УДК 004.04

АНАЛІЗ ЗАСОБІВ ЗАХИСТУ ДО ЗАДАНОГО РІВНЯ В СОЦІАЛЬНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Т. М. Хомета

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

Проаналізовано причини, які зумовлюють потребу адаптації системи доступу до інформаційної соціальної системи. Для реалізації процесу адаптації важливими є не тільки параметри, пов'язані безпосередньо з наданням доступу, а й параметри, що характеризують процес доступу загалом. Наведено визначення різних видів адаптації та рівня безпеки доступу, досліджено інші фактори, що впливають на безпеку доступу.

Ключові слова: *адаптація, автентифікація, ідентифікатор, профіль, система захисту доступу SZD, атаки, реєстраційний номер, пароль, соціальний інформаційний електронний комплекс CIEK, система адміністратора SA, повноваження користувача.*

Постановка проблеми. Адаптація систем доступу до CS_i зумовлена довгостроковими термінами експлуатації CS_i, змінами параметрів автентифікації користувачів, а також реалізацією успішної атаки на ці параметри. Будь-яка атака призводить до виникнення аномалій в середовищі даних системи CS_i. Тому актуальною є потреба аналізу атак, що безпосередньо визначають рівень безпеки системи доступу, а також дослідження методів реалізації процесу адаптації доступу користувача до соціальної системи.

Аналіз останніх досліджень та публікацій. Проблеми захисту системи доступу до інформаційних систем різного призначення широко досліджують фахівці в галузі захисту інформації, а саме: Давиденко А. М., Зима В. М., Молдавян А. А., Сміт Р. Є. та інші. У відомих нам дослідженнях розглянуті задачі захисту системи доступу до довільних інформаційних систем, що не дають можливості враховувати особливості окремих типів інформаційних систем.

Мета статті — дослідження та аналіз усіх даних, які зумовлюють потребу створення системи доступу, здатної адаптуватися до змін, що відбуваються у зовнішньому середовищі, яке становлять користувачі системи. Зміни в системі доступу, що виникають у результаті адаптації, враховують особливості вибраних інформаційних систем.

Виклад основного матеріалу дослідження. Адаптивні можливості систем доступу до CS_i є характерними для більшості інформаційних систем, орієнтованих на обслуговування широкого кола користувачів. Це зумовлено насамперед довгостроковими термінами експлуатації CS_i, оскільки з часом у середовищі, на функціо-

нування в якому орієнтовані CS_i, відбуваються зміни, які треба врахувати під час роботи з CS_i. До таких змін належать:

– зміни параметрів автентифікації користувачів;
– зміни узагальнених параметрів даних, що зберігаються у відповідних CS_i;
– зміни задач, які передбачається розв'язувати на основі використання інформаційних систем CS_i.

Зміни параметрів користувачів можуть відбуватися у зв'язку з такими причинами:

– після закінчення інтервалу часу безпечного доступу до системи окремого користувача;
– приєднання нового користувача до системи;
– реалізація успішної атаки на параметри автентифікації сталого користувача системи.

У процесі використання системи доступу до CS_i окремим користувачем, залежно від інтенсивності доступів користувача h^c, параметри ідентифікації старіють. Це означає, що такі параметри p_k^i через об'єктивні фактори функціонування h^c у соціальному середовищі CW_i стають широко відомими, що знижує їхній рівень таємності, який прийнято називати явним рівнем таємності. Такого типу параметри будемо позначати JP_k. Ці параметри потрібні для ідентифікації користувача в часі, що позначатимемо $JP_k(t)$, і вони є спільними для всіх систем, якими передбачає користуватися споживач h_i^c. Крім параметрів ідентифікації типу JP_i, користувач використовує параметри P_i, пов'язані з певною CS_i, до якої може звертатися h_i^c. На такі параметри поширюються вимоги до обмеження інтервалу часу, впродовж якого вони будуть застосовуватися. Прикладом таких параметрів є пароль, реєстраційний номер чи інші параметри, що їх генерує кожна окрема система CS_i [1].

