УДК 004.056

О.С. Потенко, ІПМЕ ім. Г.Є. Пухова НАНУ, Київ

АНАЛІЗ МОДЕЛЕЙ БЕЗПЕКИ В АСПЕКТІ ЕКСПЕРТИЗИ СПЕЦІАЛІЗОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Складність сучасних інформаційних систем визначає різноманіття сучасних інформаційних моделей безпеки. Кожна з таких моделей описує певні аспекти інформаційної взаємодії. Нажаль на сьогодні не існує єдиної моделі, яка враховує всі нюанси. Експерт, який оцінює ту чи іншу систему, з точки зору безпеки, постає перед проблемою вибору методу моделювання, для отримання адекватного результату. Моделлю політики безпеки прийнято називати формальне описання політики безпеки для заданої системи. Але так як системи суттєво відрізняються одна від одної, то і моделі повинні застосовуватись відповідні. Основними моделями безпеки інформаційної системи є [1, 3]:

Модели систем дискретного розмежування доступу
- Take-Grant
- Модель Харрисона, Руззо та Ульмана

Модели систем мандатного розмежування доступу
- Модель Белла – ЛаПадула

Моделі контролю цілісності
-Модель Кларка –Вилсона

Інформаційні моделі
- Модель невтручання
- Модель невиводимості

Коротко розглянемо ці моделі виділяючи метод представлення даних та мету моделювання.

Модели систем дискретного розмежування доступу

Модель Take-Grant

Модель Take-Grant, запропонована в 1976 р., використовується для аналізу систем дискреційного розмежування доступу, у першу чергу для аналізу шляхів поширення прав доступу в таких системах. Як основні елементи моделі використаються граф доступів і правила його перетворення. Ціль моделі - дати відповідь на питання про можливості одержання прав доступу суб'єктом системи на об'єкт у стані, описаному графом доступів. У цей час модель Take-Grant одержала продовження як розширена модель Take-Grant , у якій розглядаються шляхи виникнення інформаційних потоків у системах з дискреційним розмежуванням доступу. В моделі існує 4 правила:

- правило «Брати»
- правило «Давати»
- правило «Створити»

– правило «Видалити»

Позначимо елементи моделі:

O – множина об'єктів

S – множина суб'єктів

$R = \{r_1, r_2, r_3, r_4, ..., r_n\} \cup \{t,g\}$ – множина прав доступу

t – право брати

g – право давати

G = (S, O, E) – кінцевий граф

× - елементи множини O

• - елементи множини S

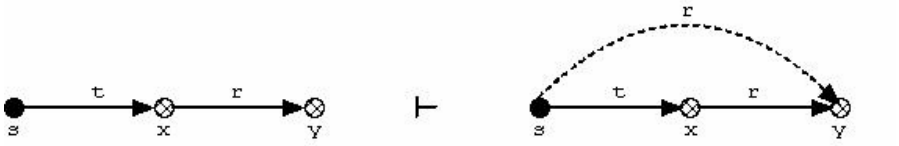
$E \in O \times O \times R$ - дуги графа, позначені непустими підмножинами із множини прав доступу R

Правило «Брати»

Брати = take(r, x, y, s), $r \in R$

Нехай $s \in S, x, y \in O$ - вершини графа G,

Тоді граф G:



Суб'єкт *S* бере у об'єкта *X* права *r* на об'єкт *Y* .

Правило «Давати»

Брати = grant (r, x, y, s), $r \in R$

Нехай $s \in S, x, y \in O$ - вершини графа G,

Тоді граф G:

Суб'єкт *S* дає об'єкту *X* права *r* на об'єкт *Y* .

Правило «Створити»

Брати = create (r, x, s), $r \in R$

Нехай $s \in S, x, y \in O$ - вершини графа G,

Тоді граф G:

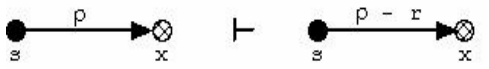
Суб'єкт *S* бере *r*-доступний об'єкт *Y*.

Правило «Видалити»

Брати = remove (r, x, y, s), $r \in R$

Нехай $s \in S, x, y \in O$ - вершини графа G,

Тоді граф G:



Методом представлення даних для даної моделі є граф доступу.

Метою моделювання являється аналіз шляхів поширення прав доступу.

Модель Харрисона, Руззо та Ульмана

В моделі Харрисона, Руззо та Ульмана захищена система складається з наступних компонентів.

1. Кінцева множина загальних прав R = {r1, …, rn}:

2. Кінцевий набір початкових суб'єктів So та кінцевій набір об'єктів Oo, кожний суб'єкт являється також об'єктом.

3. Кінцеву множину команд C, представлених у формі:

command C(X1,X2,..., Xn), де C – имя, X1,X2,..., Xn – формальні параметрі, які вказують на об'єкт.

