обумовлює доцільність синтезу відповідного базису. Для синтезу біортогонального вейвлет-базису можуть бути використані ітераційна оптимізаційна процедура уточнення масштабуючої функції, кратномасштабні співвідношення, залежності між параметрами фільтрів розкладу і реконструкції основного та дуального вейвлет-базисів.

1. *Малла С.* Вэйвлеты в обработке сигналов: Пер. с англ. – М.: Мир, 2005. – 671 с.
2. *Новиков Л.В.* Адаптивный вейвлет-анализ сигналов // Научное приборостроение. - 1999. - Т. 9, № 2. – 13 с.
3. *Добеши И.* Десять лекций по вейвлетам. – Ижевск: НИЦ "Регулярная и хаотическая динамика", 2001. – 464 с.
4. *Смоленцев Н.К.* Основы теории вейвлетов. Вейвлеты в MATLAB. – М.: ДМК Пресс, 2005. – 304 с.
5. *Cohen A., Daubechies I., Feauveau J.-C.* Biorthogonal Bases of Compactly Supported Wavelets // Communications on Pure and Applied Mathematics. - 1992. – Vol. XLV. – P. 485-560.
6. *Романишин Ю.М., Петрицька С.Р., Якимів Р.М., Копина Т.В.* Можливості побудови ортогонального вейвлет-базису на основі заданої вейвлет-функції // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ НАН України. – Вип. 67. – К.: 2013. – С. 171-177.
7. *Romanyshyn Y.M., Petrytska S.R.* Construction of orthogonal wavelet basis using specified wavelet function // Proceedings of the International Conference TCSET'2014. – 2014, Lviv-Slavske, Ukraine. – P. 674-676.
8. *Исаев Ю.Н.* Конструирование биортогональных вейвлет-базисов для оптимального представления сигналов // Известия Томского политехнического университета. - 2004. - Т. 307, № 1. - С. 37-42.

Поступила 15.02.2018р.

УДК 004.056.52

О.Р. Партика, Львів

МЕХАНІЗМИ РОЗМЕЖУВАННЯ ДОСТУПУ ДО РЕСУРСІВ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

The methods of differentiating access to resources of the corporate information system on the basis of: discretionary model and mandate (authority) model are considered. Their advantages and disadvantages are shown. A conclusion is made on the promise and the necessity of applying multi-level models of information security.

Keywords: discretionary model, mandate model, access differentiation.

Вступ. Одним з головних кроків на шляху до забезпечення конфіденційності інформації є розмежування доступу співробітників до ресурсів корпоративної інформаційної системи з метою обмежити спектр

інформації доступною тому чи іншому співробітнику межами, необхідними для виконання ним посадових обов'язків.

Основна частина

Розглянемо найбільш актуальні механізми розмежування доступу.

Дискреційна модель розмежування доступу

Дискреційна модель розмежування доступу (модель Грехема-Деннінга) визначається двома властивостями:

- всі суб'єкти і об'єкти ідентифіковані;
- права доступу суб'єктів на об'єкти системи визначаються на підставі деякого зовнішнього по відношенню до системи правила.

Основним елементом систем дискреційного розмежування доступу є матриця доступу. Матриця доступу – матриця розміром | S | x | o |, рядки якої відповідають суб'єктам, а стовпці – об'єктам. При цьому кожен елемент матриці доступу M [s, o] з R визначає права доступу суб'єкта s на об'єкт o, де R – множина прав доступу.

