УДК 004.056

АЛГОРИТМ ФУНКЦІОНУВАННЯ ЗАСОБІВ ЗАХИСТУ СОЦІАЛЬНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Б. В. Дурняк, Т. М. Хомета

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

Розглянуто розроблення методів функціонування засобів захисту систем доступу до соціальної інформаційної системи. Розроблено схему організації системи, що містить засоби захисту. Проаналізовано уявлення про різні стани безпеки соціальної інформаційної системи.

Ключові слова: *соціальна інформаційна система, захист, безпека, система доступу, діалог, обернений зв'язок.*

Постановка проблеми. Засоби *SZD* орієнтовані на розв'язання низки окремих задач, в яких є атаки несанкціонованого доступу та атаки несанкціонованого використання даних. Застосування компонент забезпечує обернений зв'язок між користувачем та системою. Система *SZD* вирішує, чи запропонована тема може бути корисна для розв'язання задачі забезпечення необхідного рівня безпеки даних. Отже, процеси адаптації стосовно користувачів являють собою діалог із користувачами, завдяки якому система може одержати додаткову інформацію про можливі небезпеки, а також адаптацію до певного рівня організації безпеки системи, оскільки *SA* в процесі діалогу отримує через *SZD* всю додаткову інформацію про можливі ознаки активізації небезпек. Досліджено розв'язання задачі методу побудови системи доступу, яка містить засоби захисту від несанкціонованого доступу та засоби захисту даних у разі зміни рівня їх захисту.

Аналіз останніх досліджень та публікацій. Над створенням систем доступу до інформаційних систем працює широке коло відомих фахівців, серед яких — Давиденко А. М., Задірака М. І., Кравченко Ю. В. та інші. У відомих нам працях системи доступу розробляються шляхом ускладнення процедур ідентифікації та автентифікації, що не завжди забезпечує необхідний рівень безпеки системи.

Мета статті — дослідження та аналіз алгоритму функціонування засобів захисту для соціальної інформаційної системи.

Виклад основного матеріалу дослідження. Основними задачами, на розв'язання яких орієнтовані засоби *SZD,* є захист від атак, що ними передусім є атаки несанкціонованого доступу та атаки несанкціонованого використання даних. Ці задачі недостатньо розв'язувати тільки в рамках самих систем *SZD*. Для їх успішного розв'язання треба використовувати окремі компоненти чи системи, які безпосередньо не належать до *SZD*. Прикладом такої компоненти є засіб, що

забезпечує обернений зв'язок між користувачем та системою. Таке розширення полягає у частковому використанні користувача під час розв'язування задач захисту його персональних даних. Такий підхід для системи типу CS_i є характерним, оскільки користувач може мати достовірну інформацію про свої персональні дані і він зацікавлений у їхній безпеці. Реалізація оберненого зв'язку потребує розв'язання та дослідження ряду окремих задач:

– визначення необхідності активізації оберненого зв'язку з окремим користувачем;
– адаптація процесу діалогу до рівня підготовки користувача типу h_i^c;
– формування чергового етапу діалогу на основі даних, отриманих на попередніх кроках діалогу;
– організація використання даних діалогу для захисту персональних даних користувача.

Потреба активізації діалогу між системою *SZD* і користувачем типу h_i^c зумовлена виникненням небезпеки зниження рівня захисту відповідних даних. Поява деякої ознаки, що характеризує небезпеку, являє собою насамперед недопустимі величини відхилення значень параметрів, що характеризують процес реалізації обслуговування користувача, які будемо називати відхиленнями керувальних параметрів (*up*). Під час перевірки процесів доступу користувача h_i^c до *SD* використовуються діагностичні параметри, які, на відміну від UP_i, є надмірними з погляду процесу управління процедурами доступу. Однією з основних причин активізації діалогу є виявлення ознак атаки $At_i(h_i^c)$ на користувача h_i^c.

