УДК 519.676:681.51

БЛАВАЦЬКА Наталія Миколаївна

АНАЛІЗ ВІДПОВІДНОСТІ ЗАСОБІВ ЗАХИСТУ СУЧАСНИХ ОПЕРАЦІЙНИХ СИСТЕМ ВИМОГАМ ДО ОБРОБЛЕННЯ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

Постановка проблеми. Операційна система є спеціально організованою сукупністю програм, яка управляє ресурсами системи (електронно-обчислювальної машини (ЕОМ), обчислювальної системи, інших компонентів інформаційно-обчислювальної мережі) з метою найбільш ефективного їх використання і забезпечує інтерфейс користувача з ресурсами.

Операційні системи, подібно апаратурі ЕОМ, на шляху свого розвитку пройшли кілька поколінь.

Операційні системи першого покоління були спрямовані на прискорення та спрощення переходу із одного завдання користувача на інше (іншого користувача), що поставило на порядок денний проблему забезпечення безпеки даних, що належать різним завданням.

Друге покоління операційних систем характеризувалося нарощуванням програмних засобів забезпечення операцій уведення-виведення і стандартизацією оброблення переривань. Надійне забезпечення безпеки даних у цілому залишилося невирішеною проблемою.

У кінці 60-х рр. XX ст. почав здійснюватися перехід до мультипроцесорної організації засобів обчислювальної техніки, тому проблеми розподілу ресурсів та їх захисту стали більш гострими і важко вирішуваними. Їх розв'язання привело до відповідної організації ОС і широкого застосування апаратних засобів захисту (захист пам'яті, апаратний контроль, діагностика тощо).

Основною тенденцією розвитку обчислювальної техніки була і залишається ідея максимальної доступності її для користувачів, що суперечить вимозі забезпечення безпеки даних.

Більшість операційних систем має дефекти у забезпеченні безпеки даних у системі, що зумовлено виконанням завдання забезпечення максимальної доступності системи для користувача.

Ступінь захищеності комп'ютера багато в чому залежить від досконалості його операційної системи. Операційна система (ОС) є найважливішим програмним компонентом будь-якої обчислювальної машини, тому від рівня реалізації політики безпеки в кожній конкретній операційній системі багато в чому залежить і загальна безпека інформаційної системи [1].

Аналіз останніх досліджень і публікацій. Розробленням питань захисту інформації, зокрема реалізації механізмів захисту сучасних операційних систем, займаються зарубіжні науковці В.Г.Проскурин, С.В.Крутов, І.В.Мацкевич [2], П.Б.Хорев [3], О.В.Казарін [4], проте стрімкий розвиток інформаційних технологій у сфері створення нових операційних систем безупинно дає матеріал для наукових досліджень.

Мета статті полягає у визначенні відповідності засобів захисту сучасних ОС класу

автоматизованих систем, на яких обробляється конфіденційна інформація.

Виклад основного матеріалу. Спочатку зупинимося на принциповій, навіть концептуальній, суперечності між реалізованими в ОС механізмами захисту й прийнятими формалізованими вимогами.

Суперечність полягає в принциповому розходженні підходів до побудови схеми адміністрування механізмів захисту, що докорінно позначається на формуванні загальних принципів реалізації політики безпеки, розподіленні відповідальності за захист інформації, а також на визначенні потенційних зловмисників (від кого захищати інформацію).

Для демонстрації цього із сукупності формалізованих вимог до системи захисту конфіденційної інформації розглянемо такі:

– право змінювати правила розмежування доступу повинне надаватися виділеним суб'єктам (адміністрації, службі безпеки тощо);

– повинні бути передбачені засоби управління, що обмежують поширення прав на доступ [5].

Ці вимоги жорстко регламентують схему (або модель) адміністрування механізмів захисту. Це повинна бути централізована схема, єдиним елементом якої виступає виділений суб'єкт, зокрема адміністратор. При цьому кінцевий користувач виключений у принципі зі схеми адміністрування механізмів захисту.

