трудов. - М.: МГУП, 2002. - С. 90-94.
8. *Поултер С.Р.* Оценка качества оттисков. Сборник докладов «Вопросы оценки качества полиграфических оттисков» / под ред. Козаровицкого Л.А. - М.: Изд-во иностр. литер., 1961.
9. *Пашуля П.Л.* Основи метрології, стандартизації і сертифікації Якість у поліграфії. Навч. посібник. – К.: – 1997.
10. *Hubler A.C.* Digital High Volume Printing: Breakthrough for Print-on-Demand?/ IS&T's NIP 15: International Conference on Digital Printing Technologies. - 1999. - P. 1-5.
11. *Шашлов Б.А*. Цвет и цветовоспроизведение. - М.: Мир книги, 1995.
12. *Пашуля П.Л.* Стандартизація, метрологія, відповідність, якість у поліграфії. – Львів.: УАД. 2011.

*Поступила 14.9.2015р.*

УДК 004.043

Б. В. Дурняк, Т. М. Хомета, Українська академія друкарства, м. Львів

## ВИЗНАЧЕННЯ НЕОБХІДНОГО РІВНЯ ЗАХИСТУ ДАНИХ В СОЦІАЛЬНИХ СИСТЕМАХ

**Анотація** В статті розглядається задача обґрунтування, встановлення певного рівня захисту для окремих фрагментів даних окремого користувача. В якості аналогу системи захисту доступу використовується система правил Діона. В статті звертається увага в першу чергу на розподіл рівнів захисту різних фрагментів, даних які грунтуються на інтерпретації тих даних у відповідній предметній області.

**Annotation** In the article is examined task of ground of establishment of certain level of defence for the separate fragments of information of separate user. The system of rules of Dion is used as an analogue of the system of defence of access. In the article attention applies above all things on distributing of levels of defence of different fragments of information which are based on interpretation of those information in the proper subject domain.

**Аннотация** В статье рассматривается задача обоснования, установления определенного уровня защиты для отдельных фрагментов данных отдельного пользователя. В качестве аналога системы защиты доступа используется система правил Диона. В статье обращается внимание в первую очередь на распределение уровней защиты разных фрагментов данных, которые основываются на интерпретации тех данных в соответствующей предметной области.

**Ключові слова:** Система захисту *SB*, міра захисту, ієрархічна система, інтерпретація даних.

**Keywords:** System of defence of SB, measure of defence, hierarchical system, interpretation of data.

**Ключевые слова:** Система защиты SB, мера защиты, иерархическая система, интерпретация данных.

**Вступ**

Способи захисту соціальних систем $(CS)$ та необхідна їх міра захисту визначається наступними факторами: втратами зі сторони приватної особи, до яких може привести несанкціонований доступ до приватних даних; порушенням законів, які стосуються захисту персональних даних громадян; необхідністю доступу до персональних даних працівниками соціальних та інших служб до відповідної системи; захищеністю доступу до персональних даних через канали міжсистемного зв'язку. Для захисту різних фрагментів даних використовується уявлення про уповноваження користувача до використання тих чи інших даних.

Втрати приватної особи до яких може привести несанкціонований доступ до її персональних даних в $CS$ визначається самою особою явним, або неявним способом. Розглянемо узагальнену шкалу міри захисту доступу до $CS$. Міру захисту систем доступу будемо позначати літерою $\mu[\alpha_1,...,\alpha_n]$, де $\alpha_i$ - деякий рівень захисту $\mu$, або $\mu(\alpha_i)$.

Явний спосіб визначення міри захисту доступу полягає у декларуванні міри захисту самою особою на основі запропонованих рівнів захисту $\mu(\alpha_1),\mu(\alpha_2),...,\mu(\alpha_k)$, а також, з врахуванням вартості вибраної міри захисту доступу, яку будемо позначати $\mu(\alpha_i,\upsilon_i)$, де $\upsilon_i$ - вартість міри захисту доступу, яка є доступною для користувача. Задача, яка розглядається в статті полягає у визначенні повноважень окремих користувачів до різних фрагментів даних на основі аналізу їх інтерпретацій.

