УДК 004.45

ПОБУДОВА МАТЕМАТИЧНОЇ МОДЕЛІ ВИЗНАЧЕННЯ РІВНЯ ЗАХИЩЕНОСТІ ОПЕРАЦІЙНИХ СИСТЕМ

ОКСІЮК О.Г., ЗЕРКО А.Л., КОХАНОВСЬКИЙ О.І.

Розглядаються основні сучасні проблеми захисту інформації. Приводяться необхідні поняття захищеності операційних систем, вказуються деякі механізми їх захисту. Проводиться аналіз захищеності операційної системи Microsoft Windows 8.1 Enterprise, системи захисту інформації ЛОЗАтм-1 (версія 4.X.Y) та програмного забезпечення антивірусного захисту інформації „Kaspersky Internet Security 15 для всіх пристроїв", що використовуються в Україні, з опором на експертні висновки. Розглядаються питання, які не мають наукових рішень, а саме: проблеми забезпечення надійності та безпеки функціонування систем захисту в середовищі ОС.

Вступ. Протягом останнього десятиліття світ, який оточує кожного з нас, став цифровим. Це результат довгого шляху розвитку мереж передачі даних, Інтернет, інформаційних технологій тощо. Україна вже не може повноцінно існувати без сучасних інформаційних мереж. Ми звикли до електронної пошти, інформаційних ресурсів Web-серверів, електронного обміну інформацією – звітність, банківські системи тощо. І без їх використання сучасне життя неможливе.

Слід зазначити, що надійність та безпека інформаційних технологій суттєво залежить від надійності та безпеки операційних систем (надалі – ОС). Дуже багато факторів впливають на безпеку ОС:

- якість самого програмного забезпечення ОС, відсутність в ядрі операційної системи помилок та вразливостей;
- відсутність в програмному забезпеченні користувачів помилок, які призводять до порушень безпеки;
- якість налаштування та конфігурування ОС, правильність включення механізмів забезпечення безпеки та захисту від несанкціонованого доступу;
- якість підтримки ОС, програмного забезпечення користувачів в середовищі ОС, якість їх тестування та перевірки властивостей забезпечення надійності та безпеки.

На поточний момент актуальним є питання гарантій забезпечення безпеки при використанні інформаційних технологій:

- чи надає використання саме даної версії ОС в наступній конфігурації гарантії забезпечення надійності та безпеки інформації користувачів в середовищі ОС?
- чи будуть збережені гарантії захищеності на протязі життєвого циклу комп'ютера – за умов змін в програмному забезпеченні ОС, програмному забезпеченні користувачів, виявленню нових видів вірусних загроз або методів злому програмного забезпечення?

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

Можна довго дискутувати 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 Windows більш повно реалізовано механізми забезпечення безпеки для використання програмного забезпечення користувачів.

Слід зазначити, що наявність механізмів захисту не дає 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 в середовищі ОС, обґрунтувати підходи до забезпечення безпеки під час життєвого циклу.

Слід зазначити, що саме питання щодо забезпечення надійності та безпеки робити ОС в процесі життєвого циклу є одним з найменш досліджених питань. З часом компоненти програмного забезпечення (та й апаратного забезпечення комп'ютера) можуть втрачати свої властивості через накопичення даних в кешах програм та процесів, виявлення помилок в роботі апаратного та програмного забезпечення, збої та відмови компонент апаратного забезпечення. Найчастіше саме накопичення таких прихованих помилок призводить до фатальної відмови програмного, а іноді й апаратного забезпечення.

В України існує законодавча база та практика проведення робіт з оцінки механізмів забезпечення безпеки в середовищі операційних систем. На підставі документів системи технічного захисту інформації проводиться оцінка захищеності механізмів забезпечення безпеки операційних систем різного класу та програмного забезпечення. Наприклад:

1. Операційна система **Microsoft Windows 8.1 Enterprise** виробництва Microsoft Corporation, США. (Експертний висновок № 486. Дійсний з 20.12.2013 до 20.12.2016).

Призначення операційної системи:
Забезпечення конфіденційності, цілісності та доступності об'єктів захисту, що циркулюють в ОС.
Відповідає вимогам НД з ТЗІ в обсязі функцій, зазначених у документі "Державна експертиза за критеріями технічного захисту інформації операційної системи Microsoft Windows 8.1 Enterprise. Технічні вимоги", сукупність яких визначається функціональним профілем:
- Довірча конфіденційність-2.
- Конфіденційність при обміні-1.
- Повторне використання об'єктів-1.
- Довірча цілісність-1.
- Цілісність при обміні-1.
- Відкат-1.
- Використання ресурсів-1.
- Гаряча заміна-2.
- Стійкість до відмов-2.
- Реєстрація-1/Реєстрація-2.
- Ідентифікація і автентифікація-1/Ідентифікація і автентифікація-2.
- Достовірний канал-1.
- Розподіл обов'язків-3.
- Цілісність комплексу механізмів захисту-2.
- Самотестування-2.
- Автентифікація при обміні-1.

