отказом в обслуживании. Если защищаемая сеть имеет выход в Internet, цифровая подпись пакетов малоэффективна.

5. Межсетевые экраны (firewalls).

Межсетевые экраны фильтруют передаваемые через маршрутизатор пакеты, не пропуская через маршрутизатор потенциально опасные пакеты, которые, возможно, были отправлены в сеть в ходе атаки сети хакером.

III Заключение

1. Анализ, оценку, проектирование системы защиты информации, экспертизу защищенности необходимо проводить независимыми организациями, имеющими государственную лицензию на проведение указанных работ.

2. Архитектура системы должна быть построена таким образом, чтобы подключение к глобальной сети осуществлялось только в случае крайней необходимости.

3. Политика размещения данных должна проводиться из расчета их максимальной недоступности.

4. Осуществление аудита и проверок целостности ПО АБС должно быть систематическим. Желательно вести журнал аудита не только в электронном, но и бумажном виде.

5. Тестирование безопасности АБС специальными программами и анализ его результатов также должны быть регулярными мероприятиями.

Литература: 1. Максименко С., Осовецкий Л. Защита и беззащитность информации в банке. http://inf.susu.ac.ru/~tyrty/banky.html. 2. Проскурин В. Г. Проблемы безопасности: финансовая безопасность. Автоматизированная банковская система глазами хакера. http://infocity.kiev.ua/hack/title/bank.html. 3. SC-Банк: Руководство программиста. http://www.gis.minsk.by/softclub/doc/BANK_P/P1_1/ADMIN1.HTM.

УДК 681.06

ПІДХІД ДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ РОЗПОДІЛЕНИХ БАЗ ДАНИХ

Ігор Нетесін

Міжнародний науковий центр технології програмування ТЕХНОСОФТ НАН України і Держкомітету зв'язку та інформатизації України

Анотація: **Аналізуються сучасні моделі та засоби захисту секретної інформації в комп'ютерних базах даних. Пропонується формалізований підхід до забезпечення безпеки розподілених баз даних, що спирається на принципи взаємодії та захисту об'єктів у комп'ютерних мережах**.

Summary: **Modern models and means of the secret information protection in computer data bases are analyzed. A formalized approach to the safety of distributed data bases that is based on principles of interaction and protection of network objects is suggested.**

Ключові слова: **Захист інформації, бази даних, моделі безпеки.**

I Вступ

Захист комп'ютерних мереж (КМ) значною мірою залежить від організації в ній доступу до інформації, що містить у собі оброблені дані і різні відомості про факти, події, явища і стани об'єктів КМ. Інформація накопичується в базах даних (БД), словниках, репозиторіях, сховищах і опрацьовується користувачами (застосуваннями, процесами); вона може бути відкритою для одних користувачів і закритою для інших або бути доступною тільки для визначеної категорії користувачів із відповідними правами і повноваженнями.

Забезпечення безпеки інформації у мережі - це спроможність КМ захищати інформацію від випадкових або навмисних впливів, різного роду поломок і відмов у системі, що завдають шкоди інфраструктурі КМ. Питанням безпеки інформації почали приділяти увагу наприкінці 80-х років. У наш час з'явилися перші моделі захисту інформації для вищих органів влади і потужних комерційних структур.

Оскільки основна шкода інформації, як правило, завдається злочинними діями (вірусами, зломами секретних ключів, викраденням даних тощо), для боротьби з ними створюються різні механізми безпеки, що включають організаційні, технічні і програмні заходи і засоби захисту інформації [1–5].

Наріжним каменем у вирішенні проблем безпеки є спеціальний документ «Критерії оцінки надійності комп'ютерних систем» в «Оранжевій книзі» [1], який визначає стандартизований підхід до оцінки

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

комп'ютерної безпеки на основі чотирьох рівнів (класів): D, C, B, A. Рівні C і B у свою чергу задаються декількома підкласами: C1, C2 і B1, B2, B3.

Даний підхід слугував джерелом розвитку фундаментальних і прикладних досліджень у галузі безпеки різних систем, мереж і БД. Склалися загальні концепції і моделі безпеки інформації, напрямки забезпечення дозволених доступів. Серед них моделі істинності, розмежування доступу, передачі прав та ін. [1–3].