**Виклад основного матеріалу**

Неявний спосіб визначення міри захисту доступу реалізується системою захисту $SB$, що входить в склад $CS$, на основі аналізу персональних даних користувача. Вартість встановленої таким чином $\mu(\alpha_j)$ покривається державними коштами, оскільки існують закони про захист персональних даних, виконання яких гарантується державними органами. Приймемо, що шкала міри захищеності $\mu_1,\mu_2,...,\mu_n$ є впорядкованою по відношенню до збільшення цієї міри, або $\mu_i < \mu_{i+1}$. В цьому випадку, для остаточного визначення $\mu_i(h_i)$, де $h_i$ - користувач, система пропонує користувачу можливість вибрати більш високий рівень захисту $\mu_{i+r}$ по відношенню до $\mu_{i+d}$, який встановлено неявно, або $\mu_{i+d} < \mu_{i+r}$. Витрати на використання $\mu_{i+d} < \mu_{i+r}$ для конкретного $h_i$, буде нести користувач. Надання можливості додаткового підвищення рівня захисту персональних даних користувачем

обумовлюється тим, що в $CS$ може не бути нових, або додаткових персональних даних, які появилися у користувача до моменту звертання останнього до $CS$. Не зважаючи на те, що $CS$ не володіє новими даними $h_i$, використання існуючих в $CS$ даних, може привести до того, що не санкціонований користувач на їх основі зможе більш легко дістатися до нових даних $h_i$, оскільки вони можуть знаходитися у іншій системі даних типу $CS$.

При доступі користувачів до даних $CS$, існує небезпека маніпулювання даними в самому середовищі $CS$, яка виникає за рахунок того, що в $CS$ можуть бути дозволені різні операції, наприклад, операції читання, операції запису, операції переносу даних з одного місця в інше в рамках середовища $CS$ та цілий ряд інших операцій. Для протидії такій небезпеці, можна використовувати системи правил контролю операцій, які є аналогічні до системи захисту Діона [1] .

Несанкціоноване використання персональних даних може приводити не тільки до втрат, які несуть окремі особи, а і до соціальних наслідків. Соціальні наслідки виникають тоді, коли кількість громадян, які понесли втрати перебільшує певну величину. Соціальні наслідки від персональних втрат відрізняються тим, що останні приводять до появи локальних претензій до установи, що користується відповідною $CS$, а в першому випадку, виникають претензії до владних структур в цілому.

Будь-який закон, крім опису його суті описує наслідки його порушення. Тому, цей аспект міри захищеності детально розглядати не будемо, оскільки він носить виключно юридичний характер. Приймемо лише умовну величину вартості такого порушення, щоб можна було врахувати цей фактор.

Крім користувачів $CS$, які розміщають свої дані в цих системах, існує цілий ряд фахівців, які, в силу своєї професійної діяльності, повинні мати доступ до $CS$. В цьому випадку, приймається, що фахівці мають досить високий рівень довіри, при роботі з системами $CS$. До таких фахівців можна віднести лікарів , якщо мова йде про медичні системи, працівників податкових служб, якщо мова йде про податкову систему та інші. Більш високий рівень довіри до цієї категорії користувачів $CS$, який будемо позначати символом $g_i$, обумовлюється тим, що по відношенню до них використовуються додаткові умови забезпечення довіри, при роботі з $CS$. Прикладом таких умов можуть служити спеціальні зобов'язання фахівців $g_i$ до санкціонованого використання персональних даних, з $CS$, які можуть впливати на можливості їх професійної діяльності та інші. В цьому випадку певна величина міри захищеності реалізується за межами системи доступу та $SB$ в цілому. Це обумовлює можливість для користувачів $g_i$ в рамках $SB$ реалізовувати менше кроків ідентифікації їх доступу.

Через канали міжсистемного зв'язку реалізується обмін даними між $CS$ різного типу з ініціативи користувачів типу $h_i$ та $g_i$, які ідентифікуються в рамках системи доступу, засобами $SB$. Тому, обмін даними по каналах зв'язку реалізується з використанням стандартних захищених протоколів.[2].