Процес приєднання нового користувача до системи не завершується наданням передбачених параметрів, якими можуть бути ідентифікатори, паролі чи інші засоби захисту доступу. Процес приєднання h_i до CS_i продовжується протягом періоду звертань користувача до системи, який є необхідним для створення профілю користувача. У цьому випадку аналізуються такі параметри, як швидкість створення профілю $v_i(h_i)$, повнота створеного профілю $q(h_i)$, особливості профілю користувача $g(h_i)$, завершеність чи незавершеність створення відповідного профілю, яку будемо позначати $\lambda(h_i)$. Параметр $v_i(h_i)$ аналізує частоту звернень h_i до CS_i. На цю величину можуть накладатися обмеження, що є елементом процесу захисту. Повнота створеного профілю $g(h_i)$ визначає кількість персональних характеристик h_i, які вносять у пароль. Прикладом таких характеристик може бути: час доби, коли користувач переважно звертається за послугою, характер даних, за якими він звертається, та інші. Особливості профілю користувача відображають характеристики використання різних ознак у процесі побудови відповідного профілю. Наприклад, для одного користувача частота звернень до системи є рівномірною протягом усього періоду $\tau(h_i)$ створення профілю, для іншого користувача h_j частота звернень до системи є нерівномірною, зокрема: на першій половині інтервалу формування профілю частота звернень має випадковий

характер, а на другій половині інтервалу $\tau(h_i)$ — періодичний характер. Іншим прикладом особливості профілю слугуватиме характер зміни моментів часу формування запитів на обслуговування у вибраному періоді інтервалу аналізу профілів. Таким інтервалом може бути денний або вечірній час доби та ін. З наведених прикладів особливостей профілів бачимо, що особливість профілю тісно пов'язана з параметрами користувача, використовуваними у профілі. Цей зв'язок можна записати у вигляді співвідношення:

$$q(h_i) = f(g(h_i^o)),$$

де $g(h_i^o)$ — особливості профілю, функція, що описує такий зв'язок, може бути додатковою характеристикою особливості профілю користувача h_i. Наприклад, якщо $g(h_i^o)$ є інтервал часу протягом доби, коли користувач звертається до системи CS_i, то $g(h_i^o)$ може являти собою частоту звертань користувача до системи. Така залежність є природною, якщо припустити, що професійна діяльність h_i пов'язана з використанням даних із CS_i, а період часу з найбільшою частотою звертань h_i до CS_i відповідає періоду часу, коли h_i перебуває в установі, в якій він працює і т. д. [2].

Будь-який профіль довільного h_i міститиме різну кількість параметрів h_i у зв'язку з тим, що інтервал, упродовж якого формується профіль, може бути різним, і час формування профілю визначається інтервалом часу τ. Вважається також, що профіль повинен мати не менш ніж n параметрів. Якщо за час τ_i у профілі сформовано m параметрів, де величина $m \le n - k$, де k — мінімальна кількість параметрів, яких не вистачає, щоб можна було вважати, що m є близька до n, то відповідний профіль вважатиметься незакінченим або буде характеризуватися параметром $\lambda(h_i)$. Припустимо, що профіль із параметром $\lambda(h_i)$ мусить перейти у закінчений профіль або $\lambda(h_i) \to \varphi r(h_i)$, де $\varphi r(h_i)$ є закінченим профілем, оскільки він уміщає $n \pm \Delta_n$ параметрів, де $\Delta_n \ge k$. Для того щоб такий перехід здійснити, треба надавати додаткові інтервали τ для формування профілю $\varphi r(h_i)$. Очевидно, що незалежно від надання користувачеві додаткових τ_i, його профіль може характеризуватися параметром $\lambda(h_i)$. Кількість додатково наданих τ_i для h_i також можна використовувати як особливість профілю, тому що h_i характеризується обмеженою кількістю параметрів P_i, та кількість додаткових h_i, яку надає користувачеві h_i система CS, є обмеженою.

Зміна параметрів для h_i у результаті успішної атаки At_i на систему захисту доступу (SZD) є особливо актуальною, оскільки одним із важливих завдань SZD є недопущення подальшої можливості успішного завершення At_i на SZD. Факт успішного завершення At_i на SZD виявляється на стадії аудиту або на основі даних про втрати чи інші прояви несанкціонованого використання даних деякого користувача. Цей випадок стосується користувача h_i^c, який відповідні втрати чи негативні наслідки безпосередньо виявляє. Момент прояву успішної атаки t_i^P та момент реалізації відповідної атаки t_i^r можуть відрізнятися на досить значний інтервал часу. Ця обставина ускладнює завдання захисту та протидії атаці, яка може повторити успішну атаку At_i^u. Для розв'язання цієї проблеми в рамках SZD реалізуються такі методи виявлення та швидкої протидії можливому повторенню At_i^u:

– метод оберненого зв'язку h_i^c із системою;
– метод, що ґрунтується на аналізі фактів використання даних довільного h_i^c в інших системах;
– метод імітації атаки або реалізація псевдоатаки, яка здійснюється окремою компонентою *SZD* щодо *SZD* [3].