Основними аспектами моделей захисту інформації є: доступність (своєчасне забезпечення доступу до інформації користувачів з повноваженнями або привілеями), цілісність (правильність, неперекрученість інформації в будь-який час, захист її від невірних модифікацій і несанкціонованого доступу) і конфіденційність (заборона на ознайомлення з інформацією осіб, які не мають прав або повноважень) [6]. Всі три аспекти тісно стикаються, і достатньо часто для їх досягнення використовується один і той самий механізм.

У даній статті продовжуються дослідження, присвячені питанням безпеки і захисту розподілених комп'ютерних середовищ [7, 8], у напрямку забезпечення безпеки БД.

II Моделі безпеки БД

Основною концепцією безпеки БД є перевірка повноважень і істинності (автентифікації) користувачів інформації [4, 5]. Вона реалізується за допомогою найпростіших моделей повноважень і істинності та базової моделі розмежування доступу.

Модель повноважень. *Перевірка повноважень* базується на тому, що кожному користувачеві або процесу КМ ставиться у відповідність набір дозволених дій, виконуваних стосовно визначених об'єктів КМ. При цьому дотримується принцип конфіденційності інформації в БД, який для даної моделі полягає у введенні обмежень на коло користувачів з повноваженнями доступу до БД і у спроможності зберігати зазначену інформацію в таємниці від користувачів, які не мають таких повноважень. Практично обмеження доступності інформації для одних користувачів полягають у необхідності захисту законних інтересів інших користувачів КМ під час перевірки їхніх повноважень на доступ до БД.

В основу перевірки повноважень покладена модель, що являє собою прямокутну матрицю, яка встановлює відношення між усіма користувачами БД і об'єктами. У кожній клітині матриці зберігається список операцій, які користувач (процес) може виконувати стосовно необхідного об'єкта.

На рис. 1 наведений приклад такої матриці, де рядки пойменовані користувачами БД *(K1, K2, ... , K6)*, а стовпчики - об'єктами *(O1, O2, ..., O5)*, до яких звертаються користувачі при виконанні операцій: *с* – створення, *ч* – читання, *з* – запис, *м* - модифікація, *у* – усунення. Ці операції задаються у клітинах по одній або по декілька і вказують на можливість їх виконання при звертанні до об'єкта.

	O1	O2	O3	O4	O5
K1	с.ч.м.		с.ч.у.		
K2	с.ч.з.м.у.				ч.
K3				с.ч.	
K4		с.ч.м.			ч.з.у.
K5	ч.з.				с.ч.з.
K6			ч.м.		

Рисунок 1 – Приклад матриці перевірки повноважень

Система керування безпекою, заснована на перевірці повноважень при виконанні будь-якого звертання до БД, використовує цю матрицю для захисту інформації і дотримання певного рівня конфіденційності (неможливості несанкціонованого доступу до інформації) та доступності (можливості своєчасного отримання неперекрученої інформації). У цій моделі, проте, не враховується ситуація, коли деякий користувач (процес) K_i видає себе за іншого - K_j і виконує дозволені K_j дії без фактичної наявності відповідних повноважень.

Модель істинності. *Перевірка істинності* - це гарантоване підтвердження того, що користувач із даним ідентифікатором, який виконує санкціоновану дію, є саме тим, за кого він себе видає.

Модель істинності формалізовано подається як набір ідентифікаторів (імен) у списку контролю доступу, заявлених користувачами для їхнього підтвердження при звертанні до БД.

Ідентифікація полягає у присвоєнні користувачам ідентифікаторів, атрибутів доступу (привілеїв, прав, повноважень, дозволів) і їхній перевірці (автентифікації) за списком контролю доступу і заданими атрибутами.

Права доступу до інформації аналогічні привілеям доступу і включають ідентифікацію користувачів і види їхнього доступу до інформації (створення, читання, запис і т.п.) із указівкою паролів (секретної інформації, що відома користувачу і системі забезпечення безпеки). На їхній основі здійснюється автентифікація користувача, який звертається до БД. При цьому під *безпекою системи автентифікації* мається на увазі ступінь забезпечення гарантій того, що зловмисник неспроможний пройти автентифікацію від імені іншого користувача й одержати недозволений для нього вид доступу до інформації.

На даний час широко застосовуються три групи методів автентифікації.

