***Турчин О.І.***

## Інформаційна безпека процесів менеджменту інтегрованих систем

*У статті розглянуто питання інформаційної безпеки процесів менеджменту інформаційного простору підприємств. Обгрунтована необхідність створення моделі захисту інформації для підприємств будь-якої форми власності, розкрита структура ролевої моделі, як засобу захисту інформації.*

*The question of informative safety of processes of management of informative space of enterprises is considered in the article. Reasonable necessity of creation of model of priv for the enterprises of any pattern of ownership, exposed structure of role model, as to the mean of priv.*

***Ключові слова:*** *управління, інформаційна безпека, базові моделі управління доступом об'єктів інформаційних систем.*

**Вступ**. У сучасному світі дуже важко уявити функціонування підприємства будь-якої форми власності і будь-якої сфери діяльності без використання інформаційних систем, адже розвиток та конкурентоспроможність більшості сучасних підприємств безпосередньо залежить від впровадження інформаційних систем, що сприяє автоматизації процесів на підприємстві.

Та не тільки впровадження інформаційних систем спрямовує підприємства у напрямку до підвищення ефективності і конкурентоспроможності: стан підприємства цілком залежить від надійності функціонування системи, підтримки захисту інформаційного простору, тому що доступ конкурентів до цієї інформація може привести до великих збитків та втрати позицій на ринку [1].

**Постановка завдання.** Мета статті – розглянути аспекти інформаційної безпеки процесів менеджменту інформаційних систем, як продуктивного напрямку до підвищення ефективності і конкурентоспроможності підприємства.

**Результати.** Сучасний ринок вимагає гнучкості комерційних структур, швидкого реагування на зміну структури споживчого попиту. Розширення

Турчин О.І., Донецький національний університет

номенклатури товарів і послуг, збільшення кількості і чисельності підрозділів підприємств, розширення географії, ускладнення виробничої інфраструктури і засобів обробки інформації і зв'язку вимагає при формуванні структури безпеки сучасних підходів.

Інформація є найбільш коштовним економічним ресурсом. Таким чином, найбільш перспективним напрямом інвестиційній діяльності є вкладення в інформаційні активи підприємств. Практика показує, що збільшення темпів науково-технічного розвитку, зростання складності і об'єму господарських зв'язків підприємства приводить до інформаційного перевантаження, неможливості ефективно обробляти і враховувати всі накопичені дані [3].

Виникає необхідність створення інформаційної інфраструктури підприємства на базі парадигми єдиного інформаційного простору підприємства, що передбачає інтеграцію різноманітною науково-технічною, інженерною, фінансовою, маркетинговою і інших видів інформації в рамках єдиної системи. Створення єдиного інформаційного простору дозволяє реалізувати єдиний безперервний цикл інноваційної діяльності підприємства, що гнучко враховує ринкові сигнали в процесі вдосконалення продукції, дозволяє якнайповніше задовольняти потреби клієнтів.

Забезпечення інформаційної безпеки є одним із головних напрямів ефективного розвитку підприємства. Сучасне забезпечення безпеки інформації в корпоративних структурах характеризуються двома основними особливостями [2]:

– ринок організаційних і технічних засобів і методів захисту представляє щонайширші можливості для вибирання вітчизняних і зарубіжних засобів забезпечення безпеки;

– слабке розуміння і недооцінка значущості і цінності інформації для корпоративних структур різної форми власності, спрощений підхід до організації діяльності служби безпеки, системний аналіз і системи управління безпекою об'єктів захисту.

Можна виділити декілька моделей управління доступом до об’єктів корпоративних систем, як засоби по забезпеченню інформаційного захисту: мандатну, дискреційну, ролеву.

Загальним підходом для усіх моделей управління доступом є розділення безлічі суті на безліч об'єктів і суб'єктів, при цьому визначення понять «об'єкт» і «суб'єкт» можуть істотно розрізнятися.

У дискреційній моделі безпеки управління доступом здійснюється шляхом явної видачі повноважень на проведення дій з кожним з об'єктів інформаційної системи (наприклад модель Харрісона-Рузо-Ульмана). Для цього служить матриця доступу, у якій визначені права доступу суб’єктів системи до об’єктів (стовбці – об’єкти, строки – суб’єкти ). З точки зору розробки модель не є складною, але при збільшенні користувачів і об’єктів стає практично не контрольованою, що може привести до великих збитків підприємства.

