УДК 004.9

ДОСЛІДЖЕННЯ МОДЕЛІ ДОСТУПУ ДО СОЦІАЛЬНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Б. В. Дурняк, Т. М. Хомета

Українська академія друкарства,
вул. Під Голоском, 19, Львів, 79020, Україна

Розглянуто модель доступу до соціальної інформаційної системи. В соціальній системі кожний інформаційний елемент є персоналізованим і реально пов'язаний з користувачами. Це означає, що засоби доступу повинні забезпечувати заданий рівень безпеки даних від моменту, коли такий запит активізується, до моменту завершення звернення. При такій інтерпретації уявлень про доступ модель доступу повинна охоплювати всі процедури, які реалізуються в системі під час виконання запиту користувача.

Ключові слова: *інтерпретація, блоки, динамічна структура, віртуальна матриця, повноваження, потоки, криптографічні алгоритми, міра безпеки, ідентифікація, автентифікація.*

Постановка проблеми. Використання динамічної структури *MD(CS)* полягає у тому, що структура, сформована до моменту активізації моделі доступу, може змінюватися в процесі функціонування самої моделі. Такі зміни можуть відбуватися на основі аналізу вихідних даних окремого блоку. Для реалізації такої структури в рамках моделі *MD(CS)* повинна існувати додаткова функція, яка проводить поточний аналіз результатів його роботи.

Аналіз останніх досліджень та публікацій: Моделі доступу до соціальних інформаційних систем досліджують вітчизняні та зарубіжні вчені — А. Л. Чмора, У. Блек, В. В. Навроцький, Ж. Г. Тардо, А. М. Аморозо, Д. П. Зегжда, О. Г. Корченко. Згадані фахівці здебільшого розглядають системи доступу в межах традиційних підходів до розв'язання цієї задачі. Проте часто не враховують особливості соціальних систем, до яких формуються відповідні засоби доступу. Це не дає змоги створити достатньо ефективні відповідні системи захисту доступу. Розділяючи систему доступу на окремі частини, одержуємо *MD(CS)* у сукупній послідовності окремих функцій, яка і відображає загальний процес функціонування *MD(CS)*.

Мета статті — дослідження моделі доступу соціальної інформаційної системи, в якій важлива не тільки ідентифікація потенційного користувача, а й перевірка його повноважень на виконання тих чи інших дій в межах *CS*.

Виклад основного матеріалу дослідження. У зв'язку з тим, що в системі типу *CS* кожний інформаційний елемент є персоналізованим і засоби доступу захищені, модель доступу повинна охоплювати всі процедури, які реалізуються в системі з моменту звертання до системи користувача і до моменту виводу відповідної послуги. Систему доступу розділимо на окремі частини:

– зовнішня частина системи доступу (*VSD*);
– встановлення функціональних повноважень (*FPK*);
– встановлення адекватності користувача щодо даних, які планує використати користувач *ADK*;
– контроль доступу в межах структурних переходів *SDD*;
– контроль процесу виводу даних із системи *KZD*;
– захист каналів зв'язку (*ZKZ*);
– контроль змін у системах після завершення надання послуги (*KVD*).

У загальному випадку модель системи доступу можна записати у вигляді співвідношення:

$$MD(CS) = F\,[VSD,\ FPK,\ ADK,\ SDD,\ KVD,\ ZKZ,\ KZD]. \qquad (1)$$

Один зі способів явного представлення полягає у тому, що останню формулу можна записати у вигляді:

$$MD(CS) = \{VSD \rightarrow FPK \rightarrow ADK \rightarrow SDD \rightarrow KVD \rightarrow ZKZ \rightarrow KZD\} \qquad (2)$$

Наведена формула відповідає інтерпретації моделі *MD(CS)* у вигляді послідовності окремих функцій, яка відображає процес функціонування *MD(CS)*. Очевидно, що можливі й інші реалізації функції *F*, до яких належать:

– відображення оберненого зв'язку між визначеними функціональними блоками;
– виконання інших послідовностей використання окремих функціональних блоків (*FB*);
– використання динамічної структури *MD(CS)*, яка відображає її залежність від результатів отриманих у межах попереднього блоку *FB*;
– повторення окремих блоків *FB* у загальній схемі реалізації моделі *MD(CS)*;
– виключення окремих блоків із загальної структури *MD(CS)*.

