УДК 621.391.7.001

С.Г. АНТОЩУК, Д.А. МАЄВСЬКИЙ, О.Ю. МАЄВСЬКА, В.М. АНТОЩУК

Одеський національний політехнічний інститут, Україна

ЗАБЕЗПЕЧЕННЯ САНКЦІОНОВАНОГО ДОСТУПУ ДО ДАНИХ В ОБЛІКОВИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Розглянуто питання забезпечення інформаційної безпеки в облікових інформаційних системах згідно вимог стандарту ISO 17779. Показано, що для облікових систем велике значення має забезпечення санкціонованого доступу до інформаційної бази з можливістю визначення умов, за яких доступ може бути наданий. Приведена інформаційна модель та програмна реалізація санкціонованого доступу при реалізації облікової системи у середовищі 1С:Підприємство.

Ключові слова: *інформаційна безпека, облікові інформаційні системи, фреймова модель.*

Вступ

У теперішній час автоматизовані системи грають вирішальну роль при забезпеченні ефективного виконання бізнес процесів як комерційних так і державних підприємств. Найбільш розповсюдженими серед них є облікові інформаційні системи (ОІС), що використовуються для ведення бухгалтерського, податкового, складського обліку, розрахунку заробітної плати та інше. Повсюдне використання ОІС для зберігання, обробки та передачі інформації веде до підвищення актуальності проблем, пов'язаних з забезпеченням їх інформаційної безпеки. У наш час інформація з абстрактного поняття перетворилася на дуже цінний товар з властивими будь-якому товару рисами бути втраченим або вкраденим. Але на відміну від звичайного товару, факт крадіжки якого зразу кидається в очі (товару просто нестає), крадіжка інформації зводиться до дуже легкого процесу виготовлення електронної копії. Тобто, користувач інформаційної системи може й не здогадуватись, що його інформація вже стала набутком ще когось.

Інформація в ОІС є найбільш цінною для підприємства та найбільш бажаною для зловмисників, оскільки вона відображає дійсний фінансовий стан підприємства, його грошові стосунки з контрагентами, податковими та державними органами. Втрата або розголошення такої інформації є неприпустимою. Тому першим питанням, яке постає перед будь-якою більш-менш крупною компанією, що намагається автоматизувати свій облік є питання безпеки ОІС. Основи безпеки інформаційної системи (ІС) не обхідно закладати на етапі її проектування. Саме на цьому етапі повинні формуватись вимоги щодо забезпечення інформаційної безпеки ОІС та накреслюватись шляхи їх реалізації.

1. Проблеми забезпечення санкціонованого доступу

Про важливість інформаційної безпеки говорить той факт, що в 2000 році міжнародним інститутом стандартів ISO розроблено та запроваджено спеціальний стандарт інформаційної безпеки – стандарт ISO 17799 [1]. Цей стандарт встановлює єдині правила та підходи до побудови системи інформаційної безпеки та встановлює можливість аудиту інформаційних систем з точки зору безпеки. Окремим розділом у стандарті виділено управління доступом до ресурсів ІС. Управління доступом передбачає контроль доступу до ресурсів системи та послуг, що надаються, а також протидію несанкціонованої активності у системі. Санкціонований доступ до ресурсів системи має дозволяє забезпечити:

- авторизацію користувачів на початку роботи з системою;
- встановлення різним користувачам системи різних прав до доступу до її ресурсів;
- контроль за діями користувача, що можуть призвести до зміни інформаційної бази;
- встановлення кожному користувачеві переліку допустимих операцій, що можуть змінювати стан інформаційної бази;
- встановлення меж та контроль доступу до перегляду інформаційних ресурсів користувачами з різними рівнями допуску.

В сучасних ОІС задача забезпечення санкціонування доступу є актуальною. Це пояснюється багаторівневістю секретності інформації у облікових системах. Так, на загальнодоступному рівні знаходиться інформація, що відноситься до загальновідомих показників діяльності підприємства, така, наприклад, як відкриті відомості про підприємство та його керівників, дані державної реєстрації,

інформація про ставки податків та зборів, що їх сплачує підприємство, тощо. Доступ до перегляду такої інформації можуть мати усі категорії користувачів. На захищеному рівні знаходиться закрита інформація, доступ до якої можуть мати лише користувачі з певними правами. До такої інформації відносяться, наприклад, дані бухгалтерського та податкового обліку, що висвітлюють фінансовий стан підприємства, дані, що використовуються для розрахунку собівартості продукції, показники прибутковості, тощо.

