УДК 004.047

ВИЗНАЧЕННЯ ЗАЛЕЖНОСТІ МІЖ ЗАСОБАМИ ЗАХИСТУ ТА ОЦІНКАМИ РІВНЯ БЕЗПЕКИ ДАНИХ В СОЦІАЛЬНИХ СИСТЕМАХ

Б. В. Дурняк, Т. М. Хомета

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

В статті проаналізовано і досліджено реальні небезпеки Nb_i, які можуть активізувати, або не активізувати атаки, що сприяють виникнення процесів зміни рівня безпеки деякої системи, а також наявність загроз, які використовують атаки для проникнення в середовище об'єкта захисту.

Ключові слова: *Профіль безпеки, загрози Zg_i, атаки At_i, елімінація, небезпека , декларований рівень, аномальні значення параметрів процесу функціональний аналізатор, ідентифікатор, етикетка.*

Постановка проблеми. Розглядається проблема з забезпеченням заданого рівня безпеки інформаційної системи, що обумовлюється можливістю використання відповідних засобів захисту, яка визначається їх ціною та функціональними можливостями забезпечення необхідного рівня захисту.

Аналіз останніх досліджень та публікацій. Вивченням методів захисту інформаційних систем, що використовуються в соціальній сфері та засобах масової інформації займалися як вітчизняні так і зарубіжні вчені серед яких Корченко, Tardo, Amorozo, Зегжда, Івашко та інші. Дослідження і розроблення методів визначеності рівня захищеності окремих компонентів в інформаційній соціальній системі необхідні 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.

Мета статті – полягає у визначенні залежності між засобами захисту та оцінками рівня безпеки даних інформаційної системи.

Виклад основного матеріалу дослідження. Визначення оцінок рівня безпеки інформаційної системи має сенс, якщо існують інструменти захисту, які можуть забезпечувати адекватний рівень безпеки. Проблема з забезпеченням заданого рівня безпеки обумовлюється наступними факторами:

- можливістю використання відповідних засобів захисту, яка визначається їх ціною та функціональними можливостями забезпечення необхідного рівня захисту;
- існуванням реальних небезпек Nb_i, які можуть активізувати, чи не активізувати атаки, що фізично обумовлюють виникнення процесів зміни рівня безпеки деякої системи;
- наявність загроз, які характеризують об'єкт захисту і є елементами, які використовують атаки для проникнення в середовище об'єкту захисту.

У відповідності із стандартами, є загальновідомими вимоги до захисту, що формуються в залежності від системи, яку необхідно захищати [1]. Такі вимоги для кожної системи формуються в рамках проекту безпеки у вигляді профілю безпеки конкретної системи [2]. В такому профілі системи сформульовані конкретні вимоги до засобів захисту, які повинні використовуватися, щоб такий профіль забезпечити. Таким чином, початковими даними, для створення профілю безпеки, є дані, що отримані на основі аналізу втрат, до яких може привести успішна атака, протидія якій могла би бути не передбачена в профілі, а також законодавчі акти, що регулюють правила та формулюють умови способів використання відповідних даних. Одним з базових юридичних документів є закон про захист персональних даних громадян держави та інші. Відповідні стандарти визначають необхідні засоби захисту, що орієнтовані на захист вказаних у стандартах компонентів *ICS* та процесів, які активізуються при використанні *ICS*. Приведені стандарти формуються таким чином, що в них важко відслідкувати однозначну залежність між вимогами до захисту та конкретними засобами захисту. Це обумовлюється наступними причинами:

- засоби захисту в багатьох випадках є багатофункціональними, тому, їх важко співставляти з вибраною небезпекою;
- різні засоби захисту, що функціонально орієнтовані на одну і ту ж небезпеку, а точніше, атаку, можуть мати різну ефективність протидії атаці;
- може мати місце ситуація, коли небезпека Nb_i не активізує атак певного типу на об'єкт, незалежно від того, що стандарт передбачає необхідність забезпечувати захист від вибраної атаки;
- кожна з атак, що активізується Nb_i, використовує відповідну загрозу Nb_i, які часто називають слабим місцем системи, при цьому, у адміністратора системи, може не бути можливості відповідну загрозу елімінувати.

