УДК 004.9.1

МЕТОДИ АДАПТАЦІЇ ПРОЦЕСІВ ЗАХИСТУ ДОСТУПУ КОРИСТУВАЧІВ ДО СОЦІАЛЬНИХ СИСТЕМ

Б. В. Дурняк, Т. М. Хомета

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

Розглянуто і розроблено методи адаптації системи доступу до користувача, який може виявитися не достатньо підготовленим до роботи з системою. Тому адаптація полягає в активізації системою доступу діалогу з користувачем. Діалог формується таким чином, щоб користувач отримав додаткову інформацію про способи спілкування із системою. Завдяки такій адаптації система стає доступнішою для звичайного користувача.

Ключові слова: *адаптація, система захисту доступу (SZD), система засобів захисту (SZZ), неоднорідність користувачів, односпрямований процес, діагностичний діалог, рівень підготовленості, модифікація, семантика.*

Постановка проблеми. Система доступу повинна адаптуватися до можливостей користувача, який має право доступу на отримання персональних даних. Така адаптація, крім інших задач, допомогає розв'язати задачу виявлення несанкціонованих користувачів. Завдяки цьому можливо протидіяти несанкціонованим спробам модифікації персональних даних або їх видалення із системи.

Аналіз останніх досліджень та публікацій. Досліджується задача захисту доступу, що стосується не тільки соціальних користувачів, персональні дані яких зберігаються в системі, але і користувачів, які є фахівцями в певній сфері обслуговування соціальних користувачів, наприклад лікарів. Подібні задачі досліджують фахівці в галузі захисту інформаційної системи, але відомі розв'язки ґрунтуються на ускладненні самих процедур доступу в результаті використання криптографічних алгоритмів чи нейронних мереж та ін.

Мета статті — дослідження методів адаптації процесів захисту доступу користувачів до соціальних систем.

Виклад основного матеріалу дослідження. Адаптація системи захисту доступу (*SZD*) до соціальної системи (*CS*) є необхідною характеристикою систем типу (*CS*) і має цілий ряд особливостей, що відрізняють її від інформаційних систем інших типів, що орієнтовані на розв'язання інших задач.

Особливості системи *CS*:

- параметри міри захищеності даних $\mu[D(CS)]$ системи є розподіленими в межах системи і можуть приймати в середовищі *CS* різні значення;
- значення параметра $\mu[D(CS)]$ може змінюватися динамічно, і такі зміни зумовлюються, як і інші фактори, також зовнішніми чинниками;

– система доступу до *CS*, як і засоби захисту доступу до *CS*, є неоднорідною та розподіленою в просторі;
– система засобів захисту (*SZZ*) являє собою окрему розподілену мережу, в якій, крім зв'язків з системою *CS*, існують зв'язки між окремими засобами захисту;
– мережа засобів системи доступу, крім контролю доступу до *CS*, розв'язує задачі контролю видачі даних та контролю послуг, що надаються в результаті звернення користувачів до системи *CS*.

З наведеного вище можна прийняти, що мережа засобів захисту *SZZ* є деяким бар'єром, який відділяє *CS* від зовнішнього оточення. Оскільки зовнішнє середовище $H(h_1, \ldots, h_n)$ являє собою певним чином організованих користувачів системи, то необхідність у реалізації адаптивних можливостей такої системи зумовлюється такими факторами:

– користувачі h_i системи *CS* є досить неоднорідні з погляду своєї підготовленості до використання системи;
– неоднорідність користувачів стосується також і їхніх намірів або цілей, з якими вони звертаються до системи;
– у процесі експлуатації системи окремі елементи системи доступу можуть виходити з ладу або з інших причин відмовляти користувачеві у доступі, але, незважаючи на це, доступ до системи повинен бути забезпечений;
– зміни, що відбуваються в середовищі *CS*, особливо ті, що стосуються рівнів захисту даних, можуть впливати на алгоритми, які реалізуються в середовищі мережі системи доступу, або системи *SZD*;
– оскільки до складу системи *CS* входить загальна система управління, необхідність в якій зумовлюється такими факторами:
– технічним обслуговуваннями системи;
– необхідністю управління зв'язками між системами CS_i і CS_j, які можуть бути системами різних типів;
– необхідністю керування мережею доступу *SZZ*, то керівні дії системи управління *SU* на *SZZ* можуть привести до змін в *SZZ*, які треба врахувати під час реалізації доступу до системи зі сторони користувачів, які мають різні рівні повноважень.