Адаптація процесу діалогу між h_i^c та *SZD* є досить проста в реалізації, оскільки вона полягає у формуванні додаткових питань користувачеві h_i^c, якщо йому не зрозуміло, що він повинен робити в результаті запрошення до діалогу. У цьому випадку система ставить питання, на які користувач відповідає, притому відповіді здебільшого потребують підтвердження або заперечення інформації, наданої користувачеві з боку системи *SZD*.

У зв'язку з адаптацією діалогу зі сторони *SZD* до рівня підготовки користувача h_i^c може бути потрібним розподіл процесу діалогу на окремі етапи. Річ у тому, що коли питання формуються таким чином, щоб відповідь мала бінарний характер, то в разі потреби перейти до виявлення деякої інформації, яка суттєво відрізняється від інформації, стосовно якої реалізувався діалог, що його називатимемо бінарним, потрібно користувача проінформувати про те, що із заданого моменту буде вестися діалог на іншу тему. Очевидно, що користувач може не згодитися на зміну теми діалогу, через те що він не володіє даними стосовно іншої запропонованої теми або тому що h_i^c з певних причин не хоче на відповідну тему розмовляти. Може виникнути ситуація, коли користувач сам запропонує нову тему для обговорення. Тоді система *SZD* вирішує, чи запропонована тема буде корисна для розв'язання задачі забезпечення необхідного рівня безпеки даних. З наведеного вище випливає, що процеси адаптації стосовно користувачів являють собою діалог з користувачами, завдяки якому система може отримати додаткову інформацію про можливі небезпеки. В цьому сенсі йдеться про адаптацію до певного рівня забезпечення

безпеки системи, оскільки *SA* в процесі діалогу отримує через *SZD* всю додаткову інформацію про можливі ознаки активізації небезпек.

Інша задача адаптації системи захисту доступу ґрунтується на використанні діалогу з користувачем типу h_i^{φ}. Активізація діалогу з h_i^{φ} відбувається відповідно до тих самих критеріїв, що й активізація діалогу з h_i^{c}. Перебіг діалогу з h_i^{φ} переважно стосується впроваджених даних відповідними h_i^{φ}, оскільки цього типу користувачі мають підготовку, що є необхідною для роботи зі системою. В цьому випадку діалог може стосуватися визначення типу атаки на основі аналізу системою *SA* аномалії даних, виявлених у CS_i. На основі діалогу *SZD* з h_i^{φ} можна виявити такі ознаки активності атак на задачі або на дані:

- чи аномалія виникла в результаті несанкціонованого доступу до *SZD* через систему доступу, орієнтовану на обслуговування користувачів типу h_i^{φ};
- визначити інтерпретацію аномалій, що дає змогу виявити можливу ціль атаки на задачі;
- виявити можливі наслідки дії атаки на задачі, що безпосередньо визначає рівень безпеки відповідної системи, включно з базою даних.

Визначення факту несанкціонованого доступу до системи є порівняно простим. Для цього достатньо перевірити у відповідних санкціонованих користувачів h_i^{φ} чи хтось з них не вводив дані, що мають певні параметри. Одним з основних параметрів $x_i \in CS_i$ є час введення даних, прикладом інших параметрів може слугувати тип даних, що вводяться в систему. Цей параметр виникає внаслідок того, що різні типи даних відрізняються не тільки своєю величиною, а й інтерпретацією відповідних даних (наприклад, дані про результати медичних аналізів, про величину прибутків за вибраний проміжок часу і т. д.). У цьому випадку системі *SZD* залишається визначити наявну загрозу. Особливістю системи *SZD*, що обслуговує CS_i та SA_i є те, що вона запам'ятовує копію процесу звертання, який будемо називати слідом звернення $[Sl_i(h_i)]$. Такий слід зберігається в *SZD* визначений час та використовується для виявлення несанкціонованого користувача. Слід $Sl_i(h_i)$ містить час і дату звернення, тип користувача, характер запиту та інші параметри, що дають змогу виявляти не тільки несанкціонованих користувачів *NK*, а й можливі аномалії. Дані, що формують слід кожного звернення, використовуються для формування історії образу користувачів. На рис. зображено функціональну схему організації системи *DIS*, в яку входить система *SZD*.