До першої відносяться методи, що використовують посвідчення, перепустки, магнітні картки тощо, широко застосовувані у програмно-апаратних засобах захисту.

У другу входять методи, засновані на паролях. Сукупність ідентифікатора користувача і його пароля утворює обліковий запис користувача, за допомогою якого здійснюється парольний захист того, хто звертається до даних.

Третю групу складають методи, що грунтуються на застосуванні устаткування для виміру і порівняння індивідуальних характеристик користувача з еталоном за голосом, райдужною оболонкою ока, відбитками пальців і т. п. Ці засоби мають високу точність автентифікації володаря біометричної ознаки, підробити котру практично не можна. Поки що вони дорогі і їхнє застосування обмежене.

Процедура автентифікації за участю двох сторін – користувача і особи, яка перевіряє, – називається безпосередньою автентифікацією. Якщо беруть участь ще й довірені особи, то автентифікацію називають сервером автентифікації або арбітром [1–3].

Механізми перевірки повноважень і істинності не можуть повністю захистити від крадіжки ідентифікаторів і паролів, а також від злочинних дій користувачів. Так, наприклад, розробник системи може вбудувати «троянського коня» у код деякої програми і пізніше здійснити зловмисні дії з метою викрадання або руйнації інформації. Для захисту системи від такого роду дій підсистема безпеки має, крім відповідних програмно-технічних заходів, забезпечити захист даних шляхом проведення прихованих перевірок, аудиту тощо.

Багаторівнева модель безпеки. Система безпеки БД, побудована на моделях перевірки повноважень і істинності, надає санкціонований доступ користувачам до закритої інформації БД за заздалегідь визначеними повноваженнями. Проте для захисту цього не достатньо, оскільки такі моделі не мають класів секретності, а в БД, як правило, зберігається інформація від відкритої до цілком таємної. Для таких цілей призначена багаторівнева модель безпеки Белла-ЛаПадула (Bell-LaPadula), яку ще називають "моделлю вищого рівня секретності" [1, 2], котра надає користувачам доступ до секретних даних БД за різними класами секретності і є класичною моделлю повноважного (мандатного) розмежування доступу до даних.

В моделі Белла-ЛаПадула використовуються такі поняття, як рівень секретності, заданий і поточні рівні допуску користувача, рівень ієрархії об'єктів, інші. Безпека системи забезпечується шляхом розмежування доступу користувачів і одержання ними дозволу на доступ до інформації залежно від того, чи володіють вони однією з наступних властивостей безпеки:

– властивість простого захисту;

– так звана властивість «зірочка»;

– властивість дискретного захисту.

Перша властивість означає, що користувач найвищого рівня має доступ до всіх рівнів секретності, які містяться нижче, за умови, що існує відповідність між рівнем доступу користувача і рівнем секретності об'єкта, до якого він звертається.

Властивість «зірочка» означає, що користувач має право на запис в об'єкт за умови, якщо його клас доступу збігається з класом доступу об'єкта, у який здійснюється запис. Дана властивість виключає появу в системі каналу витоку інформації і припускає дотримання повноважень при доступі до інформації.

Властивість дискретного захисту означає, що користувач має право доступу до інформації, похідної від раніше доступної інформації, за умови збігання поточного ідентифікатора користувача з ідентифікатором у списку контролю доступу.

Таким чином, виходячи з цих властивостей захист інформації забезпечується за допомогою контролю дозволів на доступ до цієї інформації і перевірки таких умов, як відповідність поточного рівня допуску користувача рівню секретності об'єкта, заборона на читання вгору по ієрархії об'єктів або заборона на модифікацію, якщо рівень допуску користувача нижче рівня секретності, тощо.

Багаторівневий захист БД, побудований на трьох наведених вище властивостях, визначає керування процесами, що запитують доступ до інформації й об'єктів (файлів, записів, полів і ін.). Усі об'єкти класифікуються за ієрархічною ознакою, а користувачі одержують клас доступу, що складається з двох компонентів. Перший визначає положення класу в ієрархії, а другий - множину елементів на рівні ієрархії. До першого компонента військове відомство США, наприклад, віднесло таку ієрархію класів допуску

(зверху вниз) [1, 2]:

– цілком секретно (клас A);

– секретно (клас B);

– конфіденційно (клас C);

– несекретно (клас D).

