УДК 004.9.1

ОЦІНКА РІВНЯ БЕЗПЕКИ РІЗНИХ ТИПІВ ІНФОРМАЦІЇ

Б. В. Дурняк, Т. М. Хомета

Українська академія друкарства,
вул. Підголоско, 19, Львів, 79020, Україна

Розглядається вибір рівня захисту до різних типів інформації, які визначаються вартістю засобів захисту процесів, та вартістю затрат, до яких може привести зниження рівня безпеки. Рівень безпеки визначається на основі аналізу засобів захисту, або системи безпеки SB, яка забезпечує відповідний рівень безпеки. Безпека кожної з систем визначається захистом доступу із суміжних систем, захистом доступу користувачів, захистом доступу через несанкціоновані канали зв'язку (ICS) з зовнішнім середовищем.

Ключові слова: *аутентифікація, ідентифікатор, криптографічні протоколи, алгоритми, канали зв'язку, загроза.*

Постановка проблеми. Дослідження і розроблення методів визначеності рівня захищеності окремих компонентів в інформаційній соціальній системі необхідний для вибору рівня захисту до різних типів інформації, які визначаються вартістю засобів захисту процесів, та вартістю затрат, до яких може привести зниження рівня безпеки. Рівень безпеки необхідно визначати на основі аналізу засобів захисту, або системи безпеки *SB*, яка забезпечує відповідний рівень безпеки. Тому слід розглянути безпеку кожної з систем, яка визначається захистом доступу із суміжних систем, захистом доступу користувачів, захистом доступу через несанкціоновані канали зв'язку (*ICS*) з зовнішнім середовищем.

Мета статті полягає в дослідженні методів визначення необхідних рівнів захисту окремих фрагментів інформації в інформаційній соціальній системі.

Виклад основного матеріалу дослідження. Захист будь-якої інформації потребує можливості здійснення оцінки величини міри захисту, оскільки захист, як деяка властивість інформаційної системи, не може оцінюватися в рамках бінарної шкали. Це зумовлюється тим, що досягнути повної безпеки, яку можна було б ідентифікувати одиницею, досягнути важко, і в багатьох випадках це не доцільно. Доцільність чи недоцільність визначається вартістю засобів захисту та процесів, що її забезпечують, та вартості затрат, до яких може привести зниження рівня безпеки.

Рівень безпеки, в кінцевому випадку, визначається на основі аналізу об'єкта, який передбачається захищати, та на основі аналізу засобів захисту, або системи безпеки *SB*, яка відповідний рівень безпеки забезпечує. Оскільки в цьому випадку об'єктом захисту є інформаційні системи різного характеру, що орієнтовані на обслуговування соціальних потреб населення. Припустимо, що інформація різного типу, що знаходиться в інформаційних соціальних системах (*ICS*), не мусить захищатися однаковою мірою або забезпечуватися тим самим рівнем безпеки, незважаючи на те, що у всіх *ICS* наявні персональні дані. Це зумовлюється тим, що персональні дані, які стосуються окремої особи, можуть характеризуватися певною повнотою. Залежно від послуги, яку хоче отримати певна особа при використанні *ICS*, персональні дані такої особи можуть

мати різну міру повноти. Певний тип *ICS*, в залежно від характеру послуги, на надання якої система орієнтована, потребує певної міри безпеки. Безпека кожної з систем значною мірою визначається такими факторами:

– захистом доступу із суміжних систем;
– захистом доступу користувачів;
– захистом доступу через несанкціоновані канали зв'язку *ICS* з зовнішнім середовищем.

Для кожного типу *ICS* характерною є система доступу, яка орієнтована на забезпечення доступу до *ICS* користувачів. Міру захищеності системи доступу можна визначати на основі аналізу таких чинників:

– повноти ідентифікації користувача;
– вартості даних, що можуть бути використаними при несанкціонованому доступі, та вартості засобів захисту від несанкціонованого доступу (*NSD*);
– встановлених рівнів необхідного захисту, які визначаються декларативно.