З огляду на те, що методи реалізації адаптації *SZZ* тісно пов'язані з причинами, які її зумовлюють, розглянемо кожну з причин детальніше.

Підготовка типового споживача до використання тієї, чи іншої інформаційної системи визначається мірою масовості поширення і, відповідно, використанням інформаційної системи (*IS*) та типами інших електронних інформаційно-комунікаційних засобів, що набули широкого розповсюдження у суспільстві. Одним з таких засобів є мобільний засіб зв'язку. Більшість мобільних телефонів, що масово використовуються, мають широкі функціональні можливості [1]. Тому використання мобільних телефонів для зв'язку з системою *CIS* є доцільним, оскільки в цьому випадку розв'язується задача реалізації фізичного доступу користувачів до системи доступу *CS*. Канали мобільного зв'язку є достатньо захищеними та відповідають прийнятим стандартам міри захищеності приватних даних. У такому разі регіо-

нальний пункт системи доступу до CS_i представляється у вигляді деякого абонента мобільної мережі зв'язку. Очевидно, що використання засобів безпеки каналів мобільного зв'язку, в їх стандартному вигляді, для мереж мобільного зв'язку не забезпечує необхідного захисту інформаційної системи. Особливість використання мобільного зв'язку для доступу до *CS* полягає у тому, що активізація такого зв'язку — це комунікація зі сторони користувача, яка реалізується голосовими повідомленнями і у крайньому разі — текстовими повідомленнями, що надходять зі сторони користувача у вигляді *SMS*-повідомлень. Комунікація зі сторони *SD* до *CS* також реалізується голосовим способом. Як і у випадку з користувачем, голосовий спосіб може замінятися на комунікацію за допомогою *SMS*-повідомлень.

Користувач, крім мобільних каналів зв'язку з *SD*, повинен мати можливість комунікувати із системою *CS* зі стаціонарних пунктів доступу, розміщених у відповідному регіоні. Передавання даних з *CS* до користувача може здійснюватися такими способами:

- дані можуть передаватися на адресу електронної пошти, яку вказав користувач;
- на записуючі пристрої регіонального пункту доступу до системи, яка відповідає регіону перебування користувача в момент запиту;
- на друкарські пристрої регіональних пунктів доступу до *CS*.

Позначимо рівень підготовки користувача h_i до отримання послуги з *CS* співвідношенням $P(h_i) = f(x_1, \ldots, x_n)$, де x_i — елемент, що використовується при реалізаціях доступу. Здебільшого процес реалізації доступу є послідовним. Це означає, що всі компоненти, які використовуються в процесі доступу, активізуються послідовно. Водночас у процесі аналізу чергової компоненти x_i можуть враховуватися результати використання попередніх компонент x_{i-k}. Процес реалізації доступу в поточний момент t_i, який відповідає використанню компоненти x_i, не може використовувати додатково елемент x_j, де $j > i$ і, відповідно, $t_i < t_j$. У цьому сенсі процес реалізації доступу є односпрямованим. Введемо наступне визначення.

Визначення 1. Односпрямованим процесом $P_r(x_1, \ldots, x_n)$ називається процес, для якого існує параметр синхронізації подій t_i, що разом складають процес, і подія, пов'язана з $x_j(t_j)$, не може бути активізована, якщо не активізована подія $x_i(t_i)$, де $j > i$ або $t_i < t_j$.

Визначення 2. Складним односпрямованим процесом $P_r^s(x_1, \ldots, x_n)$ називається такий процес, який полягає в активізації події $x_j(t_j)$, яка може бути зв'язана з подією $x_i(t_i)$, якщо $t_i < t_j$ або $j > i$ та має місце явна функціональна залежність типу $x_j = \varphi_j(x_i)$.