Матриця доступу може змінюватися за допомогою наступних операцій:

- enter r into (s, o)- введення права r у відповідний елемент M[s,o] матриці доступу;
- delete r from (s, o)- видалення права r з елементу M[s,o] матриці доступу;
- create subject s - створення суб'єкта s;
- destroy subject s - видалення суб'єкта s;
- create object o – створення об'єкта o;
- destroy object o – видалення об'єкта o.

Метод представлення даних є матриця доступу.

Метою моделювання є представлення прав доступу.

Модели систем мандатного розмежування доступу

Модель Белла – Лапа дула

Модель Белла - ЛаПадула (Bell-LaPadula), призначена для керування суб'єктами, тобто активними процесами, що запитують доступ до інформації, і об'єктами, тобто файлами, поданнями, записами, полями або іншими сутностями даної інформаційної моделі.

В моделі об'єкти піддаються класифікації, а кожен суб'єкт зараховується до одного з рівнів допуску до класів об'єктів. Класи й рівні допуску спільно називаються класами або рівнями доступу.

Клас доступу складається із двох компонентів. Перший з них - це ієрархічний компонент. Другий компонент являє собою деяку множину неієрархічних категорій, які можуть ставитися до будь-якого рівня ієрархії. Так, у військових відомствах США застосовується наступна ієрархія класів

(зверху вниз):

- абсолютно секретно;
- секретно;
- конфіденційно;
- без грифа таємності.

Другий компонент міг би, наприклад, приймати значення з наступного списку:

- тільки з допуском по ядерній зброї;
- не для іноземних урядів;
- не для підрядників.

Інший приклад ставиться до приватної компанії, де можливі такі рівні ієрархії (зверху вниз):

- секретно;
- для обмеженого поширення;
- конфіденційно;
- для службового користування;
- для необмеженого поширення.

Другий компонент для тієї ж компанії міг би включати такі категорії:

- не для субпідрядників;
- фінансові дані корпорації;
- дані по зарплаті.

Ясно, що можна визначити матрицю взаємозв'язків між ієрархічними й неієрархічними компонентами. Наприклад, якщо деякий об'єкт класифікований як зовсім секретний, але йому не приписаний ніякий неієрархічний компонент, то він може надаватися іноземним урядам.

У той же час секретний об'єкт може мати категорію "не для іноземних урядів", отже не повинен їм надаватися. Однак у моделі Белла - ЛаПадула створюється "ґрати", де неієрархічні компоненти кожного рівня ієрархії автоматично приписуються до наступного більш високого рівня ієрархії (так назване "зворотне спадкування"). Також існує правило що дозволяє суб'єктові мати доступ на запис до об'єкта тільки в тому випадку, якщо рівень допуску цього суб'єкта такий же або більше низький, чим клас об'єкта - операнда операції запису. Це означає, що інформація, що належить якому-небудь рівню, ніколи не може бути записана в який-небудь об'єкт, що має більше низький рівень, ніж її джерело, оскільки це могло б потенційно привести по необережності до руйнування класифікації інформації в розглянутій системі.

Методом представлення даних є визначення двох компонентів. Перший з них - це ієрархічний компонент. Другий компонент являє собою деяку множину неієрархічних категорій.

Мета моделювання є керування суб'єктами, тобто активними процесами, що запитують доступ до інформації

Моделі контролю цілісності

Модель Кларка -Вилсона

В основі даної моделі лежить два принципи:

- Внутрішня цілісність
- Зовнішня цілісність

Модель реалізована за допомогою набора правил і не являється математичною моделлю. Також суб'єкти не мають прямого доступу до об'єктів, між ними знаходиться програма, яка має доступ до об'єктів. Контроль доступу розподілений таким чином, що тільки певні програми мають доступ до певних об'єктів, а суб'єкт має доступ тільки до певного набору програм.

Всі дані діляться на 2 класи:

- Необхідний елемент даних (CDI)
- Спонтанний елемент даних (UDI)

Далі створюється набір правил, які регулюють взаємодію з обома типами даних:

- Всі початкові процедури перевірки (IVP) повинні впевнитись в тому, що всі CDI знаходяться в достовірному стані під час роботи IVP.
- Всі процедури перетворення (TP), повинны бути сертифіковані.
- Правила доступу повинні задовольняти всім вимогам розподілення обов'язків.
- Всі процедури перетворення повинні бути записані в доступний тільки на дописування журнал.
- Будь-яка процедура перетворення, яка одержала вхід UDI повинна перетворити його в CDI інакше відмінити операцію.

Також для зміцнення захисту в системі існує ще додатковий набір правил. Цей набір забезпечує додатковий захист для процедур перетворення.