При реалізації концепції побудови системи захисту, регламентованої розглянутими вимогами, користувач не наділяється елементом довіри, оскільки він може уважатися потенційним зловмисником, що і відбувається на практиці.

Розглянемо концепцію, реалізовану в сучасних універсальних ОС. Тут "власником" файлового об'єкта, тобто особою, яка одержує право на завдання атрибутів доступу до файлового об'єкта, є особа, котра створює файловий об'єкт. Оскільки файлові об'єкти створюють кінцеві користувачі, вони й призначають атрибути доступу до створюваних ними файлових об'єктів. Інакше кажучи, в ОС реалізується розподілена схема призначення атрибутів доступу, де елементами схеми адміністрування є власне кінцеві користувачі [6].

У цій схемі користувач повинен наділятися практично такою ж довірою, як і адміністратор безпеки, при цьому нести поряд із ним відповідальність за забезпечення комп'ютерної безпеки.

Зазначимо, що централізована й розподілена схеми адміністрування – це дві діаметрально протилежні точки зору на захист, що вимагають різних підходів до побудови моделей і механізмів захисту. При цьому скільки-небудь гарантований захист інформації можна реалізувати тільки при прийнятті концепції повністю централізованої схеми адміністрування, що підтверджується відомими загрозами ОС.

Можливості моделей, методів і засобів захисту розглядатимемо стосовно реалізації саме концепції централізованого адміністрування, одним із елементів якої є розгляд користувача як потенційного зловмисника, здатного здійснити НСД до інформації, що захищається.

Захист ОС сімейства Unix і Windows (NT/2000/XP) у загальному випадку базується на трьох основних механізмах:

– ідентифікація й аутентифікація користувача при вході у систему;

– розмежування прав доступу до файлової системи, в основі якого лежить реалізація дискреційної моделі доступу;

– аудит, тобто реєстрація подій.

Принципові недоліки захисних механізмів ОС сімейства Unix. Передусім в ОС сімейства Unix, унаслідок реалізованої в ній концепції адміністрування (нецентралізована), неможливо забезпечити замкнутість (або цілісність) програмного середовища. Це пов'язано з неможливістю установки атрибута "виконання" на каталог. Тому при розмежуванні адміністратором доступу користувачів до каталогів користувач як "власник" створюваного ним файла може занести у свій каталог виконуваний файл і установити на файл атрибут "виконання", після чого запустити записану ним програму. Ця проблема безпосередньо пов'язана з реалізованою в ОС концепцією захисту інформації.

Не в повному обсязі реалізується дискреційна модель доступу, зокрема не можуть розмежовуватися права доступу для користувача "root". Відповідно, всі процеси, що запускаються ним, мають необмежений доступ до захищених ресурсів.

Крім того, в ОС сімейства Unix неможливо вбудованими засобами гарантовано видаляти залишкову інформацію. Для цього у системі абсолютно відсутні відповідні механізми.

Що стосується реєстрації, то в ОС сімейства Unix не забезпечуються реєстрація видачі документів на "тверду копію", а також деякі інші вимоги до реєстрації подій.

Вбудованими засобами захисту деяких ОС сімейства Unix керування доступом до вузлів локальної обчислювальної мережі не реалізується.

Тепер коротко зупинимося на основних механізмах захисту, реалізованих в ОС сімейства Windows, і проведемо аналіз захищеності ОС сімейства Windows (NT/2000).

На відміну від сімейства ОС Unix, де всі завдання розмежувальної політики доступу до ресурсів вирішуються засобами управління доступом до об'єктів файлової системи, доступ у даних ОС розмежовується власним механізмом для кожного ресурсу.

Тут явно виділяються (у кращий бік) можливості розмежувань прав доступу до файлових об'єктів (для NTFS) – істотно розширені атрибути доступу, які установлюються на різні ієрархічні об'єкти файлової системи (логічні диски, каталоги, файли). Зокрема, атрибут "виконання" може установлюватися й на каталог, тоді він успадковується відповідними файлами.

