Відомі методи автентифікації, які передбачають використання унікальних засобів, що забезпечують більш стійкий захист, ніж парольна автентифікація. Такі фактори поділяють на дві групи: пасивні, які містять лише автентифікаційну інформацію, та активні, які мають певні обчислювальні ресурси і беруть участь у реалізації криптографічних протоколів автентифікації [1, 4, 15].

Автентифікація за допомогою унікальних засобів має низку недоліків: засіб може бути викрадений у користувача, необхідне додаткове апаратне/програмне забезпечення робочих станцій, можлива емуляція дії фактора.

Біометричні методи автентифікації ґрунтуються на використанні устаткування для вимірювання й порівняння з еталоном заданих індивідуальних характеристик користувача [4, 15]. Такі засоби дозволяють із високою точністю розпізнати власника за конкретною біометричною ознакою, а підробити такі параметри складніше порівняно з розглянутими вище. Суттєвий недолік біометричної автентифікації – необхідність додаткового обладнання кожної робочої станції пристроями для отримання біометричних характеристик.

Оскільки метою цього дослідження є покращення захисту конфіденційності інформації, пропонуємо використовувати багатофакторну автентифікацію користувачів, яка ґрунтується на знанні ним паролю та володінні пасивним унікальним засобом (флеш-носієм). Перший фактор дозволяє зменшити ризик несанкціонованого ознайомлення з інформацією внаслідок викрадення носія, а останній зменшує вплив людського фактора.

Для автентифікації робочої станції пропонуємо використовувати комбінацію з декількох унікальних параметрів цієї станції. Фактори автентифікації робочої станції використовують такі характеристики комп'ютерної системи [15]: властивості програмного забезпечення (системні файли, версію операційної системи, дату створення та контрольну суму BIOS, особливості файлової системи), властивості апаратного забезпечення (продуктивність, серійні номери основних елементів апаратного забезпечення, наявність додаткової

периферійної апаратури). Для цього дослідження обрано серійний номер жорсткого диску, дату створення та контрольну суму BIOS. Вибір цих факторів зумовлений їх порівняною сталістю та складністю прогнозування зловмисником їх значень.

У певних випадках для надання унікальності кожному з сеансів автентифікації пропонуємо до факторів автентифікації додавати криптографічну сіль – псевдовипадкові числа [4, 13, 14]. Цей захід дозволить уникнути атаки повторного передавання загешованих факторів автентифікації та приховати від зловмисників, що мають можливість аналізувати трафік, як автентифікаційні дані користувача, так і робочу станцію, за якою він працює.

Метод розмежування прав доступу до розподілених інформаційних ресурсів

Для реалізації методу пропонуємо структуру програмного засобу клієнт-серверної архітектури. Відповідно до методу розмежування прав доступу на стороні клієнта виконують такі дії:

– за допомогою модуля визначення факторів автентифікації користувача він уводить свої облікові дані – і відбувається визначення параметрів факторів авторизації (наприклад, пароля та параметрів флеш-носія);

– водночас відбувається визначення параметрів факторів автентифікації робочої станції (для задач цього дослідження – серійного номера жорсткого диску, дати створення та контрольної суми BIOS);

– за допомогою модуля ітеративного гешування на стороні клієнта отримують геш-значення від результату конкатенації значень параметрів факторів автентифікації користувача та робочої станції, а також криптографічної солі:

$$h_{ij} = f\left(h_0,\ pas_i \parallel params_j \parallel r\right); \tag{5}$$

– отриманий результат гешування, ідентифікатор робочої станції та обліковий запис користувача надсилають на сторону сервера.

На рис. 2 наведено структуру клієнтського застосунку для реалізації методу.

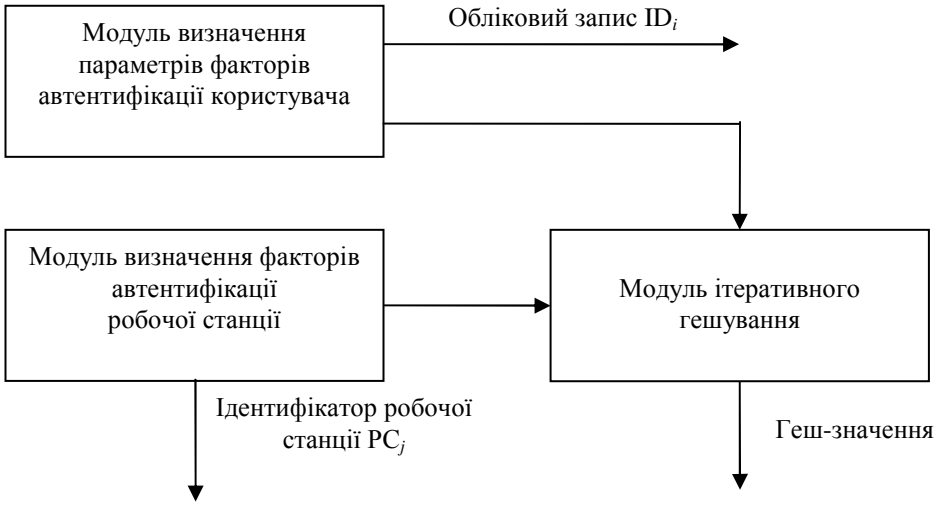


Рис. 2. Структура клієнтського застосунку для реалізації методу

Для реалізації методу на стороні сервера відбуваються такі дії:

– за отриманими від клієнта значеннями облікового запису користувача та ідентифікатора робочої станції визначають геш-значення факторів автентифікації користувача h_i та параметри робочої станції;

– відбувається гешування параметрів робочої станції та криптографічної солі:

$$h'_{ij} = f\left(h_i,\ params_j \parallel r\right); \tag{6}$$

– на основі порівняння обчисленого та отриманого геш-значень приймають рішення щодо дозволу або заборони доступу користувача.

На рис. 3 наведено структуру серверного застосунку, що взаємодіє з клієнтським застосунком.

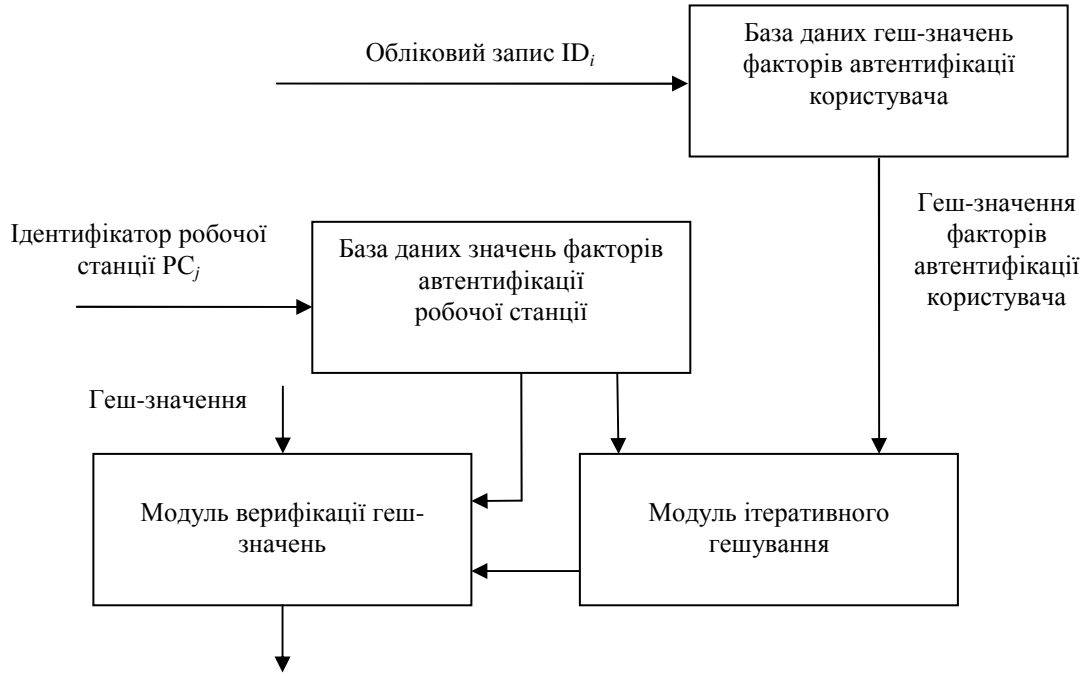


Рис. 3. Структура серверного застосунку для реалізації методу

Запропонований метод можна модифікувати шляхом попереднього обчислення геш-значень для всіх комбінацій {користувач; робоча станція}. Це дозволить зменшити завантаженість сервера, однак зробить недоцільним використання криптографічної солі, що зменшить стійкість методу до зламу.

Висновки

Виконаний аналіз моделей розмежування прав доступу виявив їх спрямованість на автентифікацію користувача. При цьому описані моделі не враховують робочу станцію, з якої авторизований користувач намагається отримати доступ. За умови розвитку мобільних обчислювальних засобів та IoT цей недолік породжує вразливість інформації, яку обробляють, оскільки зникають гарантії, що робоча станція на стороні клієнта має адекватну систему захисту інформації. Для усунення цього недоліку пропонуємо модель розмежування прав доступу, яка передбачає як обмеження користувачів, так і обмеження робочих станцій, із яких користувач може отримати інформацію. При цьому перелік робочих станцій пропонуємо обмежувати для кожного користувача окремо. Така модель не лише дозволяє забезпечити відповідний рівень захисту інформації під час її обробки користувачами, але й зменшити вразливість системи до атак інсайдерів, адже кожен працівник прив'язаний до свого робочого місця, що зменшує його можливості непомітної реалізації атаки.