Згідно з прийнятими уявленнями, ідентифікація реалізується на основі використання наступних даних [1]:

– ідентифікатора користувача;
– пароля користувача;
– особистих характеристик користувача.

Ідентифікатор являє собою деякий код, що використовується як ідентифікатор, який підтверджує особу, що відповідним ідентифікатором користується. Користувач такий ідентифікатор може використовувати у різних системах доступу, що належать до різних *ICS* до яких може звертатися користувач.

Пароль являє собою деякий код, який користувач може використовувати тільки при доступі до однієї системи *ICS* і, крім користувача, ніхто не повинен користуватися цим паролем. Цим відрізняється пароль від ідентифікатора.

Особисті характеристики споживача являють собою параметри, які фізично пов'язані безпосередньо із споживачем і досить широко використовуються у системах захисту. Типовим прикладом такого способу ідентифікації є використання відбитка пальців споживача [2].

Сучасні системи захисту для розв'язання задач аутентифікації використовують різні криптографічні протоколи, які, залежно від використання тих чи інших алгоритмів контролю та криптоалгоритмів, забезпечують досить високий рівень захисту доступу користувачів до системи. Прикладом поширених алгоритмів цього типу є алгоритми, що реалізують доведення з нульовим розголосом. Такий алгоритм реалізується шляхом використання досить великої кількості тактів перевірок і при цьому для ідентифікації передача таємниці перевіряючій стороні не здійснюється. Важливою відмінністю цього підходу є необхідність участі в процесі ідентифікації третьої сторони, яка гарантує, що таємниця, яка використовується в протоколі, не буде підмінена.

Для того щоб вибір тих чи інших методів захисту інформації був обґрунтований, що є необхідною умовою оптималізації використання певного рівня

захисту, потрібно проводити оцінку рівня захисту, або оцінку рівня безпеки інформації, в тій, чи іншій *ICS*. Відомі підходи до визначення такої оцінки використовують різні базові положення та принципи.

Один з таких підходів використовує уявлення про ризики. Уявлення про ризик передбачає необхідність аналізувати, при його визначенні, такі фактори:

– величини втрат, що зіставляються з конкретними сторонами процесів, які передбачається оцінювати параметром ризику;
– встановлення щонайменше двох сторін, які є учасниками процесу, що оцінюється величиною ризику для однієї сторони, яка визначає певну величину втрат;
– методи обчислення можливих втрат, до яких може призвести процес, який оцінюється ризиком.

Визначення значення ризику як величини втрат однією зі сторін, залежить від предметної області, в якій відповідні процеси відбуваються. Здебільшого оцінки ризику є величинами відносними.

Залежно від предметної області реалізації процесів, кількість учасників процесу може бути різна. Якщо розглядати величину ризику як бінарний параметр, наприклад, з погляду наявності втрат, тоді всі учасники діляться на дві сторони. Якщо ризик розглядається як величина, що може приймати ряд значень, то сторони, що беруть участь у певному процесі, розділяються на кількість груп, для яких визначаються різні значення величини ризику.

Наступний підхід до оцінки рівня захисту полягає у визначенні рівня безпеки системи. Цей підхід тісніше пов'язаний із засобами захисту, загрозами, що існують в об'єкті захисту, та небезпеками, які є джерелом атак на об'єкти, в даному випадку на системи *ICS*. На відміну від ризику, який, по суті, є інтегральною оцінкою безпеки деякого об'єкта, міра безпеки системи визначається на основі аналізу вартості засобів захисту та їх функціональних можливостей. Переважно розширення функціональних можливостей приводить до збільшення їх вартості. Оскільки основним фактором який обумовлює необхідність забезпечення певного рівня безпеки, який будемо позначати символом η, є атаки, що генеруються небезпеками, які виникають випадково, причому тип атаки здебільшого є фактором випадковим, тому більшість методів визначення рівня безпеки грунтуються на використанні методів теорії ймовірності [4].

