УДК 004.94

**А. В. САГУН**

***Черкаський державний технологічний університет***

# МОДИФІКАЦІЯ МОДЕЛІ БЕЛА-ЛАПАДУЛИ ДЛЯ РОЗМЕЖУВАННЯ ДОСТУПУ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

*Виділено актуальність застосування модифікації математичної моделі Бела-ЛаПадули для організації розмежування доступу в інформаційних системах. Показано, що при практичному застосуванні математичної моделі Бела-ЛаПадули для організації інформаційної системи на підприємстві з наявністю секретної інформації додатковий захист від інсайдерських атак для ієрархічної моделі доступу можна отримати за рахунок модернізації функції переходу. Запропоновано модифікацію функції переходу на базі сформульованого функціонального профілю захищеності оброблюваної інформації. Здійснено практичну реалізацію запропонованої модифікації ієрархічної моделі Бела–ЛаПадули на основі створеної матриці доступу.*

***Ключові слова**: математична модель, розмежування доступу, модель Бела–ЛаПадули, ієрархічна система, інформаційна система.*

## Вступ

Модель Бела - ЛаПадули є моделлю розмежування доступу до інформації, яка являє собою ієрархічний тип організації доступу до даних[1]. Застосування жорсткого ієрархічного принципа побудови прикладних інформаційних систем на її базі з врахуванням різної міри конфіденційності інформації може не враховувати факторів інсайдерського втручання з вищих рівнів, тому, в реальних умовах інколи виникає необхідність ввести класифікаційні обмеження до схем доступа.

Існують три основні моделі управління доступом до об'єктів інформації: мандатна, дискреційна і рольова [1]. Модель Бела–ЛаПадули є формальною моделлю мандатного управління.

Класична модель базується на правилах секретного документообігу, що використовується в урядових установах. У цієї моделі кожному об'єкту і суб'єкту (користувачеві) системи призначається свій рівень допуску. Всі можливі рівні допуску системи чітко визначені і впорядковані за зростанню секретності відповідно до правил:

– користувач може читати тільки об'єкти з рівнем допуску не вище його власного;

– користувач може змінювати тільки ті об'єкти, рівень допуску яких не нижче його власного.

Однією з проблем цієї моделі вважається безперешкодність обміну інформацією між користувачами одного рівня, так як ці користувачі можуть виконувати в організації різні функції і те, що має право робити користувач А, може бути заборонено для Б. Тому в практиці мандатну модель зазвичай використовують спільно з якоюсь іншою [2, 3].

Аналізам та методам застосування мандатної моделі Бела–ЛаПадули та її модифікаціям багато уваги приділено в роботах П. Н. Дев'яніна [4], А. А. Грушо, Е. Е. Тімонина, А. П. Баранова, Н. П. Борисенко, П. Д. Зегжда, Є. А. Рудіна [5], А. Г. Ростовцева, Е. Б. Маховенко [6], В. Жора [1], Leonard J. LaPadula, D. Elliott Bell [2] та інших.

**Актуальність** пояснюється необхідністю розробки системи керування базами даних в умовах підприємств, на яких циркулює інформація з різними типами конфіденційності та в умовах динамічних обмежень інсайдерських вторгнень.

## Формулювання задачі дослідження

Необхідність адаптації ієрархічної моделі доступу Бела–ЛаПадули до випадку інформаційної системи з адаптованим рівнем конфіденційності та підвищеною стійкістю до інсайдерських атак. Умова впровадження полягає у врахуванні існуючої моделі розподілу інформаційних потоків в існуючий ІКС комерційного підприємства та збереження ієрархічної моделі доступу та засобів автентифікації.

## Постановка задачі

Розроблюється захищена інформаційна система на базі моделі Бела–ЛаПадули для використання на приватному хлібопекарському підприємстві аграрного холдінгу.