Досить важливим фактором, що впливає на роботу *SB*, є виникнення атак активізованих небезпекою Nb_i. З різних причин такі атаки можуть не виникати, якщо відповідна Nb_i не виявляє інтересу до певних даних. У зв'язку з цим, в *SB*(*ICS*) реалізуються засоби реєстрації виникнення атак, реалізація яких була успішною, крім того, реєструються атаки, які були виявлені і проти яких були успішно використані засоби протидії атакам та на основі зібраних даних, *SB*(*ICS*) проводить статистичні оцінки, що характеризують відповідні події. Завдяки таким оцінкам, *SB*(*ICS*) має можливість провести оцінку міри необхідності окремих засобів захисту незалежно від того, чи вони визначені профілем безпеки, як необхідні, чи ні.

В даній статті, не будемо проводити аналіз різних типів атак та способів протидії атакам, оскільки, ці задачі досить широко розглядаються в цілому ряді робіт по захисту інформаційних систем [3,4]. В багатьох випадках, процеси протидії можливим атакам полягають у виявленні загроз, які існують безпосередньо в об'єкті захисту та у їх елімінації. Це означає, що по відношенню до самих небезпек ніяких дій не приймається. Відомо, що ліквідація Za_i в об'єкті переважно зводиться до модернізації окремих фраг-

ментів самого об'єкту, або до модернізації засобів захисту, які в об'єкті уже використовуються. Такий підхід може приводити до того, що відповідна Nb_i дістає можливість розвиватися в напрямку розширення та покращення своїх можливостей в здійсненні тих, чи інших атак. Для того, щоб можна було вести мову про повноцінну протидію негативним факторам, необхідно не тільки розширювати можливості системи *SB*(*ICS*), а і здійснювати міри, які дозволили би обмежувати самі Nb_i. Теоретично, така можливість існує, але нею можна скористатися лише в тому випадку, якщо стався інцидент втрат, які обумовлюються відповідною Nb_i. Така можливість використовується на основі використання зовнішніх засобів юридичного характеру, які досить важко ефективно використовувати через цілий ряд юридичних особливостей, які не мають безпосереднього відношення до *SB*(*ICS*) та системи в цілому [5]. У зв'язку з цим, в протидії засобів *SB*(*ICS*) виявленим Nb_i залишаються наступні можливості:

- реагувати на атаки At_i, що активізуються Nb_i, не тільки простою протидією At_i, що відразу виявляється системою Nb_i, а і в процеси протидії включати функції, які імітують успішність дії виявленої атаки;
- ідентифікувати Nb_i по їх виявлених атаках $At_i \in Nb_i$ і блокувати можливість взаємодії з системою, яка ідентифікована, як Nb_i, не тільки у випадках її негативної дії на об'єкт, а і у всіх інших випадках процесу функціонування Nb_i, як деякого легального учасника мережі Internet;
- у випадках реалізації цілого ряду атак на деякий об'єкт, здійснювати протидію відповідній Nb_i з ціллю унеможливити стороною Nb_i реалізації відповідних атак на вибраний об'єкт.

Перший підхід досить активно використовується, якщо затрати на такого типу протидії є нижчими від затрат, до яких приводять відповідні атаки. Однією з таких технологій є відома технологія honey pot, яка полягає у створенні імітаторів вхідних параметрів системи, до якої здійснюється несанкціоноване втручання. Дана система працює наступним методом. При звертанні деякої небезпеки, якою в мережі може бути окрема система, засоби захисту розпізнають в такому звертанні атаку і переключають її на входи засобів захисту, що моделюють оригінальну систему в рамках необхідної реакції оригінальної системи таким засобом, який відповідає випадку, в якому атака є не розпізнана. Відповідна ситуація може мати місце і в тому випадку, коли всі зовнішні потоки подаються на входи системи імітації. Остання розпізнає атаку і діє так само, як було описано вище. Якщо атака не розпізнана, то приймається, що вхідний потік є санкціонованим і в подальшому з адресатом працює оригінальна система. Для співставлення оцінки такого засобу захисту, яка визначає міру захисту, який цей засіб забезпечує, визначають наступним співвідношенням:

$$C(Zg_i) = (Sz - Ra)/(Sz + Na), \quad (1)$$

де $C(Zg_i)$ - оцінка безпеки, яку забезпечує засіб *Zgi*, *Sz* – сума всіх звернень за певний прийнятий період часу, *Na* - невиявлені атаки, *Ra* - виявлені атаки. Якщо *Ra=Na=0*, то $C(Zg_i)$=1 а це означає, що *Zgi* не доцільно використовувати.

Приведений метод оцінки ґрунтується на використанні відомих даних про кількість *Ra* та *Na*. Очевидно, що на початку процесу функціонування $C(Zg_i) = 1$ і необхідність використання відповідного Zg_i не може бути встановлена виходячи з приведеного прикладу. Але, крім реального стану безпеки, який визначається на основі даних про атаки, що відбулися на об'єкт, існує декларований рівень необхідної безпеки, який задається категоріями K_i. Очевидно, що визначення категорій грунтуються на певних методах прогнозування. Тоді, виникає питання, як вибирати для заданої категорії K_i той чи інший засіб захисту, оскільки співвідношення (1) можна використовувати для довільного Zg_i.

Вирішення цієї задачі буде ґрунтуватися на уявленнях про функціональність атак At_i та функціональність засобів захисту Zg_i. Отже, введемо наступні визначення.

Визначення 3. Міра функціональності Zg_i визначається кількістю функціональних аналізаторів, які реалізуються в рамках Zg_i.

Один функціональний аналізатор представляє собою один з алгоритмів виявлення аномальних значень параметрів процесу, що може бути носієм події, яка є елементом атаки. Наприклад, одним або одиничним функціональним аналізатором є алгоритм аналізу вхідних і вихідних адрес чергового пакету, що передається на вхід брандмауера, або мережного фільтра. Виходячи з наведеного прикладу, можна для кожного засобу захисту Zg_i встановити його міру функціональності. В цьому випадку, міра функціональності буде визначатися таким співвідношенням:

$$f_i(Zg_i) = \sum_{j=1}^{m} f_{ij}(g_i), \tag{2}$$

де $f_i(Zg_i)$ - алгоритм, що реалізує певний тип перевірки деякої компоненти, що реалізує окремий фрагмент процесу, який реалізується в середовищі, що захищається. На цьому рівні можна прийняти, що оцінка рівня безпеки, який забезпечує окремий засіб захисту *Zgi*, визначається мірою функціональності цього засобу.

Для встановлення зв'язку засобів захисту з категорією K_i, яка призначена для вибраної системи, використовується уявлення про профіль безпеки $Pr(SB)$, який є інтегральним значенням міри безпеки системи ICS_i. Профіль безпеки визначає, які фрагменти процесів, що функціонують в системі, і яким чином повинні бути захищені, що формально описується співвідношенням:

$$\Pr(ICS) = F[Za_1 * \ldots * Za_m], \tag{3}$$

де Za_1 - ідентифікатор загроз, що існують в системі, F - функція, що описує взаємозалежності між загрозами. По своїй суті, міжнародні стандарти, що визначають засоби захисту деякої системи, визначають загрози, які існують у системі або слабкі місця системи. Таким чином, профіль безпеки Pr (*ICS*) визначає загрози Za_i, що необхідно елімінувати шляхом використання засобів захисту. Такий підхід до визначення рівня безпеки не є достатньо конструктивним, оскільки в дійсності існує наступна ситуація. Відомо, що загрози елімінуються наступними методами:

– шляхом модифікації тих, чи інших функцій системи в цілому, при чому, локалізація таких модифікацій може не співпадати з локалізацією самої загрози;
– шляхом використання додаткових програмних, чи апаратних засобів, використання яких дозволяє елімінувати відомі методи використання відповідних загроз небезпекою з ціллю активізації в об'єкті захисту відповідної атаки.