Рівень гарантій Г-2 оцінки коректності їх реалізації – згідно з НД ТЗІ 2.5-004-99.
Використання в послугах безпеки КВ-1, ЦВ-1 та НВ-1 механізмів криптографічних перетворень можливе лише за наявності документів, які засвідчують відповідність цих механізмів вимогам нормативно-правових актів з криптографічного захисту інформації, що відповідають ступеню обмеження доступу до інформації, яка обробляється.
2. Система захисту інформації **ЛОЗАтм-1**, версія 4.X.Y. (Експертний висновок № 540**.** Дійсний з 08.08.2014 до 08.08.2017).
Призначення програмного забезпечення:
Захист від несанкціонованого доступу в складі комплексної системи захисту інформації в автоматизованих системах класу "1".
Відповідає вимогам НД з ТЗІ в обсязі функцій, зазначених у документі „Система захисту інформації ЛОЗАтм-1, версія 3.X.Y. Технічне завдання. Редакція 4", сукупність яких визначається функціональним профілем:
- ***Конфігурація „Підвищена безпека"***:
  - Адміністративна конфіденційність-3.
  - Повторне використання об'єктів-1.
  - Адміністративна цілісність-1.
  - Стійкість до відмов-1.
  - Гаряча заміна-1.
  - Стійкість до відмов-1.
  - Реєстрація-4.
  - Ідентифікація і автентифікація-3.
  - Достовірний канал-1.
  - Розподіл обов'язків-2.
  - Цілісність комплексу механізмів захисту-2.
  - Самотестування-2.
- ***Конфігурація „Стандартна безпека"***:
  - Адміністративна конфіденційність-2.
  - Довірча Конфіденційність-2.
  - Повторне використання об'єктів-1.
  - Довірча цілісність-1.
  - Адміністративна цілісність-1.
  - Стійкість до відмов-1.
  - Гаряча заміна-1.
  - Реєстрація-4.
  - Ідентифікація і автентифікація-2/Ідентифікація і автентифікація-3.
  - Достовірний канал-1.
  - Розподіл обов'язків-2.
  - Цілісність комплексу механізмів захисту-2.
  - Самотестування-2.

Рівень гарантій Г-4 оцінки коректності їх реалізації – згідно з НД ТЗІ 2.5-004-99.
3. Програмне забезпечення антивірусного захисту інформації **„Kaspersky Internet Security 15 для всіх пристроїв"** виробництва Kaspersky Lab UK Ltd. (Експертний висновок № 564. Дійсний з 04.02.2015 до 04.02.2018).
Призначення програмного забезпечення:
Призначене для домашніх користувачів та забезпечує комплексний захист комп'ютерів від кіберзагроз, мережевих та шахрайських атак, а також спаму.
Відповідає вимогам нормативних документів системи технічного захисту інформації в Україні в обсязі функцій, зазначених у документі „Програмне забезпечення антивірусного захисту інформації „Kaspersky Internet Security 15 для всіх пристроїв". Технічні вимоги за критеріями технічного захисту інформації", сукупність яких визначається функціональним профілем:
- Адміністративна конфіденційність-2.
- Адміністративна цілісність-1.
- Цілісність при обміні-1.
- Відкат-1.
- Стійкість до відмов-1.
- Гаряча заміна-1.
- Використання ресурсів-1.
- Реєстрація-2.
- Ідентифікація і автентифікація-2.
- Розподіл обов'язків-1.
- Цілісність комплексу механізмів захисту-1.
- Самотестування-2.
- Достовірний канал-1.
- Автентифікація при обміні-1.

Рівень гарантій Г-2 оцінки коректності їх реалізації – згідно з НД ТЗІ 2.5-004-99.

В той же час існує ряд наукових питань, які не мають рішення. Наведемо приклади таких наукових проблемних питань забезпечення надійності та безпеки функціонування систем захисту в середовищі ОС.

Приклад № 1. Розглянемо використання системи захисту інформації ЛОЗАтм-1 (версія 4.X.Y) в середовищі ОС Microsoft Windows 8.1.

Кожен з компонентів має власні механізми захисту інформації, які підтверджено в експертних висновках. Слід зазначити, що механізми системи захисту ЛОЗАтм-1 (версія 4.X.Y) виконано на рівні ядра операційної системи. Отже, маємо два засоби захисту інформації, які використовують пріоритетні механізми захисту інформації в середовищі ОС.

В даному випадку можливо зробити висновок, що ми маємо випадок конкурентної боротьби двох незалежних розробок зі створенням незалежних механізмів захисту інформації, які працюють в середовищі ОС.

При використанні системи захисту ЛОЗАтм-1 (версія 4.X.Y) в середовищі операційної системи з підтвердженими сервісами безпеки яким повинен бути профіль захищеності? Чи виконується нарощування механізмів захисту інформації при комбінуванні рішень? Чи можливе посилення або послаблення механізмів захисту інформації при такому використанні?