До інформації з обмеженим доступом [7] на підставі наказу віднесено: відомості про проекти, що розробляються та реалізуються; плани розширення діяльності підприємства; плани інвестицій, закупівель, продаж та їх техніко-економічне обґрунтуван-

ня; відомості про зміст внутрішньої документації (накази, розпорядження, інструкції, бізнес-плани, інвестиційні та маркетингові огляди); відомості про замовників, підрядчиків, постачальників, клієнтів, покупців, компаньйонів, посередників та інших ділових партнерів, а також про її конкурентів; відомості про вміст договорів, контрактів, угод та інших зобов'язань організації; відомості про порядок та стан охорони, перепускний режим, систему сигналізації, структуру внутрішніх телефонів; умови та місця зберігання матеріальних цінностей, транспортні засоби підприємства; рецептура та відомості про технологічний процес.

## Виклад основного матеріалу

Традиційно модель Бела–ЛаПадули описується кінцевим автоматом, який може перебувати в скінченній множині станів. Отже, для формулювання такої моделі слід виокремити суб'єкти та об'єкти моделі. До об'єктів слід віднести інформаційні активи, доступ до яких слід регулювати. Зокрема інформацію з обмеженим доступом.

На основі переліку відомостей, що складають комерційну таємницю та з врахуванням характеристик інформації, що захищається, можна сформулювати функціональний профіль захищеності оброблюваної інформації в ІС підприємства інформації від несанкціонованого доступу за НД – ТЗІ.2.5-005-91 та НД – ТЗІ 2.5-004-99 [8]. У зазначеній АС рекомендується використовувати ОС, КЗЗ яких реалізують профілі 3.К.х. Крім вимоги забезпечення конфіденційності, існують додаткові вимоги щодо забезпечення цілісності і доступності інформації, то використаємо профілі 3.КЦД.х: АС класу 3, з підвищеними вимогами до забезпечення конфіденційності, цілісності і доступності оброблюваної інформації: 3.КЦД.1 = {КД-2, КО-1, КВ-3, ЦД-2, ЦО-1, ЦВ-2, ДР-1, ДВ-2, НР-2, НИ-1, НК-1, НО-2, НЦ-1, НТ-1, НВ-1}.

Створимо класифікатор комерційної цінності різних видів інформації, що становлять КТ на різних рівнях ієрархічної вертикалі електронного документообігу (таблиця 1). Для цього використаємо метод експертних оцінок [4].

Відповідно до штатного розкладу підприємство складається з: директора, заступника директора, бухгалтера, технолога, п'яти пекарів, водіїв, трьох експедиторів і вантажників.

На чолі підрозділу стоїть директор підприємства, якому безпосередньо підпорядковується бухгалтер та заступник директора. Оперативний доступ до інформаційної системи, що обслуговує систему електронного документообігу мають: директор та заступник директора підприємства, бухгалтер, технолог та пекарі, експедитор. Тобто, відповідно до ієрархічної моделі доступу існує 4 рівні з відповідними обмеженнями рольових функцій.

Директор ПП (рівень L1) має доступ до інформації, що циркулює на всіх рівнях і підрівнях (з L2.1 по L4.4 включно). З аналізу існуючої ієрархічної вертикалі підприємства модель доступу до інформації, що заснована на правилах секретного документообігу моделі Бела-ЛаПадули, є оптимальною, адже на відміну від дискреційного керування даними, при якому користувачам надаються безпосередньо права на читання, запис і виконання. В мандатній моделі (модель Бела-ЛаПадули) керування доступом відбувається неявним чином [1, 5]. В такому випадку на підприємстві всі посадові особи є користувачами (суб'єктами), інформація–файлами (об'єктами), для яких призначаються рівні доступу.

Можна зупинити свій вибір на ординарній моделі Бела–ЛаПадули (таблиця 2), яка модифікована по базовому параметру доступу. Переваги такої моделі над іншими полягають в тому, що в ній існує можливість реалізації довірчих та не довірчих суб'єктів з відмінними умовами функціонування, а в її розширеннях– можливість зміни функціональності суб'єкта при реалізації інформаційного потоку по пам'яті на функціонально асоційовані з ним сутності.