Для мандатної моделі визначені таки правила функціонування: кожному об'єкту і суб'єкту (користувачеві) системи призначається свій рівень допуску (наприклад модель Белла-ЛаПадулы), усі можливі рівні допуску системи чітко визначені і впорядковані за збільшенням секретності. Користувач може отримати доступ до об'єктів з рівнем допуску не вище його власного та об’єктів, рівень допуску яких не нижче його власного.

Проблемою цієї моделі вважається безперешкодність обміну інформацією між користувачами одного рівня, оскільки ці користувачі можуть виконувати в організації різні функції (що може бути дозволено роботи користувачеві X може бути заборонено для користувача Y).

У якості управління доступом до інформаційного простору розглянемо ролеву модель.

Рольове розмежування доступу як правило застосовується в системах захисту систем управління базами даних (СУБД), а окремі елементи реалізуються в мережевих операційних системах. Але існуючі моделі розмежування прав доступу, що існують в СУБД не дозволяють реалізувати гнучкі правила, які динамічно міняються в процесі функціонування системи. Наприклад, в стандартній системі розмежування прав доступу можна використовувати чотири види дії на таблиці (додавання, зміна, видалення, перегляд записів), що не завжди забезпечує повною мірою потреби організації робочого процесу.

Виникає необхідність у розширенні стандартної ролевої моделі шляхом додавання додаткових можливостей доступу до об’єктів інформаційного простору. Для цього усі об’єкти системи об’єднаємо у єдине дерево. Для кожного об’єкту окрім єдиного кореневого, є один батьківський об’єкт будь-яка множина залежних. Роль може бути назначена користувачу у контексті будь-якого об’єкту й користувач може отримати доступ до об’єктів усієї гілки, яка

була утворена цим об’єктом. На рис. 1 представлена схема організації ролевої моделі доступу до об’єктів інформаційного простору.

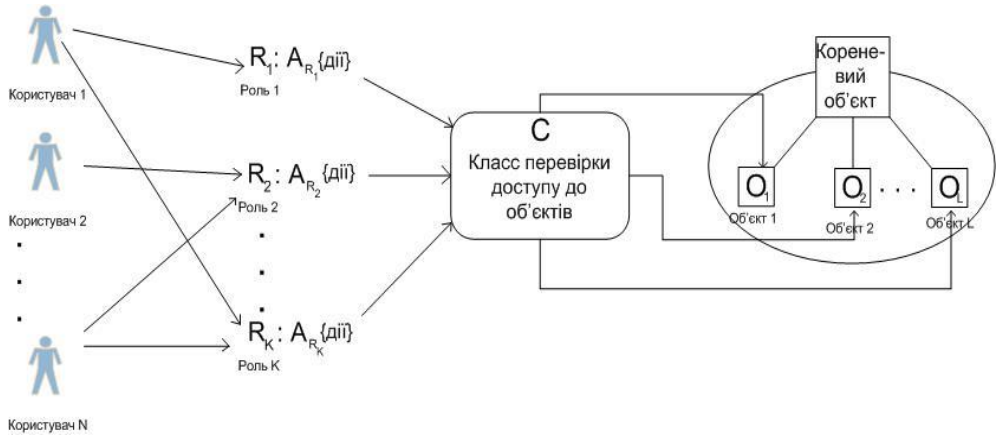


Рис. 1. Організаційна структура ролевої моделі доступу

Кожен об’єкт інформаційної системи може створити свою множину (домен), до складу якого буде входити він і усі залежні від нього об’єкти. Кожний із цих залежних об’єктів може утворити свій домен, що будуть у підпорядкуванні до батьківського домену. Ролі, призначені користувачеві в кореневому домені, мають глобальний характер і є дійсними у контексті кожного об'єкту інформаційної системи.

Роль може бути обмежена не тільки одним або декількома користувачами системи: якщо роль обмежена К користувачами, то і у контексті кожного об’єкту системи не більше К користувачам може належати ця роль.

Для створення гнучкої схеми безпеки введемо блок «клас перевірка доступу». «Клас перевірка доступу» складається із правил, що містить набір правил для визначення прав доступу по заданій дії для ролі.

Рольове управління доступом зовсім не є окремим випадком виборчого управління доступом, оскільки його правила визначають порядок надання доступу суб'єктам інформаційної системи залежно від ролей, що є у нього, в кожен момент часу. Ролевий підхід використовується в системах для користувачів, яким чітко визначено круг їх посадових повноважень і обов'язків.

