УДК 004.891.3:004.3

ЗЕНКІН М.А., ФЕДОРЧУК Д.І.
Київський національний університет технологій та дизайну

КОМПЛЕКСНА ОЦІНКА ЯКОСТІ СИСТЕМ ЗАХИСТУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Мета. *Виконати аналіз сучасних методів захисту програмного забезпечення з виділенням загальних принципів їх реалізації і класифікації, а також сформулювати вимоги до ефективної системи захисту.*

Методика. *Методи теорії інформації, методи математичного опису і дослідження інформаційних процесів, методи передачі, обробки, зберігання, витягання і класифікації інформації, методи теорії алгоритмів, методи теорії обчислювальних процедур, методи управління якістю програмного забезпечення, методи забезпечення надійності програм.*

Результати. *Розроблені рекомендації, щодо забезпечення безпеки комп'ютерної системи на основі принципів, регламентованих діючими стандартами якості і безпеки.*

Наукова новизна. *Поставлені і досліджені питання комплексної оцінки якості систем захисту програмного забезпечення.*

Практична значимість. *Розроблена комплексна модель оцінки якості систем захисту програмного забезпечення дозволяє проектувати такі системи з урахуванням вимог міжнародних стандартів, а також мати можливість не лише оцінити стійкість системи захисту до злому, але і дати цілий ряд інших, не менш важливих оцінок.*

Ключові слова: *комплексна оцінка якості, програмне забезпечення.*

Вступ. Прогрес у галузі застосування інформаційних технологій, обумовлений розвитком обчислювальних систем і програмного забезпечення, супроводжується підвищенням вимог до стабільності функціонування інформаційних систем і стійкості при спробах порушення їхньої безпеки. Все більшого значення набувають відмінності методів захисту програмного забезпечення від незаконного копіювання та розповсюдження. Це пов'язано в першу чергу з розвитком комп'ютерної техніки і глобальних комп'ютерних мереж, значно полегшує передачу, копіювання та розповсюдження великих обсягів інформації. Вірогідність несанкціонованого використання програмного забезпечення також збільшується в міру збільшення кількості користувачів персональних комп'ютерів. З цих причин сучасне програмне забезпечення повинно забезпечуватися різними засобами захисту від несанкціонованого доступу.

Недоліки систем захисту є наслідками незадовільної якості захисту програмного забезпечення. На основі цього можна зробити висновок про необхідність вдосконалення існуючих та створення нових засобів і методів оцінки якості захисту програмного забезпечення. Для цього необхідно дати формальний опис проблеми і на підставі формальної постановки задачі розробити комплексну модель оцінки якості систем захисту програмного забезпечення [1-3].

Постановка завдання. Розробити комплексну модель оцінки якості систем захисту програмного забезпечення на основі вимог міжнародних стандартів в області якості.

Результати досліджень. Невід'ємною частиною загального процесу підвищення якості інформаційних технологій (ІТ) і програмного забезпечення (ПЗ) є розробка стандартів,

пов'язаних з проблемою безпеки ІТ і ПЗ, яка придбала велику актуальність у зв'язку з тенденціями все більшої взаємної інтеграції прикладних завдань, побудови їх на базі розподіленої обробки даних, систем телекомунікацій, технологій обміну електронні дані [3, 4].

Розробка міжнародних стандартів в області інформаційної безпеки і систем захисту програмного забезпечення проводиться безперервно. При цьому послідовно публікуються проекти і версії стандартів на різних стадіях узгодження і твердження. Стандарти поетапно опрацьовуються і деталізуються у вигляді сукупності взаємозв'язаних по концепціях і структурі груп стандартів [2, 5].

Під системою захисту ПЗ від несанкціонованого копіювання і несанкціонованого використання розуміється комплексний засіб, який як правило, є частиною самого ПЗ, призначений для ускладнення, або попередження нелегального копіювання (виконання) захищеного ПЗ.

Ефективна система захисту ПЗ повинна задовольняти наступним вимогам:

- система захисту повинна виявляти факт несанкціонованого запуску захищеного ПЗ;
- система захисту повинна реагувати на факт несанкціонованого запуску ПЗ;
- система захисту повинна протистояти можливим атакам зловмисника [3, 4, 6].

Оцінка якості конкретного ПЗ робиться шляхом роздільної оцінки деякої сукупності показників якості оцінюваного ПЗ і подальшим підсумовуванням отриманих оцінок, в результаті якого виходить загальна оцінка якості. Існує міжнародний стандарт ISO 9126:1991 [7], в якому виділені характеристики (показники якості), що дозволяють оцінювати ПЗ з точки зору користувача, розробника і керівника проектом. Всього в міжнародному стандарті рекомендується шість основних показників якості ПЗ, кожен з яких деталізований декількома характеристиками.