Запропоновано фактори авторизації користувачів та робочої станції для реалізації цієї моделі. Розроблено структуру засобів розмежування прав доступу, що дозволило запропонувати метод, який реалізує розмежування прав доступу відповідно до моделі. Особливістю методу є використання ітеративного гешування, яке дозволяє без збереження

ключів гешування та факторів автентифікації користувача на стороні сервера виконувати одночасну автентифікацію і їх, і робочих станцій.

СПИСОК ЛІТЕРАТУРИ

1. Лужецький В. А. Основи інформаційної безпеки : навчальний посібник / В. А. Лужецький, А. Д. Кожухівський, О. П. Войтович. – Вінниця : ВНТУ, 2013. – 221 с.

2. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации : учебное пособие / А. А. Малюк. – М. : Горячая линия-Телеком, 2004. – 280 с.

3. Девянин П. Н. Модели безопасности компьютерных систем / П. Н. Девянин. – М. : Издательский центр "Академия", 2005. – 144 с.

4. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов / [А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов и др.] ; под ред. А. А. Шелупанова, С. Л. Груздева, Ю. С. Нахаева. – М. : Горячая линия-Телеком, 2009. – 552 с.

5. Цирлов В. Л. Основы информационной безопасности автоматизированных систем. Краткий курс / В. Л. Цирлов. – М. : Изд-во Феникс, 2008. – 174 с.

6. Миронова В. Г. Реализация модели Take-Grant как представление систем разграничения прав доступа в помещениях / В. Г. Миронова, А. А. Шелупанов, Н. Т. Югов // Доклады ТУСУРа. – 2011. – № 2 (24). – С. 206 – 210.

7. Теория и практика обеспечения информационной безопасности / [под ред. П. Д. Зегжды]. – М : Яхтсмен, 1996. – 302 с.

8. Жора В. В. Підхід до моделювання рольової політики безпеки / В. В. Жора // Правове нормативне та метрологічне забезпечення систем захисту інформації в Україні : інтернет журн. – 2003. – № 7. – С. 45 – 49.

9. Панасенко С. Методы аутентификации / С. Панасенко // Банки и технологии. – 2002 – № 3. – С. 56 – 60.

10. Баришев Ю. В. Метод автентифікації віддалених користувачів для мережевих сервісів / Ю. В. Баришев, В. А. Каплун // Інформаційні технологій та комп'ютерна інженерія. – 2014. – № 2. – С. 13 – 17.

11. Баришев Ю. В. Метод авторизації віддалених користувачів / Ю. В. Баришев, К. В. Неуйміна // Тези доповідей П'ятої Міжнародної науково-практичної конференції "Методи та засоби кодування, захисту й ущільнення інформації" м. Вінниця, 19-21 квітня 2016 року. – Вінниця : ВНТУ, 2016. – С. 65 – 67.

12. Баришев Ю. В. Метод та засіб автентифікації користувачів файлового серверу / Ю. В. Баришев, К. І. Кривешко // Праці IV Міжнародної науково-практичної конференції "Обробка сигналів і негауссівських процесів", присвяченої пам'яті професора Ю. П. Кунченка : Тези доповідей. – Черкаси : ЧДТУ, 2013. – С. 109 – 111.

13. Biham E. A Framework for Iterative Hash Functions: HAIFA [Електронний ресурс] / Eli Biham, Orr Dunkelman // Second cryptographic hash workshop. – 2006. – 9 с. – Режим доступу до ресурсу : http://csrc.nist.gov/groups/ST/hash/documents/DUNKELMAN_NIST3.pdf.

14. Баришев Ю. В. Методи та засоби швидкого багатоканального хешування даних в комп'ютерних системах. автореф. дис. на здобуття наук. ступеня канд. техн. наук : спец. 05.13.05 «Комп'ютерні системи та компоненти» / Ю. В. Баришев. – Вінниця : ВНТУ, 2012. – 20 с.

15. Дудатьєв А. В. Захист програмного забезпечення. Частина 1. Навчальний посібник / А. В. Дудатьєв, В. А. Каплун, С. П. Семеренко. – Вінниця : ВНТУ, 2005. – 140 с.

Баришев Юрій Володимирович — к. т. н., доцент кафедри захисту інформації, e-mail: yuriy.baryshev@gmail.com.

Каплун Валентина Аполінаріївна – старший викладач кафедри захисту інформації.

Неуйміна Крістіна Володимирівна — студентка кафедри захисту інформації, e-mail: kris.vladimirovna99@gmail.com.

Вінницький національний технічний університет.