Наявність оберненого зв'язку між окремими блоками дає змогу підвищити ефективність функціонування *MD(CS)*. Наприклад, якщо в рамках блоку *ADK* виявилось, що міра адекватності даних, які планує отримати користувач, та даних про користувача не відповідає заданій величині, то функціонування *MD* переходить у фазу відмови обслуговування користувача. Крім обернених зв'язків між блоками, функція *F* може відображати різну послідовність використання блоків, яка наведена в (2), або повторення використання того самого функціонального блоку в процесі функціонування моделі *MD(CS)*.

Структура активізації моделі доступу може змінюватися в процесі функціонування самої моделі. Для реалізації такої структури в рамках моделі *MD(CS)* повинен бути управляючий блок, який проводить поточний аналіз результатів роботи активного блоку і залежно від результатів цього аналізу управління передається іншому блоку. У випадку, коли послідовність використання блоків може бути довільною, структура такого блоку відповідає повному графу [1]. Практично динамічна структура реалізується в рамках неповних графів, що з функціонального погляду здебільшого буває достатньо.

Зовнішня частина системи доступу реалізується стандартними засобами, оскільки в цьому разі йдеться про початкову ідентифікацію користувача незалежно від його намірів, можливостей та інших проявів, що можуть його ідентифікувати.

Як прийнято в теорії захисту, яка досить глибоко вивчає проблему ідентифікації та автентифікації, перевіряються порівняно прості ознаки, ким є користувач, що визначається за даними, ідентифікуючими відповідну особу, які подаються в документах ідентифікації. Потім проводиться перевірка, чи користувач є тим, ким він себе ідентифікував, для чого переважно використовуються персональні характеристики, наприклад біологічні параметри, прикладом яких є відбитки пальців. Перевіряється, чи користувач, про якого відомо, хто він і чи дійсно є тою особою, якою він ідентифікувався, має деякі індивідуальні або персональні можливості, які можна вважати такими, що характеризують його не тільки біологічно, а є також ознаками, які він отримав і не мав можливості самостійно їх змінити. Прикладом таких ознак може бути пароль, який отримав користувач у рамках системи захисту або який зашитий в карту чіпу, що є його власністю. Завдяки використанню теорії чисел, усі ці процедури можна формалізувати та подати у вигляді відповідних алгоритмів. Прикладом таких процедур може бути реалізація системи *SPX* [2]. Тому, не вдаючись в деталі її реалізації, вхідну або зовнішню частину засобів захисту доступу подамо у вигляді співвідношення:

$$VDS(CS) = F\,[Pr_1 * \ldots * Pr_k];$$

де Pr_i — процедура, яка описує фрагмент загального процесу автенифікації, використовуючи можливості теорії чисел та криптографічні алгоритми. Міра захищеності, яку забезпечують такі процедури, досить висока. Це означає, що сфальсифікувати процеси реалізації Pr_i, особливо ті, що ґрунтуються на криптографічних алгоритмах, досить важко, оскільки для їх зламання необхідно розв'язати математичні задачі, трудність розв'язання яких належить до задач *NP* складних. Прикладом таких задач є задачі факторизації, обчислення дискретного логарифма та інші важкі для розв'язання математичні проблеми.

Оцінювати міру безпеки $\mu(VSD)$ на основі важкості розв'язання зазначених проблем не зовсім коректно, оскільки здебільшого атаки на такі засоби захисту ґрунтуються на використанні факторів, що характеризують реалізацію такої системи, які не мають стосунку до проблем теоретичних, що лежать в основі відповідного захисту. Прикладом таких факторів може бути деяка можливість несанкціонованого використання ідентифікаторів легального користувача, несанкціонованого отримання даних про ключі шифрування та інше. Очевидно, що вплив цих факторів на $\mu(VSD)$ можна отримати переважно на основі даних про практичне використання таких систем.