У свою чергу, захищений рівень розпадається на ряд підрівнів, доступ до яких відкривається тільки певним посадовим особам підприємства. Наприклад, залишки коштів на банківських рахунках є відкритими для керівника підприємства, головного бухгалтера та бухгалтера по розрахунках. Водночас ця інформація не повинна бути доступною, наприклад, для матеріально-відповідальних осіб на складах.

З метою вирішення питання про рівень доступу користувача до інформаційної бази облікової системи треба провести процедуру авторизації на початку роботи з системою. У відповідності до стандарту ISO 17799 процедура авторизації повинна передбачати наступне:

– не відображати дані про систему, доки повністю не завершиться процедура входу;

– не виводити повідомлення-підказки під час процедури входу з метою ускладнення роботи незареєстрованих користувачів;

– визначати максимально можливу кількість спроб входу до системи та мати можливість припинити сеанс роботи з користувачем, якщо ця кількість перевищена;

– визначити максимальний та мінімальний час, що його повинна займати процедура реєстрації та переривати роботу користувача, якщо ці значення перевищені;

– вести реєстр спроб входу у систему та всіх спроб, що завершилися некоректно.

Вимоги стандарту що до встановлення кожному користувачеві переліку допустимих операцій та меж доступу до інформаційних ресурсів в облікових системах теж мають свої особливі риси. Той самий користувач у різні моменти часу повинен мати різні права що до доступу до тих самих ресурсів. Типовий приклад – наявність в ОІС так званої «дати заборони проведення» операцій, що можуть змінювати стан інформаційної бази. Справа в тому, що штатним режимом роботи облікової системи є проведення операцій «заднім числом». При такому проведенні дата фактичного вводу операції в систему відрізняється від дати, якою повинна бути зроблена зміна облікових даних. Тобто користувач має змогу втручатись у показники обліку, що були сформовані раніш та змінювати ці показники. Дата заборони проведення встановлює межу, до якої зміна інформації є можливою. Так, наприклад, наприкінці року, згідно з діючого законодавства [2], бухгалтер повинен виконати регламентну операцію – закриття періоду та сформувати баланс. Після цієї операції ніякі втручання в дані закритого періоду неприпустимі. Датою заборони проведення стає останній день закритого року, що повинно призводити до того, що певна категорія користувачів може тільки переглядати інформацію цього періоду, але не може змінювати її. З цього витікає, що встановлення меж та контроль доступу до перегляду інформаційних ресурсів користувачами з різними рівнями допуску в облікових системах повинні носити умовний характер, тобто залежати від певних умов.

За останні роки в Україні створено велику кількість облікових систем, які використовуються у різних галузях підприємницької діяльності. Більша частина з них побудована на базі платформи 1С:Підприємство [2], що практично стала стандартом для різноманітних ОІС. Це обумовлено насамперед тим, що 1С:Підприємство є відкритою системою, яку можливо налаштовувати на виконання необхідного алгоритму обліку. Практично 1С:Підприємство являє собою розвинену систему програмування зі своєю об'єктно-орієнтованою мовою, механізмом підтримки інформаційної бази та вбудованими спеціалізованими об'єктами, за допомогою яких можна створювати свої програмні механізми для побудови своїх власних ОІС.

Система 1С:Підприємство має також свій власний вбудований механізм санкціонування доступу до інформаційних ресурсів. Цей механізм передбачає авторизацію користувача при вході в систему та визначення для нього так званої «ролі» в системі. Роль визначає ступінь допуску до перегляду та зміни інформаційної бази. Список ролей створюються на етапі розробки (конфігурування) ОІС. Він є жорстко обумовленим та передбачає тільки два варіанти доступу до конкретного об'єкту в інформаційній базі – або доступ дозволений, або ні. Ніяких інших варіантів не передбачається. Користувач на етапі експлуатації не має змоги змінити ці правила.

Таким чином, аналізуючи систему 1С:Підприємство з точки зору інформаційної безпеки можна зробити висновок, що вона не в повній мірі відповідає положенням стандарту ISO 17799 та вимогам щодо інформаційної безпеки облікових систем. Це пояснюється наступними недоліками ОІС 1С:Підприємство:

– авторизація користувача на початку роботи: користувач може отримати підказку, кількість спроб та час проходження процедури авторизації необмежені;

– встановлення меж та контроль доступу до перегляду інформаційних ресурсів користувачами:

доступ є жорстким і не може носити умовного характеру.