В цілому, оцінка рівня захисту $CS$ не може здійснюватися в абсолютних величинах, оскільки фактори, що впливають на таку оцінку є різнопланові і узгодити оцінку захисту по всіх можливих факторах є досить важко. Тому будемо розглядати оцінку рівня безпеки $CS$ поетапно:

- початкова оцінка рівня безпеки $\mu^P(CS)$;
- текуча оцінка рівня безпеки $\mu^T(CS)$;
- оцінка критичного рівня безпеки $\mu^k(CS)$;
- оцінка тенденції зміни рівня безпеки, $\mu^N(CS)$;
- персоналізована оцінка рівня безпеки $\mu^R(CS)$.

Початкова оцінка рівня безпеки реалізується перед етапом експлуатації системи. Ця оцінка здійснюється не тільки на початковому етапі після створення і початкового наповнення системи даними, а і на етапі визначеного циклу промислового використання системи. Цикл промислового використання системи представляє собою період функціонування, на протязі якого базові параметри змінюють своє значення таким чином, що останні виходять за встановлені границі. Такими параметрами і, відповідно, значеннями можуть бути наступні:

- розміри баз даних;
- час очікування на обслуговування користувачів;
- кількість успішних несанкціонованих доступів;
- текуча кількість проведених аудитів;
- частота використання $CS$.

Розмір баз даних не визначається виключно об'ємом пам'яті, який є доступним для зберігання персональних даних, а визначається конфігурацією структури, яка з появою нових даних може понизити свій рівень оптимальності. Загальний опис структури ієрархічного типу можна описати наступним чином:

$$S(CS) = S_1(e_{11},...,e_{1m})[S_2(e_{21},...,e_{2n})[,...]],$$

де $S_i$ - структура $i$ - того рівня ієрархії, $e_{ij}$ - параметр $j$ елемента структури $i$. Характер персональних даних дозволяє стверджувати, що вони підпорядковуються ієрархічній структурі, оскільки в них завжди можна виділити ряд найбільш загальних даних, перехід від яких в рамках ієрархічної структури дозволяє перейти до більш детальних даних. В цьому випадку існує можливість для кожного рівня ієрархії встановити окремий рівень доступу, який представляє собою один із параметрів $e_{ij}$. З цього виникає, що найбільш захищеними повинні бути дані, які в рамках ієрархії

значимості цих даних є на найнижчому рівні. Формально, цю умову можна записати у наступному вигляді:

$$\{(i > j)\,\&\,[S_i(CS_i)\,\&\,S_j(CS_j)]\} \rightarrow \{[b_i(CS_i) > b_j(CS_j)]\,\&\,[d_i(CS_i > d_j(CS_j)]\},$$

де $i, j$ - номери рівнів в ієрархії в структури даних, $S_i$ - рівень "$i$"-го структури - $S(CS), b_i$, - рівень захисту фрагменту даних $CS_i$, $d_i$ - міра деталізації даних, що представлені фрагментом $CS_j$. Якщо кількість рівнів ієрархії, яка передбачена загальною структурою $S(CS)$, для чергових даних виявилась недостатньою, то це означає, що об'єм пам'яті з відповідною структурою є загальний, для розміщення відповідних даних. Це обумовлено тим, що кожний рівень ієрархії даних має параметри, які пов'язані з інтерпретацією відповідних даних. Прикладом таких параметрів може служити рівень захищеності відповідного фрагменту, віддаль від вершини ієрархічної системи до заданого елемента, який є проміжною вершиною дерева ієрархії, або листом цього дерева, міра інтерпретаційної сумісності деякої вершини дерева, або вузла дерева з суміжними вузлами та інші параметри, що формуються на основі інтерпретації даних, які розміщаються $CS$. Час очікування на обслуговування визначається не тільки часом реакції системи на запит, а і часом через який користувач отримує доступ до системи. Якщо $\Delta\delta$ позначити час очікування на обслуговування, то можна записати співвідношення $\Delta\delta = \Delta t_i + \tau_i$, де $\Delta t_i$ - час реакції $CS$ на звертання $h_i$, а $\Delta\tau_i$ час, через який $h_i$ отримує доступ до $CS$. Час $\Delta t_i$ - визначається структурою баз даних, що знаходяться в $CS_i$, яка, в переважній більшості, забезпечує доступ в зручний для користувачів час, що також забезпечується можливими додатковими розв'язками задачі прискорення обслуговування користувачів. Друга складова часу $\Delta\tau_i$ визначається деякими зовнішніми факторами системи $CS$. Такі фактори характеризують різні системи доступу до $CS$, що використовуються для обслуговування клієнтів. Ці системи мають свою власну специфіку, оскільки вони повинні розв'язувати наступні задачі:

- задачу забезпечення, можливості адаптації до відповідного користувача, оскільки доступ до системи повинні отримувати користувачі різних категорій;
- задачу попередньої ідентифікації користувача, щоб уникнути необхідності розв'язку повної ідентифікації засобами безпеки самої системи $CS$;
- у випадку відмови від обслуговування, зовнішні засоби повинні реалізувати приязну та конструктивну відмову, що полягає у роз'яснені причин відмови та у наданні рекомендацій, які необхідно виконувати, щоб стало можливим уникнення відмови отриманого типу.

Перша задача є типовою для довільних систем інформаційного обслуговування. Особливістю систем типу $CS$, є те, що зовнішні засоби, при отриманні не зрозумілого звернення, повинні розпізнавати його характер та сформулювати інтерактивний зв'язок з користувачем таким чином, щоб система могла модифікувати свій інтерфейс, і користувач міг проводити, або реалізувати повторний запит системи на обслуговування. Очевидно, що ця можливість орієнтована на модифікацію інтерфейсу, яка б відповідала можливостям користувача. Наприклад, користувач може бути фахівцем в медичній галузі, чи у будь-якій іншій галузі, в якій працює відповідний користувач.

Задача попередньої ідентифікації користувача дозволяє розвантажити засоби базової системи доступу та виявляти найбільш масові проби не санкціонованого доступу. Це особливо важливо для виявлення спамів та інших шкідливих даних, що приходять на недавно додатково захищений фрагмент системи.

У випадку негативної реакції системи на запит користувача, система повинна провести аналіз всіх даних, що стосуються користувача з точки зору цілі запиту. На основі такого аналізу система реалізує діалог з користувачем і, виходячи з даних діалогу та даних попереднього аналізу, формує рекомендації, які могли б допомогти споживачу успішно звернутися до системи за наданням необхідної послуги. Очевидно, що аналіз, про який йшла мова та дані, що отримані в процесі діалогу, можуть виявитися підставою для активізації додаткових подій в зовнішній системі доступу та в $SB$ системи $CS$, що пов’язані з забезпеченням підвищеного рівня захисту системи, в тому числі, і по відношенню до користувача, з якими співпрацює система в текучий момент часу.

Кількість успішних несанкціонованих доступів є важливим показником міри захищеності системи, або міри її безпеки. Цей параметр на початку окремого, загального циклу функціонування дорівнює нулю. Виявити успішну атаку можна лише у наступних випадках:

- при проведені аудиту системи $CS$;
- при виявленні зовнішніх ознак успішного несанкціонованого втручання, які безпосередньо не пов’язані з функціонуванням системи;
- на основі активізації засобів виявлення аномалій в системі $CS$ та системі $SB$, які активізуються в рамках моніторингової перевірки системи $CS$.

В другому і третьому випадку робота системи переривається, що інтерпретується, як ознака, що приводить до зниження рівня безпеки $CS$. Така інтерпретація ґрунтується на наступних факторах:

- користувач не може певний період використовувати систему, для вирішення власних задач, що може привести до тих, чи інших затрат для користувача;

- серед всіх користувачів може існувати група таких користувачів, персональні дані яких були отримані не легально, що в більшості випадків приводить до виникнення втрат у цих споживачів, що безпосередньо інтерпретується як зменшення рівня безпеки системи;
- несанкціоноване втручання в систему може реалізуватися з ціллю знищення системи в цілому, що інтерпретується як виникнення катастрофічної ситуації.

Особливості цього параметру, який визначає зменшення рівня безпеки, полягає у тому, що величина цього параметру не може з часом зменшуватися, його величина може тільки зростати з різною швидкістю, або залишатися без змін. Оскільки успішні, несанкціоновані доступи є найбільш небезпечними для $CS$, то кількість останніх залишиться в якості параметра $CS$ на весь період функціонування системи і представляє собою її історичний параметр. У зв'язку з цим, складова, що визначає величину зменшення міри захисту визначається досить просто і описується співвідношенням:

$$\mu(I) = -\sum_{i=k}^{k} At_i^U,$$ де $At_i^U$ - успішна атака на систему $CS$.