При використанні дискреційного механізму управління доступом до нього ставляться такі вимоги:

- система захисту повинна контролювати доступ найменованих суб'єктів (користувачів) до найменувати об'єктів (файлів, програм, томів і т.д.);
- для кожної пари (суб'єкт – об'єкт) в засобі обчислювальної техніки (ЗОТ) має бути задане явне і недвозначне перерахування допустимих типів доступу (читати, писати і т.д.), тобто тих типів доступу, які є санкціонованими для даного суб'єкта (індивіда або групи індивідів) до даного ресурсу (об'єкту);
- система захисту повинна містити механізм, втілювати в життя дискреційні правила розмежування доступу;
- контроль доступу повинен бути застосовний до кожного об'єкту і кожному суб'єкту (індивіду або групі рівноправних індивідів);
- механізм, який реалізує дискреційний принцип контролю доступу, повинен передбачати можливості санкціонованого зміни правил або прав розмежування доступу (ПРД), в тому числі можливість санкціонованого зміни списку користувачів ЗОТ і списку об'єктів, що захищаються;
- право змінювати ПРД має надаватися виділеним суб'єктам (адміністрації, службі безпеки і т.д.);
- повинні бути передбачені засоби управління, що обмежують поширення прав на доступ.

До переваг дискреційної політики безпеки можна віднести відносно просту реалізацію системи розмежування доступу. Це обумовлений тим, що в даний час більшість комп'ютерних систем забезпечують виконання вимог саме даної політики безпеки.

До недоліків дискреційної політики безпеки відноситься статичність визначених у ній правил розмежування доступу. Дана політика безпеки не враховує динаміку змін станів комп'ютерної системи. Крім того, при

використанні дискреційної політики безпеки виникає питання визначення правил поширення прав доступу і аналізу їх впливу на безпеку комп'ютерної системи. У загальному випадку при використанні даної політики безпеки перед системою захисту, яка при санкціонуванні доступу суб'єкта до об'єкта керується деяким набором правил, стоїть алгоритмічно нерозв'язне завдання – перевірити, чи приведуть її дії до порушення безпеки чи ні.

У той же час є моделі комп'ютерних систем, реалізуючих дискреційну політику безпеки, які мають алгоритми перевірки безпеки.

Проте, в загальному випадку дискреційна політика розмежування доступу не дозволяє реалізувати ясну і чітку систему захисту інформації в комп'ютерній системі. Цим обумовлений пошук інших, більш досконалих політик безпеки.

Мандатна (повноважна) модель розмежування доступу

Мандатна (повноважна) модель розмежування доступу заснована на мандатному розмежування доступу (Mandatory Access Control), яке визначена такими умовами:

- всі суб'єкти і об'єкти системи однозначно ідентифіковані;
- задана решітка рівнів конфіденційності інформації;
- кожному об'єкту системи привласнений рівень конфіденційності, що визначає цінність інформації, що міститься в ньому;
- кожному суб'єкту системи привласнений рівень доступу, що визначає рівень довіри до нього в комп'ютерній системі.

Основна мета мандатної політики безпеки – запобігання витоку інформації від об'єктів з високим рівнем доступу до об'єктів з низьким рівнем доступу, тобто протидія виникненню в комп'ютерній системі несприятливих інформаційних потоків зверху вниз.

Метою її розробки було усунення недоліків матричних моделей. Були розроблені так звані багаторівневі моделі захисту. Вони припускають формалізацію процедури призначення прав доступу за допомогою використання, так званих міток конфіденційності або мандатів, що призначаються суб'єктам і об'єктам доступу. Так, для суб'єкта доступу мітки, наприклад, можуть визначатися відповідно до рівня допуску особи до інформації, а для об'єкта доступу (власне дані) – ознаками конфіденційності інформації. Ознаки конфіденційності фіксуються в мітці об'єкта. Права доступу кожного суб'єкта і характеристики конфіденційності кожного об'єкта відображаються у вигляді сукупності рівня конфіденційності і набору категорій конфіденційності. Рівень конфіденційності може приймати одне з строго упорядкованого ряду фіксованих значень, наприклад: конфіденційно, таємно, для службового користування, нетаємно і т.п.

Основу реалізації управління доступом складають:

- формальне порівняння мітки суб'єкта, що запитав доступ, і мітки об'єкта, до якого запропоновано ввести відповідний доступ;
- прийняття рішень про надання доступу на основі деяких правил, основу яких складає протидія зниженню рівня конфіденційності

інформації, що захищається.