Досить поширеним підходом до оцінки міри захищеності є декларативний підхід, який передбачає визначення певної системи оцінок компонент, які передбачається захищати. На основі аналізу тих чи інших елементів предметної області призначається їм оцінка необхідної величини захисту і, в залежно від інтерпретації відповідної оцінки щодо різних компонентів використовуються засоби захисту, можливості яких визначаються на основі порівняльного аналізу з іншими засобами захисту. Прикладом такого підходу може служити модель Белла-Лападули, в якій система оцінок захисту визначається наступними категоріями: надтаємний, таємний, довірчий і відкритий (*SS,S,DS,O*) [4]. Відповідні оцінки необхідного рівня захисту призначаються різним компонентам предмет-

ної області, наприклад, інформація про проведення певних операцій вибраними службами, інформація про особовий склад деякої служби та інші. Перший тип інформації може отримати категорію *SS*, а другий тип інформації – категорію *S*.

У рамках цієї роботи використовуватимемо підхід до оцінки необхідного рівня захисту, який буде ґрунтуватися на таких положеннях:

– інформація, що зберігається в різних типах систем *ICS*, яка може перекриватися;
– інформація, що знаходиться в рамках однієї системи і може бути розділена на різні класи, або, за аналогією з системою Белла-Лападули, буде ділитися на різні категорії, які встановлюються при проектуванні *ICS*, декларативно на основі аналізу предметної області;
– категорії даних, що знаходяться в різних *ICS* можуть змінюватися в процесі функціонування відповідних систем;
– можливі зміни категорії даних у *ICS* активізуються на основі аналізу зовнішніх втручань у систему;
– для характеристики даних або інформаційних фрагментів може використовуватися уявлення про надійність певних інформаційних образів у системах *ICS*.

Аналіз параметра, що характеризує перекриття тих чи інших даних, є досить важливим, оскільки в ситуації, коли в ICS_i певна інформація або інформаційний образ (Io_t) має категорію K_i, а той сам образ в ICS_j має категорію K_j, де $K_i<K_j$, то буде мати місце системне порушення безпеки інформації. Зазначимо, що інформаційні образи Io_i, які розміщаються в різних ICS_i змінюють свої характеристики в процесі функціонування системи, що може приводити до фактичної зміни категорії відповідного образу. Під інформаційним образом в цьому випадку будемо розуміти сукупність даних та текстів, які семантично складають одне ціле, яке називатимемо семантичною сутністю (*Ss*), або окремими елементами сюжету. Прикладом такого образу, який є спільним для всіх систем, є дані, що використовуються для ідентифікації користувача, або персональні дані, що використовуються для ідентифікації останнього, наприклад, дата народження, адреса проживання чи реєстрації і т. д.

При обслуговуванні користувача деякою системою ICS_i, обслуговування, що полягає у наданні користувачу Io_i, може мати різну глибину та різні розміри. Будь-яка інформація може бути виміряна углиб, якщо вона може бути представлена у вигляді деревовидної структури або деякої ієрархічної структури.

Визначення 1. Глибина відображення інформаційного фрагмента, який являє собою Io_i, визначається величиною максимальної віддалі між вершинами структури Io_i та кінцевими вершинами відповідної структури, що формально записується у вигляді співвідношення:

$$Гg_i\ (Io_t)=max_k \sum_j^{(mi-1)}[v_{i[j,(j+1)]} \in S(Io_t)],$$

де $S(Io_t)$ – структура опису Io_i,$v_{(i[j,(j+1)])}$ – ребро, що складає *i*-тий відрізок між вершиною структури $S(Io_t)$ та кінцевою вершиною m_{i-1} окремої дороги в структурі $S(Io_t)$.

Визначення 2. Повнотою образу Io_i називається сума всіх доріг від вершини структури $S(Io_i)$ до всіх її кінцевих вершин, що формально описується співвідношенням:

$$Po_i(Io_i)=\sum_{(i=1)}^{k}\sum_{j}^{(mi-1)}[v_{i[j,(j+1)]}\in S(Io_i)],$$

де k – кількість доріг у структурі $S(Io_i)$, m_i – кількість вузлів окремої дороги від вершини до одного з кінцевих вузлів структури $S(Io_i)$.