Другий компонент задає категорію об'єкта не ієрархічного типу для використання у зазначених класах доступу, наприклад:

– ядерна зброя;

– недоступність до інформації іноземних громадян;

– заборона на доступ для контрактних службовців і т. п.

Співвідношення між ієрархічними і не ієрархічними компонентами встановлюється за допомогою матриці, яка визначає взаємодію користувачів та об'єктів і дозволяє проводити автоматичне приписування не ієрархічних компонентів в усі більш високі рівні класів, створюючи так зване "обернене спадкування" даних. Згідно з властивістю простого захисту моделі Белла-ЛаПадула, користувачі, які мають відповідні права, можуть одержати доступ до класів інформації униз по ієрархії класів: цілком секретно, секретно, конфіденційно, несекретно.

Таким чином, модель Белла-ЛаПадула орієнтована на розмежування доступу в системах з багаторівневим захистом і може бути використана для контролю звертання до об'єктів БД користувачів різних рівнів допуску.

III Системні засоби захисту БД

У дволанковій архітектурі «клієнт - сервер» прикладна частина виконується клієнтом (на робочій станції, вузлі мережі і т. п.), а сервер здійснює доступ до БД. У випадку складності і ємності прикладної обробки у цю архітектуру додається сервер застосувань, що бере на себе основну логіку опрацювання інформації і доступу до БД. При цьому БД може бути централізованою (один сервер) або розподіленою (декілька серверів). У розподіленій БД основною умовою збереження даних є автономність і відсутність прямих і транзитивних зв'язків між таблицями, що розташовані у віддалених розділах БД. Оскільки ця умова обмежує цілісність даних, то до складу серверу включаються збережені процедури, за допомогою яких встановлюються посилання на інші розділи БД.

Як правило, захист БД здійснює спеціальний сервер. До його функцій входить забезпечення парольного захисту, шифрування, установлення прав доступу до об'єктів БД, захист полів і записів таблиць тощо.

Паролі встановлюються кінцевими користувачами або адміністраторами БД, зберігаються у захищеному вигляді у спеціальних файлах і використовуються сервером під час доступу користувачів до БД.

Шифрування здійснюється за допомогою ключів фіксованої і нефіксованої довжини для засекречування збереженої в БД інформації або при передачі інформації мережею від відправника до одержувача й навпаки.

Встановлення прав доступу до БД полягає у реєстрації користувачів для захисту від несанкціонованого доступу. До прав доступу відносяться: читання, модифікація, додавання, вилучення, зміна структур таблиць і т. ін. За допомогою дозволених для кожного користувача прав здійснюється контроль їх доступу до об'єктів БД і приймаються заходи для захисту окремих рядків, стовпчиків, полів або БД у цілому.

До основних заходів щодо проведення захисту даних БД відносяться:

– режимні, що включають парольну, криптографічну перевірки користувачів тощо;

– технологічні, що містять резервне копіювання даних, правильне їхнє збереження, експлуатацію й ін.;

– системні, з процедурами автоматизованої перевірки повноважень і істинності користувачів, які запитують доступ до даних, їх привілеїв, аудиту подій, що відбуваються, тощо.

Режимні і технологічні заходи підтримуються методичними матеріалами і стандартами, що регламентують дії групи осіб, відповідальних за безпеку БД. Системні – утворюють сервіс безпеки, що включає сервер БД із функціями захисту.

Особливістю розподілених БД (РБД) є розміщення окремих розділів даних на різних вузлах мережі, інформація про розташування яких відображається в глобальному словнику даних і використовується при доступі до РБД різних користувачів.

Для забезпечення безпеки розподілених, багаторівневих і інших БД до складу серверу БД включаються збережені процедури перевірки прав і повноважень користувачів, визначені моделями захисту, засобами контролю доступу, реалізованими у сервісі безпеки БД. На рис. 2. наведено приклад архітектури розподіленої системи керування базой даних (СКБД) із захистом інформації.

Користувачі *1, 2, ..., N* звертаються до даних через сервіс безпеки, що контролює доступ і виконує тільки дозволені операції над БД, у яких утримуються окремо цілком секретні, секретні і несекретні дані. У запитах

на доступ до цілком секретних, секретних та конфіденційних даних указуються права і/або повноваження користувача, що перевіряються сервісом безпеки за списком контролю доступу і таблицею повноважень.