При цьому істотно обмежені можливості керування доступом до інших ресурсів, які захищаються, зокрема до пристроїв уведення (неможливо заборонити запуск несанкціонованої програми з дисководів).

Принципові недоліки захисних механізмів ОС сімейства Windows (NT/2000/XP). У межах концепції реалізації розмежувальної політики доступу до ресурсів (для NTFS) розмежування для файла більш приорітетне, ніж для каталогу, а в загальному випадку – розмежування для файлового об'єкта, який включається, приорітетніше, ніж для того, що включає. Тому користувач, створюючи файл і будучи його "власником", може призначити будь-які атрибути доступу до такого файла (тобто дозволити до нього доступ будь-якому іншому користувачеві). Звернутися до цього файла може користувач незалежно від установлених адміністратором атрибутів доступу на каталог, у якому користувач створює файл. Така проблема безпосередньо пов'язана з реалізованою в ОС Windows концепцією захисту інформації.

В ОС сімейства Windows (NT/2000/XP) також не у повному обсязі реалізується дискреційна модель доступу, зокрема не можуть розмежовуватися права доступу для користувача "Система". В ОС присутні не тільки користувацькі, але й системні процеси, які запускаються безпосередньо системою. При цьому доступ системних процесів не може бути розмежований. Відповідно, всі системні процеси, що запускаються, мають необмежений доступ до захищених ресурсів.

В ОС сімейства Windows (NT/2000/XP) неможливо в загальному випадку забезпечити замкнутість (або цілісність) програмного середовища; вбудованими засобами гарантовано видаляти залишкову інформацію. У системі просто відсутні відповідні механізми.

Крім того, ОС сімейства Windows (NT/2000/XP) не володіють у повному обсязі можливістю контролю цілісності файлової системи. Вбудовані механізми системи дозволяють контролювати тільки власні системні файли, не забезпечуючи контроль цілісності файлів користувача. Крім того, вони не вирішують найважливіше завдання цих механізмів – контроль цілісності програм перед їхнім запуском, контроль файлів даних користувача та ін.

Що стосується реєстрації, то в ОС сімейства Windows (NT/2000/XP) не забезпечується реєстрація видачі документів на "тверду копію", а також деякі інші вимоги до реєстрації подій.

Механізм управління доступу до вузлів локальної обчислювальної мережі у повному обсязі також не реалізується.

Щодо розподілених мережевих ресурсів, то фільтрації піддається тільки вхідний

доступ до розподіленого ресурсу, а запит доступу на комп'ютері, з якого він здійснюється, фільтрації не підлягає.

Отже, багато механізмів, необхідних із погляду виконання формалізованих вимог, ОС сімейства Windows не реалізовані в принципі або реалізовані лише частково.

Крім цього, наявна велика статистика загроз ОС, спрямованих на подолання вбудованих в ОС механізмів захисту, що дають змогу змінити налаштування механізмів безпеки, обійти розмежування доступу тощо. Таким чином, статистика фактів несанкціонованого доступу до інформації свідчить, що більшість поширених систем (універсального призначення) досить уразливі із погляду безпеки. І це попри виразну тенденцію до підвищення рівня їх захищеності.

Тут необхідно зазначити, що на практиці сучасні інформаційні системи, призначені для оброблення конфіденційної інформації, будуються уже з урахуванням додаткових заходів безпеки, що також побічно підтверджує початкову уразливість сучасних ОС.

Розглянемо операційні системи сімейства ОС: Unix і MS Windows.

Загальна кількість відомих успішних атак для різних груп ОС (за даними RootShell, Rhino9, SecurityFocus) представлена у табл. 1, а їх відсоткове співвідношення – на діаграмі рис. 1.