Визначення необхідної міри захищеності, яка визначається декларативно, здійснюється для інформаційних образів Io_i за допомогою використання параметрів $Гg_i$ та Po_i. Для того щоб семантика окремих фрагментів образу $i0_j \in Io_i$ була узгоджена з категоріями, що визначають необхідну міру захисту, при формуванні ICS_i необхідно виконувати такі вимоги:

– формування образів $Io_i ICS$ повинно здійснюватися із вибраною структурою, яка приймається для всіх типів *ICS* і якості інваріанта;
– рівні міри захищеності, що визначаються категоріями K_i, повинні бути спільними для структурно інваріантних фрагментів Io_i та системи *ICS* в цілому;
– кількість категорій, що використовуються системою захисту, або системою безпеки, може розширюватися;
– міра захищеності окремих Io_i в процесі експлуатації *ICS* може мінятися;
– для модифікації системи *ICS* повинні використовуватися правила, які враховують значення категорій ($K_i Io_i$).

Структура довільних ICS являє деяку деревоподібну структуру, яка фактично є графом типу дерева. Такий граф буде описуватися співвідношенням:

$$G^D(ICS)=F\{K_1[S_1(Io_1)], \ldots, K_m[S_m(Io_m)]\}$$

де G^D – граф типу дерева, $K_i[S_i(Io_i)]$ – категорія міри захищеності K_i для фрагменту структури S_i дерева G^D, Io_i – окремий інформаційний образ, структура якого є S_i, F – функція, що описує взаємозв'язок між окремими структурними фрагментами S_{ij}, які враховують відповідні значення категорії K_i. Оскільки G^D являє собою деревоподібний граф, то функція F описується оператором імплікації, який визначає послідовність з'єднання окремих фрагментів структур. Формально це означає, що функція F на G^D задає впорядкованість між окремими $S_i(Io_i)$ та $S_j(Io_j)$, яка не обов'язково відповідає натуральній послідовності величин індексів кожного зі структурних фрагментів.

Оскільки різні системи *ICS* орієнтовані на обслуговування тих самих користувачів, то це означає, що у різних ICS_i та ICS_j повинні існувати структурно спільні інформаційні фрагменти. Наприклад, якщо в ICS_i існує фрагмент $i0_j Io_i$, що відображає дані для ідентифікації користувача p_i, та в системі ICS_j, до якої може звертатися цей самий користувач, буде фрагмент, що вміщає ті самі дані, які є аналогічними чи модифікованими персональними даними, то відповідні фрагменти $i0_{jk} \in Io_i$ в ICS_i та $i0_{er} \in Io_j$ з ICS_j будуть структурно еквівалентними. Формально це описується таким співвідношенням:

$$\{[[io_{jk}=t(p_i)]\in S(ICS_i)]\&[[i0_{er}=t(p_i)]S(ICS_j)]\}\rightarrow$$
$$\rightarrow In[S(io_{jk})\&S(i0_{er})]=In[S(io^*(i,j))],$$

де $t(p_i)$ – опис даних, що ідентифікують користувача p_i, io_{jk} – інформаційний образ ідентифікації p_i в ICS_i, $i0_{er}$ – інформаційний образ ідентифікації p_i в ICS_j, $i0_{er}$ і $io^*(i,j)$ – узагальнений, ідентифікуючий образ p_i, In – ідентифікатор інваріантності двох інформаційних образів, що ідентифікують того самого користувача. Розглянемо наступне твердження.

Твердження. Якщо два інформаційні образи структурно інваріантні, то вони оцінюються однаковою категорією.

Формально це твердження описується таким чином:

$$In[S(io_{jk})\&S(i0_{er})]\rightarrow\{[K_j(io_{jk})=K_e(io_{er})]\rightarrow(K_j=K_e)\}.$$