Перший метод за своєю суттю є найпростішим, але його реалізація не завжди технічно можлива. Це зумовлено тим, що різні h_i^c можуть мати різні засоби зв'язку зі системою CS_i. Крім того, у h_i^c може бути лише телефонний зв'язок з обслугою системи CS_i. Єдиною вимогою для реалізації цього підходу є надання користувачеві h_i^c інформації про те, що його дані, можливо, будуть несанкціоновано використовуватися у тій чи іншій системі. Користувач повинен надати відповідь системі *SZD*, бо інакше дані користувача h_i^c будуть заблоковані і стануть недоступними. Система CS_j, яка виявилася першою в послідовності звернення до систем, дані якої може використовувати користувач для роботи як обернений зв'язок у системі загалом. Такий обернений зв'язок системи CS_i, що є джерелом інформації з користувачем h_i^c та із системою CS_j, в якій передбачається застосовувати дані з CS_i, являє собою природний спосіб розв'язання задачі виявлення успішної атаки на h_i^c, що її будемо позначати $At_i^u(h_i^c)$. Для реалізації обмежених обернених зв'язків у $SZD(CS_i)$, як і в усіх інших системах, існують засоби підтримки відповідних дій. Для випадку $At_i^u(h_i^c)$ такі засоби стосовно h_i^c передбачені, оскільки h_i^c є клієнтом CS_i, а для використання зв'язку між $CS_j \rightarrow CS_i$, в CS_i повинні існувати дані про те, в яких системах типу CS_k можуть використовуватися дані h_i^c. У межах цієї задачі системи CS_i, в яких можуть використовуватися $x_i(h_i^c) \in CS_i$, називатимемо санкціонованими стосовно даних типу $x_i(h_i^c) \in CS_i$, що будемо позначати символом $S(CS_j)$.

Наведений опис різних типів атак і способів їх виявлення ілюструє можливості реалізації методів адаптації системи доступу до користувачів h_i^c та до задач, що розв'язуються за допомогою використання відповідних даних в інших системах типу CS_j. Для забезпечення однозначності в інтерпретації понять, вжитих у статті, введемо їх визначення.

Визначення 1. Адаптацією стосовно користувача h_i^c системи захисту доступу *SZD* називається процес, який забезпечує підвищення рівня безпеки доступу користувачів до системи.

Визначення 2. Рівень безпеки *SZD* визначається складністю процесів перевірки уповноваження користувача h_i^c при його звертанні до CS_i за даними.

Активізація процесів адаптації *SZD* стосовно користувача h_i^c може реалізуватися через виявлення успішної атаки типу $At_i^u(h_i^c)$.

Визначення 3. Адаптацією по відношенню до задачі, що розв'язується в рамках систем CS_i, називається процес підвищення рівня безпеки доступу користувача, який вводить дані в систему CS_i і є фахівцем у галузі, до якої такі дані належать.

Процес адаптації стосовно задачі в одному із випадків активізується у результаті виявлення успішної атаки на задачу $At_i^u(h_i^\varphi)$. У процесі адаптації системи *SZD* важливим параметром є інтервал часу між завершенням успішної атаки At_i^u

та моментом її виявлення. Оскільки аудит проводиться здебільшого відповідно до графіку, то цей випадок для визначення інтервалу часу між At_i^u та моментом виявлення At_i^u, який будемо позначати δ_i^A, не розглядатимемо.

Опишемо задачу мінімізації часу δ_i^R, який являє собою величину запізнення реакції *SZD* на подію, що полягає в реалізації At_i^u. Для конструктивного розв'язання цієї задачі приймаємо ряд положень та визначення.

Положення 1. Кожна атака At_i реалізується на основі використання загроз zg_i, що існують в системі *SD*.