На рис. подано такі позначення:

- *KC* — засоби доступу користувача типу h_i^{c};
- *KF* — засоби доступу користувача типу h_i^{φ};
- *KA* — засоби доступу користувача типу h_i^{A};
- *SDC* — система контролю доступу користувача h_i^{c};
- *SDF* — система контролю доступу користувача h_i^{φ};
- *SOZC* — система оберненого зв'язку з користувачем h_i^{c};
- *SOZF* — система оберненого зв'язку з користувачем h_i^{φ};
- *SDA* — система контролю доступу користувача типу h_i^{A};
- *SZD* — загальна система захисту доступу;

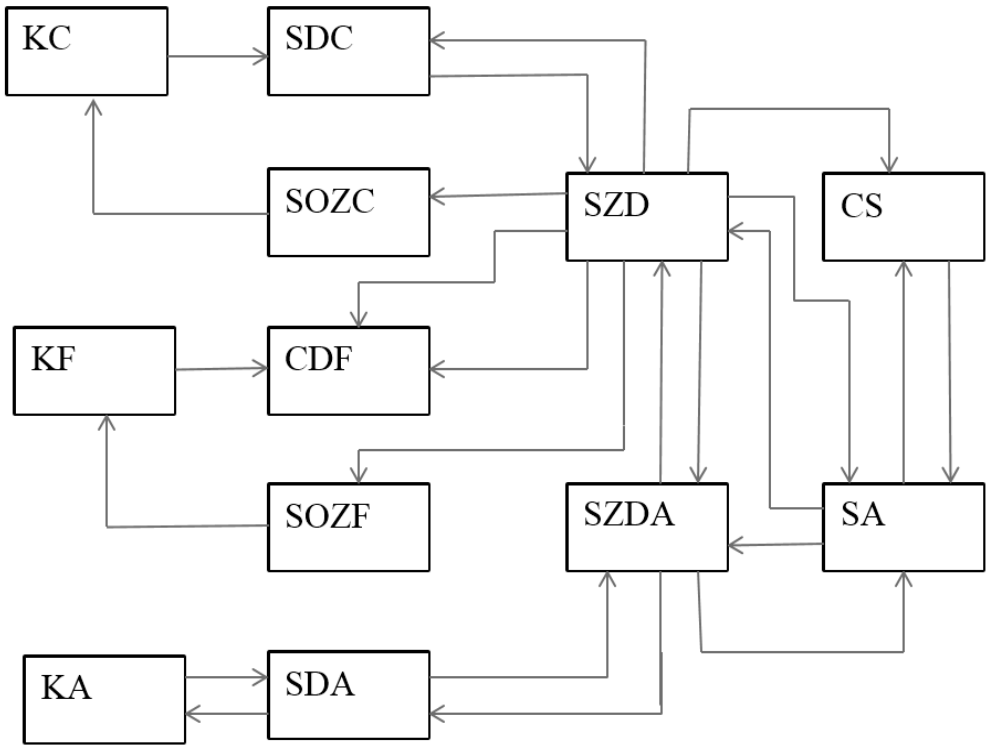

Рис. Схема організації системи

– *SZDA* — система модифікації захисту доступу з ініціативи користувача h_i^A;
– *CS* — база персональних даних соціальних користувачів;
– *SA* — система аналізу параметрів бази даних.

Ще однією компонентою, зовнішньою стосовно *SZD,* є система адміністрування роботою DCS_i. Система адміністрування складається з таких компонент:

– засоби доступу адміністратора *KA*;
– система контролю доступу адміністратора *SDA*;
– система аналізу рівня безпеки та модифікації захисту доступу з ініціативи адміністратора *SZDA*.

