НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова праця
на правах рукопису

Кассем Халіфе

УДК 004.05 (0.43.3)

ДИСЕРТАЦІЯ

ПРОЕКТУВАННЯ ПРОГРАМНИХ ЗАСОБІВ КОМП'ЮТЕРНИХ СИСТЕМ КРИТИЧНОГО ЗАСТОСУВАННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

05. 13. 05 – Комп'ютерні системи та компоненти

Подається на здобуття
наукового ступеня кандидата технічних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

Кассем Халіфе

Науковий керівник
Семенов Сергій Геннадійович
доктор технічних наук,
старший науковий співробітник

Харків – 2018

АНОТАЦІЯ

Кассем Халіфе. Проектування програмних засобів комп'ютерних систем критичного застосування для забезпечення інформаційної безпеки. - Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук (доктора філософії) за спеціальністю 05. 13. 05 – «Комп'ютерні системи та компоненти» (123 – Комп’ютерна інженерія). - Національний технічний університет «Харківський політехнічний інститут», Харків, 2018.

Отримано теоретичне узагальнення та нове вирішення важливої науково-технічної задачі, що складається в розробці методів проектування програмних засобів комп'ютерних систем критичного застосування для забезпечення інформаційної безпеки.

Об'єкт дослідження – процес проектування програмних засобів комп'ютерних систем критичного застосування.

Предмет дослідження – методи проектування програмних засобів для забезпечення інформаційної безпеки комп'ютерних систем критичного застосування.

Проведено аналіз основних вимог до якості системного програмного забезпечення комп'ютерних систем критичного застосування показав, що в умовах підвищення інтенсивності зловмисних дій в комп'ютерних системах які використовуються в даний час методології проектування системного ПЗ, не дозволяють забезпечити необхідний рівень інформаційної безпеки. Дослідження основних підходів математичного моделювання технології управління та тестування програмного забезпечення дозволили зробити аргументований вибір напрямку математичної формалізації та обґрунтувати напрям дисертаційного дослідження.

Вперше розроблено комплекс математичних моделей технологій управління та тестування програмних засобів, який складається з GERT-моделей тестування та системи управління тест-кейсами, що враховує всі

етапи життєвого циклу багів та управління тест-кейсами. Розроблений комплекс дозволив підвищити точність результатів математичного моделювання в умовах тестування на уразливості до різного роду загроз зловмисних хакерських вторгнень та проводити попередню оцінку часових витрат одного з найбільш трудомістких процесів життєвого циклу програмного забезпечення – розробки технічної документації проекту.

Одержав подальший розвиток комплекс математичних моделей основних етапів розробки програмних засобів, який заснований на концептуальних положеннях Agile і відрізняється від відомих врахуванням показників безпечного програмування, що дозволило підвищити точність результатів моделювання.

Отримав подальший розвиток спосіб масштабування існуючої методології розробки з врахуванням вимог безпеки програмних засобів, що відрізняється від відомих, включенням і використанням в команді розробників додаткових фахівців безпеки. Це дозволить підвищити безпеку проекту і забезпечувати як швидке зростання функціоналу, так і прийнятний рівень якості сервісу.

У комплексі синтез розроблених математичних моделей етапу ініціалізації процесу розробки програмних засобів та етапу реалізації їх функціоналу, а також способу масштабування існуючої методології розробки дозволили удосконалити метод масштабування методології проектування програмних засобів з врахуванням вимог безпеки, що відрізняється від відомих можливістю управління існуючими в організації (фірмі) силами (фахівцями) як в складі команди, так і в площині фахівців суміжного напряму (фахівців безпечного програмування і тестування безпеки програмних засобів).

Удосконалено спосіб оцінки вразливості системних програмних засобів. Його відмінною рисою є врахування можливості масштабування процесу розробки програмного забезпечення шляхом впровадження фахівців безпеки (PersonNon, SecDev). За допомогою розробленого

способу оцінки уразливості системних програмних засобів доведено доцільність використання розробленого методу масштабування методології розробки системних програмних засобів з урахуванням вимог безпеки. Це дозволить знизити показник відносного збитку на всіх етапах життєвого циклу системних програмних засобів до 6 разів, в залежності від можливої тривалості атаки.