Метод представлення даних - необхідний елемент даних, спонтанний елемент даних.

Мета моделювання – створення набору правил, згідно з якими програма буде надавати або не надавати права певним суб'єктам.

Інформаційні моделі

Дані моделі накладають *обмеження на інтерфейс програмних модулів* системи з метою досягнення безпечної реалізації. При цьому подробиці реалізації визначаються розробником системи. Дані моделі є результатом застосування теорії інформації до проблеми безпеки систем. До інформаційних моделей ставляться моделі невтручання й невиводимості . Достоїнствами даного типу моделей , на відміну від моделей надання прав , є:

- відсутність у них прихованих каналів витоку інформації ;
- природність їхнього використання для реалізації мережних захищених обчислювальних систем.

Теорія даних математичних моделей бурхливо розвивається в цей час.

Модель невтручання

Модель невтручання розглядає систему, що складається з чотирьох об'єктів: високе введення (high-in), низьке введення (low-in), високе виведення(high-out), низьке виведення (low-out).

Розглянемо систему, виведення якої користувачеві *u* визначене функцією out(u, hist.read(u)), де hist.read(u) - історія введення системи (traces), чиє останнє введення було read(u) (команда читання , виконана користувачем u). Для визначення безпеки системи необхідно визначити термін очищення *(purge*) історій уведення , де *purge* знищує команди , виконані користувачем, чий рівень безпеки не домінує над рівнем безпеки u. Функція clearence(u) - визначає ступінь довіри до користувача.

Система задовольняє вимозі невтручання , якщо для всіх користувачів u, всіх історій T і всіх команд виведення з out(u,T.c(u)) = out(u,purge(u,T).c(u)).

Для того, щоб перевірити, чи задовольняє система вимогам невтручання, була розроблена множина умов («unwinding conditions»), виконання яких досить для підтримки невтручання в моделі.

Метод представлення даних - списки команд

Мета моделювання – визначення рівня довіри

Модель невиводимості

Розглянемо модель невиводимості, що також базується на розгляді інформаційних потоків у системі.

Система вважається невиведено безпечною, якщо користувачі з низькими рівнями безпеки не можуть одержати інформацію з високим рівнем безпеки в результаті будь-яких дій користувачів з високим рівнем безпеки. Інакше кажучи, у таких системах витік інформації не може відбутися в результаті посилки високорівневими користувачами високорівневої інформації до низькорівневих користувачів. Інтуїтивно це визначення відноситься не до інформаційних потоків, а до поділу інформації. Однак таке визначення безпеки не захищає інформацію високорівневих користувачів від перегляду низькорівневими користувачами. Дане визначення вимагає, щоб низькорівневі користувачі не були здатні використати доступну їм інформацію для одержання високорівневої інформації (це пояснює, чому визначення назване невиводимістю).

Метод представлення даних є мітки доступу

Мета моделювання – запобігання перевищенню прав доступу

Висновки.

Розглянувши вищезазначені моделі можна зробити висновки, що кожна з них має свої як переваги так і недоліки. Модель Take-Grant служить для аналізу систем захисту з дискреційною політикою безпеки. У моделі визначені умови, при яких відбувається передача або викрадення прав доступу. Однак на практиці рідко виникає необхідність у використанні

зазначених умов, тому що при аналізі більшості реальних систем захисту не виникають настільки складні по взаємозв'язку об'єктів графи доступів. Модель Харрисона – Руззо – Ульмана використовується для аналізу системи захисту, що реалізує дискреційну політику безпеки, і її основного елемента - матриці доступів. Модель Белла-Лападула - формальна автоматна модель політики безпеки, що описує множину правил керування доступом. Отже всі ці моделі відрізняються одна від одної, а отже модель, яка підходить до однієї системи не може бути застосована до іншої. На основі проведеного аналізу можна визначити параметри, які критичні для певної автоматизованої системи.

1. *Девянин П.Н.* Модели безопасности компьютерных систем – М.: Издательский центр «Академия», 2005. – 144 с.
2. *Зегжда Д.П., Ивашко А.М.* Основы безопасности информационных систем. – М.: Горячая линия - телеком, 2000. – 452 с
3. *Корт С.С.* Теоретические основы защиты информации. – М. : Гелиос АРВ, 2004. - 240 с.
4. *Зегжда Д.П., Корт С.С., Каулио В.В.* Теоретические основы информационной безопасности. Руководство к практическим занятиям. - под редакцией проф. Зегжды П.Д. СПб.: СПбГТУ, 1998. 34 с.
5. *Давиденко А.Н.* Математическое моделирование систем и средств защиты критической информации // Збірник наукових праць Інституту проблем моделювання в енергетиці НАН України, Львів «Світ», 1998 Вип4 – с. 109-113.