В результаті аналізу інформаційних потоків на підприємстві та з огляду даних таблиці 1 можна виділити наступну схему їх циркулювання (рис. 1).

Таблиця 1

Класифікатор комерційної цінності інформації ПП «В'ялих»

| № | Назва інформації | Коефіцієнт цінності | Рівні циркуляції в ієрархії ПП |
|---|---|---|---|
| 1 | Бухгалтерська документація | 0,8 | L2.2, L3.3 |
| 2 | Плани розвитку бізнесу | 0,85 | L1, L2.1 |
| 3 | Рецептура | 1 | L3.1, L4.1 |
| 4 | Договори з постачальниками | 0,5 | L2.1, L2.2 |
| 5 | Клієнтська база | 0,85 | L2.1 |
| 6 | Сервер корпоративної пошти | 0,5 | Всі рівні |
| 7 | Документація відділу кадрів | 0,3 | L2.1 |
| 8 | Зберігання цінностей | 0,75 | L1, L2.1,L2.2 |

Таблиця 2

Базові критерії функціонування моделей доступу

| Критерій функціонування | Модель Take-Grant | Модель Бела – ЛаПадули | Модель СВС | Розширена модель Бела–ЛаПадули |
|---|---|---|---|---|
| Різниця в умовах реалізації інформаційних потоків в пам'яті та часі | - | - | - | - |
| Наявність ієрархічної структури сутностей та можливість її використання при реалізації інформаційних потоків у часі | - | - | + | - |
| Можливість об'єднання частини суб'єктів при передаванні прав доступу або реалізації інформаційних потоків | + | - | - | - |
| Можливість реалізації довірчих та недовірчих суб'єктів з відмінними умовами функціонування | - | + | - | + |
| Можливість протидії довірчими суб'єктами передаванню прав доступу/реалізації потоків недовірчими суб'єктами | + | - | - | - |
| Можливість зміни функціональності суб'єкта при реалізації інформаційного потоку по пам'яті на функціонально асоційовані з ним сутності | - | - | - | + |
| Необхідність встановлення різних правил керування доступом та потоками для розподілених компонент | - | - | - | - |