Проте можливості системи 1С:Підприємство дозволяють програмно усунути ці недоліки. Тому безумовно актуальним є створення механізмів забезпечення вимог стандарту ISO 17799 обліковими системами, які створені на базі платформи 1С:Підприємство. У представленій роботі запропоновані засоби, що дозволяють зробити контроль доступу до інформаційних ресурсів більш гнучким та надають користувачеві можливість самому задавати умови щодо рівня доступу.

2. Адаптивні можливості ОІС

Для створення ОІС з адаптивними можливостями щодо вимог користувача у роботі [3] запропоновано підхід, якій базується на ідеї застосування «відокремленого коду» та бази знань. Особливість роботи ОІС характеризується тим, що програмний код критичних для роботи системи алгоритмів не є «вмонтованим» в загальний програмний код, а відокремлюється від неї.

При необхідності виконання алгоритму вступає в роботу спеціальна програма-інтерпретатор, на вхід якої поступає цей відокремлений програмний код. За принципом дії інтерпретатор є кінцевим автоматом, переходи якого саме й записані в відокремленому коді. Такий підхід дозволяє вирішити багато питань, що постають перед розробниками ОІС:

– адаптація системи до вимог законодавства, що постійно змінюється;

– можливість створення користувачем своїх власних алгоритмів проведення господарських операцій, властивих саме цьому підприємству;

– супроводження системи, яке при змінних алгоритмах зводиться до передачі користувачеві тільки невеликих текстових файлів зі зміненими алгоритмами.

Крім того відкривається можливість створення системи із потрібним для даного підприємства санкціонуванням доступу, враховуються вимоги:

– правила доступу користувачеві до інформаційної бази є формуються відповідним чином;

– користувач має змогу динамічно змінювати ці правила в залежності від своїх потреб.

Для побудови інформаційної бази (бази знань) систем із змінним програмним кодом авторами запропонована модель багатомірного дискретного простору. В цьому просторі координатами можуть бути деякі значення довільного типу, а точці на перетині координат відповідає деяка сукупність параметрів, кожен із котрих зберігає якесь інформаційне значення. Поняття такого простору є подальшим удосконаленням поняття фреймового підходу до представлення знань [4]. Фрейм являє собою систему так званих слотів, кожен з яких має особисте ім'я та особисте значення. Система слотів у фреймовій моделі дуже вдало описує координати у багатомірному просторі. Дійсно, для того, щоб визначити координати у просторі треба задати ім'я кожної з них та конкретне значення. Тобто один слот фреймової моделі цілком описує одну координату. Система таких слотів (кількість котрих є довільною) і виступає в якості системи координат.

Складнішим є представлення значень, що зберігаються на уявному перетині координат (вузлах). Система таких значень є самостійною фрейм-системою, яка у свою чергу має свій набір слотів. Кожен з цих слотів описує одне із значень, що зберігаються на перетині вимірів. Складність полягає у тому, що конкретній комбінації слотів-вимірів треба поставити у відповідність конкретний фрейм-значення. Традиційна фреймова модель не вирішує цієї проблеми. Потрібна реалізація своєрідного гіперпереходу з одного простору, що має k вимірів (фрейм координат) до іншого, що має z вимірів (фрейм значень). Назвемо таку систему, що об'єднує фрейм координат, фрейм вимірів та має механізмом однозначного переходу між ним «гіперфреймом». З позицій об'єктно-орієнтованого підходу гіперфрейм може представити базовим класом «ГіперФрейм», що має визначений перелік властивостей та методів. При створенні конкретного об'єкту цього класу застосовується механізм успадкування, за яким користувач може доповнювати перелік властивостей та методів. Властивостями конкретного екземпляру цього класу е конкретні виміри (координати) та конкретні значення для конкретного реєстру. Тобто, базовий клас «ГіперФрейм»» не повинен накладати жодних обмежень на доповнення базового (на початку пустого) переліку координат та значень.

Застосовуючи поняття гиперфрейму до цілей створення системи із санкціонованим доступом треба визначитись із кількістю координат (кількістю вимірів простору) та типом їх значень. Для цього розглянемо алгоритм роботи санкціонованого доступу та його інформаційну базу.

Інформаційну базу для функціонування санкціонованого доступу повинні складати декілька списків, у кожному з яких зберігається інформація про об'єкти одного типу.