Основний недолік такого підходу полягає у тому, що деякий засіб захисту буде відповідати вимогам Pr (*ICS*) в тому випадку, коли його використання дозволить протидіяти активізації атаки тоді, коли цей засіб протидіє тільки одній версії реалізації атаки. Якщо атаки ідентифікувати не по способу її дії на об'єкт атаки, а по способу реалізації атаки, які описуються послідовністю подій, виникнення яких приводить до виникнення атаки, то у випадку зміни хоча би однієї події в процесі реалізації атаки, остання прийме форму нової версії атаки. Така нова версія атаки уже може бути не передбачена тим, чи іншим засобом захисту. Це обумовлюється тим, що довільний Zg_i спочатку розпізнає факт активізації атаки і тільки після цього здійснює протидію відповідній атаці. Якщо ознаки атаки змінилися, то атака не буде розпізнана і остання успішно подолає відповідний засіб захисту.

Важливим випадком порушення рівня безпеки системи *ICS*, є порушення, яке не достатньо повно розглядається та вивчається. Таке порушення полягає у скритому несанкціонованому доступі, який будемо позначати символами *SND*. Суть цієї небезпеки полягає у наступному. Можуть мати місце ситуації, коли санкціонований користувач відноситься до цієї групи користувачів тільки тому, що він має необхідні атрибути для отримання доступу, наприклад, пароль та ідентифікатор. Такий користувач, отримавши доступ до системи, може здійснювати операції, які можна віднести до несанкціонованих. Розпізнавання такого типу порушень є досить складним і може ґрунтуватися на наступних принципах та методах виявлення *SND*:

– для виявлення *SND* деякого користувача p_i, можна використовувати профіль користувача, який вміщає історію функціонування p_i в системі;
– якщо, для формування профілю p_i не має необхідної інформації про історію функціонування p_i в середовищі *ICS*, то для виявлення *SND*, використовуються профілі даних, з якими відповідний p_i планує працювати в *ICS*, або які p_i планує використовувати;
– для протидії *SND* можна використовувати спеціальні етикетки окремих об'єктів системи, до яких користувач планує звертатися після отримання доступу в *ICS*.

Кожний користувач, який володіє актуальними засобами аутентифікації, може характеризуватися характером використання засобів *ICS*, який формується на основі даних про цей характер на попередніх етапах співпраці p_i з *ICS*. Такий профіль p_i являє собою опис об'єктів, які використовувались користувачем у попередніх сеансах роботи користувача з системою, характер перетво-

рень відповідних об'єктів, наприклад, тільки читання, чи тільки модифікація даних та інші. Крім цього, такий профіль вміщає зовнішні дані, наприклад, час роботи з системою, період її використання та інші характеристики, що відносяться, в основному, до p_i. Параметри, про які йде мова у профілі користувача, характеризуються попередньо визначеними допустимими відхиленнями.

Формування профілю об'єкту, з яким може працювати той, чи інший користувач, є подібним до профілю користувача, але, на відміну від профілю користувача, профіль об'єкту з системи не зв'язаний з окремим користувачем, а характеризує сам об'єкт. Якщо об'єкт, по своїй, суті, передбачає можливість тільки одного способу використання, то профіль об'єкту вміщає цілий ряд даних, що є зовнішніми по відношенню до об'єкту. До таких даних відносяться, час доступу до об'єкту, період його використання, фрагменти об'єкту, що безпосередньо використовуються та інші параметри. Профіль об'єкту $\Pr(Ob_i)$ і профіль користувача $\Pr(p_i)$ можуть використовуватися одночасно для захисту *ICS* від несанкціонованого доступу *SND*, що якісно приводить до збільшення міри безпеки.