Проведено обґрунтування достовірності результатів математичного моделювання. Результати проведених експериментів показали, що для всіх досліджуваних видів даних довірча ймовірність того, що значення статистичної величини часу тестування «не відхиляється» від математичного очікування цієї характеристики більш ніж на 1 дорівнює: $P \approx 0{,}94$.

Наведено ряд практичних рекомендацій з використання методу розробки системних програмних засобів і виділені деякі недоліки (використання зовнішніх бібліотек та інструментів, створення великого виконуваного образу на диску та в пам'яті, довіра неперевіреним інструментам і т.і.). Це дозволило зробити висновок про необхідність вдосконалення існуючих методів проектування програмних засобів та можливість подальших досліджень.

Практичне значення отриманих результатів для систем критичного застосування полягає в адаптації процесу проектування програмних засобів до підвищених вимог безпеки у комп’ютерних системах, а також в можливості застосування запропонованого методу при реалізації гнучкої методології розробки програмного забезпечення.

Практична значимість отриманих результатів полягає в наступному.

1. Комплекс математичних моделей технології управління і тестування програмних засобів в сукупності з комплексом математичних моделей основних етапів розробки програмних засобів дозволили отримати аналітичні вирази для розрахунку часу безпечного програмування системних програмних засобів і вдосконалити алгоритм визначення вимог до часових характеристик. Це дало можливість в середньому на 3% підвищити точність

результатів оцінки часових характеристик.

2. Синтез основних складових методу проектування програмних засобів комп'ютерних систем критичного застосування (розроблених математичних моделей і способу масштабування) дозволив знизити показник відносного збитку на всіх етапах життєвого циклу програмного забезпечення до 6 разів, в залежності від можливої тривалості атаки.

Результати роботи впроваджені: при проведенні SCRUM-заходів компанії Line Up; при вдосконаленні програмних засобів у Державному підприємстві «Південний державний проектно-конструкторський та науково-дослідний інститут авіаційної промисловості», при вдосконаленні програмних засобів у Державному підприємстві «Харківський науково-дослідний інститут технології машинобудування», в навчальному процесі Національного технічного університету "Харківський політехнічний інститут".

Ключові слова. Проектування програмних засобів, управління та тестування програмного забезпечення, безпека програмного забезпечення.

Список публікацій здобувача

1. Халіфе К. Gert-модель прогнозування параметрів функціональної безпеки технічних систем / Кассем Халіфе, С.Г. Семенов, С.Ю. Гавриленко // Зб. наукових праць. Системи обробки інформації. – Х.: ХУ ПС, 2016. – Вип. 2(139). – С.50-52.

2. Халифе К. GERT-модель процесса безопасного тестирования программного обеспечения / Кассем Халіфе, А Є Горюшкина, В.Н. Змиевская // Зб. наукових праць. Системи обробки інформації. – Х.: ХУ ПС, 2016. – Вип. 3(140) . – С.21-24.

3. Халифе К. Модель расчета временных границ проектов разработки программного обеспечения / Г.Г. Швачич, М.И. Главчев // Системи управління, навігації та зв’язку. – Полтава.:ПНТУ ім. Ю Кондратюка, 2017. – Вип. 1(41). – С.43-49

4. Халифе К. Усовершенствованный способ масштабирования гибкой методологии разработки программного обеспечения / Кассем Халифе, С. Семенов, М. Захарченко // Сучасні інформаційні системи. – Х.: НТУ «ХПІ», 2017. – Вип 1 (1). С. 79-84

5. Халифе К. Способ оценки уязвимости системного программного обеспечения / Кассем Халифе, Г.Я. Криховецький, Г.А. Кучук // Системи управління, навігації та зв'язку. – Полтава.:ПНТУ ім. Ю Кондратюка, 2017. – Вип. 4(44). – С.141-144