Таким чином, багаторівнева модель попереджує можливість навмисного або випадкового зниження рівня конфіденційності інформації, що захищається. Тобто ця модель перешкоджає переходу інформації з об'єктів з високим рівнем конфіденційності та вузьким набором категорій доступу в об'єкти з меншим рівнем конфіденційності та більш широким набором категорій доступу.

Вимоги до мандатної механізму полягають у наступному:

- кожному суб'єкту і об'єкту доступу повинні зіставлятися класифікаційні мітки, що відображають їх місце у відповідної ієрархії (мітки конфіденційності). За допомогою цих міток суб'єктами об'єктів повинні призначатися класифікаційні рівні (рівні уразливості, категорії секретності і т.п.), які є комбінаціями ієрархічних і неієрархічних категорій. Дані мітки повинні служити основою мандатного принципу розмежування доступу;
- система захисту при введенні нових даних в систему повинна запитувати і отримувати від санкціонованого користувача класифікаційні мітки цих даних. При санкціонованому занесенні в список користувачів нового суб'єкта йому повинні призначатись класифікаційні мітки. Зовнішні класифікаційні мітки (суб'єктів, об'єктів) повинні точно відповідати внутрішнім мітках (всередині системи захисту);
- система захисту повинна реалізовувати мандатний принцип контролю доступу стосовно всіх об'єктів при явному і прихованому доступі з боку будь-якого із суб'єктів:
  - суб'єкт може читати об'єкт, тільки якщо ієрархічна класифікація в класифікаційному рівні суб'єкта не менша, аніж ієрархічна класифікація в класифікаційному рівні об'єкта. При цьому ієрархічні категорії в класифікаційному рівні суб'єкта повинні включати в себе всі ієрархічні категорії в класифікаційному рівні об'єкта;
  - суб'єкт здійснює запис в об'єкт, тільки якщо класифікаційний рівень суб'єкта в ієрархічній класифікації не більший, ніж класифікаційний рівень об'єкта в ієрархічній класифікації. При цьому всі ієрархічні категорії в класифікаційному рівні суб'єкта повинні включатися в ієрархічні категорії в класифікаційному рівні об'єкта.
- реалізація мандатних ПРД повинна передбачати можливість супроводу, зміни класифікаційних рівнів суб'єктів і об'єктів спеціально виділеними суб'єктами;
- у ЗОТ повинен бути реалізований диспетчер доступу, тобто засіб, що здійснює перехоплення всіх звернень суб'єктів до об'єктів, а також, розмежовує доступ відповідно до заданого принципу розмежування

доступу. При цьому рішення про санкціонованість запиту на доступ має прийматися тільки при одночасному вирішенні його і дискреційними, і мандатних ПРД. Таким чином, повинні контролюватися не тільки одиничний акт доступу, а й потоки інформації.

Висновок. Практика показує, що багаторівневі моделі захисту знаходяться набагато ближче до потреб реального життя, ніж матричні моделі, і являють собою добру основу для побудови автоматизованих систем розмежування доступу. Причому, так як окремо взяті категорії одного рівня рівнозначні, то, щоб їх розмежувати поряд з багаторівневою (мандатною) моделлю, потрібно застосування матричної моделі. За допомогою багаторівневих моделей можливе істотне спрощення завдання адміністрування. Причому це стосується як вихідної настройки розмежувальної політики доступу (не потрібно такого високого рівня деталізації завдання відносини суб'єкт-об'єкт), так і подальшого включення в схему адміністрування нових об'єктів і суб'єктів доступу.

1. *Баришев Ю. В., Каплун В. А., Неуйміна К. В.* Дискреційна модель та метод розмежування прав доступу до розподілених інформаційних ресурсів // Інформаційні технології та комп'ютерна техніка. – Наукові праці ВНТУ, 2017, № 2.
2. *Девянин П. Н.* Модели безопасности компьютерных систем. – М. : Издательский центр "Академия", 2005. – 144 с.
3. *Цирлов В. Л.* Основы информационной безопасности автоматизированных систем. Краткий курс. – М. : Изд-во Феникс, 2008. – 174 с

Поступила 12.02.2018р.