УДК 004.75, 539.3.623 DOI: https://doi.org/10.33099/2304-2745/2021-1-71/93-98

Руденська Г. В. (0000-0002-4719-3765)

Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського, Київ

Шляхи удосконалення тестування спеціального програмного забезпечення інформаційної системи управління оборонними ресурсами на етапі експлуатації

Резюме. Проведено аналіз методів тестування спеціального програмного забезпечення на етапі експлуатації, які відповідають регламентам міжнародних стандартів STANAG та ISO/ДСТУ і направлені на виявлення потенційної вразливості *(vulnerability)*. Запропоновано шляхи удосконалення тестування спеціального програмного забезпечення інформаційної системи управління оборонними ресурсами DRMIS (*Defense Resources Management Information System)* для впровадження на етапі експлуатації.

Ключові слова: управління оборонними ресурсами; інформаційна система; спеціальне програмне забезпечення; тестування; процедури тестування, уразливість; міжнародні стандарти; система менеджменту; початкові коди.

Постановка проблеми. Використання інформаційних систем (ІС) у сфері державного військового управління і оборонного планування передбачає застосування відповідного спеціального програмного забезпечення (СПЗ). Однією з вимог до СПЗ є забезпечення потрібного рівня його захищеності під час можливих кібератак та несанкціонованого доступу.

Основні заходи, які використовуються для захисту ІС – мережеві екрани, системи виявлення і попередження вторгнень та антивірусні системи на основі аналізу сигнатур трафіку, спрямовані на відбиття атак з мережі [1]. Високий рівень уразливості СПЗ може мати такі наслідки, як отримання доступу до конфіденційної інформації неавторизованими користувачами, порушення нормального режиму функціонування (виконання довільного коду), виконання команд з підвищеними привілеями користувачем, який їх не має та ін. Крім того, є проблеми довіри до СПЗ ІС воєнного призначення, в розробленні або тестуванні яких взяли участь компанії інших країн і рівень його уразливості не підтверджений.

Отже, актуальним стає впровадження сучасних процедур тестування та виявлення вразливості СПЗ, яке використовується або планується до використання в сучасних ІС воєнного призначення, зокрема DRMIS.

Аналіз останніх досліджень та публікацій. Концептуальний підхід до тестування СПЗ викладено в [2]. Існує значна кількість сучасних наукових досліджень з питань загального менеджменту ІС, аналізу коду, проведення тестування на проникнення [3, 4]. Агенція передових оборонних дослідницьких проєктів (DARPA) Міністерства оборони США, яке відповідає за розроблення нових технологій для Збройних сил США, на етапі розроблення нового СПЗ застосовує чотири основні процедури тестування (табл. 1).

Таблиця 1

Дослідження DARPA щодо тестування СПЗ ІС воєнного призначення

Процедура	Мета процедури
Перевірка програмних і апаратно-програмних засобів (VET)	Контроль відповідності заявленим спроможностям, виявлення закладок у СПЗ ІС
Аналіз програм для забезпечення кібербезпеки (APAC)	Автоматизація виявлення вразливостей СПЗ ІС у реальному часі
“Великий кібервиклик” (CGC) та академічні дослідження вразливостей	Упровадження нових процедур тестування
Системний аналіз програмних комплексів	Підвищення надійності СПЗ та удосконалення процедур верифікації, зокрема статичних аналізаторів

Однак процедури тестування та виявлення уразливості СПЗ безпосередньо на етапі експлуатації ІС вивчені недостатньо та розглядаються як питання технічного регулювання [5]. Дослідження з цього питання носять фрагментарний характер або обмежені внутрішніми “кращими практиками” розробників програм. Так, у [6] добре опрацьовані загрози ланцюжків поставок, а

процедури виявлення уразливості СПЗ на етапі експлуатації описані недостатньо.

Водночас понятійний і методичний апарат тестування СПЗ та оцінювання вразливості програм уже склався і знаходиться на відповідному рівні ітераційного розвитку. У статті використанні визначення, прийняті міжнародними організаціями зі стандартизації, у яких бере участь Україна, а саме: STANAG, ISO, IEC, ITU.