6. Халифе К. Анализ и исследование моделей и методов разработки системного программного обеспечения / Кассем Халифе, Т.Н.Шипова // Системи управління, навігації та зв'язку. – Полтава.:ПНТУ ім. Ю Кондратюка, 2017. – Вип. 5(45). – С.60-65

7. Халифе К. Комплекс математичних моделей процесу розробки програмного забезпечення / Кассем Халифе, С.Г. Семенов // Інформаційні технології та комп'ютерна інженерія. – В.: ВНТУ, 2017. – №2. – С. 14-20

8. Khalife Kassem Development of Gert model of management system by using test cases / Kassem Khalife, S. G. Semenov, V N. Zmiyevskaya // Journal of Qafqaz university-mathematics and computer science 2016. – Vol.(4). – № 1. – С. 52-59

9. Халифе К. Метод прогнозирования временных затрат на отдельные этапы разработки программного обеспечения / К. Халифе, С.Г. Семенов // Матеріали IV Міжн. НТК «Проблеми інформатизації» Черкаси-Баку-Бельсько-Бяла-Полтава, 2016. – С. 39.

10. Халифе К. Усовершенствованный метод масштабирования методологии разработки программного обеспечения с учетом требований безопасности / К. Халифе, С.Г. Семенов, И.В. Рубан // Матеріали II НПК «Проблеми науково-практичного та правового забезпечення кібербезпеки у сучасному світі» Харків-Київ-Дніпро- Баку-Бельсько-Бяла, 2017. – С.10.

11. Халифе К. Метод масштабирования методологии разработки программного обеспечения с учетом требований безопасности / Кассем Халифе,

С.Г. Семенов, А.С. Семенова // Матеріали 17 Міжнародної НПК «Проблеми інформатики і моделювання». – Х: НТУ «ХПІ», 2017. – С. 7.

12. Халифе К. Масштабирование гибкой методологии разработки программного обеспечения с учетом требований безопасности / Кассем Халифе, С.Г. Семенов, В.Н. Змиевская // Матеріали 6 Міжнародної НПК «Методи та засоби кодування, захисту й ущільнення інформації». – В: ВНТУ, 2017. – С. 81.

13. Халифе К. Комплекс математичних моделей технологии управления и тестирования программного обеспечения / Кассем Халифе, С.Г. Семенов // Матеріали 5 Міжнародної НТК «Проблеми інформатизації». – Ч: ЧДТУ, 2017. – С. 51.

14. Халифе К. Спосіб оцінки вразливості системного програмного забезпечення / Кассем Халіфе, С.Г. Семенов, В.Н. Зміївська // Матеріали Всеукраїнської НПК «Актуальні питання протидії кіберзлочинності та торгівлі людьми». – Х: ХНУВС, 2017. – С. 149-151.

SUMMARY

Kassem Khalifa Designing software tools for critical computer applications to provide information security. - Qualifying scientific work on the rights of manuscripts.

Dissertation for the degree of a candidate of technical sciences (doctor of philosophy), specialty 05. 13. 05 - "Computer systems and components" (123 - Computer engineering). - National Technical University "Kharkiv Polytechnic Institute", Kharkiv, 2018.

A theoretical synthesis and a new solution of an important scientific and technical problem, which consists in the development of methods for designing software tools of computer systems of critical application for providing information security, is obtained.

The object of research is the process of designing software tools for critical systems.

Subject of research - methods of designing software to provide information security of computer systems critical applications.

Analysis of the basic requirements of quality system software computer systems critical application showed that in terms of increasing the intensity of misconduct in computer systems that are currently used system software design methodology, does not allow for the required level of information security.

Research of the basic approaches of mathematical modeling of technology of management and software testing allowed to make an argumentated choice of the direction of mathematical formalization and to substantiate the direction of the dissertation research.

For the first time developed a set of mathematical models of technology management and testing software, which consists of GERT-model testing and control system test cases, taking into account all stages of the life cycle management of bugs and test cases.

Designed complex allowed to improve the accuracy of the results of mathematical modeling in terms of testing for vulnerability to various threats and malicious hacker intrusion conduct a preliminary assessment of time-consuming one of the most labor-intensive processes of software life cycle - development of design documentation.