Адміністратор системи h_i^A є користувачем, який має найширші повноваження для роботи із системою. Це означає, що він повинен мати засоби управління рівнем безпеки системи, якими може користуватися на основі об'єктивних даних про такий рівень системи загалом, головною компонентою якої є база персональних даних CS_i. Тому користувач, який претендує на повноваження адміністратора, повинен перевірятися системою доступу повніше, ніж користувач типу h_i^c та h_i^φ. Це зумовлено ще й тим, що адміністратор має виконувати свої функції в рамках розподіленої системи і може не мати в момент співпраці зі системою окремих фізично виділених засобів доступу, які могли б міститися тільки в одному місці.

Очевидно, це не означає, що повне навантаження щодо автентифікації адміністратора покладається на стандартні для цієї розподіленої системи засоби. В рамках системи засобів захисту адміністратор, крім стандартних атрибутів доступу, володіє спеціальними атрибутами ідентифікації, що являють собою певне програмне забезпечення, вміщене на мобільному носії, який є власністю адміністратора. Таким носієм може бути пам'ять, що досить широко використовується, наприклад, пристрій типу «флеш пам'яті». Ця програма реалізована таким способом, що автентифікація адміністратора відбувається на основі випадково вибраних кроків процесу автентифікації. Алгоритми автентифікації адміністратора в разі, коли він реєструється з віддаленого хосту, сформовані так, що спосіб ідентифікації адміністратора на поточному кроці процесу передбачити досить складно. Функції автентифікації адміністратора виконує окрема компонента *SDA*.

Компоненти *SDC* і *SDF* реалізують процеси автентифікації користувачів h_i^c і h_i^φ не тільки у разі звертання останніх до системи, а й під час реалізації діалогу. В цьому випадку процес автентифікації виконується на кожному етапі реалізації діалогу. На різних етапах застосовуються різні алгоритми автентифікації, орієнтовані на використання різних персональних параметрів, які можуть бути відомими користувачеві. Система захисту доступу типу *SDC* і *SDF* для реалізації процесів автентифікації використовує персональні дані відповідних користувачів, якщо йдеться про користувачів h_i^c та інформацію про дані, які були введені відповідними користувачами типу h_i^φ в базу даних системи CS_i.

Наступною компонентою, яка застосовується для розв'язання задач захисту і не є функціональною частиною системи *SZD,* є система аналізу параметрів даних, що містяться в CS_i і позначаються як *SA* відповідно до рис. 1. Використання *SA* для задач захисту ґрунтується на таких положеннях. У CS_i, крім структурної інтерпретації даних, використовується описова інтерпретація даних, яка доповнює структурну та інші неявні форми інтерпретації. Описова інтерпретація являє собою текстові описи в нормалізованій формі параметрів, що характеризують групи даних, окремі дані та вибрані характеристики таких даних. Відповідні текстові описи реалізуються на мові користувача. Такі описи доповнюються числовими величинами, що безпосередньо стосуються відповідних даних $x_i \in CS_i$. Прикладом таких параметрів, що розміщуються в рамках текстових описів, можуть бути граничні значення, які визначають допустимі границі величини відповідних параметрів [3]. Система *SA* проводить аналіз даних $x_i \in CS_i$ на основі використання поточних значень цих даних, що порівнюються з параметрами даних, які містяться в їхніх інтерпретаційних описах. Інтерпретаційні описи даних у CS_i будемо позначати символами:

$$J(CS_i) = j(x_{i1}, \ldots, x_{im}) * j(x_{j1}, \ldots, x_{jki}) * \ldots * j(x_{r1}, \ldots, x_{rg}),$$

де $j(x_{k1}, \ldots, x_{kg})$ — група даних, що з погляду їх інтерпретаційного опису належать до одного класу даних, який ідентифікується індексом «*k*». У наведеному випадку використання відповідної (зовнішньої щодо *SZD*) компоненти потрібно розв'язати задачі, необхідні для реалізації функцій забезпечення потрібного рівня безпеки CS_i:

– визначити умови активізації процесів аналізу в рамках компоненти *SA*;
– сформувати алгоритм аналізу даних, який був би пов'язаний або обумовлений задачами захисту;
– розробити методи використання результатів задачі аналізу відповідних даних.