Метою статті є аналіз методів тестування СПЗ для виявлення уразливості та шляхів удосконалення тестування СПЗ DRMIS на етапі експлуатації.

Виклад основного матеріалу дослідження. Тестування СПЗ (*Custom Software Testing*) - це процес аналізу і визначення надійності функціонування програмного продукту в інформаційному середовищі, у якому він використовується. Надійність функціонування програмного продукту *(Software Reliability)* визначається ймовірністю його роботи без відмов протягом встановленого періоду часу, з урахуванням вартості кожної відмови [8]. Ймовірність роботи СПЗ без відмов на практиці визначається ймовірністю того, що оператор не зможе ввести в систему деякий конкретний набір даних, що визначається як відмова у обслуговуванні, яка впливає на результат функціонування DRMIS, наприклад, своєчасне направлення необхідних боєприпасів на вогневу позицію артилерії, що в кінцевому варіанті, приводить до суттєвих втрат. Під уразливістю СПЗ *(System Vulnerability)* розумітимемо нездатність протистояти впливу певної кіберзагрози або сукупності кіберзагроз: помилок програмування, недоліків проєктування, ненадійних паролів, вірусів та інших шкідливих програм, використання мов програмування загального призначення (наприклад, PHP скриптов) і SQL-ін'єкцій [9]. Тобто, це певні недоліки в СПЗ, які можуть порушити її цілісність та надійність експлуатації.

Примітка.

PHP - скриптова мова загального призначення, інтенсивно застосовується для розроблення вебдодатків. На сьогодні підтримується переважною більшістю хостинг-провайдерів і є одним з лідерів серед мов, що застосовуються для створення динамічних веб-сайтів.

SQL ін'єкція - один з поширених способів злому сайтів і програм, які працюють з базами даних, заснований на впровадженні в запит довільного SQL-коду.

Програма-експлойт (en: exploit - експлуатувати) – комп'ютерна програма, фрагмент програмного коду або послідовність команд, які використовують уразливості в програмному забезпеченні та застосовують для проведення атаки на обчислювальну систему. Метою атаки може бути як захоплення контролю над системою (підвищення привілеїв), так і порушення її функціонування (DoS-атака).

Повний перелік процедур тестування СПЗ на етапі експлуатації включає [9]:

аналіз початкового коду для визначення уразливості;

визначення причин виникнення уразливості;

забезпечення надійності функціонування СПЗ.

Аналіз початкового коду. Аналіз початкового коду СПЗ для виявлення уразливості базується на різних методах тестування: статичному, динамічному, експертно-документальному, фазінгу. Це пов'язано з тим, що помилки і уразливості СПЗ мають різну природу і різні характерні ознаки.

Статичний метод базується на ідентифікації початкових кодів, які беруть участь у компіляції об'єкта сертифікації для фіксування повного переліку файлів вихідних текстів. Під час застосування *динамічного методу аналізу початкового коду* проводиться формування переліку шаблонів атак, які є актуальними для СПЗ із використанням послідовності дій, які представлені в розділі 6.1 стандарту ISO/IEC TR 20004. Під час застосування *експертно-документального аналізу* крім інформації, представленої в початкових кодах СПЗ, експерти використовують представлену для тестування документацію (технічну, програмну, експлуатаційну), інформацію про вразливості СПЗ об'єкта, схожого з об'єктом сертифікації. *Фазінг-тестування* базується на визначенні актуальних вразливостей СПЗ за результатами виконання тестів на проникнення.

Результативність застосування цих методів аналізу початкового коду СПЗ, визначеної через відсоток від загальної кількості виявлених вразливостей, наведена на рис. 1 [9].

Отже, не зважаючи на використання різних методів тестування СПЗ, допустимий рівень надійності функціонування СПЗ неможливо забезпечити без надання доступу до початкового коду СПЗ. Динамічний метод і фазінг-тестування не дають змоги виявити "плаваючі" помилки і програмні закладки,

ініціювання яких пов'язане з рідкісними комбінаціями вхідних даних, і які, за статистикою, є однією з найбільших проблем функціонування СПЗ. Тільки доступ до початкових кодів СПЗ дає високу ймовірність усунення уразливості.