Такий параметр, як кількість проведених аудитів, по своїй інтерпретації є досить простий і приймається, що його величина до певної міри приводить до підвищення рівня безпеки. Очевидно, що таке підвищення рівня безпеки має свої межі, оскільки аудит або перериває можливість обслуговування системою $CS$ користувачів на заданий період, або ускладнює доступ користувачів до системи.

Початкова оцінка рівня безпеки ґрунтується на визначенні декларованих мір захисту, які забезпечуються засобами захисту, що використовуються в рамках $CS$. У зв'язку з цим, приймаємо, що кожний засіб захисту $Zg_i$ функціонально орієнтований. Під такою орієнтацією розуміється клас, або сукупність типів атак, на протидію яким відповідний засіб захисту орієнтований. Такі засоби, як кожний технічний продукт, не залежно від того, чи він реалізований апаратно, чи програмно, має свої власні параметри, які їх характеризують з точки зору забезпечення тих функцій, які вони повинні реалізувати в процесі їх експлуатації. Відомим аналогом таких параметрів може служити параметр надійності функціонування деякого виробу. Більш відповідним прикладом такого параметру є параметр, що визначає відповідність процесу функціонування виробу технічним вимогам, що визначають спосіб його функціонування [3]. У випадку $Zg_i$, також існують технічні вимоги, які окреслюють відповідні функціональні можливості $Zg$, як деякого продукту. Виходячи з цього, можна прийняти, що міра безпеки, яка забезпечується на початковому етапі функціонування $CS$ визначається наступними факторами:

- типи атак, які залежать від типів небезпек, передбачаються в $CS$ і,

відповідно до них, система $SB$ комплектується відповідними $Zg_i$;

- оскільки загроза $Za_i$ розглядається, як параметр $CS$ і відомою є кожна з можливих атак $At_i$, то відповідні засоби $Zg_i$ повинні, в рамках $CS$, організовуватися у вигляді структури, яка адекватна у необхідній мірі структурі системи $CS$ яку $Zg_i$ повинні захищати;
- у зв'язку з тим, що відомі небезпеки не обов'язково будуть по відношенню до $CS$ активізувати всі доступні відповідній небезпеці атаки, то кожний з $Zg_i$ буде представляти собою деяку версію реалізацій $Zg_i$, яка визначається особливостями самої $CS$ та особливостями процесу функціонування такої системи.

Тоді міру безпеки $\mu(CS)$ на початковому етапі можна описати наступним співвідношенням:

$$\mu^P(CS) = F[Zg_1, Zg_2, ..., Zg_n],$$

де $F$ є описом відповідної структури $Zg_i$. Оскільки, структура $CS$ є відомою і представляє собою $S(CS)$, кожний засіб $Zg_i$ має певні визначені можливості протидіяти атакам $\{At_{i1}, ..., At_{im}\}$, то цей факт слід представити у вигляді $\alpha_i Zg_i$, де $\alpha_i$ описує міру ефективності протидії $\{At_{i1}, ..., At_{im}\}$. В цьому випадку, попереднє співвідношення можна записати як:

$$\mu^P(CS) = S(\alpha_1 Zg_1 * ... * \alpha_n Zg_n),$$

де * - функція, що використовується, для формування з $Zg_1, ..., Zg_n$ структури $S$. Як уже зазначалось, такою структурою є ієрархічна структура. Тоді, кожний запис даних, або їх група може мати, в залежності від вибраної структури $S$, той, чи інший $Zg_i$ з відповідними коефіцієнтами $\alpha_i$.

Задача визначення текучої оцінки рівня безпеки є більш складною, оскільки рівень безпеки залежить від виникнення можливих атак, що можуть виникати та не були передбачені, при проектуванні початкового рівня безпеки. В даній роботі приймається, що виділені рівні безпеки є незалежними складовими загального рівня безпеки:

$$\mu(CS) = \mu^P(CS) + \mu^T(CS) + \mu^K(CS).$$

Текуча оцінка рівня безпеки $\mu^T(CS)$ буде визначатися на основі використання моделей прогнозування [4]. Перш ніж формувати модель прогнозування, визначимо, які параметри прогнозованої події необхідно визначити. До таких параметрів відносяться наступні:

- клас атаки, яка може виникнути, $(Pa_i^N)$;
- час, коли відповідна атака може виникнути $(Pa_i^T)$;
- додаткові параметри, що характеризують атаку $(Pa_i^D)$.