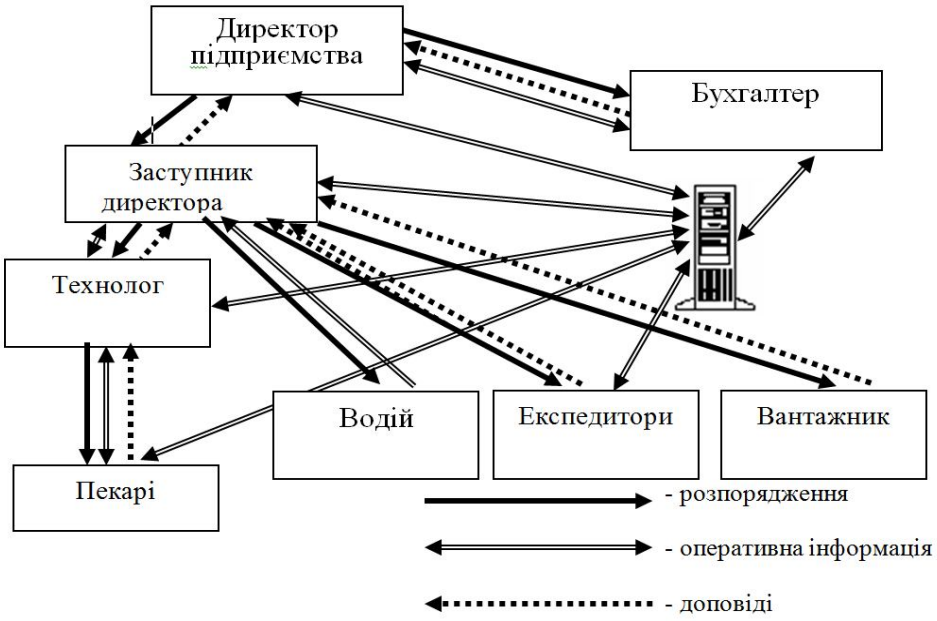


Рис. 1. Схема циркуляції інформаційних потоків

Рівні доступу впорядковуються за ступенем домінування: директор над заступником директора та бухгалтером ( L1 над L2.1 та L2.2 ) (рис. 2).

Будемо мати на увазі, що об'єкти моделі є деякими контейнерами з інформацією, а суб'єкти - користувачами, які виконують різні операції над цими об'єктами.

Відповідно до теореми безпеки Мак–Ліна система безпечна в будь-якому стані і в процесі переходів між ними, якщо її початковий стан є безпечним, а функція переходу задовольняє критерію Мак–Ліна [1, 5]. Протилежне твердження невірно. Отже, система може бути безпечною за визначенням Бела–ЛаПадули, але не мати безпечної функції переходу. Таке формулювання основної теореми безпеки надає для розробки захищених систем базовий принцип їх побудови, відповідно до якого для того, щоб забезпечити безпеку системи як у будь–якому стані, так і в процесі переходу між ними, необхідно реалізувати для неї таку функцію переходу, яка відповідає зазначеним умовам.

$$\begin{pmatrix} L1.1 & ... & L1.m \\ L2.1.1 & & L2.m \\ ... & ... & ... \\ ... & ... & ... \\ ... & ... & ... \\ ... & ... & ... \\ Ln.1 & ... & Ln.m \end{pmatrix}$$

Рис. 2. Схема рівнів доступу

Формулювання основної теореми безпеки в інтерпретації Мак–Ліна дозволяє розширити область її застосування в порівнянні з класичною теоремою Белла–ЛаПадули, проте використовуваний критерій безпеки переходу не завжди відповідає вимогам контролю доступу, що виникають на практиці, оскільки в процесі здійснення переходів можуть змінюватися рівні безпеки сутностей системи, бажано контролювати цей процес, явним чином дозволяючи або забороняючи суб'єктам здійснювати подібні переходи.

Система з вповноваженими суб'єктами описується множинами $S$, $O$ і $L$, зміст яких збігається з аналогічними поняттями моделі Бела - ЛаПадули, а її стан також описується набором впорядкованих пар $F, M$, причому функція переходу $T^a$ і матриця доступу $M$ грають таку ж роль. Новим елементом моделі є функція управління рівнями $L: S \cup O \to (S)$, де $(S)$ – безліч всіх підмножин $S$.

Дана функція визначає підмножини суб'єктів, яким дозволено змінювати рівень безпеки для заданого об'єкту чи суб'єкту.

Таким чином, модель системи у вигляді кортежу $\sum(v_0, R, T^a)$ складається з початкового стану $v_0$, безлічі запитів $R$ і функції переходу $T^a$, яка переводить систему зі стану в стан за мірою виконання запитів. Але тепер у функції переходу, яка визначає наступний стан системи після виконання певним суб'єктом деякого запиту, з'явився ще один аргумент - суб'єкт, від якого виходить цей запит, оскільки результат переходу залежить від того, який суб'єкт його ініціював, тобто $T^a : (S \times V \times R) \to V$. Коли система, що знаходиться в стані $v \in V$, при отриманні запиту $r \in R$ від суб'єкта $s \in S$ переходить зі стану $v$ до стану $v^* = T^a(s, v, r)$. Іншими словами, в ході авторизованого переходу рівень безпеки суб'єкту або об'єкту може змінюватися тільки тоді, коли суб'єкт, що виконує перехід, належить безлічі суб'єктів, уповноважених змінювати рівень цього суб'єкта або об'єкта.