Для інформаційної системи є важливою не тільки ідентифікація потенційного користувача, а й перевірка його повноважень на виконання певних дій в рамках *CS*. Перевірка відповідних повноважень здійснюється в рамках функцій *FPK*. Відомі моделі перевірки повноважень, які фактично контролюють доступ до тих чи інших дій з даними, ґрунтуються на використанні матриць повноважень *MAC*, динамічно модифікованих матриць *DAC* та уявлень про ролі [3]. У цьому випадку розширимо функцію надання повноважень додатковою ідентифікацією процесу, який активізований користувачем h_i. Для цього центральним елементом перевірки повноважень буде віртуальна матриця, яка заповнюється даними, що описують суб'єктів,

які звертаються за повноваженнями. Користувач, після його успішної ідентифікації функцією *VSD*, формує запит на певний тип повноваження, який залежить від типу перетворень, що передбачається здійснювати з відповідними даними. Такий оператор може бути використаний об'єктом h_i тільки тоді, коли система доступу надала суб'єкту h_i відповідні повноваження. Для надання повноваження h_i на використання перетворень або оператора q_i в рамках системи блоку *FPK* аналізується залежність між користувачем h_i, оператором q_i та іншими параметрами, які визначають можливість надання відповідних повноважень. Формально така залежність описується співвідношенням:

$$h_i = \varphi_i [q_i, I(h_i)],$$

де $I(h_i)$ — історія співпраці h_i з *CS*. Така історія являє собою ланцюг елементів типу $e_i [q_i, \lambda(h_i)]$, де e_i — ідентифікатор елемента історії користувача h_i в середовищі *CS*, що відображає повноваження, які використовував h_i, $\lambda(h_i)$ — опис залежностей між параметрами, що характеризують історію h_i та повноваження q_i. У загальному вигляді наша історія для h_i може описуватися співвідношенням:

$$I(h_i)=\{e_1 [h_i (q_i);(x_{1i}, \ldots, x_{1k})], \ldots, [e_n [h_i (q_i), (x_{n1}, \ldots, x_{nk})]]\}.$$

До таких параметрів, як x_{ij}, належать:

- відповідність повноважень s_i користувачу $V_i(h_i)$;
- рівномірність використання s_i користувачем $R_i(h_i)$;
- частота використання повноважень s_i користувачем $C(h_i)$;
- наслідки використання оператора q_i на попередніх етапах функціонування h_j в середовищі $CS,N(h_i)$;
- додаткові параметри історії функціонування h_i в $CS,D(h_i)$.

Параметр відповідності повноваження $s_i = \{q_1, \ldots, q_m\}$ користувача h_i, якого відповідно до прийнятої термінології, називають суб'єктом, визначається матрицею повноважень *MP*, яка містить відповідні значення величин відповідності. Така матриця заповнюється експертами. Відповідні міри, що містить *MP*, у процесі функціонування h_i в *CS* можуть мінятися залежно від інтерпретації результатів такого функціонування. Наприклад, дані, передані користувачу, були використані несанкціонованим способом. Очевидно, що всі зовнішні системи, в яких можуть використовуватися дані з *CS*, результати такого використання повинні передавати у систему *CS*. У наведеному прикладі міра відповідності користувача до використання певних повноважень буде зменшуватися. Правила зміни величини міри відповідності реалізуються з використанням системи правил та критеріїв, що містяться в *FPK*. Очевидно, що ці правила та критерії формуються на основі інтерпретації відповідних даних у предметній галузі, яку описує система *CS*.

Частота використання повноважень s_i суб'єктом h_i з погляду інтерпретації цього параметра повністю відповідає уявленням про частоту. Збільшення величини цього параметра набуває позитивного значення.

Параметр рівномірності використання повноваження з погляду його інтерпретації також є зрозумілим і, наприклад, з точки зору параметра частоти використання означає, що частота використання s_i об'єктом h_i міняється з постійною швидкістю протягом визначеного періоду використання *CS* користувачем h_i.