Категорія K_i визначає оцінку міри захищеності. Структура деякого фрагмента інформації в рамках системи ICS_i відображає послідовність перетворень деяких вхідних даних $\{f_{i1}(a_i)^*...^*f_{ik}(a_i)\}$, яка дозволяє на кінцевому кроці перетворень одержати інформаційний елемент, що охороняється, а міра охорони визначається категорією K_i. Якщо K_i задається декларативно, то відповідно до K_i задаються перетворення, які забезпечують рівень захисту, що відображає K_i. Очевидно, що для різних io_{jk}, що в рамках $S(ICS_i)$ мають однакову структуру $S(io_{jk})=S(i0_{er})$, то це означає, що має місце співвідношення:

$$\{f_1(a_i^k)^*...^*f_m(a_i^k)\}\propto\{f_1(a_i^r)^*...^*f_m(a_i^r)\},$$

де a_i^k і a_i^r використовуються як параметри процедур перетворень, що орієнтовані на збереження рівня захисту категорії K_i. Таким чином, може мати місце співвідношення:

$$(io_i^k\neq io_i^r)\&[K_j(io_{jk})=K_j(io_{ek})].$$

Оцінка міри захищеності може змінюватися в процесі функціонування інформаційної системи. Така зміна може ініціюватися:

– авторами даних, що впроваджуються в ICS_i;
– адміністраторами, що обслуговують систему;
– при активізації вибраних процедур, які передбачаються в системі [5].

Будь-яка інформація, що стосується користувача P_i, вноситься в ICS_i обслуговуючим персоналом відповідної системи згідно з вказівками авторів відповідної інформації. Переважно системи типу ICS_i забезпечуються прив'язуючими інтерфейсами if_i, які орієнтовані на різних фахівців, що мають повноваження на впровадження даних, що стосуються P_i, у ту чи іншу систему ICS_i. Прикладом таких фахівців можуть бути лікарі, якщо мова йде про медичні ICS_i працівники тієї чи іншої служби, якщо ICS_i використовується при функціонуванні відповідної служби і т. д. Згідно з регламентуючими документами, кожний з фахівців, що використовує ICS_i, вводить, крім самих даних, категорію цих даних, яка, по суті, являє собою міру оцінки їх захисту. Очевидно, що в цьому випадку в рамках систем безпеки SB, що обслуговує відповідну ICS_i, або $SB(ICS_i)$, існують засоби захисту Zg_i, які можуть забезпечувати задану міру захисту K_i. В цьому випадку може виникати ситуація, коли користувач системи або фахівець, що використовує систему, впроваджує той, чи інший рівень захисту деякого $io_{jk}\in Io_i(P_i)$ у вигляді впровадження категорії $K_i(io_{jk})$, що може привести до виникнення аномалії безпеки, яку будемо позначати ab_i. Можливість виникнення таких аномалій пов'язана з наступним. Інформаційний фрагмент

io_{jk}, що вводиться користувачем, який є фахівцем P_i^{φ}, може отримати категорію K_i, яка є несумісною з категорією фрагмента io_i^v, для якого фрагмент io_{jk} є розширенням, а рівень захисту $K_i(io_i^v)>K_i(io_{jk})$. Це означає, що інформаційний образ io_{jk} є розширенням інформаційного образу io_i^v, а призначений фахівцем P_i^{φ} рівень захисту K_i. для нового фрагмента io_{jk} є менший, ніж відповідний рівень захисту фрагмента io_i^v. Оскільки $K_i(io_i^v)$ визначається структурою $S_i(io_{iv})$, то розширення io_i^v. з іншим K_i, потребували б проведення зміни структури у відповідному інформаційному образі. Це є недопустимо, оскільки структуризація системи ICS_i реалізується на основі аналізу семантики інформаційних образів, їх взаємозв'язків та образних залежностей між ними. Прикладом такої структуризації може бути наступний спосіб поділу інформації в медичній ICS_i:

– персональна інформація, що використовується для аутентифікації p_i;
– інформація про загальний стан здоров'я p_i;
– інформація про окремі специфічні захворювання;
– інформація про профілактичні огляди і т. д.

Відповідні правила узгодження наявних категорій з категоріями, що вводяться у зв'язку з розширеннями та модифікацією існуючих Io_i, стосуються не тільки розширення фрагментів Io_i, а і всіх інших операцій, які можна здійснювати з інформацією. До таких операцій модифікації належать такі:

– дописування нових даних, що позначається символом запису W;
– заміною інформації в існуючих фрагментах, що позначається символом *Z*;
– перенесенням фрагмента Io_{jk} з одного структурного вузла в інший структурний вузол *H*;
– усунення фрагменту Io_{jk} зі структурного вузла $S_i(io_i^v)$, що позначається символом *D*;
– формування нового вузла структури інформаційного образу, що позначається символом *N*.