З точки зору моделі уповноважених суб'єктів система $\sum(v_0, R, T^a)$ вважається безпечною в тому випадку, якщо:

1. Початковий стан $v_0$ і всі стани, досяжні з нього шляхом застосування кінцевого числа запитів з $R$ є безпечними за критерієм Бела-ЛаПадули;

2. Функція переходу $T^a$ є авторизованою функцією переходу згідно запропонованим визначенням та є дозволеною селектором.

Доступ до захищених файлів відбувається за двома основними правилами [4-6,10]:

1. Користувач має право читати тільки ті документи, які не перевищують його власний рівень безпеки. Це правило забезпечує захист інформації, що обробляється більш високорівневими користувачами, від доступу з боку низькорівневих користувачів.

2. Користувач має право заносити інформацію тільки в ті документи, рівень безпеки яких не нижче його власного рівня безпеки.

Це правило попереджає порушення режиму доступу з боку високорівневих учасників процесу обробки інформації до низькорівневих за схемою: $L1.n > L2.n > ... > Ln.n$.

Різні види інформації циркулюють на існуючих чотирьох рівнях ієрархічної структури підприємства.

На основі викладеного вище можна розробити функціональну схему модернізованої моделі доступу Бела-ЛаПадули (рис. 3).

На даному рисунку $T^a$ – функція переходу; $L$ – рівень доступу; $Sub$ – суб'єкт доступу; $Obj$ – інформаційний ресурс; ОПР–особа, що приймає рішення; IDS–система фіксації вторгнень; $Exp$ – блок експертної оцінки.

В модернізованій моделі (з уповноваженими суб'єктами) вона називається авторизованою функцією переходу в тому випадку, якщо для кожного переходу $T^a(s, v, r) = v^*$, для якого одночасно виконується як умова авторизації виду: для $\forall x \in S \cup O$, якщо $F^*(x) \neq F(x)$, то $S \in C(x)$.

Значення функції переходу $T^a$ визначається, як:

$$T_i^a = \arg\min_s \prod_{i=1}^{n} \Pr\left(x_i \middle| s_i\right) \Leftrightarrow \min \Pr\left(s_i\right) = \Pr \begin{vmatrix} (s_1) \\ (s_1) \\ ..... \\ (s_n) \end{vmatrix},$$

де $\Pr(x_i | s_i)$ – умовна ймовірність того, що функція переходу заборонена ОПР для суб'єкта $x_i$ з множини $S$.

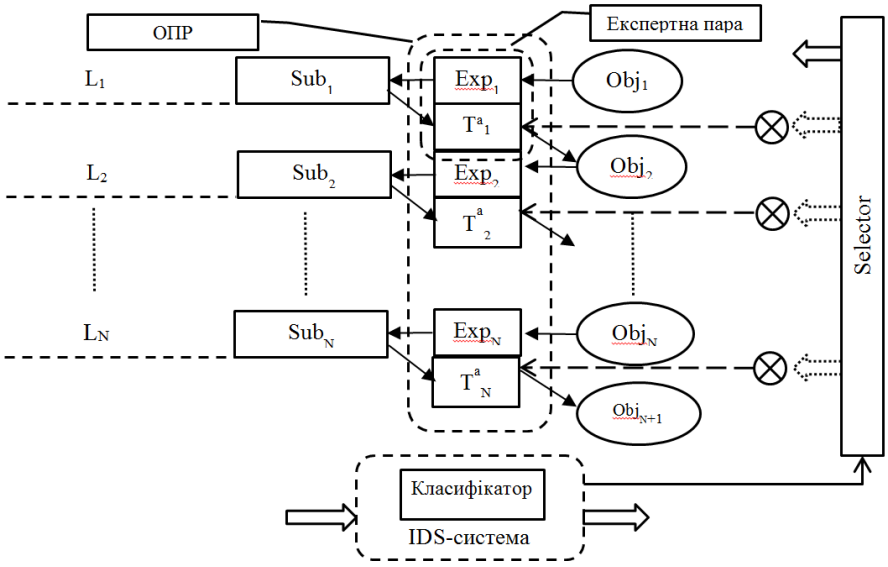


Рис. 3. Функціональна схема модернізованої моделі доступу Бела-Лападули

Рішення про заборону або обмеження доступу ОПР приймається на основі розрахованого критичного порогу ймовірності, тобто самою системою IDS на базі методу експертних оцінок [9]. Такий поріг може бути встановлений системою внаслідок навчання [11].