Використання етикеток об'єктів, що знаходяться в *ICS*, відрізняється від використання $Pr(Ob_i)$ наступними особливостями та параметрами:

- етикетка може вміщати додаткові вимоги до користувача і, тим самим, активізувати додатковий інтерактивний процес контролю;
- етикетка може вміщати інформацію, яка вимагає доповнення ідентифікації користувача, для надання доступу до відповідних даних;
- на етикетці може записуватися інформація про додаткові особливості використання відповідної інформації.

Активізація додаткового інтерактивного введення параметрів доступу до даних, що було уже введено, при початковій аутентифікації користувача підвищує рівень контролю доступу до окремо вибраних даних. Очевидно, що така додаткова інформація може бути не відомою користувачу, якщо у останнього не має повноважень використання помічених етикеткою даних. У випадку, коли етикетка вміщає доповнення ідентифікації, то таке доповнення повинно вибиратися з системи доступу, яка вміщає необхідну інформацію, якщо відповідний користувач уповноважений до використання відповідних даних. На відміну від випадку, коли етикетка активізує інтерактивний процес контролю, в даному випадку, етикетка вибирає додаткові ідентифікаційні дані з системи доступу, що має весь комплект даних про потенціального користувача.

Якщо доступ користувача відноситься до типу *SND*, то відповідний p_i доступу до об'єкту захищеного етикеткою не відбудеться. В третьому випадку, на етикетці знаходиться інформація про особливості роботи з даними. Якщо користувач не знайомий з такими особливостями і не передбачив їх при звертанні до системи, то можливості отримати доступ до таких даних у користувача не буде.

Розглянемо, для наведених випадків розв'язку задач захисту, способи оцінки рівня захищеності об'єктів. Наведемо випадок, коли у відповідності з зо-

внішніми вимогами, системі призначено категорію захисту K_i. У відповідності з профілем безпеки, який відповідає категорії K_i, система повинна бути забезпечена відповідним рівнем безпеки. Оскільки декларований рівень безпеки K_i визначається профілем безпеки, що записується у вигляді:

$$Pr^*(ICS) = F^{Pr}[Za_1, \dots, Za_n] \rightarrow R(SB) = F^R[Zg_1, \dots, Zg_n] \quad (4)$$

де на відміну від співвідношення (3) аргументами є не загрози Za_i, а засоби захисту, для відповідних загроз є Zg_i. Іншою відмінністю (4) від (3) є наступне. Кількість загроз $Za_i \in ICS$ може бути більша ніж кількість засобів захисту Zg_i, оскільки, декілька загроз (Za_i, ..., Za_{i+k}) може бути елімінованe одним засобом захисту Za_i, що умовно записується у вигляді $Za_i = \varphi_i(Za_i, \dots, Za_{i+k})$. Для того, щоб профіль безпеки Pr(*ICS*) відповідав рівню безпеки, що задається категорією K_i, то необхідно, щоб K_i було рівне безпеці R(*SB*), що описується співвідношенням:

$$R(SB) = F^R[Zg_1, \dots, Zg_n] \leftrightarrow \Pr(ICS) = F^{Pr}[Za_1, \dots, Za_n].$$

Оскільки K_i= Pr(*ICS*), а $R(SB)=F^R[Zg_i, \dots, Zg_n]$, то ці вирази будуть рівними лише в тому випадку, коли при функціонуванні системи *ICS* не виникне деякої атаки $At_i(Za_i)$, де Za_i деяка загроза, яка не могла бути передбачена профілем безпеки Pr(*ICS*). Формально, цю умову можна записати у вигляді наступного співвідношення, в якому, для спрощення, приймемо, що виникає тільки одна непередбачувана атака:

$$K_i[\Pr(ICS)] - R[SB(ICS)] = At_j(Za_j^*),$$

де At_i - атака, що не була передбачена, при реалізації профіля безпеки, Za_j^* - загроза, яка не була визнана при проектуванні системи безпеки SB(*ICS*), яка описується профілем системи $\Pr^*$[SB(*ICS*)]. Оцінку рівня безпеки слід розглядати в динаміці функціонування системи *ICS*. Приймемо, що величина рівня безпеки визначається кількістю засобів захисту Zg_i, що використовуються в *SB*, і відповідає уявленням про міру функціональності окремого Zg_i. Тоді, перед початком процесу функціонування *ICS* оцінка рівня безпеки $R(SB) = \sum_{i=1}^{m} Zg_i$, де функція F^R із співвідношення (4) замінена сумою. Категорія K_i, згідно з профілем безпеки, описується Pr(*ICS*), представляє собою деяку послідовність загроз Za_i, які необхідно елімінувати, або $K_i(SB) = \sum_{i=1}^{m} Za_i$. Оцінку безпеки кожного засобу захисту $C(Zg_i)$ описується співвідношенням (1), яке відображає оцінку по відношенню до атак At_i, що активізуються Nb_i по відношенню до *ICS*. На основі (4) можна записати вираз для оцінки безпеки у вигляді наступного співвідношення:

$$C[R(SB)] = F^R[C(Zg_1), \dots, C(Zg_n)] .$$

Замінимо F^R функцією суми на основі положення про те, що різні атаки є незалежними випадковими подіями. Тоді, приведене співвідношення можна записати у вигляді:

$$C[R(SB)] = \sum_{i=1}^{m} C_i(Zg_i). \quad (5)$$

На основі співвідношення (5) і (4) можна записати, що

$$C\{\Pr[\mathrm{SB}(ICS)] = C\{R(SB)\},$$

де $C\{\Pr[\mathrm{SB}(ICS)]\}=K_i[\Pr(ICS)]$, де засоби, що реалізують профіль Pr, представляють собою Zg_i, які в сукупності представляють собою SB(*ICS*). Завдяки (5), можна проводити аналіз $C\{\mathrm{R(SB)}\}$ в межах одного засобу захисту Zg_i і, відповідно для цього засобу захисту кількості атак *Sz*.

Виходячи із співвідношення (1), можна визначити, що $maxC_i(Zg_i)=1$, оскільки $Ra=Na=0$. Максимальне значення $C_i(Zg_i)=1$ можна інтерпретувати, як оцінку рівня безпеки рівною 100%. Приймемо, що $Ra\neq0$, а $Na=0$. Тоді, виходячи із співвідношення (1) можна записати:

$$C_i(Zg_i) = (Sz - Ra)/Sz = \alpha \to \alpha < 1.$$

Це означає, що з ростом кількості виявлених атак *Ra* і відсутністю не виявлених атак *Na*, рівень безпеки все одно буде зменшуватися не залежно від того, що $Na_i=0$. З точки зору уявлень про At_i, як деяку випадкову подію, це означає, що з ростом таких випадкових подій росте ймовірність, про те що серед них появиться атака типу Na_i. Сформулюємо наступну гіпотезу, яка стосується кількості виявлених і не виявлених At_i.

Гіпотеза 1. Якщо At_i є незалежними випадковими подіями на множині всіх можливих подій, що записуються, як $At_i=\{at_{i1}, ..., at_{in}\}$, то із збільшенням таких подій, при $n\to\infty$ існує зростаюча ймовірність виникнення події типу Na_i.

Згідно з цією гіпотезою, при збільшенні кількості подій At_i, при $[(i=n)\&(n\to\infty)]$, крім подій типу *Ra*, будуть появлятися і події типу Na_i.

