УДК 004.45
Андрій ЗЕРКО
volcebk@ukr.net
Олександр ОКСІЮК
м. Київ

АНАЛІЗ ПИТАНЬ ЗАХИСТУ ІНФОРМАЦІЇ В ОПЕРАЦІЙНИХ СИСТЕМАХ НА ПРИКЛАДАХ ЗАХИЩЕНИХ ОПЕРАЦІЙНИХ СИСТЕМ

Розглянуто основні сучасні проблеми захисту інформації. Приведено поняття захищеності операційних систем. Розглянуто основні механізми захисту інформаційних систем. Проведено порівняльний аналіз, розглянутих операційних систем.

Ключові слова: інформаційна безпека, захищена операційна система, захист інформації.

Вступ. Глобальна інформатизація світу призвела до проникнення комп'ютерів та комп'ютерних систем в повсякденні процеси роботи всього людства. На поточний час не можливо уявити життя без електронної пошти, інформаційних ресурсів мережі Інтернет, банківських систем online-платежів, електронних інформаційних ресурсів та банків даних, тощо. Більшість важливої інформації зберігається саме в електронному виді.

Людство залежить від надійності роботи комп'ютерних та обчислювальних систем. І така залежність продовжую зростати. Питання забезпечення безпеки інформації про повсякденному використанні електронних систем стає надзвичайно важливим.

Серед операційних систем, що використовуються на комп'ютерах, найбільш поширеними є операційні системи сімейства «MicrosoftWindows». А чи цілком захищена інформація в ОС від «Microsoft»? Чи існує можливість, при правильних налаштуванні, додатково встановленому програмному забезпеченні, досягти оптимального захисту інформації? Чи можливо отримати математичну оцінку захищеності інформації – з урахуванням можливостей механізмів захисту операційної системи, важливості та вартості інформації на комп'ютері?

У відкритих ОС більш гнучкі налаштування механізмів та компонент захисту. При цьому потребують набагато більше знань та навичок для правильного налаштування та використання. Це призводить до необхідності висококваліфікованого налаштування відкритих систем. Як наслідок безпека у відкритих операційних системах залежить від рівня кваліфікації не лише програмістів, а й адміністратора системи.

Побудова методів та методик математичного оцінювання та доведення захищеності інформації в середовищі закритих і відкритих ОС – потребує реального розгляду та опрацювання.

Метою дослідження є:

- Аналіз систем захисту інформації, проведення оцінки захищеності;
- Розробка пропозицій щодо математичних моделей з налаштування методів захисту ОС для досягнення заздалегідь обґрунтованих параметрів надійності та безпеки.

Виклад основного матеріалу. Вважається, що операційні системи та інформаційно-телекомунікаційні системи, такі як локальні мережі – внутрішні та зовнішні, не можуть бути цілком захищеними. Якою б сучасною та бездоганною, з першого погляду, системою захисту не була б оснащена операційна система та інформаційно-телекомунікаційна система, завжди знайдеться спосіб для несанкціонованого доступу до інформації.

Але при правильному підході до реалізації та експлуатації системи, її компонент – можливо максимально зменшити ризик втрати чи витоку інформації, яка оброблюється та зберігається в системі, забезпечити максимальну працездатність системи навіть за критичних обставин.

Будемо вважати операційну систему – ***захищеною***, якщо вона забезпечує збереженість інформації та цілісність даних власними засобами, без використання допоміжного програмного забезпечення. Визначення не претендує на завершеність, лише на більш чітке розуміння термінів, що використовуються.

Основними завданнями захищених операційних систем є:

– Забезпечення захисту свого власного середовища від несанкціонованого доступу, підміни компонент та даних;

– Захист інформації, що обробляється, накопичується та зберігається в середовищі захищеної операційної системи, від несанкціонованого доступу.

У сучасних операційних системах розробниками реалізовано певний перелік механізмів забезпечення безпеки – алгоритми шифрування інформації, автентифікації при доступі до інформації, захисту від несанкціонованого доступу тощо. Комбінація цих механізмів, їх можливості цілком залежать від фантазії розробника ОС або програмного забезпечення.

Можливо довго дискутувати з питання щодо повноти та достатності даних механізмів. Цілком зрозуміло, що механізми забезпечення безпеки більш сильно реалізовані в операційних системах серверного застосування – Linux, BSD. Це пов'язано з галуззю призначення даного типу ОС – серверне застосування в середовищі відкритих систем – Інтернет.

В той же час в операційній системі Windowsбільшповно реалізовано механізми забезпечення безпеки для використання програмного забезпечення користувачів.

Основні механізми забезпечення безпеки в операційній системі:

1. Ідентифікація – один к компонентів найбільш поширеного способу доступу до інформації – реєстрації. Суть ідентифікації полягає, в тому що у кожному користувачеві при реєстрації, присвоюється унікальний ідентифікатор. За цим ідентифікатором можливо визначити ідентичність користувача;

2. Автентифікація – використовується для підтвердження доступу до інформації, що прив'язана або надається за унікальним ідентифікатором. Зазвичай автентифікація відбувається способом надання:

– Унікального предмету або атрибуту (електронний ключ, старт-карта, криптографічний сертифікат тощо);

– Паролю (найбільш розповсюджений вид автентифікації);

– Біометричних даних (голос, відбитки пальців, підпис, форма долоні тощо)

3. Контроль цілісності та автентичності даних – використовується для контролю важливих складових системи (наприклад: системних файлів) на пошкодження, або спотворення. Необхідний механізм для виявлення порушень та забезпечення стабільної роботи системи;

4. Резервне копіювання – виконується для забезпечення можливості відновлення оригіналу інформації або важливих компонент системи на випадок спотворення або пошкодження;