Такими об'єктами є:

– перелік імен користувачів, яким дозволено вхід у систему;

– повний перелік об'єктів інформаційної бази, з якими теоретично можуть працювати користувачі. до таких об'єктів відносяться інформаційні списки, регістри, у яких фіксується облікова інфо-

рмація та програмні об’єкти, що відображають цю інформацію у вигляді звітів;

– перелік дій, що їх теоретично можуть виконувати користувачі із цими об’єктами інформаційної бази.

У системі 1С:Підприємство для зберігання інформації про однотипні об’єкти використовуються так звані довідники. Фактично довідник є аналогом двомірної таблиці, яка може мати довільну кількість стовпців та рядків. Кількість стовпців задається програмістом на етапі конфігурування системи й визначається тією інформацією, що повинна зберігатися у довіднику. Кількість рядків визначається потребами користувача, який має змогу вільно додавати до довідника нові рядки, редагувати вже введені та видаляти непотрібні. Кожен довідник у системі може відображатися для користувача за допомогою довільної кількості екранних форм, що їх проектує розробник системи.

Для потреб встановлення санкціонованого доступу запропоновано використовувати довідники:

1. довідник з іменем «Перелік користувачів», який містить інформацію про імена та паролі тих користувачів, що мають доступ до системи;

2. довідник з іменем «Об’єкти системи», що містить інформацію про всі об’єкти, до яких користувачі теоретично мають змогу звертатися. у якості такої інформації повинні використовуватись системні ідентифікатори цих об’єктів та їхні синоніми, які будуть відображатися в екранних формах користувача;

3. довідник з іменем «Дії з об’єктами», що містить назви усіх можливих дій, що їх теоретично можуть виконувати користувачі з переліченими об’єктами.

Щодо переліку дій, то виходячи з проведеного аналізу фактично можливими для користувача є наступні:

– можливість відкриття тої чи іншої екранної форми для перегляду;

– додавання нового елементу (рядка);

– редагування інформації в об’єкті;

– проведення змін в облікових реєстрах системи (проведення тих чи інших господарських операцій);

– видалення інформації в об’єкті (наприклад, строки в довіднику).

Ці три довідники визначають перелік можливих значень, які можуть приймати три виміри у просторі гіперфрейму (рис. 1). В вузлах гіперфрейму має міститися відокремлений від системи програмний код, що буде інтерпретуватися системою в той час, коли користувач замовить виконання певної дії з певним об’єктом.

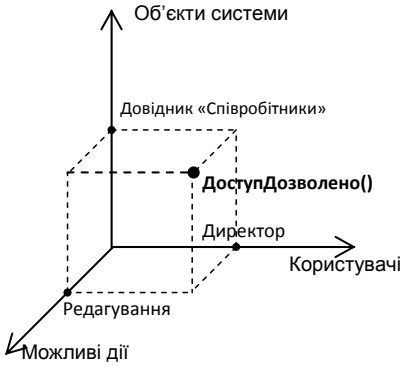

Рис. 1. Графічне представлення тримірного гіперфрейму

Три координатні осі відповідають об’єктам «Користувачі» (ось «X»), «Об’єкти системи» (ось «Y») та «Можливі дії» (ось «Z»). Конкретними координатами є значення «Директор» по осі «Користувачі», «Довідник «Співробітники» по осі «Об’єкти системи» та одна з можливих дій – «Редагування» по осі «Можливі дії».

Особливістю запропонованої моделі є:

– точки в цьому тримірному просторі можуть займати лише дискретні положення (простір є дискретним, будь-які точки між значеннями, наприклад, «директор» та «менеджер» не мають сенсу);

– значення координат мають не числовий тип, а посилання на строки конкретних таблиць-довідників.

На перетині осей з названими координатами міститься вузол гіперфрейму – у нашому випадку це рядок програмного коду системи 1С:Підприємство – виклик процедури, що дозволяє директору доступ до редагування довідника «Співробітники».

Практична реалізація вузла гіперфрейму залежить від обраної версії системи 1С:Підприємство. В системі 1С:Підприємство 7.7 в якості вузла може виступати або об’єкт типу «Регістр», або спеціально створений довідник. У більш досконалій версії 8.0 або 8.1 для цих цілей доцільно використовувати об’єкт «Регістр відомостей».

Висновки

Запропонований механізм реалізовано в обліковій інформаційній системі «АгроКомплекс», призначеної для автоматизації обліку у сільському господарстві. Робота по санкціонуванню доступу до об’єктів цієї системи відбувається таким чином.