Рівень підготовленості користувача $\pi(h_i)$ визначається на основі використання односпрямованої функції процесу доступу $P_r(x_1, \ldots, x_n)$. Завдяки односпрямованості функції доступу, яку можна представити у вигляді $P_r(SD)$, процес доступу являтиме послідовність подій, або $\{x_1, \ldots, x_n\}$. Подія x_i є елементом діалогу, який будемо позначати $x_i^P = (h_i \rightarrow SD) \rightarrow (SD \rightarrow h_i)$. Якщо ця компонента записана у вигляді $x_i^N = (SD \rightarrow h_i) \rightarrow (h_i \rightarrow SD)$, то така компонента означає крок діалогу, до якого користувач не підготовлений. Елемент x_i^P визначає, що h_i підготовлений до кроку x_i. Очевидно, що $x_i^N = x_1$. Якщо функція $P_r(x_1, \ldots, x_n)$ є відомою, то на її основі можна визначати рівень підготовленості або непідготовленості h_i до отримання послуги h_i.

Визначення 3. Рівень підготовленості h_i до реалізації процесу $P_r(SD)$ визначається кількістю компонент типу x_i^P, що формально описується співвідношенням:

$$\pi(h_i) = \sum_{i=1}^{m} x_i^P; \neg\pi(h_i) = \sum_{i=1}^{n-m} x_i^N.$$

Можна прийняти й інші інтерпретації рівня підготовленості та непідготовленості h_i. Наприклад, якщо h_i передає до *SD* дані, які не відповідають заданим в *SD* інтерпретаціям. Ця ситуація може відповідати таким випадкам:

– користувач h_i є несанкціонованим і не має необхідних даних для реалізації доступу;
– користувач не підготовлений до реалізації кроку діалогу, що відповідає елементу x_i.

Система захисту доступу повинна розпізнавати наведені ситуації. Припустимо, що наявний другий випадок, тоді формально відповідний крок діалогу запишемо у вигляді:

$$[(x_i \rightarrow SD) \rightarrow \neg(SD \rightarrow x_i)] \rightarrow \{[(SD \rightarrow h_i(x_i)) \rightarrow (h_i(x_i)) \rightarrow SD]\},$$

де h_i — визначено як санкціонованого користувача, що визначає система захисту $Z(SD)$. Цей фрагмент у наведеному співвідношенні не відображено. Запис $h_i(x_i)$ означає, що h_i на кроці x_i є визначений як санкціонований користувач. Визначення санкціонованості користувача чи несанкціонованості реалізується такими способами:

– при використанні $P_r^S(SD)$, засоби захисту $Z(SD)$ відповідно до закладеного алгоритму проводять аналіз попередніх кроків реалізації діалогу h_i з *SD*, які функціонально пов'язані з поточним кроком, якщо такий зв'язок в $P_r^S(SD)$ існує; якщо ж такого зв'язку немає, то активізується псевдозв'язок між x_i та x_j і перевіряється їх узгодженість та відповідність, що визначається критеріями, які формуються в системі захисту *SZD*;
– у разі використання довільної процедури захисту P_r^S чи P_r^P перевірка h_i на санкціонованість реалізується на основі використання активованого і підтримуваного системою *SZD* діагностичного діалогу.

Особливість діагностичного діалогу полягає у тому, що він орієнтований на використання індивідуальних даних h_i. Розглянемо твердження.

Твердження 1. Якщо існує $P_r^S(SD)$ для h_i, то існує такий процес $P_r^D(SD)$, який може виявити $\neg h_i$, якщо мала місце підміна $h_i \rightarrow \neg\, h_i$.

Доведення. За умовою твердження існує $P_r^S(SD)$, який відповідає $h_i(x_i)$. Це означає, що правильним є співвідношення:

$$P_r(SD) = \{[h_i(x_1) \rightarrow SD)] \rightarrow [SD \rightarrow h_i(x_1)]\} \rightarrow \ldots \rightarrow \{h_i(x_n) \rightarrow SD\}.$$

Приймемо, що $h_i \rightarrow (\neg\ h_i = h_i^*)$. Тоді в $P_r(SD)$ є фрагмент, для якого $\{[h_i^*(x_j) \rightarrow SD] \rightarrow \neg[SD \rightarrow h_i^*(x_j)]\}$. Це може означати два випадки:

– перший випадок полягає в тому, що $\pi(\neg h_i(x_j)) < \pi_Z \lfloor h_i(x_j) \rfloor$, де π — поточний рівень підготовки $\neg h_i$, а π_Z – заданий рівень необхідної підготовки $h_i(x_j)$;
– другий випадок відповідає ситуації, коли відбулася підміна h_i на $\neg\ h_i$, або $h_i \rightarrow (\neg h_i = h_i^*)$, де h_i^* несанкціонований користувач.