Можна стверджувати, що в ході авторизованого переходу рівень безпеки суб'єкта або об'єкта може змінюватися тоді і тільки тоді, коли суб'єкт, що виконує перехід, належить множині суб'єктів, що вповноважені змінювати рівень цього суб'єкту або об'єкту.

Кожному суб'єкту присвоюється свій рівень доступу, відповідний ступеню конфіденційності. Аналогічно, об'єкту присвоюється рівень секретності. Перехід між станами описується функціями переходу. Система знаходиться в безпечному стані в тому випадку, якщо у кожного суб'єкта є доступ тільки до тих об'єктів, до яких дозволений доступ на основі поточної політики безпеки. Для визначення, чи має суб'єкт права на отримання певного виду доступу до об'єкта, рівень секретності суб'єкта порівнюється з рівнем секретності об'єкта, і на основі цього порівняння вирішується питання, надати чи ні запитуваний доступ. Набори: рівень доступу/рівень секретності описуються за допомогою матриці доступу, що формується на базі схеми рівнів доступу (рис. 2).

Для практичної реалізації сформовано матрицю доступу, права на доступ до різних субєктів якої формуються ймоворнісним класифікатором IDS–системи [11] (рис. 4).

В звязку з тим, що передбачається мережна взаємодія суб'єктів та обєктів моделі, то передбачається, що створюється головна сторінка, оформлена за допомогою стандартної мови розмітки веб-сторінок в Інтернеті, мовою на якій здебільшого створюються веб-сайти, а саме HTML.

Передбачається наявність: 1) задання формата поля; 2) закріплення формата поля; 3) задання централізації екрану; 4) задання тягучих блоків; 5) закріплення тягучих блоків; 6) розміщення фону сайта; 7) закріплення фону сайта.

Дані, які потрібні для входу, Username та Password, оформлені за допомогою стандартної мови розмітки веб-сторінок в Інтернеті, мовою на якій здебільшого створюються веб-сайти, а саме HTML:

| назва | canAddGroup | canEditGroup | canDelGroup | canAddPage | canEditPage | canDelPage | canAddRec | canAddUser | canEditUser | canApprove | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | Створить | |
| admin | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | Зберегти | Видалить |
| guest | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☑ | ☐ | ☐ | Зберегти | Видалить |
| registered | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☑ | ☑ | ☐ | ☐ | Зберегти | Видалить |
| redactor | ☐ | ☐ | ☐ | ☑ | ☑ | ☐ | ☑ | ☐ | ☐ | ☑ | Зберегти | Видалить |

Рис. 4. Матриця доступу суб'єктів

– створення блоків авторизації;
– створення форми заповнення Username;
– створення форми заповнення Password;
– створення кнопки Login;

розміщення кнопки Login в блоках авторизації.

Сторінка реалізації метода, оформлена за допомогою стандартної мови розмітки веб-сторінок в Інтернеті, мовою на якій здебільшого створюються веб-сайти, а саме HTML, також за допомогою скриптової мови програмування, яка створена для генерації HTML-сторінок на стороні веб-сервера, а саме PHP.

Створюється база даних, в якій записано дані для доступу службовців підприємства, а також час останнього підключення до системи, кількості разів підключення та інформація про рівні доступу (рис. 5). Поле status відображає стан функції $T^a$ .