Положення 2. Всі події, пов'язані зі взаємодією зовнішніх факторів із CS_i, реєструються в системі *SZD*, при цьому їх повний аналіз у реальному часі не проводиться.

Положення 3. Будь-яка атака, успішна чи неуспішна, At_i^u чи At_i^N, приводить до виникнення аномалій в середовищі SD_i і, відповідно, в середовищі даних системи CS_i.

Визначення 4. Кожна успішна атака At_i^u, яка, закінчивши реалізацію своїх функцій, елімінує аномалії, що сформувалися в процесі її реалізації, називається латентною атакою At_i^L.

Розв'язувати задачі захисту тільки в рамках систем *SZD*, *SD* чи CS_i окремо некоректно, оскільки At_i різних типів є факторами зовнішніми і діють на всі перераховані компоненти комплексно. Тому треба розглянути процеси взаємодії між собою окремих компонент у рамках деякої спільної структури. Така структура повинна охоплювати всіх користувачів різних типів, системи CS_i та *SZD*. Таким чином, до складу цієї структури входять такі компоненти:

- розподілена система доступу до CS_i або RSD_i для користувачів типу h_i^c;
- база соціальних даних CS_i;
- розподілена система доступу $RSD_i(h_i^\varphi)$ для користувачів типу h_i^φ;
- система адміністратора $SA(CS_i)$ або (SA).

Сукупність цих систем називатимемо соціальним інформаційним електронним комплексом (*CIEK*). Уявлення про *CIEK* як про єдиний комплекс зумовлює певні функціональні зобов'язання всіх користувачів цього комплексу, а саме:

- користувач типу h_i^c зобов'язаний не тільки отримувати персональні дані по запиту до *CIEK*, а й виконувати подальші дії в рамках роботи з *CIEK*;
- перевіряти відповідність доступних йому даних тій інформації, яку він вважає правильною, і в разі розбіжностей виходити на зв'язок з $SA(CS_i)$ та інформувати її про виявлені ним розбіжності;
- після отримання з *CIEK* даних, запит на які він подавав у систему, користувач h_i^c повинен проінформувати $SA(CS_i)$ про способи їх використання, якими можуть бути: передавання даних в іншу CS_i через ту саму систему доступу, передавання даних для розв'язання певних задач третій стороні, вводячи при цьому всі необхідні дані про третю сторону, яку позначатимемо *TSK*;
- передавати в $SA(CS_i)$ всю інформацію про виявлені порушення щодо використання його персональних даних з надання інформації про можливі джерела, в яких такі порушення відбулися чи відбуваються.

Виконання наведених вище функцій реалізується в діалоговому режимі, який є максимально доступний для користувача, і в процесі діалогу в автоматичному режимі проводиться адаптація діалогу до рівня підготовки кожного з користувачів типу h_i^c. Активізація такого діалогу реалізується зі сторони *CIEK* з використанням усіх можливих засобів зв'язку користувачем, про які він увів інформацію в систему *CIEK*, включно з електронною поштою, телефонною комунікацією та іншими засобами зв'язку. Виконання такого типу зобов'язань зі сторони h_i^c зумовлює певний рівень безпеки персональних даних відповідного користувача. Якщо користувач h_i^c не хоче або не може реагувати на запрошення до діалогу з *CIEK*, то рівень безпеки персональних даних відповідного користувача отримує певну кількість індексів можливого зниження рівня захисту, що формально описується $RZ(n)[h_i^c]$, де n — кількість отриманих індексів можливого зниження рівня захисту $x_i(h_i^c) \in CS_i$. Ці індекси n_i означають, що в разі виникнення негативних факторів, орієнтованих на дані $x_i(h_i^c)$, останні можуть виявитися більш вразливими до атак різних типів. Це означає, що невиконання користувачем типу h_i^c відповідних обов'язків, пов'язаних зі співпрацею із системою *CIEK*, може привести до зниження рівня безпеки відповідних даних. Для забезпечення умов функціонування всього комплексу в рамках CS_i повинні реалізовуватися процедури динамічної модифікації структури даних. Це означає, що дані, які мають вищий рівень захищеності, повинні розміщуватися в одному структурно визначеному місці системи, а дані, що у зв'язку з описаними умовами перейшли на нижчий рівень захищеності, незалежно від їх інтерпретації, мають переноситися в елементи структури з нижчим рівнем захищеності. Очевидно, що повинні також реалізовуватися протилежні переміщення даних, якщо користувач h_i^c активізував свою співпрацю із системою [4].