Базовим параметром в моделі прогнозування $\mu(Pg)$ приймемо час виникнення події, яка дозволить визначити інтервал часу між моментом активізації $\mu(Pg)$ та моментом виникнення атаки, яку, на відміну від передбачуваних, або відомих атак $At_i$, будемо позначати $At_i^N$. Якщо не займатися прогнозуванням $Pa_i^N$, то розпізнавання типу атаки $At_i^N$. необхідно реалізувати після її виникнення, що з точки зори безпеки є менш доступним [5]. Очевидно, що розпізнавання $Pa_i^N$ може здійснюватися незалежно від прогнозування $Pa_i^T$, але в цьому випадку між $Pa_i^T$, і $Pa_i^N$ буде неявний зв'язок, який закладається системою *SB*. Встановлення такого зв'язку полягає у наступному. Оскільки атака, яку передбачається прогнозувати є не відомою, вона по своїх параметрах повинна відрізнятися від параметрів відомих атак $At_i(\xi_{i1},...,\xi_{im})$. В цьому випадку система *SP* повинна на основі аналізу $At_i(\xi_{i1},...,\xi_{im})$ зпрогнозувати $At_j^N(\xi_{i1}^n,...,\xi_{ik}^n)$ таким чином, щоб можна було встановити параметри $\xi_{ij}^n \neq \xi_{ij}$ з усіх параметрів, що характеризують $At_1,...,At_n$. Такий алгоритм ґрунтується на використанні наступних принципів:

- атака типу $At_i^N$ може представляти собою модифікацію атаки $At_i$ по обмеженій кількості параметрів $\xi_{ij}$;
- час виникнення атаки $At_i^N$ обумовлюється спеціальними умовами, що створюються в *SB* на основі аналізу часових характеристик поведінки небезпек, що активізують атаки різних типів;
- тип атаки $At_i^N$ в значній мірі залежать від типів загроз, що існують в *CS*.

Перша умова означає, що атака $At_i^N$ буде відрізнятися від $At_i$ одним, або двома параметрами, що дозволяє на основі відповідності $At_i^N \propto At_i$ здійснювати прогноз можливого типу атаки. Співвідношення відповідності встановлюється на основі особливостей небезпек, що тісно пов'язані з конкретною реалізацією окремої *CS*. В цьому випадку, для $\mu^k(CS)$ можна записати співвідношення: $\mu^K(CS) = f(At_i^N)$, де

$$At_i^N = At_j(\xi_{i1},...,(\xi_{ik} \to \xi_{ig}^n),...,\xi_{im}).$$

Вибір параметра $\xi_{ik}$ для заміни його на $\xi_{ig}^n$ будується на основі трендів модифікації атак $At_i$, що є передбачуваними на початковому етапі. Приймається, що всі можливі $\xi_{ij}$ відомих атак $At_1,...,At_n$ мають власну інтерпретацію, яка може полягати у використанні певної небезпеки, чи

реалізації іншої послідовності кроків дії атаки $At_i$ і інші. В цьому випадку, рівень безпеки, що визначається складовою $\mu^T(CS)$ обчислюється на основі визначення точності прогнозування, яка забезпечується моделлю $M(Pg_i)$. В цьому випадку, для $\mu^T(CS)$ можна записати співвідношення $\mu^T(CS) = \delta[M[Pg(t)]] + \delta[M[Pg(\xi_{ij})]]$, де $\delta$ -точність прогнозування моменту виникнення $At_i$, та точність прогнозування типу атаки, що може виникнути та визначається параметром $\xi_{ij}$. В цьому випадку $\mu^T(CS)$ та $\mu^k(CS)$ об'єднуються в одну оцінку.