Таблиця 1

Загальна кількість успішних атак для різних груп ОС

Тип ОС	Кількість атак
MS Windows	230
Unix	660

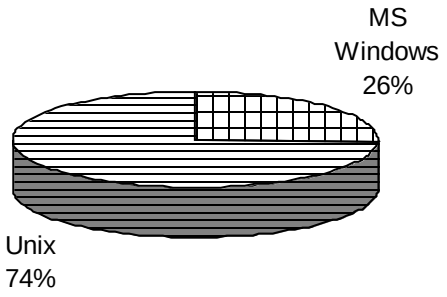

Рис. 1. Статистика співвідношення загроз для родин ОС

Аналізуючи зазначені атаки, всі методи, що дозволяють несанкціоновано втрутитися у роботу системи, можна розподілити на такі групи:

– дозволяють несанкціоновано запустити виконуваний код;

– дають змогу здійснити несанкціоновані операції читання/запису файлових або інших об'єктів;

– дозволяють обійти установлені розмежування прав доступу;

– призводять до відмови (Denial of Service) в обслуговуванні (системний збій);

– використовують вбудовані недокументовані можливості (помилки й закладки);

– використовують недоліки системи зберігання або вибору (недостатня довжина) даних про аутентифікації (паролі) й дозволяють шляхом реверсування, підбору або

повного перебору всіх варіантів отримати ці дані;

– троянські програми;

– інші.

У контексті цієї класифікації атаки можна надати в таких співвідношеннях: для ОС сімейства Windows – на діаграмі рис. 2, для ОС сімейства UNIX – на діаграмі рис. 3.

З огляду на зазначене загрози, описані в більшості груп, безпосередньо використовують різні недоліки ОС і системних додатків і дозволяють при повністю сконфігурованих і працюючих вбудованих в ОС механізмах захисту здійснювати несанкціонований доступ, що підтверджує необхідність посилення вбудованих механізмів захисту.

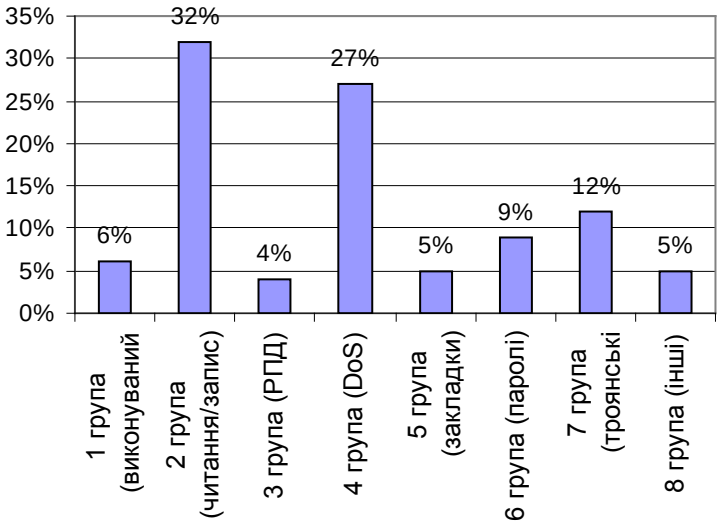

Рис. 2. Співвідношення груп атак для ОС сімейства Windows

Аналізуючи представлену статистику загроз, можна дійти висновку, що більша їх частина пов'язана саме з недоліками засобів захисту ОС, зазначеними вище, тобто із невиконанням (повним або частковим) формалізованих вимог до захисту, серед яких можуть бути виокремленні:

– некоректна реалізація механізму управління доступом, насамперед, при розмежуванні доступу до захищених об'єктів системних процесів і користувачів, які мають права адміністратора;

– відсутність забезпечення замкнутості (цілісності) програмного середовища.

Як видно, більшість атак здійснювалося з використанням або деяких прикладних програм, або вбудованих у віртуальні машини засобів програмування, тобто ймовірність більшості атак безпосередньо пов'язана з можливістю запуску зловмисником відповідної програми. При цьому запуск може бути здійснено як явно, так і приховано, у межах можливостей вбудованих у додатки інтерпретаторів команд.