Показники якості ПЗ можна розділити на наступні класи:

- показники супроводу – структурна і інформаційна складність ПЗ, структурність ПЗ, наочність, повторюваність;
- показники надійності;
- показники зручності роботи – легкість освоєння, доступність експлуатаційної програмної документації, зручність експлуатації і обслуговування.
- показники ефективності – рівень автоматизації, тимчасова ефективність, ресурсоємність;
- показники універсальності – гнучкість, мобільність, модифікованість;
- показники коректності – логічна коректність, повнота реалізації, узгодженість, перевіреність.

Якістю системи захисту ПЗ називається сукупність споживчих властивостей системи захисту ПЗ, що характеризують її здатність задовольняти потребу користувачів в захисті ПЗ. Під користувачами розуміються розробники ПЗ, яке треба захистити і користувачі ПЗ, захищеного цією системою захисту [2, 5].

Розглянемо функціонування системи «Захищуване ПЗ – система захисту ПЗ». Для цього представимо цю систему у вигляді моделі, яка складається з двох блоків:

- захищуване ПЗ;
- система захисту ПЗ.

Ці блоки пов'язані функціонально (рис. 1). Всі зв'язки можна розділити на наступні класи:

- ініціалізація роботи зазищуваного ПЗ (*I*);
- перевірка середовища функціонування захищуваного ПЗ (*C*);
- функції, які необхідні для роботи захищуваного ПЗ (*F*);
- деініціалізація роботи захищуваного ПЗ (*D*).

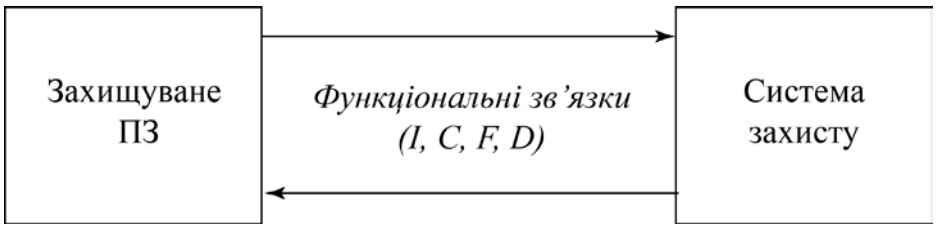

Рис. 1. Модель системи «Захищуване ПЗ – система захисту ПЗ»

Ініціалізація роботи захищуваного ПЗ (*I*) – це виконання системою захисту ПЗ дій, необхідних для початку роботи захищуваного ПЗ. Це можуть бути: початкове завантаження даних і виконуваного коду в пам'ять, їх розшифровка, передача управління захищуваного ПЗ, початкова перевірка середовища функціонування захищуваного ПЗ [1, 2, 5].

Перевірка середовища функціонування захищуваного ПЗ (*C*) – виклики захищуваного ПЗ системи захисту для виконання поточних перевірок середовища його функціонування. При цьому система захисту захищуваного ПЗ виконує ці перевірки і повідомляє про їх результат ПЗ. Можливий варіант, при якому система захисту захищуваного ПЗ сама приймає рішення про подальше функціонування захищуваного ПЗ, ґрунтуючись на результатах перевірок. При цьому не виконуються ніяких дій, необхідних для функціонування захищуваного ПЗ.

Функції, необхідні для роботи захищуваного ПЗ (*F*) – виклики ПЗ системи захисту захищуваного ПЗ для виконання дій, необхідних для роботи захищуваного ПЗ: розшифровка ділянок даних або виконуваного коду необхідних по ходу роботи ПЗ; виконання елементів алгоритму роботи захищуваного ПЗ.

Деініціалізація роботи захищуваного ПЗ (*D*) – виконання системою захисту ПЗ дій, необхідних для коректного завершення роботи захищуваного ПЗ, і, можливо, очищення середовища функціонування від слідів роботи захищуваного ПЗ, і самої системи захисту з тим, щоб унеможливити вивчення цих слідів з метою отримання інформації про алгоритми роботи захищуваного ПЗ, або системи його захисту.

Таким чином, систему «Захищуване ПЗ – система захисту ПЗ» можна представити у вигляді набору великих множин (*I, C, D, F*). При цьому міра захисту ПЗ визначається кількістю зв'язків кожного виду і кількістю передаваної ними інформації.

Оцінка якості системи захисту програмного забезпечення здійснюється загальноприйнятим способом – шляхом оцінки сукупності показників якості, які дають в цілому загальну оцінку [2, 4, 6].

Показники якості, характерні як для систем захисту ПЗ, так і для ПЗ загального призначення – це коректність і надійність.

Показники коректності характеризують здатність системи захисту ПЗ виконувати свої функції за відсутності обурюючих чинників, таких, як спроби злому системи захисту.

Надійність ПЗ – здатність ПЗ в конкретних сферах застосування виконувати задані функції відповідно до програмних документів в умовах виникнення відхилень в середовищі функціонування, викликаних збоями технічних засобів, помилками у вхідних даних, помилками обслуговування і іншими дестабілізуючими діями. Показники надійності системи захисту ПЗ характеризують здатність цієї системи виконувати свої функції за наявності обурюючих чинників, до яких, в числі інших, відносяться і спроби злому.