Для роботи із секретною інформацією в БД можуть бути наведені багатозначні відношення у вигляді множини кортежів з тим же самим значенням первинного ключа.

Прикладом такого відображення можуть служити дані про співробітників військового закладу, для яких під однаковим прізвищем зазначені, поряд із їхніми реальними званнями і видами діяльності, також фальшиві дані для їхнього прикриття. БД із такими даними потребують багаторівневого захисту, або використання механізмів маскування даних порожніми значеннями.

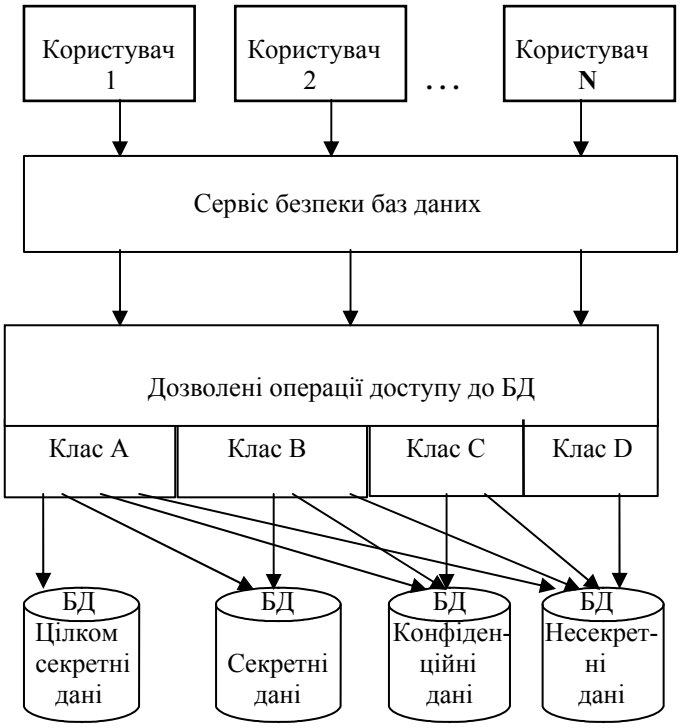

Рисунок 2 – Приклад архітектури розподіленої СКБД із захистом інформації

При модифікації порожніх значень багаторівневий захист СКБД може видати відмову в доступі, якщо у користувача (або процесу) відсутні повноваження на проведення модифікацій у шуканому кортежі даних. Модифікація звичайно проводиться за допомогою непрямого каналу, що являє собою механізм, завдяки якому користувач, котрий володіє високим рівнем повноважень і прав, може надати інформацію користувачеві з меншими правами і повноваженнями [3].

Багаторівневий захист даних може проводитися за допомогою мандатного керування доступом, що грунтується на властивостях моделі Белла-ЛаПадула для похідних базових відношень і SQL-подання. Сучасна мова SQL містить оператори захисту даних: *grant і revoke*. Оператор *grant* дає можливість надавати привілеї для доступу і модифікації об'єктів, а також передавати іншим користувачам права на привілеї (за допомогою конструкції *with grant option*). Оператор *revoke* дозволяє відбирати права, що надані раніше деякому користувачу. Багато SQL-орієнтованих СКБД мають власні засоби безпеки БД, реалізовані на засобах захисту даних мовою SQL.

Для забезпечення безпеки неоднорідних систем мультибаз застосовуються потужні засоби багаторівневого захисту даних, захищені бази даних і інформаційні менеджери, які управляють захистом даних. Користувач, котрий має певні повноваження, одержує доступ до мультибаз тільки в тому випадку, коли у запиті зазначений відповідний параметр автентифікації. СКБД із багаторівневим захистом звичайно розширюються мовними засобами DDL (Definition Data Language), які призначені для специфікації класів безпеки стосовно мультирівневої мови SQL.

Ступінь безпеки в об'єктно-орієнтованих БД нижче, ніж у розвинених реляційних СКБД. Принципи багаторівневого захисту, розроблені для реляційних баз даних, такі, як багатозначність і модель Белла-ЛаПадула, одержали розвиток в об'єктно-орієнтованій системі SODA (Secure Object-oriented Database). У ній

модель Белла-ЛаПадула об’єднана зі стратегією присвоювання міток безпеки двох видів: об'єктів і змінних об'єктів.