Для розв'язання цих задач треба встановити залежності, які визначали б порядок застосування кожної із зовнішніх компонент. Враховуючи інтерпретацію ефективності застосування кожної з компонент, приймемо пріоритети, згідно з якими система безпеки може використовувати зовнішні компоненти. Найефективнішим засобом виявлення небезпек є засіб, який реалізує діалог між *SZD* та користувачами h_i^c та h_i^φ. Ефективність у цьому випадку зумовлюється тим, що найповнішу інформацію про ймовірні небезпеки можна отримати від санкціонованих користувачів, які є авторами даних, що вводять у систему. Це дає можливість (щонайменше на основі порівняння даних від користувачів та даних, що є в системі) визначити наявність аномалій в CS_i, які могли виникнути в результаті успішних атак на задачі $A_t^u(Z_a)$. Враховуючи алгоритм використання даних, щоб виявити аномалії, вважатимемо, що засіб, який реалізує діалог з користувачами, повинен мати найвищий пріоритет його використання під час розв'язання задачі виявлення аномалій в CS_i.

Система адміністрування як зовнішня компонента, що використовується під час розв'язання задач захисту, має найширший асортимент можливостей щодо реалізації алгоритму виявлення та протидії атакам. Цей асортимент поширюється на реалізацію різних дій, на систему захисту, починаючи від призупинення вибраних процесів функціонування і закінчуючи діями, що приводять до елімінації тих чи інших фрагментів із системи CS_i. Можливості системи адміністрування використовуються насамперед тоді, коли необхідно терміново вживати певні заходи протидії атакам, які вже виявлені та ідентифіковані, або ця система застосовується в тих випадках, коли треба усунути можливі наслідки дії на систему успішних атак, що вже призвели до виникнення аномалій в системі. Це означає, що система адміністрування (*SAD*) для реалізації профілактичних дій має другий або нижчий пріоритет щодо системи діалогу. Але якщо потрібно реалізувати термінові дії для захисту системи, *SAD* має найвищий пріоритет. Отже, пріоритети є динамічними і залежать від поточного стану безпеки системи, який позначатимемо $RB(t_i)$, де t_i — поточний момент, в якому визначається значення величини *RB*. Для встановлення різних станів безпеки системи треба розглянути подані нижче визначення.

Визначення 1. Система CS_i перебуває у стані профілактичного забезпечення безпеки CS_i, якщо система захисту *SZ* реалізує поточний аналіз системи з ціллю виявлення аномалій в системі даних або загроз Zg_i, що можуть виникнути в системі CS_i.

Визначення 2. Система CS_i перебуває у стані аварійного забезпечення безпеки (*AZB*) в CS_i, якщо система захисту *SZ* реалізує процеси протидії атакам, які успішно реалізують свої функції.

Стан *AZB* виникає тоді, коли виявлені аномалії або атака, що їх необхідно елімінувати, щоб не допустити зміни величини *RB*, яка може набути недопустимих значень, що характеризують аварійний стан системи. Це означає, що той чи інший стан безпеки системи визначається величиною рівня безпеки RB_i. Крім рівнів RB_i,

що зумовлюють стан системи типу *PZB* і *AZB*, уведемо такі стани, в яких може перебувати система CS_i. Для цього розглянемо деякі визначення.

Визначення 3. Система CS_i перебуває в безпечному стані, що визначається системою захисту (*BZS*), якщо CS_i функціонує у штатному режимі.