Розглянемо на якісному рівні аналогічні задачі, що виникають стосовно користувачів типу h_i^φ. Користувач h_i^φ відрізняється від користувача типу h_i^c такими характеристиками і можливостями:

- користувач h_i^φ повинен мати сертифікат для використання тієї чи іншої соціальної бази даних CS_i, що означає наявність у нього спеціальної підготовки до використання відповідної системи CS_i та *CIEK* загалом;
- користувач h_i^φ має повноваження не тільки на отримання даних, що стосуються користувача h_i^c, а й повноваження на введення в систему нових даних про користувача h_i^c, які узгоджені з повноваженнями користувача h_i^φ;
- крім зчитування та впровадження даних, що стосуються h_i^c, користувач h_i^φ може мати повноваження на перетворення або модифікацію даних користувача типу h_i^c;
- на відміну від множини користувачів типу h_i^c, множина користувачів типу h_i^φ має власну структуру, яка в багатьох випадках є ієрархічною, що зумовлює певні залежності між різними групами h_i^φ, а це, своєю чергою, приводить до надання різних повноважень різним групам користувачів типу h_i^φ [5].

Так само як і щодо користувачів типу h_i^c, система *CIEK* може активізувати діалог між компонентами *CIEK* та користувачем h_i^φ. У цьому випадку така можливість участі h_i^φ у діалозі з компонентами з *CIEK* передбачена умовами отримання тих чи

інших сертифікатів користувачами h_i^{φ}. Тому організація співпраці між h_i^{φ} та *CIEK* є простішою і не потребує процедур адаптації системи до користувача. Попри це, діалог між h_i^{φ} та *CIEK* також є доступний для h_i^{φ}. Наприклад, h_i^{φ} зобов'язаний відповідно до свого сертифіката активізувати діалог із системою *CIEK*, якщо h_i^{φ} виявив у даних, отриманих із CS_i, аномалії, розпізнавати які h_i^{φ} має повноваження. Як і у випадку з h_i^c, активізація такого діалогу може ініціюватися не тільки зі сторони h_i^{φ}, а й зі сторони комплексу *CIEK*. У першому випадку h_i^{φ} інформує комплекс про можливі недопустимі зміни в CS_i, що могли бути зумовлені діючими атаками At_i або атаками At_i^u, що успішно завершилися. У другому випадку активізація діалогу з h_i^{φ} комплексом *CIEK*, що пов'язано з виявленням атак чи аномалій системою *SZD*, зумовлює необхідність підтримки такого діалогу користувачем h_i^{φ}. Системі *SZD* такий діалог може бути потрібний для визначення додаткових даних про виявлену атаку, які необхідні для реалізації процесів, пов'язаних із забезпеченням заданого рівня захисту даних.

Система адміністратора *SA* орієнтована на співпрацю з користувачами типу h_i^A. На відміну від користувачів h_i^c та h_i^{φ}, користувач h_i^A має значно ширші повноваження, які стосуються не тільки даних із CS_i, а й процесів, що реалізуються в різних системах комплексу *CIEK*. Користувач h_i^A, крім описаних повноважень, має спеціальні повноваження щодо користувачів h_i^c та h_i^{φ}, а саме:

- повноваження на управління діалогом між h_i^c *SD* і, відповідно, з *CS*;
- повноваження на відміну та модифікацію сертифікатів користувачів типу h_i^{φ};
- повноваження на активізацію діалогу між комплексом *CIEK* та користувачами h_i^c і h_i^{φ}.

Система *SA* і користувачі h_i^A мають власну специфіку, яка полягає в таких особливостях:

- система *SA* може функціонувати в автоматичному та автоматизованому режимі роботи;
- користувачі h_i^A організовані у певну структуру, яка визначає залежності між ними;
- користувачі типу h_i^A, як і користувачі h_i^{φ}, повинні мати сертифікати на право виконання функцій адміністрування комплексу *CIEK*;
- переважно структура множини користувачів h_i^A є ієрархічною, що дає змогу класифікувати за функціональною ознакою сертифікати окремих h_i^A чи їх груп.