Проведений аналіз відомих загроз сучасним універсальним ОС повністю підтверджує, що більша їх частина зумовлена саме реалізованим в ОС концептуальним підходом, що полягає у реалізації схеми розподіленого адміністрування механізмів захисту. У межах цієї схеми користувач розглядається як довірена особа, яка є елементом схеми адміністрування і має можливість призначати/змінювати правила розмежування доступу. При цьому він не сприймається як потенційний зловмисник, який може свідомо чи несвідомо здійснити несанкціонований доступ до інформації, отже, призначення механізмів додаткової захисту ОС полягає в реалізації централізованої схеми адміністрування механізмів захисту, у межах якої буде здійснюватися протидія несанкціонованому доступу користувача до інформації.

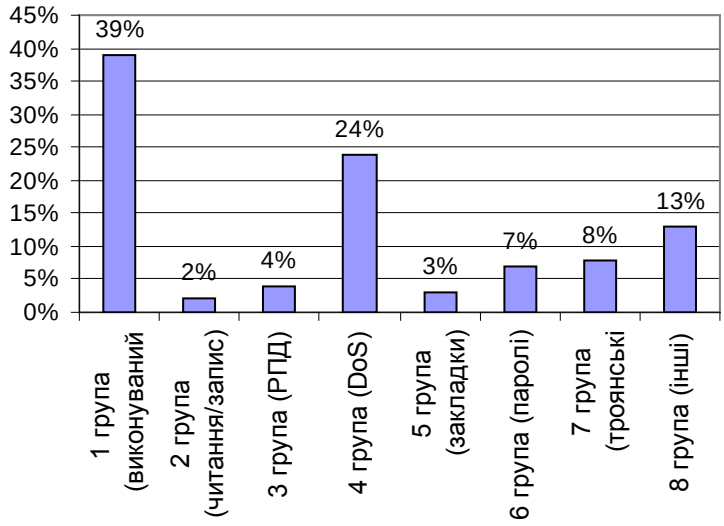

Рис. 3. Співвідношення груп атак для ОС сімейства UNIX

Висновки. З урахуванням зазначеного більшість сучасних універсальних ОС не виконують у повному обсязі вимоги до захисту автоматизованих систем для оброблення конфіденційної інформації. Тому, вони не можуть без використання додаткових засобів захисту застосовуватися для захисту навіть конфіденційної інформації. Утім, основні проблеми захисту тут викликані не тим, що не виконані окремі вимоги до механізмів захисту в ОС, а недосконалістю реалізованої в ОС концепції захисту, розроблення якої потребує подальшого наукового дослідження.

Список використаних джерел

1. Безбогов А.А. Безопасность операционных систем / А.А.Безбогов, А.В.Яковлев, Ю.Ф.Мартемьянов. – М. : Изд-во “Машиностроение-1”, 2007. – 220 с.

2. Проскурин В.Г. Защита в операционных системах / В.Г.Проскурин, С.В.Крутов, И.В.Мацкевич. – М. : Радио и связь, 2000. – 168 с.

3. Хореев П.Б. Методы и средства защиты информации в компьютерных системах / П.Б.Хорев. – М. : Академия, 2005. – 256 с.

4. Казарин О.В. Безопасность программного обеспечения компьютерных систем / О.В.Казарин. – М. : МГУЛ, 2003. – 212 с.

5. Галатенко В.А. Основы информационной безопасности / В.А.Галатенко. – М. : Изд-во ИНТУИТ.ру, 2005. – 208 с.

6. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа / А.Ю.Щеглов ; под ред. М.В.Финкова. – СПб. : Наука и Техника, 2004. – 384 с.

Аннотация: В статье рассмотрено соответствие средств защиты современных ОС класса автоматизированных систем, обрабатывающих конфиденциальную информацию, что позволяет утверждать, что большинство современных универсальных ОС не могут без использования средств защиты применяться для защиты конфиденциальной информации.

Ключевые слова: операционная система, защитный механизм, угроза, атака, несанкционированный доступ к информации.

Abstract: The article considers the compliance of protective means of modern operating systems with class automated systems, which handle confidential information. That allows to assert that most modern general-purpose operating systems can not be used without protective equipment to secure
sensitive information.

Key words: operating system, a defense mechanism, the threat, attack, unauthorized access to information.