У глобальному модулі системи реалізовано функцію – інтерпретатор «ВизначитиПраваДоступу()». Призначення цієї функції – виконання програмного коду, що знаходиться у вузлі. Програмний код побудовано таким чином, що обчислене

ним значення дорівнює одиниці, якщо доступ дозволено або нулю у протилежному випадку.

У програмний код кожної екранної форми, за допомогою яких здійснюється доступ до даних інформаційної системи на етапі її ініціалізації або запросу на виконання передбачених дій визначається ім'я користувача, що намагається отримати доступ до форми й здійснюється виклик функції ВизначитиПраваДоступу(). Ця функція звертається до спеціального довідника (представленого у вигляді гіперфрейму).

На підставі визначених координат визначається потрібний вузол, з якого зчитується програмний код, що буде визначати можливість доступу у конкретному випадку. Цей програмний код інтерпретується й обчислене ним значення повертається як значення функції ВизначитиПраваДоступу(). Якщо ця функція повернула одиницю, то запрошена дія виконується, а якщо нуль - блокується.

Для зручності користувача зроблено спеціальну екранну форму, що допомагає встановлювати та змінювати права санкціонованого доступу до об'єктів інформаційної бази. Ця форма дозволяє настроювати права як окремо по кожному об'єкту та користувачу, так і для груп об'єктив та користувачів. Розроблено перелік спеціальних функцій системи, що визначають права доступу у найбільш поширених випадках.

Запропонована методика та розроблені програмні засоби відрізняються тим, що можуть бути легко інтегровані з існуючими ІС з метою забезпечення виконання умов стандарту ISO 17799 та підвищення рівня інформаційної безпеки облікових систем.

Література

1. Стандарт ISO 17799 [Электрон. ресурс]. – Режим доступа к ресурсу: http:// www.17799.com.

2. Закон від 16.07.1999 р. № 996-XIV "Про бухгалтерський облік та фінансову звітність в Україні"

3. Маевский Д.А. Основные принципы построения учетных систем операционного управления / Д.А. Маевский, Е.Ю. Маевская // Сб. Электромашиностроение и электрооборудование. 2008. – № 70. – С. 123-126.

4. Minsky M.A. Framework for Representing Knowledge / M.A.Minsky // Cambridge: MIT Press, 1974. – P. 12-18.

Надійшла до редакції 11.02.2009

Рецензент: д-р техн. наук, проф., зав. кафедри О.Є. Федорович, Національний аерокосмічний університет ім. М.Є. Жуковського, Харків, Україна.

ОБЕСПЕЧЕНИЕ САНКЦИОННОВАНОГО ДОСТУПА К ДАННЫМ В УЧЕТНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

С.Г. Антощук, Д.А. Маевский, Е.Ю. Маевская, В.Н. Антощук

Рассмотрены вопросы обеспечения информационной безопасности в учетных информационных системах согласно требованиям стандарта ISO 17779. Показано, что для учетных систем большое значение имеет обеспечение санкционированного доступа к информационной базе с возможностью определения условий, по которым этот доступ может быть предоставлен. Приведена информационная модель и методика программной реализации санкционированного доступа при реализации учетной системы у среде 1С:Предприятие. Предложенная программная реализация может быть встроена в существующие информационные системы.

Ключевые слова: Інформаційна безпека, облікові інформаційні системи, фреймова модель

PROVIDING OF ACCESS TO DATA IN REGISTRATION INFORMATIVE SYSTEMS

S.G. Antoschuk, D.A. Maevsky, E.J. Maevskaya, V.N. Antoschuk

The questions of providing of informative safety are considered at registration informative systems in obedience to the requirements of standard of ISO 17779. It is retained that for the registration systems a large value has providing of the sanctioned access to the informative base with possibility of determination of terms which this access can be given on. An informative model and method of programmatic realization of the sanctioned access is resulted during realization of the registration system at to the environment of 1S:Predpriyatie. The offered programmatic realization can be built-in in the existent informative systems.

Keywords: informative safety, registration informative systems**,** frame model.

Антощук Світлана Григорівна – д-р техн. наук, проф., зав. кафедрою, Одеський національний політехнічний інститут, e-mail: svetlana_onpu@mail.ru.

Маєвський Дмитро Андрійович – канд. техн. наук, доц., зав. кафедрою, Одеський національний політехнічний інститут, e-mail: toe-onpu@ukr.net.

Маєвська Олена Юріївна – канд. техн. наук, доц., Одеський національний політехнічний інститут, e-mail: toe-onpu@ukr.net.

Антощук Віталій Миколайович – аспірант кафедри менеджменту, Одеський національний політехнічний інститут.