Акцентуємо увагу на дві основні проблеми забезпечення надійності та безпеки сучасних ОС:

- строге доведення захищеності та надійності ОС як єдиного комплексу програмного забезпечення та застосувань в середовищі ОС;
- виконання математичних оцінок захищеності та надійності ОС під час життєвого циклу з урахуванням компонентів, які працюють в середовищі ОС (наприклад – програмного забезпечення антивірусного захисту).

Вирішення таких питань без використання математичних методів не уявляється можливим. На наш погляд, повинні бути виконані дослідження за такими напрямами:

- розробка алгебри обчислення сум механізмів захисту інформації в середовищі ОС. Дані методи повинні давати відповіді на питання результату від використання комбінованих механізмів захисту інформації в середовищі ОС;
- розробка механізмів ймовірнісної оцінки надійності та й захищеності ОС та компонентів у середовищі ОС з урахуванням часових змін. При побудові математичних підходів для вирішення даної задачі необхідно буде використовувати моделі життєвого циклу програм, ймовірнісні підходи до оцінки комбінацій моделей.

Висновок. Розглянуто сучасні проблеми захисту інформації в середовищі ОС. Для безпечної роботи з даними та інформацією необхідні певні гарантії захищеності ОС. Проаналізовано сучасний стан забезпечення збереженості та цілісності інформації в операційних системах. Приведено перелік деяких компонентів захисту, що використовуються в сучасних ОС.

Проаналізовано захищеність з переліком та рівнем компонентів захисту операційної системи Microsoft Windows 8.1 Enterprise, системи захисту інформації ЛОЗАтм-1 (версія 4.X.Y) та програмного забезпечення антивірусного захисту інформації „Kaspersky Internet Security 15 для всіх пристроїв", що використовуються в Україні, з опором на експертні висновки Державної служби спеціального зв'язку та захисту інформації України.

Розглянуто проблемність забезпечення надійності та безпеки функціонування системи захисту інформації в середовищі ОС.

Обґрунтовано необхідність подальшої розробки математичних методів оцінювання захищеності ОС з інтеграцією в її середовище допоміжних програмних забезпечень зі своїми компонентами захисту інформації. Необхідна подальша розробка механізмів ймовірнісної оцінки надійності та захищеності ОС та компонентів в середовищі ОС з урахуванням часових змін.

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

Transliterated bibliography:

1. © Derzhavna sluzhba spetsialnogo zv'yazku ta zahistu informatsiyi Ukrayini. http://www.dstszi.gov.ua/dstszi/control/uk/index.

2. *Kompaniya* «ATMNIS», https://atmnis.com/files/user_files/BBOS.pdf

3. *Kompaniya* «Maylinuks», http://mylinux.ua/press-release5

4. *Kompaniya* TOV NDI «Avtoprom», http://avtoprom.kiev.ua/rproduct2.html

5. *Nesterov S. A.* Informatsiyna bezpeka ta zahist informatsiyi: Ucheb. posibnik. SPb.: Vidavnitstvo politehn. un-tu, 2009. 126 s.

6. *Makarenko S. I.* Informatsiyna bezpeka: navchalniy posibnik dlya studentiv vuziv. Stavropol: SF MDGU im. M. A. Sholohova, 2009. 372 s.

Надійшла до редколегії 14.05.2017

Рецензент: д-р техн. наук, проф. Безрук В.В.

Оксіюк Олександр Глібович, завідувач кафедри кібербезпеки та захисту інформації, доктор технічних наук, професор, Київський національний університет імені Тараса Шевченка. Адреса: Україна, Київ, 01033, вул. Володимирська, 60.
Зерко Андрій Леонідович, аспірант кафедри кібербезпеки та захисту інформації, Київський національний університет імені Тараса Шевченка. Адреса: Україна, Київ, 01033, вул. Володимирська, 60, e-mail: a.l.zerko@ukr.net, тел.: 0966759139.
Кохановський Олексій Ігорович, директор ТОВ «Авалекс Текнолоджи». Адреса: Україна, Київ, e-mail: o.i.kokhanovskyi@avaleks.kiev.ua,

Oksiyuk Oleksandr Hlibovych, Head of the Department of Cybersecurity and Information Protection, Doctor of Technical Sciences, Professor, Taras Shevchenko Kyiv National University. Address: st. Vladimirskaya, 60, Kyiv, 01033, Ukraine.
Zerko Andriy Leonidovich, PhD student, Department of Cybersecurity and Information Security, Taras Shevchenko Kyiv National University. Address: st. Vladimirskaya, 60, Kyiv, 01033, Ukraine, e-mail: a.l.zerko@ukr.net, tel. 0966759139.
Kokanovsky Alexey Igorovich, Director of Open Access Technologies, e-mail: o.i.kokhanovskyi@avaleks.kiev.ua, Kiev Ukraine,.