Параметр, який визначається як $N(h_i)$, означає, що в рамках *FPK* на основі даних, що надаються в CS_i із зовнішніх систем, проводиться аналіз наслідків, які мають негативну інтерпретацію в рамках відповідної зовнішньої системи CS_j. Очевидно, що цей параметр негативно впливає на процес рішення про надання повноважень s_i об'єкту h_i в поточний момент активізації останнім свого процесу функціонування в середовищі *CS*.

Додаткові параметри передбачаються в системі прийняття рішень, що реалізується в *FPK* у випадку, якщо такі параметри можуть привести до відмови у наданні повноважень s_i об'єкту h_i. Визначення таких параметрів формується на основі аналізу особливостей чи специфіки окремих CS_i. Додаткові параметри призначені для розширення аналізу, який проводиться в *FPK* і призначений для прийняття рішень про надання повноважень, які просить користувач для реалізації своїх задач у *CS*.

Система прийняття рішення про надання чи ненадання повноважень на використання операції, яку потребує h_i, використовує деяку логічну систему виводу, яка проводить аналіз наведених параметрів та матрицю *MP*. Залежно від вимог до захисту *CS* така система правил може розширюватися, якщо розширюється опис предметної галузі аналізу.

Частина системи захисту, яка перевіряє адекватність даних h_i, до яких h_i звертається, є досить важливою. Належність даних тому чи іншому користувачеві в процесі функціонування системи може мінятися. Це відбувається через те, що будь-яке перетворення даних може змінити їх сутність або інтерпретацію. Основною ознакою, за якою дані можуть належати або бути адекватними для h_i, є їхня інтерпретація, яка позначається $j(d_i)$. Якщо інтерпретація $j(d_i)$ змінюється на $j(d_k)$, то дані d_k, через те, що $j(d_i) \neq j(d_k)$, можуть уже не належати h_i, або d_k буде адекватне h_k. Введемо таке визначення.

Визначення 1. Користувач h_i, який отримав доступ до CS_i, є повноважним користувачем CS_i, або має місце співвідношення:

$$[(h_i \rightarrow CS_i) \,\&\, (h_i \in CS_i)] \rightarrow h_i\,[U(CS_i)].$$

Будемо повноваження h_i позначати записом $h_i^U\,(CS_i)$. Розглянемо твердження:

Твердження 1. Перетворення $f(d_i)$ в CS_i є коректне, якщо результат цього перетворення є адекватним або відповідним деякому користувачеві h_i системи *SC*.

Доведення. Припустимо, що $f(d_i) \rightarrow d_i^P$ і в CS_i не існує h_j такого, що $h_j \Rightarrow \mathrm{j}(d_i^P)$. Це означає, що $j(d_i^P) \notin I(V_i)$, де $I(V_i)$ — опис інтерпретації предметної галузі V_i, яку обслуговує CS_i. Тоді d_i^P є суперечним до V_i, що записується у вигляді: $f_i(d_i) \rightarrow [d_i^P \rightarrow [(d_i^P \in V_i) \vee \neg(d_i^P \,\&\, V_i)]]$. Це можливо в тому випадку, коли $f_i(d_i)$ є не коректне, що означає:

$$f_i(d_i) \rightarrow \neg[f_i(d_i) \,\&\, I(f_i)],$$

а це суперечить умові твердження.

Твердження 2. Якщо умова твердження 1 має місце, а в CS_i не існує $h_i^U\,(d_i^P)$, то це означає, що виконується така умова:

$$\{[f_i(d_i) \in CS_i\,] \rightarrow [j(d_i^P) \in I(V_i)]\} \rightarrow \forall\,(h_i \in I(V_i)\ \exists\ h_i\,[h_i\,(j(d_i^P))]). \qquad (3.2)$$

Доведення. Уважатимемо, що перетворення $f_i(d_i)$ є коректне згідно з твердженням (1). Це означає, що $f_i(d_i) \rightarrow d_i^P \in CS_i$. Приймемо, що не існує в CS_i такого h_j,

який адекватний d_i^P, або $\neg(h_i^P(d_i^P))$. Приймемо також, що умова (3.2) не виконується. Тоді не існує h_j [j(d_i^P)] в $I(V_i)$. З цього випливає, що $I(d_i^P) \notin I(V_i)$. Але $f_i(d_i) \in CS_i$, при цьому $\neg[j(d_i^P) \in I(V_i)]$. Оскільки $CS_i \in V_i$ за визначенням CS_i, то співвідношення $\neg[j(d_i^P) \in I(V_i)]$ приводить до суперечності, що і доводить твердження.