Для наведених способів модифікації використовуються наступні правила встановлення нових значень необхідної міри захисту, або типу категорії K_i.

Правило 1. При розширенні фрагмента Io_i, для якого встановлено категорію K_i, фрагмент Io_{jk}, для якого визначена категорія K_j, розширений фрагмент приймає категорію, яка визначається наступним співвідношенням:

$$\{[K_i(Io_i)\cup K_j(io_j)]\&(K_i>K_j)\}\rightarrow K_i(Io_i,io_j),$$
$$\{[K_i(Io_i)\cup K_j(io_j)]\&(K_i<K_j)\&[\alpha(Io_i)<\beta(io_j)]\}\rightarrow K_j(Io_i,io_j),$$

де α і β – значимість міри захисту відповідних фрагментів.

Правило 2. Якщо у фрагменті $Io_i=\{io_{i1},...,io_{im}\}$ проводиться заміна io_{ij} на io_{ik}, і для Io_i встановлено категорію K_i, а для io_{ik}, встановлено категорію K_j, то після проведеної заміни $Io_i^*=\{io_{i1},\ldots,io_{ik},\ldots,io_{im}\}$, фрагмент Io_i^* отримує категорію відповідно до наведеного співвідношення:

$$\{[K_i(Io_i)*K_j(io_{ij})]\&(K_i>K_j)\}\rightarrow K_i[(Io_i/(io_{ij}))\cup io_{ik}]=K_i(Io_i^*),$$
$$\{[K_i(Io_i)*K_j(io_{ij})]\&(K_i<K_j)\&[\alpha(Io_i)<\beta(io_{ik})]\}\rightarrow K_j(Io_i^*).$$

Правило 3. При перенесенні фрагментів io_{ik} з структурного вузла Io_i у структурний вузол Io_j, відповідні вузли приймають категорії відповідно до співвідношення:

$$\{[K_i(Io_i/io_{ik})\rightarrow[io_{ik}\rightarrow K_j(Io_j)]]\&(K_i>K_j)\&[\alpha(io_{ik})>\beta(Io_j)]\}\rightarrow[K_i(Io_j\cup io_{ik})=K_i(Io_j^*)],$$
$$\{[K_i(Io_i/io_{ik})\rightarrow[io_{ik}\rightarrow K_j(Io_j)]]\&(K_i<K_j)\}\rightarrow[K_j(Io_j\cup io_{ik})=K_j(Io_j^*)].$$

Правило 4. Якщо з фрагмента Io_i, який являє собою вузол структури $S(Io_i)$, усувається фрагмент io_{ik}, то перетворення фрагмента вузла $S(Io_i)$, який має категорію K_i, реалізується наступним чином:

$$\{[K_i(Io_i/io_{ik}]\&\forall(io_{ik}\in Io_i)\exists io_{ik}[K_i(io_{ik})]\}\rightarrow[K_{i-1}(Io_i/(io_{ik})=K_{i-1}(Io_i^*)].$$

Правило 5. Для формування нового вузла деякої структури $S(ICS)=\{K_i(Io_i)*...*K_{i+m}(Io_{i+m})\}$ формується новий вузол Io_j, то перетворення структури $S(ICS)$ реалізується згідно з наступним перетворенням:

$$\{\{[K_i(Io_i)*\ldots*K_{i+m}(Io_{i+m})]\&K_j(Io_j)\&[j\in(i,...,m)]\}\rightarrow[\forall K_i\exists K_i[j=(i+j)\in (i,...,i+m)]]\rightarrow[K_i(Io_i)*...*K_j(Io_{i+j})*...*K_{i+m}(Io_{i+m})]\}.$$

Наведені вище правила можуть бути розширені у випадку використання додаткових операторів у середовищі інформаційних образів системи ICS_i. Оскільки категорії відносяться до інформаційних образів, то їх категорії на початковому етапі визначаються на основі спеціальних списків елементарних інформаційних образів io_{ik}, які в сукупності складають структурний вузол всієї системи ICS_i. та всіх її розширень.