He received further developed complex mathematical models of the main stages of software development, which is based on the conceptual provisions Agile differs from known secure coding parameters into account, thus improving the accuracy of simulation results. There has been further development of a way to scale up the existing development methodology, taking into account the security requirements of software, which differs from the known, inclusion and use in the team of developers of additional security professionals. This will increase the security of the project and provide both a rapid growth of the functional and an acceptable level of quality of service.

The complex synthesis developed mathematical models step initialization process of software development and implementation phase of functionality and scaling methods existing development methodology allowed to improve the method of scaling methodology for designing software with regard to safety requirements, which differs from the known ability to control existing in the organization (company) forces (specialists) as a part of the team, and in the area of specialists of the adjacent direction (experts in safe programming and testing wares of software). Improved method for evaluating vulnerabilities in system software. Its distinctive feature is taking into account the possibility of scaling the software development process by introducing security experts (PersonNon, SecDev).

With the help of the developed method of estimating the vulnerability of system software, the feasibility of using the developed method of scaling the methodology of developing system software with the consideration of security requirements has been proved. This will reduce the relative loss index for all stages of the life cycle of system software up to 6 times, depending on the possible

duration of the attack. The validity of the results of mathematical modeling has been substantiated.

The results of the conducted experiments showed that for all investigated types of data, the probability that the value of the statistical value of the test time "does not deviate" from the mathematical expectation of this characteristic is more than 1 is: $P \approx 0{,}94$

An number of practical recommendations on the use of method development system software and dedicated some drawbacks (use of external libraries and tools to create a large executable image on disk and in memory, trust untested tools, etc.). This made it possible to conclude that there is a need to improve the existing methods of designing software and the possibility of further research.The practical value of the results obtained for critical applications systems is to adapt the design of software to the increased security requirements in computer systems, as well as the possibility of using the proposed method in implementing a flexible software development methodology.

The practical significance of the results obtained is as follows.

1. Complex of mathematical models of technology of control and testing of software in conjunction with the complex of mathematical models of the main stages of software development allowed to obtain analytical expressions for calculating the time of safe programming of system software and to improve the algorithm for determining requirements for time characteristics. This allowed an average of 3% to improve the accuracy of the results of the time characteristics.

2. Synthesis of the main components of the method of designing software tools for critical applications (developed mathematical models and the method of scaling) allowed to reduce the relative loss index at all stages of the software life cycle up to 6 times, depending on the possible duration of the attack.

The results of the work are implemented: during the conduct of SCRUM-measures of the company Line Up; with the improvement of software at the State Enterprise "Southern State Design and Research Institute of Aviation Industry", with the improvement of software tools at the State Enterprise "Kharkiv Research

Institute of Mechanical Engineering", in the educational process of the National Technical University "Kharkiv Polytechnic Institute".

Keywords. Software design, software management and testing, software security.

List of publisher publications

1. Khalife K. Gert-model′ prohnozuvannya parametriv funktsional′noyi bezpeky tekhnichnykh system / Kassem Khalife, S.H. Semenov, S.YU. Havrylenko // Zb. naukovykh prats′. Systemy obrobky informatsiyi. – KH.: KHU PS, 2016. – Vyp. 2(139). – S.50-52.

2. Khalife K. GERT-model′ protsessa bezopasnoho testyrovanyya prohrammnoho obespechenyya / Kassem Khalife, A YE Horyushkyna, V.N. Zmyevskaya // Zb. naukovykh prats′. Systemy obrobky informatsiyi. – KH.: KHU PS, 2016. – Vyp. 3(140) . – S.21-24.