У відповідності з цією гіпотезою, рівняння (1), з якого витікає, що при збільшенні *Ra*, або атак, що розпізнаються і, відповідно, блокуються. Рівень безпеки буде зменшуватися, не залежно від того, чи появились успішні атаки Na_i. Таке зниження рівня безпеки визначається ростом ймовірності, при збільшенні кількості *Ra*, появи атаки типу Na_i. Така залежність обумовлена іще і тим, що виникнення однієї атаки типу Na_i, яка є успішною, може привести до повної дискредитації системи *ICS*. Наприклад, якщо ця атака полягає у знищенні даних про користувачів, або знищення їх персональних даних. В кращому випадку, виникнення Na_i в *ICS* приведе до збільшення швидкості зменшення рівня безпеки, яке відображається співвідношенням (1). Наприклад, якщо $Ra\neq0$, то $R(SB)$ зменшується у відповідності з ростом кількості *Ra*. Якщо до *Ra* додається виникнення Na_i, то швидкість зменшення величини $R(SB)$ збільшується. Виходячи з формули (1), якщо $Ra\neq0$ і $Na_i=0$, то оцінка рівня безпеки така $C_i(\mathrm{R}(ICS))=(Sz\text{-}RA)/Sz$. Якщо $Ra\neq0$ і $Na_i\neq0$, то $C_i(\mathrm{R}(ICS))=(Sz\text{-}RA)/(Sz+Na)$, де збільшення знаменника, при появі *Na*, приводить до збільшення швидкості зменшення рівня безпеки в рамках засобів захисту.

Приведена гіпотеза є підставою для того, щоб уявлення про забезпечення необхідного рівня безпеки не обмежувалося лише створенням засобів захисту

системи *ICS*, а розширювалось засобами протидії процесам функціонування зовнішніх небезпек Nb_i, що ініціюють атаки At_i.

Оскільки, система *ICS* орієнтована на реалізацію деяких процесів, а система типу Nb_i орієнтована тільки на генерацію різних типів At_i по відношенню до *ICS*, то остання, в процесі розвитку системи Nb_i зіткнеться з тим, що у *ICS* не вистачить ресурсів для адекватного розвитку власної системи *SB*, для протидії системі Nb_i.

Висновки. В статті досліджується оцінка визначення залежності між засобами захисту та оцінками рівня безпеки даних інформаційних систем, яка формується у вигляді профілю безпеки конкретної системи. Даними, для створення профілю безпеки, є дані, що отримані на основі аналізу втрат, до яких може привести успішна атака, протидія якій могла би бути не передбачена в профілі, а також законодавчі акти, що регулюють правила та формулюють умови способів використання відповідних даних.

Список використаних джерел

1. Порядок проведення робіт по створенню комплексної системи захисту інформації в інформаційно-комунікаційних системах : НДТЗИ 3.7-003-2005.
2. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. НД ТЗІ 2.5-005-99.
3. Корченко О.Г. Системи захисту інформації. Київ: НАУ, 2004.
4. Канеев И.Р., Беляев А.В. Информационная безопасность предприятия. СПб.: БХВ-Петербург, 2003.
5. Мельников И.И. Информационная безопасность. СПб.: БХВ-Петербург, 2003.

References

1. Poryadok provedennya robit po stvorennyu kompleksnoyii systemy zakhystu informacii v informaciyno-komunikaciynykh systemakh: NDTZI, 2005. 3.7-003 (in Ukrainian**).**
2. Klasyfikaciya avtomatyzovanykh system i standartni funkcionalni profili zakhyshchenosti obroblyuvalnoyi informacii vid nesankcionovanogo dostupu. NDTZI, 2005. 2.5-99 (in Ukrainian).
3. Korchenko O.G., (2004). Systemy zakhystu informacii. KYIV: NAU (in Ukrainian).
4. Kaneev I.R, Belyaev, A.V., (2003). Informacionnaya bezopasnost" predpriyatiya. SPB: BHV-Peterburg (in Russian)
5. Melnikov I.I., (2003). Informacionnaya bezopasnost. SPB: BHV-Peterburg (in Russian)

DETERMINATION OF DEPENDENCE BETWEEN PROTECTION MEANS AND ESTIMATIONS OF DATA SECURITY IN SOCIAL NETWORKS

B. V. Durniak, T. M. Khometa

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

The real dangers of Nb_i which can activate, or not activate attacks which are instrumental in the origin of processes of change of strength of some system security, and also presence of threats which use attacks for penetration in the environment of protection object have been analysed in the article.

Keywords: *safety profile, threats Zg_i, attacks At_i, elimination, danger Nb_i, declared level, anomalous values of process parameters, a functional analyzer, identifier, label.*

Стаття надійшла до редакції 04.03.2015
Received 04.03.2015