Оскільки привілеї не призначаються користувачам безпосередньо, і отримуються ними лише через свою роль (або ролі), управління індивідуальними правами користувача по суті зводиться до призначення йому ролей. Це спрощує операції додавання користувача або зміну ролі користувачем.

Ролева модель безпеки визначає і змушує використовувати специфічні політики безпеки підприємства, щоб природно узгоджувалось з організаційною структурою підприємства. Ролева модель стає домінуючою в управлінні доступом до інформаційних систем оскільки зменшує вартість і адміністрування безпеки.

Хоча рольова модель безпеки може бути занадто ускладненою серед невеликих підприємств з декількома користувачами (наприклад, всім співробітникам дозволено переглядати, видаляти, або змінювати всі дані), вона є надзвичайно потужним інструментом для контролю складних середовищ. Ця концепція найбільш зручна, коли треба дозволити працювати у корпоративній системі багатьом співробітникам підприємства, встановити для деяких співробітників індивідуальні права доступу до об'єктів інформаційного простору у системі та інше.

Розглянемо математичну модель перевірки доступу до об'єктів інформаційної системи.

Визначимо множину зареєстрованих користувачів:

$U = \{u_l\}_{l=1}^{L_u}$, де $L_u$ - кількість користувачів.

Визначимо множину об'єктів:

$O = \{o_i\}_{i=1}^{L_o}$, де $L_o$ - кількість об'єктів.

Визначимо множину дій:

$A = \{a_k\}_{k=1}^{L_A}$, де $L_A$ - список дій.

Визначимо множину ролей:

$R = \{r_t\}_{t=1}^{L_R}$, де $L_R$ - список ролей.

Визначимо множину дозволень:

$P = \{p_b\}_{l=1}^{L_P}$; $p_b = (k,i)$, де $k$ - індекс дії, $i$ - індекс об'єкту.

Визначимо множину $R'_c$ для усіх ролей перевіряємого користувача $u_c$.

$$R'_c = \bigcup_{L_R} r_t^c .$$

Визначимо множину $P'_c$ усіх дозволень стосовно перевіряємого користувача $u_c$:

$$P_c^{'} = \bigcup_{r_c \in R_c^{'}} p : \forall r_t \; \exists p \supset P .$$

Функція перевірки повноважень:

$$F(U_d, O_d, A_d) = \begin{cases} 1, \exists\, p_n \in P'_{U_d} : p_n.o = O_d \;\; и \;\; p_n.a = A_d \\ 0, \; інше \end{cases}.$$

Функція повертає 1, якщо перевіряємий користувач має повноваження до обраного обєкту.

Таким чином був продемонстрований ролевий підхід доступу до об'єктів інформаційної системи. В рамках ролевої моделі формуються близькі до реального життя правила контролю доступу і обмеження, дотримання яких є критерієм безпеки системи корпоративної інформаційної системи, що є важливішим фактором збереження конкурентоспроможності підприємства та подальшого розвитку.

**Висновки.** У статті розглянуто забезпечення інформаційної безпеки процесів менеджменту інформаційних систем, на прикладі ролевої моделі управління доступом. Були приведені існуючи методи захисту інформаційного простору підприємства. Розглянута необхідність підтримки захисту інформаційного простору, як основи подальшого ефективного розвитку підприємства.

Розкрита структура рольової моделі доступу до об'єктів інформаційного простору підприємства для підтримки безпеки інформації від несанкціонованого доступу, як засіб захисту інформаційної системи.

## Література


1. Афанасьев Э.В., Ярошенко В.Н. Эффективность информационного управления. - М.: Экономика, 1997. - 109 с.
2. Зингер И.О., Кругликов Б.И., Садовников В.И. Информационное обеспечение в организационных системах управления. – М.: Наука, 1987. – 207 с.
3. Короткий С. Концепция построения комплексных информационных систем.- М.: Корпоративный менеджмент, 2001.- С.1-10.
4. Игнатьев В.А. И 266 Информационная безопасность современного коммерческого предприятия: Монография. — Старый Оскол: ООО «ТНТ», 2005. — 448 с. ISBN 5-94178-070-2
5. Гринберг А.С., Король И.А. Информационный менеджмент М.: ЮНИТИ-ДАНА, 2003. - 415 с.