У цьому випадку потрібно відрізнити несанкціонованого користувача h_i^* від непідготовленого користувача $\neg h_i \rightarrow [h_i = \neg h_i \& (d_{i1}, \ldots, d_{ir})]$. Оскільки $P_r^D[Z(SD)]$ можна формувати довільним чином, то будемо формувати його так, щоб у процесі

діалогу $P_r^D[Z(SD)]$ орієнтувався на використання персональних даних h_i, якими є $d_{i1}^*, \ldots, d_{ik}^*$.

$$P_r^D[Z(SD)] = \{[\neg h_i(x_j) \rightarrow SD] \rightarrow [SD \rightarrow \neg h_i(x_j)]\} \rightarrow \{[\neg h_i(x_j) \& (d_{i1}^*, \ldots, d_{ik}^*)] \rightarrow SD\} \rightarrow [SD \rightarrow [\neg h_i(x_j) \& (d_{i1}^*, \ldots, d_{ik}^*)], \ldots,] \quad (1)$$

Якщо $\neg h_i \rightarrow h^*$, то h_i є санкціонований, але не підготовлений для того, щоб сформувати необхідний $\lfloor \neg h_i(x_j) \rightarrow SD \rfloor$. Якщо наведене співвідношення не виконується, то серед $d_{i1}^*, \ldots, d_{ik}^*$ немає даних або хоча б одного елемента, який би відповідав індивідуальним даним h_i. Це означає, що відповідний $\neg h_i$ є несанкціонованим. Отже, можна побудувати $P_N^D(Z(SD))$ так, щоб останній розпізнавав несанкціонованого h_i і $\neg h_i$, який є недостатньо підготовленим, але санкціонованим.

Твердження ґрунтується на наступній гіпотезі, яка є досить природною та полягає у тому, що несанкціонований користувач не володіє даними про всі особисті характеристики санкціонованого користувача. В іншому разі між санкціонованим і несанкціонованим користувачем не існувало б різниці. Таке розпізнавання h_i і $\neg h_i$ може розвиватися шляхом побудови діалогу, який передбачає аналіз історичних даних, що містяться в *CS*, та іншими способами ідентифікації h_i [2].

У цьому випадку адаптація системи $Z(SD)$ полягає у модифікації процесу авторизації користувача з метою виявлення несанкціонованого користувача.

Наступний фактор полягає у виявленні намірів санкціонованого користувача стосовно цілей використання даних, які містяться в системі. Актуальність цієї задачі зумовлена такими причинами:

- дані, які містяться в *CS*, використовуються не тільки для інформування власника цих даних, а й для інформування інших уповноважених осіб чи служб, які можуть потребувати дані про відповідного користувача для вирішення питань, що стосуються останнього;
- користувач може мати на меті модифікувати дані для того, щоб при їх використанні певними уповноваженими службами можна було отримати ті чи інші потрібні користувачеві результати;
- користувач може мати ціль, яка полягає у тому, щоб отримати дані, які стосуються цього користувача, і використати їх недопустимим способом і т. д.

Беручи до уваги вказані причини, можна стверджувати, що система доступу повинна адаптуватися до намірів користувача, який є санкціонований після використання отриманих із системи даних. Така адаптація спрямована на виявлення некоректних намірів з подальшою протидією останнім. Ці задачі розв'язуються засобами аналізу повноважень користувача стосовно таких можливостей:

- перетворення або модифікація даних;
- видача даних за межі системи;
- усунення даних з системи;
- змін щодо потенційних користувачів в умовах визначання повноважень користувачів;
- впровадження нових повноважень новим користувачам.

Ця задача стосується не тільки соціального користувача, яким є особа, про яку розміщується інформація в *CS*, а користувачів, які відповідно до виду своєї

діяльності отримують певні повноваження на їх використання або на зміну даних про соціальних користувачів [3]. Таких користувачів будемо називати фаховими користувачами і, на відміну від соціальних користувачів h^C, позначатимемо їх h_i^{φ}, а також розпізнаватимемо системних користувачів, які забезпечують процес функціонування системи *CS* разом із мережею доступу та всіма компонентами, які стосуються соціальної системи. Таких фахівців вважатимемо адміністраторами *CS* з різними повноваженнями та позначатимемо їх символом h^A.