Система *SA* орієнтована на розв'язання таких задач:

- управління комплексом *CIEK* загалом;
- забезпечення захисту, на який орієнтована система *SZD*;
- забезпечення оберненого зв'язку системи *SD* чи *RSD* із користувачами різних типів;
- реалізація стратегії функціонування комплексу *CIEK*.

Управління комплексом *CIEK* загалом полягає в реалізації таких процесів у *SA*:

- управління процесом функціонування системи *SZD*;
- забезпечення можливості розширення системи розподіленого доступу для користувачів;
- аналіз інтегральних параметрів окремих систем комплексу *CIEK*.

Система *SZD*, орієнтована на розв'язання задач захисту CS_i від атак різних типів, у процесі їх розв'язання може потребувати даних, які стосуються факторів зовнішнього середовища. Такими факторами можуть бути різноманітні небезпеки, які активізують певні атаки. В цьому випадку досить важливо виявити тип атаки та інші її параметри. Оскільки система CS_i, по суті, є базою даних, то вона може лише містити образи аномалій як результат виникнення активізації атак. У такому разі доцільно обмежитися атаками, що використовують *SD* для реалізації своєї цілі. До *SD* насамперед звертаються користувачі різних типів, тому вважатимемо, що основною загрозою виникнення успішної атаки є можливість реалізації несанкціонованого доступу до системи. У цьому випадку не розглядаються атаки на *SZD*, атаки безпосередньо на CS_i і тим паче атаки на систему типу *SA*. Останнє можливе, беручи до уваги положення 4.

Положення 4. Несанкціонований доступ до *CIEK* у рамках повноважень користувачів типу h_i^A є неможливим і, відповідно, не розглядаються атаки на систему *SA*.

Доцільність використання положення 3 зумовлена тим, що множина користувачів h_i^A вважається абсолютно безпечною.

Висновки. Проаналізовано фактори, що зумовлюють необхідність реалізації процесів адаптації в рамках системи доступу. Проведено аналіз атак, які є одними з основних факторів, що безпосередньо визначають рівень безпеки системи доступу. Досліджено методи реалізації обернених зв'язків між користувачами та системою доступу до інформаційної соціальної системи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Медведковский И. Д. Атака на Internet / И. Д. Медведковский, П. В. Суянов, Д. Г. Леонов. — М. : ДМК, 1999.
2. Брагг Р. Система безопасности Windows 2000 / Р. Брагг. — М. : Издательский дом «Вильсон», 2001.
3. Зима В. М. Безопасность глобальных сетевых технологий / В. М. Зима, А. А. Молдавян, Н. А. Молдавян. — СПб. : БХВ-Петербург, 2000.
4. Смит Р. Э. Аутентификация: от паролей до открытых ключей / Р. Э. Смит. — Издательский дом «Вильсон», 2002.
5. Блек У. Интернет, протоколы, безопасность : уч. курс. / У. Блек. — СПб. : Питер, 2001.

REFERENCES

1. Medvedkovskyi, V., Suyanov, P., & Leonov, D. (1999). Ataka na Internet. Moskva: DMK (in Russian).
2. Brag, R. (2001). Systema bezopasnosti Windows 2000. Moskva: Izdatelskyi Dom «Vilson» (in Russian).
3. Zyma, V., Moldavian, A., & Moldavian, N. (2000). Bezopasnost globalnykh setevykh tekhnologiy. Sankt-Peterburh, SPB-BHV (in Russian).
4. Smith, R. (2002). Autentifikaciya: ot paroley do otkrytykh kluchey. Moskva: Izdatelskyi Dom «Vilson» (in Russian).
5. Blek, U. (2001). Internet, protokoly, bezopasnost. Sankt-Peterburh: Piter (in Russian).

ADAPTATION OF PROTECTION FACILITIES TO THE SET LEVEL IN SOCIAL INFORMATION SYSTEMS

T. M. Khometa

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

The analysis of reasons has been conducted in a process of work which stipulate the necessity of adaptation of the access system to the information social system. For realization of the adaptation process not only parameters are important that are related directly to the access but also parameters which characterize the process of access in general. Determinations of different types of adaptation and determination of access security level are brought in a process of work and other factors that influence the access security have been researched.

Keywords: *adaptation, authentication, identifier, profile, system of protection of SZD access, attacks, registration number, password, social information electronic complex CIEK, system of SA administrator, authority of a user.*

Стаття надійшла до редакції 16.06.2016.
Received 16.06.2016.