Для оцінки таких показників якості, як легкість освоєння ПЗ і зручність обслуговування і експлуатації ПЗ, часто застосовуються методи експертних оцінок. Показники якості ПЗ оцінюються групою експертів.

Структура систем захисту програмного забезпечення, їх функціонування відрізняються рядом особливостей, що відрізняються від ПЗ загального призначення. В зв'язку з цим розробка показників якості і способів їх оцінки в застосуванні до систем захисту ПЗ є дуже актуальним завданням.

Висновки. На основі усебічного аналізу міжнародних і вітчизняних стандартів, присвячених якості програмного забезпечення, сформована номенклатура показників якості програмного забезпечення, що включає наступні показники: супроводу, надійності, зручності роботи, ефективності, універсальності і коректності. Проаналізовані показники якості програмного забезпечення і сучасні методи їх оцінки. Виконана класифікація методів оцінки показників якості програмного забезпечення, що входить в номенклатуру. Показано, що нині основними є методи експертних оцінок, евристичні методи і оцінки із застосуванням різних математичних методів.

Список використаної літератури

1. Анисимов А.В., Иванов И.Ю. Подходы к защите программного обеспечения от атак злонамеренного хоста. // Проблеми програмування, С. 41-61 – Киев, 2006.
2. Бекетова Е.А. Методы и средства оценки качества программ имитационных моделей: Автореф. дисс. к.т.н. – Харьков, 1992. – 16 с.
3. Богданов Д.В, Фильчаков В.В. Стандартизация жизненного цикла и качества программных средств //Учеб. пособие. Минобразование РФ. С. – Петерб. гос. ун-т аэрокосм, приборостроения СПб.: С.-Петерб. гос. ун-т аэрокосм, приборостроения, 2000. – 209 с.
4. Казарин О.В. Безопасность программного обеспечения компьютерных систем. – М.: МГУЛ, 2003. – 212 с.
5. Карповский Е.Я., Чижов С.А. Надежность программной продукции. – Киев: Техника, 1990.
6. Куприков М.Ю. Применение информационных технологий на этапах жизненного цикла изделия //Качество и жизнь, 2004, № 4. – С.210-213.

7. ISO/IEC 9126:1991. Информационные технологии. Оценка программных продуктов. Характеристики качества и руководящие положения по их применению

КОМПЛЕКСНАЯ ОЦЕНКА КАЧЕСТВА СИСТЕМ ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

ЗЕНКИН Н.А., ФЕДОРЧУК Д.И.
Киевский национальный университет технологий и дизайна

Цель. Выполнить анализ современных методов защиты программного обеспечения с выделением общих принципов их реализации и классификации, а также сформулировать требования к эффективной системе защиты.

Методика. Методы теории информации, методы математического описания и исследования информационных процессов, методы передачи, обработки, хранения, вытягивания и классификации информации, методы теории алгоритмов, методы теории вычислительных процедур, методы управления качеством программного обеспечения, методы обеспечения надежности программ.

Результаты. Разработанные рекомендации, относительно обеспечения безопасности компьютерной системы на основе принципов, регламентированных действующими стандартами качества и безопасности.

Научная новизна. Поставлены и исследованы вопросы комплексной оценки качества систем защиты программного обеспечения.

Практическая значимость. Разработанная комплексная модель оценки качества систем защиты программного обеспечения позволяет проектировать такие системы с учетом требований международных стандартов, а также иметь возможность не только оценить стойкость системы защиты к взлому, но и дать целый ряд других, не менее важных оценок.

Ключевые слова: *комплексная оценка качества, программное обеспечение.*

COMPLEX EVALUATION OF QUALITY SYSTEMS PROTECTION SOFTWARE

ZENKIN N., FEDORCHUK D.
Kiev National University of Technology and Design

Purpose: To execute the analysis of modern methods of defence of software with the selection of general principles to their realization and classification, and also to set forth requirement to the effective system of defence.

Methodology. Methods of information theory, methods of mathematical description and research of informative processes, methods of transmission, treatment, storage, drawing out and classification of information, methods of theory of algorithms, methods of theory of calculable procedures, management methods by quality of software, methods of providing of reliability of the programs.

Results. Worked out recommendations, in relation to providing of safety of the computer system on the basis of the principles, regulated by the operating standards of quality and safety.

Scientific novelty. The questions of complex estimation of quality of the systems of defence of software are put and investigational.

Practical meaningfulness. The worked out complex model of estimation of quality of the systems of defense of software allows to design such systems taking into account the requirements of international standards, and also to have the opportunity not only to estimate firmness of the system of defense to breaking but also give a number of other, no less important estimations.

Keywords: *complex estimation of quality, software.*