У рамках CS_i, в якій існує структура $S_i(CS_i)$, що визначає різні рівні захисту, можуть за певних умов виникати скриті канали передачі даних з одного фрагмента структури CS_{ik} з вищим рівнем захищеності до фрагмента CS_{ir} з нижчим рівнем захищеності в рамках системи надання повноважень. Наприклад, приймемо, що маємо два фрагменти даних з різними рівнями уповноважень. Такі фрагменти разом можуть створити скритий канал, який буде використовувати користувач h_i з низьким рівнем повноважень до зчитування інформації з процесу, що активізується користувачем h_i, який має вищий рівень повноважень. Обидва процеси можуть узгодити фрагмент пам'яті, або фрагмент даних CS_{ie}, як об'єкт, що є для них доступний. Об'єкт з низьким рівнем повноважень може записувати дані в CS_{ie}, а об'єкт з високим рівнем повноважень може їх зчитувати. Щоразу, коли h_j хоче переказати один елемент даних до h_i, і в цей момент пробує записати дані у відповідний об'єкт.

Дані, що належать h_i, можуть мінятися в процесі функціонування CS_i, яке активізується іншими h_j. Якщо $f_i(d_i) \rightarrow d_k$, то d_k уже не буде адекватне h_i, це означає, що h_i може втратити доступ до d_j. Зауважимо, що специфікою перетворень даних d_i в CS_i є те, що в результаті $f_i(d_i) \rightarrow d_j$, d_j складається з d_i та розширень δd_i, які виникають у результаті перетворень d_i. Прикладом цієї ситуації може бути наступне. Нехай CS_i є системою медичного обслуговування. Фрагмент CS_{ij}, адекватний h_i, являє собою сукупність даних обстеження. Якщо h_j є лікарем, який на основі даних обстеження формує діагноз, то цей діагноз являє собою розширення $\delta\, d_i$, яке здебільшого є недоступне для h_i.

Система CS_i сформується в рамках ієрархічної системи, оскільки така структура є характерною для соціальних систем. На кожному з рівнів ієрархії в межах окремих ланцюгів переходу від вершини до листків такої деревовидної структури можуть існувати окремі фрагменти даних $CS_{ij}(\omega_{ik})$, де ω_{ik} — ланцюг k у структурі i. Рівень ієрархії може визначати, крім залежностей між фрагментами CS_{ij}, рівень необхідного захисту окремих фрагментів даних CS_{ikj}, де k — ідентифікатор ланцюга, j — ідентифікатор рівня ієрархії. Очевидно, що рівень ієрархії та рівень міри захисту повинні бути узгодженими. Якщо маємо фрагмент CS_{ijk} і фрагмент CS_{ije}, то $k<e$ і рівень захисту $Z_k(CS_{ijk}) < Z_e(CS_{ije})$.

Розглянемо ще одне твердження, яке стосується соціальних систем CS_i та їх ієрархічних структур $S(CS_i)$.

Твердження 3. Якщо міра захищеності Z_i даних d_k є меншою від міри захищеності Z_j даних d_e, то має місце співвідношення: $j(d_e) \rightarrow j(d_k)$. Це означає, що в CS_i з інтерпретації $j(d_e)$ може бути виведена інтерпретація $j(d_k)$, якщо $(d_k \,\&\, d_e) \in \omega_i$, де ω_i є ланцюгом структури $S(CS_i)$.