Формуючи систему категорій, необхідно враховувати такі особливості:

– індексація категорій впорядковує останні в порядку зростання необхідної міри безпеки, яка повинна забезпечуватися засобами захисту та $SB(ICS_i)$ в цілому;
– кількість різних категорій не обов'язково повинна відповідати кількості різних засобів захисту з ICS_i;
– різний рівень захисту може забезпечуватися комбінацією різних категорій.

Використання індексації для впорядковування рівнів захисту, які ідентифікуються категоріями K_i де $(i=1,...,m)$, є відомим та широко використовуваним способом впорядковування множин. Тому більш детально розглядати цей аспект немає сенсу.

З огляду на те, що кількість категорій не обов'язково мусить відповідати кількості засобів захисту Zg_i з SB, можна прийняти, що ряд категорій може забезпечуватися наступними способами:

– використанням певних комбінацій $Zg_i\in SB$;
– залежностями між категоріями, які в рамках одного структурного вузла можуть відповідати різним рівням захисту по відношенню до окремих складових фрагментів інформаційного образу $io_{ik}\in Io_i$, які визначаються як елементарні інформаційні образи;
– окремі категорії можуть визначатися також на основі значимостей міри захисту окремих фрагментів, яка встановлюється на основі семантичного аналізу окремих елементарних інформаційних образів і описується наступним чином $a(io_{ij})$.

Висновки. В статті досліджується оцінка рівня захисту інформації яка ґрунтується на наступних положеннях: інформація, яка зберігається в різних

типах систем *ICS*, може перекриватися, інформація, по системі Белла-Лападули ділиться на різні категорії, які можуть змінюватися в процесі функціонування відповідних систем. Можливі зміни категорії даних в *ICS* активізуються на основі аналізу зовнішніх втручань в систему.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях. — М. : КУДИЦ-ОБРАЗ, 2001.
2. Биометрическая аутентификация: Обзор // Защита информации. — 1994. — N2. С. 29-30.
3. Вентцель Е. С. Теория случайных процессов и её инженерные приложения. — М. : Наука, 1990.
4. Зегжда Д. П., Ивашко А.М. Как построить защищённую информационную систему. — СПб. : Мир и семья – 95, 1997.
5. Анин Б. Ю. Защита компьютерной информации. — СПб. : БХВ — Санкт-Петербург, 2000.

REFERENCES

1. Ivanov, M.A. (2001). *Kriptograficheskie metody zashchity informatsii v kompiuternykh sistemakh i setiah.* M.: KUDITS-OBRAZ [in Russian].
2. Biometricheskaia autentifikatsiia: Obzor. (1994). *Zashchita informatsii*, 2, 29–30 [in Russian].
3. Venttsel, E.S. (1990). *Teoriia sluchainyh processov i eio inzhenernye prilozheniia.* M.: Nauka [in Russian].
4. Zegzhda, D.P., & Ivashko, A.M. (1997). *Kak postroit zashchishchonnuiu informatsionnuiu sistemu.* SPb.: Mir i Semia [in Russian].
5. Anin, B.Yu.(2000). *Zashchita kompiuternoi informatsii.* SPb.: BKhV – Sankt-Peterburg [in Russian].

ASSESMENT OF THE SECURITY LEVEL OF DIFFERENT TYPES OF INFORMATION

B. V. Durniak T. M. Khometa

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

The choice of protection level for different types of information is studied. They are determined by the cost of means of protection processes, and cost of expenses which can be the result of decreasing of security level. Security level is defined on the basis of analysis of security means, or SB security system, which provides the relevant security level. The safety of each system is determined by the access protection from contiguous systems, users access protection, access protection through unauthorized ICS data links with external environment.

Keywords: *authentication, identifier, cryptographic protocols, algorithms, data links, threat.*

Стаття надійшла до редакції 30.06.2015.
Received 30.06.2015.