# БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ ШЛЯХОМ СТВОРЕННЯ ЯКІСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

***С. Л. Демчик, студент***
*Житомирський військовий інститут ім. С.П. Корольова*
*Angelachek@mail.ru*

*В статті розглядаються засоби та методи зменшення ризику порушення шкідливим програмним забезпеченням безпеки інформаційної системи.*

*Demchyk S. L. Security of information systems by creating quality software. In the article are discussed the means and methods of reducing the risk of infringement by malicious software security information system.*

*Ключові слова*: ІНФОРМАЦІЙНА СИСТЕМА, ТЕСТУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ЗАХИСТ ІНФОРМАЦІЇ.
*Keywords:* INFORMATION SYSTEM, SOFTWARE TESTING, DATA PROTECTION.

Крім помилок осіб, які обслуговують інформаційні системи, існує ряд загроз, що пов’язані з розробленням, впровадженням та супроводом програмного забезпечення. Часто помилка в програмі викликає колапс системи і призводить до порушення критеріїв конфіденційності, цілісності чи доступності при захисті інформації від несанкціонованого доступу. Аналізуючи можливі загрози з точки зору найбільшої небезпеки для інформаційної системи, слід виділити шкідливе програмне забезпечення. Шкідливе програмне забезпечення - це будь-яка програма, що може бути написана з метою нанесення шкоди або для використання ресурсів атакованого комп'ютера або програмні продукти, що під час розроблення містили.

Джерелами помилок у програмному забезпеченні (ПЗ) можуть бути логічні помилки розробників програмного забезпечення, непередбачені ситуації, які проявляються при

модернізації, заміні чи додаванні нових апаратних засобів, встановленні нових додатків, виході на нові режими роботи ПЗ, появі раніше не зафіксованих нештатних ситуацій, віруси, якими інфіковані програми, спеціальні програмні компоненти, які передбачені розробниками ПЗ для різного роду цілей. Однак, практика доводить, що винуватцями помилок у програмах найчастіше бувають самі програмісти. Один із загальних законів практичного програмування полягає в тому, що жодна програма не дає бажаних результатів при першій спробі трансляції та виконання.

Найкращим шляхом для розроблення якісного програмного забезпечеггя є тестувааня програм та систем.

Тестування - оцінка якості ПЗ методом експериментальної перевірки - шляхом виконання тестів. Мета тестування - виявити наявність помилок/неузгодженостей. Іншими словами, це знаходження помилок (локалізація - задача діагностики), досягнення відсутності помилок (відладка). Це спосіб семантичної перевірки програми, який полягає в опрацюванні програмою послідовності різноманітних контрольних наборів тестів з відомими результатами. Тести підбираються так, щоб вони охопили найрізноманітніші типи можливих ситуацій.

Тестову перевірку можна провести також шляхом додання до програми, що перевіряється, додаткових операторів, які будуть сигналізувати про перебіг її виконання й отримання результатів.

Після проведення необхідних змін програмне забезпечення повинне бути перетестовано.

Для усунення можливості модифікації розробленого і протистованого програмного забезпечення слід застосувати інструменти криптографічного захисту, які реалізуються шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства.

Найкращим вибором для розробленого програмного комплексу є встановлення зашифрованого паролю на системну/адміністративну частину, використання ключів, що будуть відомі лише спеціалістам з необхідним рівнем доступу в інформаційній системі. Процес входу в програму таким способом подібен до процесу авторизації /аутентифікації, однак

має ключову відмінність - дані для входу кодуються з використанням одного зі стандартів шифрування даних, що значно підвищує криптостійкість програми та унеможливлює її шкідливу модифікацію.

Зашифровані дані однозначно залежать від ключа складним і запутаним способом. Кожний біт початкових даних впливає на кожний біт зашифрованих даних, що відкидає можливості розшифрування зловмисником. Поширення одного незашифрованого біта на велику кількість зашифрованих бітів приховує статистичну структуру початкових даних. Визначити, як статистичні характеристики зашифрованих даних залежать від статистичних характеристик початкових даних, досить непросто. Для бездоганного захисту ідентифікаторів має місце вровадження додавання контекстного ідентифікатора до кожного блоку шифротексту. Міжнародний стандарт шифрування даних IDEA з цього погляду є дуже ефективним алгоритмом

В доповіді запропонований метод зменшення ризику порушення шкідливим програмним забезпеченням безпеки інформаційної системи. Він реалізується шляхом тестування розробленого програмного забезпечення на всіх етапах його життєвого циклу, а також впровадження в програму інструментів криптографічного захисту для посилення безпеки при несанкціонованому втручанні в роботу комп'ютерних, інформаційних і телекомунікаційних систем. Отримані результати теоретичного аналізу доводять, що методика значно покращує криптостійкість програми та інформаційної системи в цілому.

## *Література*

1. Комич Б.М.Основні принципи діяльності із захисту інформації. Захист інформації в інформаційних системах. – 2012. – № 2 (22). – С. 216-230.

2. Корченко О.Г., Сіденко В.П., Дрейс Ю.О. Прикладна криптологія: системи шифрування // К.: ДУТ,2014. – С. 245-269.