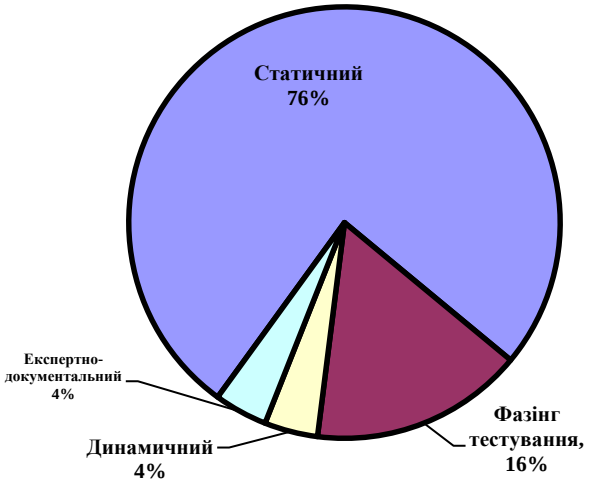

Рис. 1. Методи аналізу початкових кодів СПЗ DRMIS

Визначення переліку причин виникнення уразливості СПЗ базується на двох методах:

статистичному, з використанням статистики провідних баз даних уразливості програмного забезпечення, таких як CAPEC, OWASP, *Mitre CVE*;

тестуванні загальновідомими програмами-експлойтами.

У межах дослідження пілотної версії DRMIS [10] методом співставлення зі статистичними даними *Mitre CVE*, яка перевищує 100 000 вразливостей [11], встановлений визначальний вплив на причини виникнення уразливості СПЗ рівня менеджменту розробника та критичної структурної складності СПЗ.

Рівень менеджменту істотно впливає на ймовірність уразливості та можливості оперативного виправлення СПЗ, встановлена строга зворотна пропорційність вірогідності уразливості рівню менеджменту розробників програм. Цей висновок підтверджується компанією Microsoft, ймовірність уразливостей в програмному забезпеченні якої вдалося знизити на 80 % за умови введення відповідної підсистеми менеджменту (*Microsoft Secure Software Development Life Cycle)* [12].

Критична структурна складність СПЗ DRMIS обумовлює значне зниження рівня надійності її експлуатації. Критичною до вразливості вважають структурну складність СПЗ, коли довжина вихідного тексту на мові високого рівня, досягає 20 Гб, а число логічних операторів (вузлів графа програми) може становити близько десятка мільйонів, що знаходиться далеко за рамками когнітивних спроможностей тестувальника [13]. Відомо багато прикладів, коли помилка кодування або проєктування (тобто уразливість, що не ідентифікується як навмисна) ІС воєнного призначення приводила до катастроф і критичних збитків. Крім того, наведені методи аналізу і тестування програм, за винятком експертних методів, потрапляють в зону "прокляття розмірності". Відповідно, незважаючи на удосконалення процедур тестування, число вразливостей не зменшується. Так, на сьогодні обсяг міжнародної бази вразливостей *Mitre CVE* перевищує 100 000 вразливостей, збільшується і число комп'ютерних атак, зокрема цілеспрямованих APT-атак, які використовують уразливості нульового дня, а також загальний збиток від них.

Крім того, під час проведення тестування СПЗ DRMIS необхідне врахування таких потенційних причин виникнення уразливості: відсутність доступу до вихідного коду СПЗ, недоліки проєктування, помилки програмування, ненадійні паролі, віруси та інші шкідливі програми, розширення спектру навмисних загроз, особливо в частині віддалених, прихованих і недоведених атак і загроз компрометації даних надвеликого обсягу *(Big Data)*; недостатня результативність формальних методів аналізу і тестування, за винятком експертних методів у зоні даних з великою розмірністю, використання розробниками послуг краудсорсингу, проведення відкритих конкурсів *(Bugbounty)* з виявлення уразливості

в СПЗ; протиріччями між вимогами за колаборативною сертифікацію (на основі колаборативного профілю захисту) і вимогами міжнародних стандартів; використання програмної продукції, яка пройшла сертифікацію в інших країнах; політика імпортозаміщення і обмежень з використання імпортного СПЗ; дискредитація міжнародної системи технічного та правового регулювання інформаційної та кібербезпеки.