У першому випадку класифікація об'єктів здійснюється шляхом визначення одного загального класу для всього кортежу або для одного його об'єкта.

У другому випадку кожному змінному об'єкту присвоюється незалежна мітка, що відповідає діапазону класифікації об'єктів на рівні елементів кортежів, при котрому кожний стовпчик відношення має власний припустимий діапазон класифікації, а елемент кортежу – індивідуальну класифікацію, незалежну від інших елементів.

За допомогою таких міток класифікуються складові або нескладові об'єкти об'єктно-орієнтованих БД і створюється набір правил для керування рівнями захисту класів об'єктів і відношень між об'єктами.

IV Формалізований підхід до захисту розподілених БД

Розглянуті моделі безпеки орієнтовані на підтримку декількох рівнів захисту і стосуються здебільше БД із реляційною архітектурою. Ефективність моделей істотно підвищується, якщо додатково застосовується шифрування інформації. Проте кожна з розглянутих і будь-яка інша відома модель не надають повного захисту інформації.

У зв'язку з бурхливим розвитком комп'ютерних мереж, електронної комерції й електронного бізнесу з використанням Інтернет усе більшу актуальність набуває проблема забезпечення безпеки РБД і серверів БД. Використовуючи об'єктно-орієнтований підхід будь-яку розподілену БД, що взаємодіє з користувачами, можна розглядати як мережну структуру, для котрої застосовуються розроблені для мережних середовищ методи забезпечення безпеки і захисту інформації.

Сумісний розгляд моделей, методів і засобів взаємодії та забезпечення безпеки об'єктів КМ [7–9] з вищевикладеними моделями захисту інформації дозволяє по-новому глянути на питання безпеки інформації в середовищі РБД.

Запропонована в [9] модель взаємодії (МВ) об'єктів комп'ютерної мережі, що застосована до РБД, дозволяє описати модель безпечної роботи РБД у наступному вигляді:

$$МВ\ (РБД) = \{\{БД_i\}, \{I_i\}, \{K_j\}, \{ОД_{ji}\}, M_{РБД}\},$$

де $РБД = \bigcup_i БД_i$, $БД_i$ – незалежна локальна компонента РБД з номером i;

$I_i \subset БД_i$, I_i – інформація, що зберігається в $БД_i$;

$I_i = \bigcup_{n \in |I_i|} I_{i_n}$, I_{i_n} – інформаційні об'єкти $БД_i$; $|I_i|$ - потужність (кількість) об'єктів у I_i;

K_j – користувач даної РБД з номером j;

$ОД_{ji} = \bigcup_{n \in |I_i|} ОД_{ji_n}$, $ОД_{ji_n}$ – операція доступу користувача K_j до об'єкта I_{i_n};

Доступ користувача K_j до об'єкта I_{i_n} виражається співвідношенням

$$K_j(ОД_{ji_n}) = I_{i_n}.$$

Модель безпеки [8], що застосована до РБД, приймає вигляд

$$M_{РБД} = \{M_З, УГР, I_З\},$$

де $M_З$ – модель захисту сервісу безпеки РБД;

УГР – сукупність зовнішніх і внутрішніх навмисних і ненавмисних погроз;

$I_З$ – захищені інформаційні ресурси РБД.

У свою чергу $M_З = \{M_{КМ}, M_{ЗІ}\}$, де $M_{КМ}$ – модель захисту комп'ютерної мережі, у якій функціонує дана РБД. $M_{КМ}$ базується на механізмах авторизації, автентифікації, парольного і рольового захисту, обмеження і контролю доступу, блокування послуг, аудиту й ін. [8]; $M_{ЗІ}$ – це моделі захисту інформації, засновані на поняттях повноважень, істинності, розмежування доступу, передачі прав тощо, розглянутих вище.

У термінах запропонованого формалізму умова безпечної роботи РБД записується у вигляді

$$K_j(ОД_{ji_n}) = \begin{cases} I_{i_n}, & якщо \quad ОД_{ji_n} \in M_З, \\ \varnothing, & якщо \quad ОД_{ji_n} \notin M_З \end{cases}$$

для усіх $I_{i_n} \subset I_З$.