Оцінка критичного рівня безпеки є досить важливою характеристикою, оскільки вона вказує на те, що система $CS$ знаходиться на грані загальної небезпеки функціонування $CS$. Загальну небезпеку функціонування будемо позначати $\eta^z(CS)$. Очевидно, що $\mu^Z = \beta / \eta^Z(CS)$. На основі цього параметру формуються рекомендації по перериванню процесу експлуатації $CS$ у зв'язку з можливістю виникнення значних втрат. Використання цього параметру є характерним для системи типу $CS$, оскільки в них зберігаються дані втрат, які можуть мати значні соціальні наслідки. Критеріями визначення величини $\eta^z(CS)$ можуть служити наступні фактори, або події, що виникають у $CS$:

- збільшення інтенсивності атак на $CS(It)$;
- перевищення кількості успішних атак на $CS$ деякого встановленого порогу $\left|\sum_{i=1}^{m} At_i^U > k_i\right|$;
- виникнення несанкціонованих змін персональних даних в соціальних системах, $Nz[D(CS)]$;
- виникнення структурних змін, які приводять до зміни асиметрії структури, яка є не допустимою;
- кількість версій системи $CS$, яка перевищує заданий поріг та інші.

Збільшення інтенсивності атак на $CS$ є прямою ознакою того, що рівень безпеки $CS$ мусить бути підвищений. Аналіз збільшення інтенсивності атак полягає на використанні допустимих порогів такої інтенсивності. Аналогічна ситуація з кількістю успішних атак, які були виявлені за встановлений період функціонування $CS$. Структурні зміни виникають у випадках розширення локальних структур, що відображають дані одного користувача. Ця ознака є більш складною і потребує окремого аналізу. Аналогічна ситуація з ознакою, що характеризує кількість версій системи $CS$, що знаходяться в експлуатації.

**Висновок.** Визначення оцінки рівня безпеки є більш складною, оскільки рівень безпеки залежить від виникнення можливих атак, що можуть виникати та не були передбачені, при проектуванні початкового рівня безпеки. В даній

статті проведено аналіз можливості створення системи правил визначення повноважень по використанню різних операцій з персональними даними.

1. *Мельников Ю.И.* Защита информации в компьютерных системах. / Ю.И. Мельников. Финансы и статистика, – М.: Электроинформ., 1997.
2. *Петров А.А.* Компьютерная безопасность. /А.А Петров. Криптографические методы защиты.– М.: ДМК, 2000.
3. *Половко А.М.* Основы теории надёжности. / С.В Гуров – СПб.: БХВ Петербург, 2006.
4. *Демидова Л.А., Пылькин А.Н., Скворцов С.В., Скворцова Т.С.* Гибридные модели прогнозирования коротких временных рядов. / С. В. Скворцов, Т. С. Скворцова – М.: Горячая линия – Телеком, 2012.
5. *Лукацкий А.В.* Обнаружение атак. / А.В. Лукацкий – СПб.: БХВ Петербург, 2001.

*Поступила 21.9.2015р.*

УДК 004.9

О.В.Тимченко[7 8], Р.О.Кульчицький [8]

## ПОСТАНОВКА ЗАДАЧІ РЕКОНСТРУКЦІЇ ОБ'ЄМНОГО ЕЛЕМЕНТУ З ОДНОЇ ФОТОГРАФІЇ НА ОСНОВІ МАРКІВСЬКИХ СИСТЕМ

На даний момент існує велика кількість методів реконструкції об'ємних елементів. Умовно, методики відновлення поділяють на активні (впливають на атомарну структуру об'єкта, нагрівають чи руйнують його) та пасивні (дослідження легкими частинками, наприклад фотонами). Відновлене зображення можна одержати з допомогою алгоритмів обробки серії фото, лазерного, ультразвукового, мікрохвильового сканування чи електронного бомбардування досліджуваного об'єкта. Особливої уваги заслуговують проблеми реконструкції зображення з однієї фотографії, які на даний момент активно досліджуються. У даній роботі побудовано загальну структурну схему реконструкції об'ємного елементу, визначено задачу у математичній формі, описано існуючі шляхи вирішення даної проблеми та визначено недоліки даних підходів.

**Ключові слова:** 3D реконструкція, реконструкція з одної фотографії.

Currently, there are many methods for reconstruction of three-dimensional elements. Conventionally, recovery techniques are divided into active (affecting the atomic structure of the object, heated or destroy it) and passive (study of light particles, such as photons). Refurbished image can be obtained using a series of

[7] Uniwersytet Warmińsko-Mazurski w Olsztynie
[8] Українська академія друкарства