З огляду на викладене, для удосконалення процедур тестування СПЗ DRMIS для виявлення вразливості пропонується:

упровадити єдину систему менеджменту на пост виробничих етапах життєвого циклу DRMIS;

доповнити стандартні процедури управління життєвим циклом DRMIS додатковими, які направлені на своєчасне виявлення та усунення вразливості СПЗ;

підвищити рівень технічного регулювання та оцінку відповідності у формі обов'язкової сертифікації СПЗ DRMIS з наданням доступу до вихідних текстів на етапі тестування СПЗ;

удосконалити систему тестування СПЗ через упровадження триетапної процедури та апаратних методів виявлення уразливості в режимі реального часу.

Впровадження єдиної системи менеджменту на етапі експлуатації підвищить надійність функціонування DRMIS завдяки зниженню рівня уразливості та підвищення оперативності їх виправлення.

Стандартні процедури управління життєвим циклом DRMIS [8] пропонується доповнити чотирма додатковими, які спрямовані на запобігання уразливості СПЗ (рис. 2).

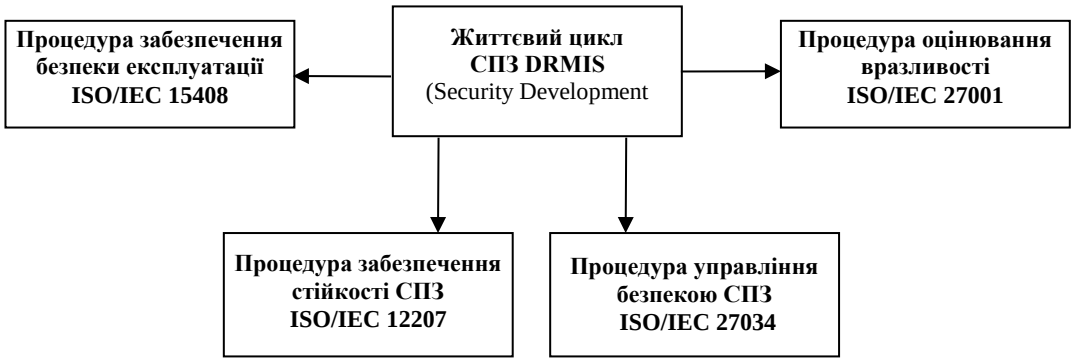

Рис. 2. Додаткові процедури тестування СПЗ DRMIS

Процедура забезпечення безпеки експлуатації встановлює загальні критерії оцінювання надійності функціонування СПЗ на основі вимог ISO/IEC 15408. Процедура оцінювання вразливості встановлює необхідні критерії (рівні) уразливості, за яких можливо введення в експлуатацію СПЗ DRMIS, базується на вимогах ISO/IEC 27001. Процедури забезпечення стійкості визначають граничні параметри, за яких СПЗ DRMIS забезпечує надійність функціонування в умовах впливу кібератак визначеної інтенсивності. Процедури управління безпекою відповідають вимогам ISO/IEC 27034 та забезпечують контроль програмних і апаратних методів тестування.

Підвищення рівня технічного регулювання та оцінки відповідності у формі обов'язкової сертифікації СПЗ DRMIS з наданням доступу до вихідних текстів на етапі тестування на сьогодні є проблемним питанням. Основною загрозою з погляду розробника є загроза крадіжки інтелектуальної власності. Водночас досвід тестування СПЗ показав, що створення автономного захищеного стенду в захищеному приміщенні або "c1ean-room" забезпечує повне виконання вимог з безпеки коду У такому приміщенні на території замовника (під контролем служби ТЗІ замовника) на період проведення тестування організовується доступ до вихідного коду програм. У межах такої процедури в закритому захищеному середовищі виконується тестування, фіксуються контрольні суми і проводяться інші необхідні процедури. Без погодження зі службою ТЗІ замовника не допускається винесення будь-якого носія інформації, ініціювання сеансу зв'язку зовні та ін. Усі документальні підтвердження проведених перевірок і висновки обговорюються і затверджуються замовником. Зазначені процедури мають низку переваг і гарантій, а саме:

дають змогу підвищити рівень надійності експлуатації DRMIS завдяки консолідації зусиль розробників і допущених фахівців лабораторії з тестування СПЗ;

виявленні уразливості будуть виправлені в межах сертифікації в обов'язковому порядку, а відомості щодо них не будуть відомі третій стороні;

перевірки абсолютно прозорі, всі дії (організація доступу, контроль і моніторинг роботи, обговорення результатів, підготовка звітних документів тощо) технічно і нормативно забезпечуються службою ТЗІ замовника;

завжди є ймовірність виявити потенційно небезпечний код (або продемонструвати його відсутність), у чому зацікавлені обидві сторони сертифікації.

Зазначений підхід прийнятий і пройшов апробацію в Агенції НАТО з підтримки та постачання, на сьогодні не зафіксовано жодного компрометуючого його випадку.

Крім того, питання відкриття доступу до вихідного коду для проведення тестування підтримується потужними розробниками програм. Так, Microsoft відкрила доступ до вихідного коду своїх програмних продуктів у понад тридцяти країнах світу.

Для удосконалення системи тестування СПЗ DRMIS пропонується впровадження три етапної процедури (рис. 3).

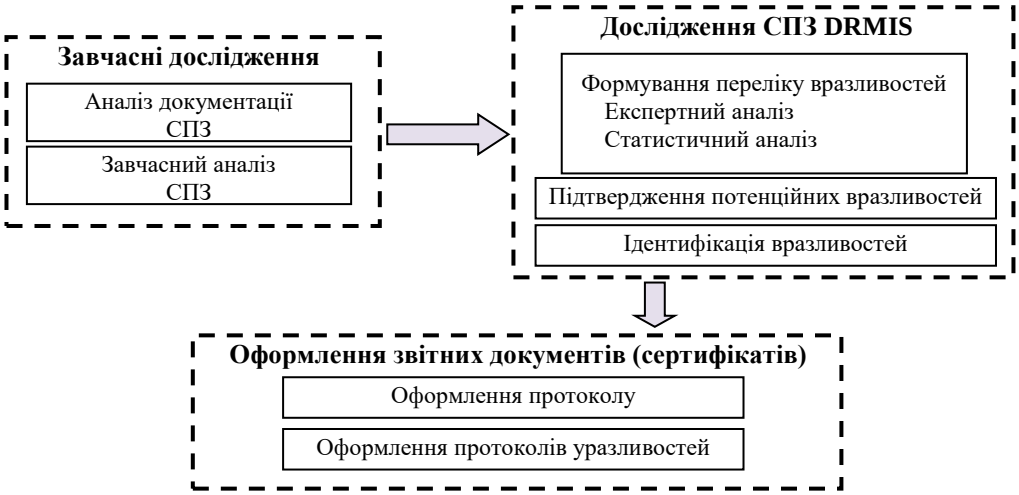

Рис. 3. Порядок тестування СПЗ DRMIS для виявлення вразливостей

Для виявлення вразливостей СПЗ у реальному часі доцільно впровадження апаратних методів [14]. Прикладами таких технологій є механізм *Stack Guard* компілятора *GCC* (внесенням збитковості на етапі виконання перевіряється стан стеку), режим безпеки GS компілятора *OCC* (внесенням збитковості на етапі виконання перевірки стану стеку), технологія процесорів *Intel Execute Disable Bit* (забороняє виконання команд у сегменті стеку та сегменті тексту), механізми безпеки *JVM* (*Java Virtual Machine*) та CLR (*Common Language Runtime*).

Висновок. Отже, представлене дослідження дає змогу вдосконалити тестування СПЗ DRMIS та підвищити надійність її експлуатації.