Відповідно до початкових положень, описаних у профілях безпеки, кожний h_i^c має визначені повноваження, що сформовані на основі даних, які надаються користувачами типу h_i^{φ} та h_i^A. Насамперед розглянемо процеси надання або змін повноважень користувачам h_i^{φ}, які стосуються даних користувачів h^C. Зміна повноважень ґрунтується на використанні та аналізі інтерпретаційних описів відповідних даних $j(d_i)$, на інтерпретаційних описах користувачів $j(h^C)$ та на основі аналізу інтерпретаційних описів або характеристик категорій K_i, що свідчать про необхідний рівень захисту відповідних даних, зокрема і від модифікації останніх. Модифікація даних у цьому випадку є можливою тільки за умови відповідних узгоджень модифікації з користувачами типу h_i^{φ}, які формують відповідні дані, та узгодження з користувачами типу h_i^A. Розглянемо відмінності між h_i^C та h_i^{φ}, які впливають на можливість модифікації d_i^c. Належність даних d_{ij} користувачу h_i^C будемо позначати так: $h_i^c(d_{ij}, \ldots, d_{ij+k})$. Оскільки йдеться про адаптацію щодо h_i^c, а адаптація стосується даних, які визначають і надають здебільшого фахівці або користувачі h_i^{φ}, то адаптація складається з таких етапів:

- перевірки допустимості змін, які пропонує користувач h_i^c, що є власником цих даних, під час реалізації запиту до системи;
- надання дозволу на проведення відповідних змін в даних;
- перевірка допустимості змін повноважень та зміни категорії даних, якщо відповідна зміна сформована користувачем у запиті до системи;
- модифікація повноважень щодо користувачів типу h_i^{φ} стосовно даних $h_i^c(d_{i1}, \ldots, d_{ik})$;
- модифікація або адаптація способу реалізації процесу надання повноважень.

Будь-які зміни в системі *CS* визначаються повноваженнями, які передбачають можливість здійснення певних змін. Зміни в цьому випадку будемо розглядати з погляду зміни семантики даних. Тому приймемо такі типи змін:

- елімінацію даних, що призводить до втрати семантики разом із відповідними даними;
- модифікація семантики даних, яка може здійснюватися внаслідок зміни фрагментів в $j(d_{i1}, \ldots, d_{ik})$;
- зміна категорії даних $K_i(d_{i1}, \ldots, d_{ik}) \rightarrow K_j(d_{i1}, \ldots, d_{ik})$;
- формування прихованих каналів несанкціонованого переміщення даних та їх семантичних описів;
- формування або введення нових даних $(d_{i1}, \ldots, d_{jm})$ разом з їх семантикою $j(d_{j1}, \ldots, d_{jm})$.

Перевірка допустимості змін, пропонованих користувачем h_i^c, здійснюється засобами, що визначають для кожного користувача h_i^c його повноваження. Такі

засоби здебільшого являють собою динамічні матриці управління повноваженнями. Змінювати повноваження для окремих h_i^c можуть лише користувачі вищих рівнів, до яких належать фахівці h_i^φ. Якщо повноваження позначити $U(d_{i1}, \ldots, d_{im})$, то повноваження для h_i^c запишемо у вигляді:

$$U(h_i^c) = \{R_1[OP_{i1}(d_{i1}, \ldots, d_{im})], \ldots, R_m[OP_{im}(d_{m1}, \ldots, d_{mk})]\},$$

де R_i — рівень повноважень, OP_{ij} — операції, що визначають тип повноважень, d_{ij} — дані, над якими проводяться зміни, що відповідають оператору OP_{ij}. Крім повноважень користувачів, існують повноваження об'єктів, до яких передбачається здійснювати доступ. Ці повноваження визначаються на основі інтерпретаційного опису відповідних даних $j(d_{i1}, \ldots, d_{ik})$. Необхідність введення цього поняття зумовлена тим, що самі дані можуть визначати можливість здійснення з ними тих чи інших перетворень. Це визначається їх семантикою, яка описується $j(d_{i1}, \ldots, d_{ik})$. Наприклад, зміна даних, які описують факти, що були в минулому і з погляду семантики такі дані не підлягають змінам (час і місце народження деякого користувача і т. д.).