Доведення. Особливістю CS_i є існування для даних системи CS залежностей між описами цих даних, або маємо, що $j(d_i) \rightarrow j(d_j)$. Таку залежність описує структу-

ра $S_i(CS_i)$. Приймемо, що $Z_i(d_k) > Z_j(d_j)$. Відповідно до уявлення про $I[S_i(CS_i)]$, існує поняття про рівні загальності опису даних d_i і d_j, які є різними та визначаються $S_i(CS_i)$. Міра загальності λ_i та λ_j визначається інтерпретаційними описами та $j(d_j)$. Тоді на основі прийнятого вище припущення можна записати:

$$\{\lambda_j [j(d_k)] \rightarrow \lambda_i [j(d_e)]\} \rightarrow [Z_i(d_k) < Z_j(d_e)],$$

що суперечить припущенню, прийнятому у доведенні, і таким чином доводить твердження.

Доведення цього твердження ґрунтується на використанні двох розглянутих нижче гіпотез.

Гіпотеза 1. З більш детального опису даних d_j можна вивести загальніший опис даних d_i, що можна записувати у вигляді співвідношення:

$$(d_j \rightarrow d_i) \rightarrow \lfloor j(d_j) \rightarrow j(d_i) \rfloor.$$

Гіпотеза 2. Більш загальний опис даних, або більш загальні дані d_i, можуть мати рівень захищеності Z_i, який є меншим від рівня захищеності Z_j детальніших даних, або $Z_i(d_i) < Z_j(d_j)$.

Потоки переміщення даних, пов'язаних з експлуатацією CS_i, можна розділити на такі класи:

- потоки переміщення даних в середині системи CS_i $P_v(CS_i)$;
- потоки переміщення даних між різними системами CS_i та CS_j, коли дані передаються по системних каналах зв'язку, або $P_s(CS_i, CS_j)$;
- потоки передачі даних користувачам системи $P_k(CS_i)$.

Потоки типу $P_v(CS_i)$ регулюються засобами надання повноважень суб'єктам на їх переміщення в середині системи.

Потоки типу $P_s(CS_i, CS_j)$ реалізуються в рамках методів захисту транзакцій, що використовуються в системах веб-серверів. До відомих засобів захисту транзакцій належать захищені протоколи IP_{sek}, *SSL*, *PVN* та інші [4].

Детальніше розглянемо потоки типу $P_k(CS_i)$, які з системи CS_i передаються через системи доступу користувачам. Повний цикл реалізації такого потоку складається з частин, до яких належать:

- запит користувача на обслуговування системою CS_i;
- визначення повноважень відповідного суб'єкта доступу до даних, по які звертається користувач;
- передача даних користувачу на вказаний останнім засіб приймання даних.

Перша частина запиту реалізується в рамках функцій *VSD* і всі процеси, пов'язані з захистом у цьому випадку, було розглянуто.

Друга частина, пов'язана з визначенням повноважень до виконання операцій з даними, реалізується в рамках функцій *FPK*, що також уже розглядалась.

Докладніше зупинимося на третій частині реалізації захисту користувача після надання йому інформації. На відміну від попередніх запитів λ_i, в цьому випадку повинно бути вказано тип кінцевого пристрою, на який передбачається приймати дані з системи CS_i. Основними типами зовнішніх пристроїв для приймання даних є [5]:

- обчислювальний пристрій, яким найчастіше може бути комп'ютер, або пристрій типу гаджет та інші;

– засоби відображення даних, до яких належать різного типу екрани або інші пристрої, які не дають можливості запам'ятовувати дані, а орієнтовані на відображення, незалежно від того, чи є в них власна пам'ять, чи її немає;
– засоби друкування, які відповідають вимогам, аналогічним до вимог для засобів відображення;
– засоби запам'ятовування даних, до яких належать автономні вінчестери, флеш-пам'ять чи *CD*-диски та інші засоби, що не забезпечують реалізації інших функцій, крім функцій, замовлених користувачем.

Очевидно, що зовнішній термінал системи CS_i реалізується на основі комп'ютера або спеціалізованого пристрою, який забезпечує замовлену функцію чи спосіб відбору користувачем відповідної інформації. Функція *KVD*, що реалізується в рамках *SB* системи CS_i, виконує такі дії:

– забезпечує взаємозв'язок з *VSD*, оскільки запит на передавання даних користувачу відразу активізує *KVD* на основі відповідних управляючих даних з *VSD*;
– забезпечує взаємозв'язок з *FPK*, оскільки *KVD* передає в *FPK* додаткові умови для прийняття рішення про надання повноважень користувачу h_i;
– реалізує процедуру контрольованого виводу даних, якщо всі кроки функціонування *KVD* виконані з успішним результатом.