Надалі, за результатами експериментального тестування дослідного зразка СПЗ DRMIS планується розроблення методики тестування та виявлення вразливості СПЗ інформаційної системи управління оборонними ресурсами.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Scambray J., Shema M. Hacking exposed web applications. California : McGraw-Hill, 2002. 416c.
2. ISO/IEC TR 20004:2015. Інформаційна технологія. Методи і засоби забезпечення безпеки. Уточнений аналіз уразливості програмного забезпечення по ISO/IEC 15408 та ISO/IEC 18045.
3. Барабанов А. В., Марков А. С., Цирлов В. Л. Международная сертификация в области информационной безопасности. *Стандарты и качество*. 2016. № 7. С. 30–33
4. Шерстюк В. П. XIV научная конференция Международного исследовательского консорциума информационной безопасности // Международная жизнь. 2017. № 14. С. 42–180.
5. Марков А. С., Шеремет И. А. Теоретические аспекты сертификации средств защиты информации. *Оборонный комплекс – научно-техническому прогрессу* 2015. № 4 (128). С. 7–15.
6. Клянчин А. И. Каталог закладок АНБ (Spigel). Часть 1. Инфраструктура. Вопросы кибербезопасности. 2014. № 2 (3). С. 60–65.
7. ДСТУ ISO/IEC 27032:2016. Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT). [Чинний від 2018-01-01]. Вид. офіц. Київ, 2018.
8. Руденська Г. В. Моделі і процеси життєвого циклу інформаційної системи управління оборонними ресурсами. *Збірник наукових праць Центру воєнно-стратегічних досліджень*

Національного університету оборони України імені Івана Черняховського. Київ, 2020. № 1 (68). С. 59–65.
9. Баранов А. В., Марков А. С. Статистика выявления уязвимостей программного обеспечения при проведении сертификационных испытаний. *Вопросы кибербезопасности*, 2017. № 2 (20). С. 2–8.
10. Сиротенко А. М. Інформаційна система управління оборонним плануванням на спроможностях J-DARTS і можливості її впровадження у Збройних Силах України. *Наука і оборона*. 2018. № 4. С. 29–34.
11. Common Vulnerabilities and Exposures (CVE) – база даних загальновідомої уразливості інформаційної безпеки. URL: https://cve.mitre.org (дата звернення: 20.07.2020).
12. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 1.1-003-99 : затв. наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.1999 р. № 22. Київ : ДСТСЗІ СБ України, 1999. 30 с.
13. Основні вразливості програмного забезпечення (за версією проєкту ТОП 10 OWASP). URL: https://beasthackerz.ru/uk/skype/uyazvimost-eto-chto-takoe.html (дата звернення: 20.07.2020).
14. Левшенко О. С., Руденська Г. В. Питання воєнно-наукового супроводження створення інформаційних систем військового призначення. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. Київ, 2016. № 2 (57). С. 61–66.

Стаття надійшла до редакційної колегії 25.08.2020

Ways to improve testing of special software of the defense resource management information system at the operational stage

Annotation

With the growing role of modern information systems, the complexity of special open source software increases and the likelihood of its vulnerability increases. The exploitation of the DRMIS, which is based on open source software with vulnerability, can have such consequences as gaining access to confidential information by unauthorized users, disrupting the operating mode, and others.

The purpose of the article is to analyze testing procedures and identify vulnerabilities in open source software to increase the security level of the DRMIS operation.

Testing special open source software of the DRMIS in order to identify vulnerabilities includes three sequential stages: identifying potential vulnerability of open source software and assessing the possibility of their implementation by modeling cyber-attacks for various purposes; identification and response to incidents related to ongoing cyber-attacks; elimination of the consequences of successful cyber-attacks. With the purpose of decreasing vulnerability of the DRMIS open source software the next requirements were identified:

Low level of developer management;

Critical structural complexity of the DRMIS open source software;

Lack of access to the source code of open source software;

Design flaws, programming errors, weak passwords, viruses and other malware;

Expanding the range of intentional threats;

Insufficient effectiveness of formal methods of analysis and testing;

Use of crowdsourcing services by developers, holding open tenders to identify open source vulnerabilities;

Contradictions between the requirements for collaborative certification and the requirements of international standards;

Use of software products that have passed certification in China and Russia;

Import substitution policy and restrictions on the use of imported open source software;

Discrediting of international system of technical and legal regulation of information and cyber security.

Reliable operation of the DRMIS provides that the international system is developed for taking into account procedures that reduce the level of vulnerability. If any vulnerability of the DRMIS open source software detected it will be fixed.

Keywords: defense resource management; Information system; special software; testing; vulnerability; the likelihood of vulnerability; operational reliability; international standards; management system.