Переважно внесення даних в *CS* здійснюють фахівці або користувачі h_i^φ. Це пов'язано з тим, що користувач h_i^c є непідготовленим до співпраці з *CS* настільки, щоб при введені даних він міг забезпечити всі необхідні умови реалізації цього процесу. Друга причина полягає у тому, що стосовно даних у *CS* існує досить широкий аспект вимог до захисту відповідних даних, який стосується забезпечення їх інтегральності, адекватності предметній галузі, та інші вимоги, виконання яких передбачені різними нормативними документами. Для того щоб h_i^φ міг ввести ті чи інші дані, він повинен відповідати ряду обов'язкових умов, до яких насамперед належить наявність повноважень, які тісно пов'язані з предметною інтерпретацією даних, що h_i^φ планує ввести. Всі необхідні умови та вимоги відображаються у системі доступу та у системі забезпечення повноважень. Наприклад, якщо йдеться про фахівця, який є лікарем, то він повинен мати сертифікат на введення тих чи інших даних в систему. Це зумовлено тим, що на основі таких даних можуть прийматися рішення про певні дії щодо пацієнта, який є користувачем типу h_i^c. У цьому випадку адаптація полягає в реалізації у *SD* можливостей модифікації сертифікатів доступу з повноваженнями запису даних. Необхідність існування можливості модифікації зумовлена:

- потребою зміни раніше введених даних у зв'язку з тим, що факти, які відображають ці дані, можуть з часом змінюватися, оскільки останні відображають процеси, що відбуваються в середовищі, в якому перебуває h_i^c;
- через умови, що виникають стосовно процесу пов'язаного, з h_i^c, може з'явитися потреба зміни даних про h_i^c, які не передбачені повноваженнями, що надаються користувачу h_i^φ, який вводить дані про користувача h_i^c.

Наведені причини необхідності модифікації або адаптації повноважень, потреба яких зумовлена процесами в предметній галузі інтерпретації, можуть залежно від особливостей предметної галузі розширятися або зменшуватися. По суті, такі умови виникають з моделей тих процесів, в яких бере участь h_i^c і які обслуговуються відповідною базою даних. Наприклад, якщо йдеться про процеси, пов'язані з податковою діяльністю, то модель, яка описує відповідні процеси,

являє собою систему нормативних документів, що регулює всі процеси, пов'язані з функціонуванням відповідного податкового процесу, і таким чином є її модель. У рамках такої моделі передбачені всі повноваження різних h_i^{φ}, що реалізують податкові процеси. Такі повноваження проектуються безпосередньо на відповідну інформаційну систему [4].

Припустимо, що найважливішою небезпекою для *CS* є користувач h_i^C, оскільки він як об'єкт, якого стосується інформація, розміщена в *CS*, найбільше може бути зацікавленим у тих чи інших, в окремих випадках несанкціонованих, змінах у *CS*. Як уже зазначалось, здатність окремого h_i^c отримувати доступ до системи та певні повноваження на перетворення даних в *CS* значною мірою залежить від рівня підготовленості h_i^C до роботи з системою $\pi(h_i^c)$. Очевидно, що однією з функцій системи захисту є визначення такої міри підготовленості. Очевидно, що системи типу CS не орієнтовані на h_i^c, які можуть мати міру $\pi(h_i^c)$ таку, яка відповідає $\pi(P_i^A)$ або $\pi(h_i^{\varphi})$. Тому користувачі типу h_i^c, стосовно яких виявиться, що рівень їх підготовленості більший або близький до величини $\pi(h_i^{\varphi})$, можуть належати до класу користувачів, які можуть бути носіями небезпеки. Система захисту доступу *SZZ* повинна надавати можливість перевіряти потенційних користувачів типу h_i^c. Перевірка цих користувачів стосується визначення їх рівня підготовленості до реалізації процесів доступу $\pi(h_i^c)$. Процес доступу $Pr(SD)$, який призначений для h_i^c, будемо позначати $Pr_i[h_i^c(SD)]$. Він являє собою послідовність подій $Pr_i[h_i^C(SD)] = \{x_{i1} * \ldots * x_{im}\}$. Кожна подія описує етап діалогу $(h_i^c \rightarrow SD) \vee (SD \rightarrow h_i^c)$. Таким чином, подія x_{ij} визначається даними або повідомленням, які отримує *SD* від h_i^c, або $h_i^c(IO_{ij+1})$, та повідомленням або інформаційним образом IO_{ij+1}, який отримує h_i^c від *SD*, що можна записати як $SD(IO_{i(j-1)})$. У загальному випадку цей елемент діалогу запишемо у вигляді:

$$[h_i^c(IO_{i(j+1)}) \rightarrow SD] \rightarrow [SD(IO_{i(j-1)}) \rightarrow h_{ij}^c].$$