Функція *KVD*, на відміну від *FPK*, у процесі обслуговування користувача активізує діалог системи з останнім. На відміну від *VSD*, який активізує відповідний діалог лише у випадку виникнення в ньому необхідності, блок *KVD* реалізує такий діалог як обов'язковий етап свого функціонування під час обслуговування h_i. Розглянемо детальніше окремі етапи функціонування *KVD*, до яких належать:

– активізація *KVD* по даних, що передаються з *VSD*;
– вступний діалог *KVD* з h_i за посередництвом *VSD*;
– активізація *FPK* та передача додаткових умов контролю запиту на отримання повноважень;
– функціональний діалог з h_i, який використовується для реалізації процесу передачі даних користувачу;
– завершення обслуговування h_i, яке пов'язане з наданням послуги виводу персональних даних за межі CS_i.

Вступний діалог *KVD* з h_i через *VSD* використовується для додаткового визначення міри необхідності здійснення відповідного процесу. Це пов'язано з тим, що CS_i стосується персональних даних, несанкціоноване використання яких може призводити до особистих втрат користувача. В рамках цього діалогу визначається така інформація:

– з якою метою користувач потребує персональних даних;
– протягом якого часу користувач планує використати чи використовувати отримані дані;
– наскільки терміново ці дані потрібні;
– якщо дані необхідні для вирішення певних справ, то чи є у h_i підтвердження третьої сторони про потребу їх використання та інші.

Висновки. Проаналізовано належність даних користувачеві, а також статус даних, що визначає правомірність надання йому цих даних. Показано, що в процесі функціонування системи статус окремих фрагментів цих даних може змінюватися, що зумовлює заборону надання відповідних фрагментів користувачу. Розроблено і обґрунтовано метод зміни статусу даних та умови їх зміни.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Зыков А. А. Основы теории графов / А. А. Зыков. — М. : Наука, 1987.
2. Чмора А. Л. Современная прикладная криптографія / А. Л. Чмора. — М. : Гелиос, 2002.
3. Смит Р. Э. Аутентификация: От паролей до открытых ключем / Р. Э. Смит. — М. : Издательский дом «Вильямс», 2002.
4. Блек У. Интернет: протоколы безопасности : учеб. курс / У. Блек. — СПб. : Питер, 2001.
5. Nawrocki W. Komputerowe systemy pomiarowe / W. Nawrocki. — W. : WKL, 2002.

REFERENCES

1. Zykov, A. (1987).Osnovy teorii grafov. Moscow: Nauka (in Russian).
2. Chmora, A. (2002).Sovremennaya prykladnaya kriptografiya. Moscow: Gelios (in Russian).
3. Smit, R. (2002).Autentifikaciya: Ot paroley do otkrytyh klyuchey. Moscow: Villiams (in Russian).
4. Bleck, U. (2001). Internet: protokoly bezopasnosti. S. Petersburg: SPB (in Russian).
5. Navrocki, W. (2002). Komputerowe systemy pomiarowe. Warchawa: WKL (in Polish).

RESEARCH OF MODEL OF ACCESS TO SOCIAL INFORMATION SYSTEM

B. V. Durniak, T. M. Khometa

Ukrainian Academy of Printing,
19, Pid Holoskom St., Lviv, 79020, Ukraine
taraskhometa@gmail.com

The model of access to the social information system has been examined. In the social system every information element is personalized and connected with users. It means that facilities of access must provide the set safety of information security from the moment when such query activates to the moment of completion of appeal. During such interpretation of pictures of access, the model of access must engulf all procedures which will be realized in the system at implementation of the user's query.

Keywords: *interpretation, blocks, dynamic structure, virtual matrix, plenary powers, streams, cryptographic algorithms, safety measure, identification, authentication.*

Стаття надійшла до редакції 19.02.2016.
Received 19.02.2016.