Таким чином, в системі присутні користувачі декількох груп з парольним доступом, зокрема: baker; driver; forwarde; porter; technologist; accountant; director assistant та director , що має безпарольний доступ до нижчих шарів ієрархії.

## Висновки

В результаті проведених досліджень та практичного застосування їх результатів було проведено адаптацію ієрархічної моделі доступу Бела–ЛаПадули до випадку інформаційної системи з динамічним рівнем конфіденційності та підвищено її стійкість до інсайдерських атак шляхом модифікації функції переходу та механізму фільтрації інформаційного потоку ОПР. Умова впровадження полягає у врахуванні існуючої моделі розподілу інформаційних потоків в існуючий інформаційній системі комерційного підприємства та збереження ієрархічної моделі доступу та засобів автентифікації.

## Література


*1. Жора, В. Підхід до моделювання рольової політики безпеки [Текст] / В. Жора // Правове, нормативне та метрологічне забезпечення системи захисту інформації в України. – 2003.– Вип. 7. – С. 45-49.*

*2. LaPadula, Leonard J. Secure Computer Systems: A Mathematical Model [Electronic resource] / Leonard J. LaPadula and D. Elliott Bell // MITRE Corporation Technical Report 2547. – Volume II, 31 May 1973. – Access mode: http://www.albany.edu/acc/courses/ia/classics/belllapadula2.pdf. – 14.04.2014.*

*3. Bryce, Ciaran. Lattice-Based Enforcement of Access Control Policies [Text] / Ciaran Bryce // Arbeitspapiere der GMD (Research Report), Nummar 1020, August 1996.*

*4. Девянин, П. Н. Модели безопасности компьютерных систем. Учебное пособие для вузов [Текст] / П. Н. Девянин. – М. : Академия, 2005. – 144 с.*

*5. Зегжда, П. Д. Основы информационной безопасности [Текст] : учебное пособие / П. Д. Зегжда, Е. А. Рудина. – СПб. : Изд-во Политехн. ун-та, 2008. – 224 с.*

*6. Ростовцев, А. Г. Теоретическая криптографія [Текст] / А. Г. Ростовцев, Е. Б. Маховенко. – СПб. : Изд-во НПО «Профессионал», 2004. – 490 с.*

*7. Закон України «Про інформацію» [Електронний ресурс]. – Режим доступу: http://kodeksy.com.ua/pro_informatsiyu/statja-21.htm. – 14.04.2014.*

*8. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу [Текст]. – Чинний з 1999-07-01. – Київ : ДСТСЗІ СБ України, 1999. – 16 с.*

*9. Метод експертних оцінок [Електронний ресурс]. – Режим доступу: http://pidruchniki.ws/19650323/ekonomika/metodi_ekspertnih_otsinok. – 14.04.2014.*


| | id | uname | passwd | team | level | status | lastlogin | logincount |
|---|---|---|---|---|---|---|---|---|
| ☐ | 38 | forwarder2 | 22 | forwarders | 3 | active | 2013-04-07 01:04:08 | 3 |
| ☐ | 37 | forwarder1 | 21 | forwarders | 3 | active | 0000-00-00 00:00:00 | 0 |
| ☐ | 34 | driver3 | 12 | drivers | 3 | active | 2013-04-07 00:58:32 | 1 |
| ☐ | 35 | driver4 | 13 | drivers | 4 | active | 2013-04-07 00:18:36 | 3 |
| ☐ | 36 | driver5 | 14 | drivers | 3 | inactive | 0000-00-00 00:00:00 | 0 |
| ☐ | 33 | driver2 | 11 | drivers | 3 | inactive | 0000-00-00 00:00:00 | 0 |
| ☐ | 31 | driver1 | 10 | drivers | 3 | active | 0000-00-00 00:00:00 | 0 |
| ☐ | 29 | baker5 | 5 | bakers | 3 | active | 2013-04-07 00:56:43 | 12 |
| ☐ | 28 | baker4 | 4 | bakers | 3 | active | 2013-04-07 00:56:37 | 37 |
| ☐ | 25 | baker1 | 1 | bakers | 3 | inactive | 0000-00-00 00:00:00 | 0 |
| ☐ | 26 | baker2 | 2 | bakers | 3 | inactive | 0000-00-00 00:00:00 | 0 |
| ☐ | 27 | baker3 | 3 | bakers | 3 | active | 2013-04-07 01:25:08 | 41 |
| ☐ | 24 | Technologist | 41 | technologists | 3 | active | 2013-04-07 01:01:16 | 4 |
| ☐ | 22 | director assist | 111 | assistants | 2 | active | 2013-04-07 01:08:31 | 1 |
| ☐ | 23 | Accountant | 51 | accountants | 2 | active | 2013-04-07 01:07:29 | 1 |
| ☐ | 1 | director | | Admin | 1 | active | 2013-04-07 20:29:25 | 22 |
| ☐ | 39 | forwarder3 | 23 | forwarders | 3 | active | 0000-00-00 00:00:00 | 0 |