Для опису інформації, що передається в *SD* і з *SD* до h_i^c, використовується уявлення про інформаційний образ $IO_{i(j\pm1)}$, де індекс $(j+1)$ означає, що IO_{ij} передається від h_{ij}^c до *SD*, а індекс $(j-1)$ означає передачу образу від *SD* до h_i^c. Отже, весь діалог можна записати у вигляді:

$$D(h_{ij}^c, SD) = \{x_{i1} \rightarrow x_{i2} \rightarrow \ldots \rightarrow x_{im}\}.$$

Для реалізації перевірки користувача h_{ij}^c система *SZZ* застосовує принципи, що закладені в системах, які використовують технології honeypot [5]. У межах цієї технології система *SZZ* реалізує діалог, який є наближеним до діалогу, що відповідає запиту користувача за послугою до *CS*, але *SZZ* модифікує процес діалогу так, щоб запит вийшов за рамки повноважень користувача h_i. Якщо це вдається, то система відносить h_i^c до класу потенційних небезпек.

Висновки. У дослідженні вперше розроблено метод підвищення рівня безпеки доступу до соціальної інформаційної системи, який ґрунтується на застосуванні методів адаптації системи захисту доступу до забезпечення необхідного рівня захисту від несанкціонованих користувачів. В основі такого методу використовуються процеси діалогу з користувачами, завдяки якому система доступу уможливлює отримання додаткової інформації про користувача, що дає змогу підвищити загальний рівень безпеки доступу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Микси М. Безопасность безпроводных сетей / М. Микси, Д. Поллино. — М. : Компания АйТи; ДМК Пресс, 2004.
2. Русев Д. Технология безпроводного доступа : справочник / Д. Русев. — СПб. : БХВ — Петербург, 2003.
3. Ирвин Дж. Передача данных в сетях: инженерный поход / Дж. Ирвин, Д. Харль. — СПб. : БХВ — Петербург, 2003.
4. Мещеряков Е. Публикация баз данных в Интернете / Е. Мерещенков, А. Хомоненко. — СПб. : БХВ — Петербург, 2003.
5. Rash M. IPS Zapobieganie i aktywne przeciwdzialanie intruzom / M. Rash, A. Orebauch, G. Clark, B. Pinkard, J. Bablin. — W. : PWN, 2007.

REFERENCES

1. Miksi, M., & Polino, D. (2004). Bezopasnost bez provodnyh setei. Moscow: Company IT, DMK Press (in Russian).
2. Rusev, D. (2003).Tekhnologiya bezprovodnogo dostupa. Spravochnik. SPB: BHV — Petersburg (in Russian).
3. Irvin J., & Kharl D. (2003). Peredacha danykh v setyah: inghenernyi podkhod. SPB: BHV — S. Petersburg (in Russian).
4. Meshcheryakov, E., &Khomonenko, A. (2003). Publikaciya baz dannykh v internete. SPB: BHV — S. Petersburg (in Russian).
5. Rash, M., Orebauch, A., Clark, G., Pinkard, B., & Bablin,. J. (2007). Zapobeganiye i aktyvne prshecivdelaniye intruzom. Warchwa: PWN (in Polish).

METHODS OF PROCESS ADAPTATION OF USERS ACCESS SECURITY TO SOCIAL SYSTEMS

B. V. Durniak, T. M. Khometa

Ukrainian Academy of Printing,
19, Pid Holoskom St., Lviv, 79020, Ukraine

In this article the methods of adaptation of the access system to the user have been examined and developed, which can appear to be not prepared enough to work with the system in a necessary measure. Therefore the adaptation consists in the access activation of the dialog with a user by the system. The dialog is formed thus, that a user can get additional information about the methods of connection with the system. Due to such adaptation the system becomes friendlier for an ordinary user.

Keywords: *adaptation, system of access security (SZD), system of facilities of security (SZZ), heterogeneity of users, one-way process, diagnostic dialog, measure of preparation, modification, semantics.*

Стаття надійшла до редакції 22.01.2016.
Received 22.01.2016.