V Висновки

Проаналізовані найчастіше використовувані у практиці і теоретично обґрунтовані моделі захисту інформації в комп'ютерних системах. Розглянуто особливості реалізованих засобів захисту даних у середовищі реляційних, розподілених, об'єктно-орієнтованих СКБД.

Подано формалізований підхід до забезпечення безпеки розподілених баз даних, заснований на інтеграції моделей і засобів взаємодії і безпеки об'єктів у комп'ютерних мережах із моделями захисту інформації. Даний підхід у сполученні з організаційними, режимними і системними засобами безпеки КМ забезпечує не тільки високий рівень захисту даних, але й достатній рівень захисту РБД від багатьох загроз, що виникають у КМ.

Література: 1. Russel D., Gangemi G. T. Sr. Computer Security Basics. – N. Y.: O`Reilly & Associates, Inc., 1992. 2. National Computer Security Center. Trusted Network Interpretation // NCSC-TG-005, 1987. 3. Castano S., Fugini M., Martella G., Samarati P. Database Security. – Addison-Wesley, 1995. – 407 p. 4. Мельников Г. В. Защита информации в компьютерных системах. - М.: Финансы и статистика, 1997. – 368 с. 5. Герасименко В. А. Защита информации в автоматизированных системах обработки данных: В 2-х т. – М.: Энергоатомиздат, 1994. 6. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу // НД ТЗІ 1.1–002–99, ДСТСЗІ СБ України, Київ, 1999. 7. Нетесин И. Е. Вопросы безопасности и пути их решения в современных компьютерных сетях // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. – Київ: НТУУ «КПІ» . – 2000. – С. 199 – 203. – (Труди конф. «Безпека інформації в інформаційно–телекомунікаційних системах», Київ, 11 – 14 квітня 2000 р.) 8. Нетесин И. Е. Модели безопасности и защиты в распределённых компьютерных средах / / Проблемы программирования. –2000. – № 3–4. – С. 148–158. 9. Нетесин И. Е. Определение основ взаимодействия объектов в компьютерных сетях // Проблемы программирования.–2000.–№1–2.– С. 191–203.- (Спец. вып. "Материалы Второй Междунар. науч.-практ. конф. по программированию УкПРОГ'2000", Киев, 23-26 мая 2000 г.).

УДК 681.513

МОДЕЛИРОВАНИЕ ПОВЕДЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ С ТОЧКИ ЗРЕНИЯ БЕЗОПАСНОСТИ

Алексей Новиков, Сергей Кащенко

Физико-технический институт НТУУ «КПИ»

Анотація: **Детектори вторгнень продемонстрували на практиці свою високу ефективність у посиленні безпеки розподілених комп'ютерних систем. Існує два підходи до виявлення атак – заснований на поведінці та заснований на знаннях. Більш широкого розповсюдження набули системи, що використовують другий підхід. Це пояснюється недостатньою пропрацьованністю теоретичних й практичних аспектів першого. У статті пропонується модель поведінки програмного забезпечення з точки зору безпеки у вигляді стохастичного автомату та аналізується застосовність моделі.**

Summary: **Intrusion detection systems have demonstrated on practice their high efficiency in strengthening of distributed computer system security. There are two approaches to attack detection – behaviour-based and knowledge-based. More widespread are systems based on latter one. It can be explained by insufficient development of theoretical and practical aspects of former one. Model of software behaviour based on stochastic automaton is proposed and its applicability is analysed in the article.**

Ключевые слова: **Безопасность, системы обнаружения атак, стохастический автомат.**

I Введение

Развитие Internet и intranet-сетей создало необходимость дополнения традиционных средств обеспечения безопасности компьютерных систем (КС), таких как средства контроля доступа операционных систем и средства защиты периметра распределенных КС (межсетевые экраны), средствами мониторинга безопасности. Как правило, в роли таких средств выступают системы обнаружения атак (СОА). Рост доли инцидентов, выявленных при помощи СОА, а также рост рынка коммерческих систем свидетельствуют о высокой эффективности и признании роли средств мониторинга в задаче обеспечения безопасности распределенных КС [1].

СОА осуществляют сбор информации о связанных с безопасностью событиях в КС, преобразование (сжатие) этой информации в удобную для анализа форму, анализ или собственно выявление признаков атаки,