Рис. 5. Рівні доступу облікових даних працівників

*10. Общая схема мандатных моделей безопасности и ее применение для доказательства безопасности систем обработки информации [Електронний ресурс]. – Режим доступу: http://www.ssl.stu.neva.ru/ssl/publications/magazine/2000/2/6/zegzhda.pdf. – 14.04.2014.*

*11. Сагун, А. В. Оптимізація моделі розподілу мережного трафіку в інформаційній системі з врахуванням політики доступу [Текст] / А. В. Сагун // Радіоелектронні та комп'ютерні системи. – 2014. – № 1(65). – С. 122-126.*

*Поступила в редакцию 4.04.2014, рассмотрена на редколлегии 19.05.2014*

**Рецензент:** д-р техн. наук, професор каф. інтелектуальних систем прийняття рішень С. В. Голуб, Черкаський національний університет ім. Б. Хмельницького, м. Черкаси

## МОДИФИКАЦИЯ МОДЕЛИ БЕЛЛА-ЛАПАДУЛЫ ДЛЯ РАЗГРАНИЧЕНИЯ ДОСТУПА В ИНФОРМАЦИОННЫХ СИСТЕМАХ

***А. В. Сагун***

Выделена актуальность применения модификации математической модели Белла-ЛаПадулы для организации разграничения доступа в информационных системах. Показано, что при практическом применении математической модели Белла-ЛаПадулы для организации информационной системы на предприятии при наличии секретной информации дополнительная защита от инсайдерских атак в иерархической модели доступа может быть получена за счет модернизации функции перехода. Предложена модификация функции перехода на базе сформулированного функционального профиля защищенности обрабатываемой информации. Произведена практическая реализация предложенной модификации иерархической модели Белла–ЛаПадулы на основе созданной матрицы доступа.

**Ключевые слова**: математическая модель, разграничение доступа, модель Белла-ЛаПадулы, иерархическая система, информационная система.

## THE MODIFICATION OF BELL'S-LA PADUL'S MODEL FOR ACCESS DIVIDE IN THE INFORMATION SYSTEMS

***A. V. Sagun***

The actuality of using the modification of math–model of Bell's–La Padul's for access divide in the information systems was highlighted. In cases of practical using of Bell's–La Padul's model for enterprises while organization of information system included confidential information, additional protection against insiders attacks may be got by the modernization of transmitted function. The modification of transition function on the base of formulated functioned security profile of the processed information was proposed. On the base of created access matrix was done the practice realization of hierarchical Bell's–La Padul's model.

**Key words:** math–model, access divide, Bell's–La Padul's model, hierarchic system, information system.

**Сагун Андрей Викторович** – канд. техн. наук, доцент кафедры информатики и информационной безопасности, Черкасский государственный технологический институт, Украина, e-mail: avd29@ukr.net.