3. Khalife K. Model′ rascheta vremennykh hranyts proektov razrabotky prohrammnoho obespechenyya / Kassem Khalife, H.H. Shvachych, M.Y. Hlavchev // Systemy upravlinnya, navihatsiyi ta zv″yazku. – Poltava.:PNTU im. YU Kondratyuka, 2017. – Vyp. 1(41). – S.43-49

4. Khalife K. Usovershenstvovannyy sposob masshtabyrovanyya hybkoy metodolohyy razrabotky prohrammnoho obespechenyya / Kassem Khalife, S. Semenov, M. Zakharchenko // Suchasni informatsiyni systemy. – KH.: NTU «KHPI», 2017. – Vyp 1 (1). S. 79-84

5. Khalife K. Sposob otsenky uyazvymosty systemnoho prohrammnoho obespechenyya / Kassem Khalife, H.YA. Krykhovets′kyy, H.A. Kuchuk // Systemy upravlinnya, navihatsiyi ta zv″yazku. – Poltava.:PNTU im. YU Kondratyuka, 2017. – Vyp. 4(44). – S.141-144

6. Khalife K. Analyz y yssledovanye modeley y metodov razrabotky systemnoho prohrammnoho obespechenyya / Kassem Khalife, T.N.Shypova // Systemy upravlinnya, navihatsiyi ta zv″yazku. – Poltava.:PNTU im. YU Kondratyuka, 2017. – Vyp. 5(45). – S.60-65

7. Khalife K. Kompleks matematychnykh modeley protsesu rozrobky prohramnoho zabezpechennya / Kassem Khalife, S.H. Semenov // Informatsiyni tekhnolohiyi ta komp″yuterna inzheneriya. – V.: VNTU, 2017. – №2. – S. 14-20

8. Khalife Kassem Development of Gert model of management system by using test cases / Kassem Khalife, S. G. Semenov, V N. Zmiyevskaya // Journal of Qafqaz university-mathematics and computer science 2016. – Vol.(4). – № 1. – C. 52-59

9. Khalife K. Metod prognozirovaniya vremennykh zatrat na otdel'nyye etapy razrabotki programmnogo obespecheniya / K. Khalife, S.G. Semenov // Materíali IV Mízhn. NTK «Problemi ínformatizatsíí» Cherkasi-Baku-Bel's'ko-Byala-Poltava, 2016. – S. 39.

10. Khalife K. Usovershenstvovannyy metod masshtabyrovanyya metodolohyy razrabotky prohrammnoho obespechenyya s uchetom trebovanyy bezopasnosty / K. Khalife, S.G. Semenov, Y.V. Ruban // Materialy II NPK «Problemy naukovo-praktychnoho ta pravovoho zabezpechennya kiberbezpeky u suchasnomu sviti» Kharkiv-Kyyiv-Dnipro- Baku-Bel′s′ko-Byala, 2017. – S.10.

11. Khalife K. Metod masshtabyrovanyya metodolohyy razrabotky prohrammnoho obespechenyya s uchetom trebovanyy bezopasnosty / Kassem Khalife, S.G. Semenov, A.S. Semenova // Materialy 17 Mizhnarodnoyi NPK «Problemy informatyky i modelyuvannya». – KH: NTU «KHPI», 2017. – S. 7.

12. Khalife K. Masshtabyrovanye hybkoy metodolohyy razrabotky prohrammnoho obespechenyya s uchetom trebovanyy bezopasnosty / Kassem Khalife, S.G. Semenov, V.N. Zmyevskaya // Materialy 6 Mizhnarodnoyi NPK «Metody ta zasoby koduvannya, zakhystu y ushchil′nennya informatsiyi». – V: VNTU, 2017. – S. 81.

13. Khalife K. Kompleks matematychnykh modeley tekhnolohyy upravlenyya y testyrovanyya prohrammnoho obespechenyya / Kassem Khalife, S.G. Semenov // Materialy 5 Mizhnarodnoyi NTK «Problemy informatyzatsiyi». – CH: CHDTU, 2017. – S. 51.

14. Khalife K. Sposib otsinky vrazlyvosti systemnoho prohramnoho zabezpechennya / Kassem Khalife, S.G. Semenov, V.N. Zmiyivs′ka // Materialy Vseukrayins′koyi NPK «Aktual′ni pytannya protydiyi kiberzlochynnosti ta torhivli lyud′my». – KH: KHNUVS, 2017. – S. 149-151.

ЗМІСТ