5. Розмежування доступу до інформації – виконується шляхом обов'язкової авторизації користувачем в системі. Використовується для надання авторизованому користувачу доступу і прав на користування інформацією та функціями системи, встановлених адміністратором системи;

6. Шифрування – використовується для шифрування важливої інформації на носії. Для зашифровки використовується криптографія. Система активує одностороннюю функцію, яку не важко обчислити, але дуже важко підібрати зворотну дію;

7. «Firewall» (пакетний фільтр) – використовується для контролю вхідного та вихідного трафіку. Забезпечує контроль за заданими правилами;

8. Аудит – використовується для спостереження. Система веде протоколювання:

– дій користувачів системи (авторизація, використання системних функцій);

– помилки та повідомлення системи;

– помилки та повідомлення програмного забезпечення;

– помилки та повідомлення центру безпеки.

Слід зазначити, що наявність механізмів захисту не призводить до позитивної відповіді на питання щодо можливості надання будь яких гарантій захищеності інформації в середовищі ОС. Насамперед необхідно визначити комплекс вимог до механізмів захисту інформації, забезпечення надійності та безпеки роботи програмного забезпечення користувачів в середовищі ОС, обґрунтувати підходи до забезпечення безпеки під час життєвого циклу.

Саме питання щодо забезпечення надійності та безпеки робити ОС в процесі життєвого циклу є одним з найменш досліджуваних питань. З часом компоненти програмного забезпечення (та й апаратного забезпечення комп'ютеру) можуть втрачати свої властивості за рахунок різних процесів:

– накопичення даних в кешах програм;

– виявлення помилок в роботі апаратного та програмного забезпечення;

ISSN 2520-2820 (online), ISSN 2524-0978 (print)

– збоїв та відмов компонент апаратного забезпечення, інформація про які не доступна пересіченому користувачеві.

Найчастіше саме накопичення таких прихованих помилок призводить до фатальної відмови програмного та апаратного забезпечення.

За результатами розгляду питань захисту інформації у сучасних операційних системах виникає питання щодо необхідності побудови математичних методів та моделей для оцінки захищеності інформації в середовищі операційних систем. Математичні методи та моделі повинні передбачати наступне:

– оцінку методів захисту інформації, які наявні в середовищі ОС;

– оцінку ризиків втрати інформації, що обробляється, зберігається, накопичується в середовищі ОС, з урахуванням значимості та вартості втрати або пошкодження інформації;

– оцінку якості програмного забезпечення користувача, яке функціонує в середовищі ОС, механізмів захисту інформації, які використовується програмним забезпеченням користувача;

– оцінку можливостей організації надійної та безпечної взаємодії між користувачем, адміністратором ОС та самим середовищем ОС.

Побудова таких математичних методів та методик дозволить:

– проводити оцінку ризиків при створенні та використанні складних інформаційних та телекомунікаційних систем;

– створювати інтегровані інформаційні системи з впровадженням виважених рішень з використанням механізмів захисту інформації;

Висновки. Аналіз питань захисту інформації у сучасних інформаційних та телекомунікаційних системах призводить до необхідності створення математичних методів оцінювання захищеності інформації, яка обробляється, накопичується, зберігається в середовищі ОС. Це досить складне завдання, яке потребує значного наукового опрацювання.

Слід також зазначити, що дане дослідження не є вичерпним та не претендує на завершеність. Основний висновок, який можливо зробити – дослідження необхідно продовжувати.

Список використаних джерел

1. Державна служба спеціального зв'язку та захисту інформації України [Електронний ресурс]. — Режим доступу: http://www.dstszi.gov.ua/dstszi/control/uk/index.
2. Компанія «АТМНІС» [Електронний ресурс]. — Режим доступу: https://atmnis.com/files/user_files/BBOS.pdf.
3. Компанія «Майлинукс» [Електронний ресурс]. — Режим доступу: http://mylinux.ua/press-release5.
4. Компанія ТОВ НДІ «Автопром» [Електронний ресурс]. — Режим доступу: http://avtoprom.kiev.ua/rproduct2.html.
5. Нестеров С. А. Інформаційна безпека та захист інформації : учеб. посібник / С. А. Нестеров. — СПб. : Видавництво політехн. ун-ту, 2009. — 126 с.
6. Макаренко С. І. Інформаційна безпека: навчальний посібник для студентів вузів / С. І. Макаренко. — Ставрополь : СФ МДГУ імені М. А. Шолохова, 2009. — 372 с.

Andrii ZERKO, Oleksandr OKSIIUK
Kyiv

ANALYSIS OF DATA SECURE IN OPERATING SYSTEMS ON EXAMPLES OF PROTECTING OPERATING SYSTEMS

Considered the main current problems of data secure.Considered to concept of protecting operating systems.The basic components for protecting operating systems described. Analyzed and compared chosen operating systems on object of secure.

Key words: information security, secure operating system protection.

Андрей ЗЕРКО, Александр ОКСИЮК
г. Киев

АНАЛИЗ ВОПРОСОВ ЗАЩИТЫ ИНФОРМАЦИИ В ОПЕРАЦИОННЫХ СИСТЕМАХ НА ПРИМЕРАХ ЗАЩИЩЕННЫХ ОПЕРАЦИОННЫХ СИСТЕМ

Рассмотрены основные современные проблемы защиты информации. Приведены понятия защищенности операционных систем. Рассмотрены основные механизмы защиты информационных систем. Проведен сравнительный анализ, рассмотренных операционных систем.

Ключевые слова: информационная безопасность, защищенная операционная система, защита информации.

Стаття надійшла до редколегії 13.03.2017