Штатний режим функціонування означає, що параметри, які визначають процес її функціонування, перебувають у діапазоні значень, визначених технічними умовами на відповідну систему. Введемо шкалу рівнів захисту системи:

- безпечний рівень безпеки системи *BZS*;
- профілактичний рівень безпеки системи *PZS*;
- активний рівень безпеки системи *RZS*;
- стратегічний рівень безпеки системи *SZS*;
- небезпечний рівень безпеки системи *NZS*;
- аварійний рівень безпеки системи *AZS*.

Розглянемо визначення рівнів захисту системи, що позначається *RZS* (активний рівень), стратегічний рівень захисту (*SZS*) та небезпечний рівень захисту системи.

Визначення 4. Система CS_i перебуває на активному рівні безпеки, якщо процеси захисту системи реалізуються в мультиплексному режимі роботи CS_i.

Мультиплексний режим роботи CS_i означає, що на фоні процесів реалізації основних функцій системи реалізуються процеси її захисту [4]. Такий режим є можливий також у рамках всього комплексу CS_i, оскільки окремі системи, що входять до комплексу, реалізуються на окремих обчислювальних засобах і свої процеси функціонування у разі потреби синхронізують із процесами, що реалізують основні функції системи CS_i.

Визначення 5. Система CS_i перебуває на стратегічному рівні безпеки, якщо на цей рівень система перейшла відповідно до стратегії функціонування системи безпеки.

Визначення 6. Система CS_i перебуває на небезпечному рівні безпеки, якщо в CS_i засоби захисту виявили недопустимі відхилення значень параметрів функціонування, при яких основні функції системи ще зберігаються.

Виділення стану *NZS* зумовлене тим, що вихід окремого параметра, який характеризує штатний режим функціонування CS_i, не завжди призводить до порушень у процесі функціонування CS_i. Це пов'язано з тим, що CS_i функціонує в рамках різних процесів, кожний з яких визначається окремою задачею, на яку орієнтована CS_i. Тому така зміна функціонального параметра в CS_i може привести лише до того, що в рамках CS_i не буде розв'язуватися одна із задач. Таким чином, на фоні функціонування CS_i система *SB* активізує засоби діагностування, які дають змогу розв'язати такі задачі:

- виявлення причин, які призвели до недопустимого відхилення окремого параметра;
- виявлення несправності, що виникла в CS_i;
- виявлення атаки на CS_i, якщо несправність зумовлена зовнішнім фактором, який діє на систему;
- визначення типу несправності.

Процес виявлення несправності передбачає визначення її типу та місця локалізації в системі. Визначення типу несправності потребує з'ясування причини її виникнення. Виділення стану стратегічної безпеки зумовлене тим, що стратегія функціонування CS_i передбачає переходи системи з одного стану безпеки в інший у зв'язку з такими причинами:

– перехід на вищий чи нижчий рівень безпеки, зумовлений особливостями різних задач, які розв'язуються за допомогою системи CS_i;
– на основі дій, що пов'язані з адмініструванням системи, яке може полягати у проведенні фонових регламентних чи інших робіт, пов'язаних з аналізом CS_i.

Стратегічний стан системи не може співпрацювати зі суміжними станами *RZB* та *NZB*, а використовує визначені додаткові рівні безпеки, які перебувають на інтервалах [*RZB*, *SZB*] та [*SZB*, *NZB*]. Незалежно від стратегії функціонування CS_i загалом, у рамках системи CS_i можуть здійснюватися переходи з одного стану безпеки в інший стан безпеки, що відбуватиметься відповідно до схеми, поданої співвідношенням:

$$BZS \rightarrow PZS \rightarrow RZB \rightarrow SZS \rightarrow NZB \rightarrow AZS.$$

Подана функціональна схема відображає зміну рівня захисту, починаючи від безпечного рівня захисту і закінчуючи аварійним рівнем захисту. Очевидно, що в таких схемах можуть відображатися зв'язки між різними рівнями захисту, наприклад, між *RZB* і *PZS*, *NZS* і *SZS* та іншими. Наведені у співвідношенні послідовності допускають різну інтерпретацію величини безпеки системи. Наприклад, якщо припустити, що рівень захисту *AZS* або рівень безпеки $RB(AZS) > RB(NZS)$. Це означає, що при $RB(AZS)$ використовується максимальна кількість засобів захисту, а аварійність означає наявність факторів, що діють на CS_i, які можуть привести систему до аварійного стану. Попри це, з рівня безпеки *AZS* система може переходити на рівень безпеки *NZB*, якщо в CS_i використовуються засоби протидії негативним факторам, особливо зовнішнім, які діють на джерело атак, що його прийнято називати небезпекою, щоб унеможливити відповідну небезпеку генерувати атаки на CS_i [5]. Стан безпеки *NZS* передбачає наявність несправності в CS_i, яка виникає в результаті дії атаки At_i на CS_i, що була згенерована в небезпеці до моменту її блокування або нейтралізації засобами протидії небезпекам, наявними в рамках *SB* у комплексі, сформованому на базі CS_i.

Висновки. У статті розроблено структурну схему захищеної системи доступу до інформаційної системи. Запропоновані розширення засобів захисту системи доступу дають можливість не тільки підвищити захищеність системи від несанкціонованого доступу, але й оперативно змінювати величину безпеки окремих груп даних, що зберігаються в системі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Patton R. Issues of fault diagnosis for dynamic systems / R. Patton, P. Frank, R. Clark. Berlin : Spinger, 2000.
2. Chiang L. H. Fault Detection and Diagnosis for Dynamic Systems / L. H. Chiang, E. L. Russel, R. D. Bratz. Londjn : Springer Verlag, 2001.

3. Коростіль О. Ю. Аналіз параметрів текстових форм представлення інформації / О. Ю. Коростіль // Збірник наукових праць Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова. — 2013. — Вип. 67. — С. 89–97.
4. Gfrdner J. W. Mierosensors, MEMS, and smart devices / J. W. Gfrdner, V. K. Varadan, O. O. Awadelkarim. — Wiley&Sons, NewYork : Chichester, 2001.
5. Лукацкий А. В. Обнаружение атак / А. В. Лукацкий. — СПб. : БХВ-Петербург, 2001.

REFERENCES

1. Patton, R., Frank, P., & Clark, R. (2000). Issues of fault diagnosis for dynamic systems. Berlin: Spinger (in English).
2. Chiang, L. H., Russel, E. L., & Bratz, R. D. (2001). Fault Detection and Diagnosis for Dynamic Systems. Londjn: Springer Verlag (in English).
3. Korostil, O. (2013). Analiz parametriv tekstovykh form predstavlenniya informacii. NAN Ukraine. Zbirnyk naukovykh prats Instytutu problem modeliuvannia v enerhetytsi im. H. Ie. Pukhova, 67, 89–97 (in Ukrainian).
4. Gfrdner, J. W., Varadan, V. K., & Awadelkarim, O. O. (2001). Mierosensors, MEMS, and smart devices. Wiley&Sons. New-York: Chichester (in English).
5. Lukatskyi, A. (2001). Obnaruzheniye atak. Sankt-Peterburh: SPB: BHV (in Russian).

ALGORITHM OF PROTECTION FACILITIES FUNCTIONING OF THE SOCIAL INFORMATION SYSTEM

B. V. Durniak, T. M. Khometa

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

In the article the development of methods of protection facilities functioning of the access systems to the social information system has been examined. The system organization's chart which contains facilities of protection has been developed. The pictures of the different states of safety of social information system have been analyzed.

Keywords: *social information system, protection, security, system of access, dialog, feed-back connection.*

Стаття надійшла до редакції 24.02.2016.
Received 24.02.2016.