Удальцов К.Р. Искусство тестирования программного обеспечения: методы и подходы к созданию надежных тестов// Международный журнал информационных технологий и энергоэффективности.– 2024. – Т. 9 № 6(44) с. 11–15

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.052

ИСКУССТВО ТЕСТИРОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ: МЕТОДЫ И ПОДХОДЫ К СОЗДАНИЮ НАДЕЖНЫХ ТЕСТОВ

Удальцов К.Р.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: 2003.06.10kr@gmail.com

В данной статье рассматривается важность и методы создания надежных тестов программного обеспечения. Описываются методы черного ящика, такие как тестирование эквивалентных классов и тестирование граничных значений, а также методы белого ящика, включая тестирование покрытия кода и тестирование путей выполнения. Автоматизированное тестирование рассматривается как эффективный способ повышения надежности и ускорения процесса тестирования. В заключение подчеркивается важность планирования и организации тестирования, анализа результатов и составления отчетов для обеспечения качества программного обеспечения.

Ключевые слова: Тестирование программного обеспечения, надежные тесты, черный ящик, белый ящик, тестирование эквивалентных классов, тестирование граничных значений, тестирование покрытия кода, тестирование путей выполнения, автоматизированное тестирование, планирование тестирования, анализ результатов, отчеты о тестировании.

THE ART OF SOFTWARE TESTING: METHODS AND APPROACHES TO CREATING RELIABLE TESTS

Udaltsov K.R.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: 2003.06.10kr@gmail.com

This article discusses the importance and methods of creating reliable software tests. Black box methods such as equivalent class testing and boundary value testing are described, as well as white box methods including code coverage testing and execution path testing. Automated testing is considered as an effective way to increase reliability and speed up the testing process. In conclusion, the importance of planning and organizing testing, analyzing results, and compiling reports to ensure software quality is emphasized.

Keywords: Software testing, reliable tests, black box, white box, equivalent class testing, boundary value testing, code coverage testing, execution path testing, automated testing, test planning, results analysis, test reports.

Введение

Тестирование программного обеспечения является неотъемлемой частью разработки программных продуктов. Это процесс, который позволяет выявить ошибки и дефекты в программе, а также убедиться в ее соответствии требованиям и ожиданиям пользователей. Качество тестирования напрямую влияет на качество и надежность программного

обеспечения. В данной статье рассматриваются различные методы и подходы к созданию надежных тестов, которые помогут повысить эффективность и эффективность тестирования.

1. Методы черного ящика

Методы черного ящика основаны на анализе программы без учета ее внутренней структуры. [1] Этот подход позволяет проверить функциональность программы, не зная о ее внутренней реализации. Вот некоторые методы черного ящика:

- Тестирование эквивалентных классов

Этот метод основан на разделении возможных входных данных на эквивалентные классы, которые должны вести себя одинаково. Затем выбираются представители каждого класса для тестирования. Это позволяет сократить количество тестов, сохраняя при этом покрытие различных сценариев.

- Тестирование граничных значений

Метод тестирования граничных значений заключается в проверке программы на предельных значениях входных данных. Это позволяет выявить ошибки, которые могут возникнуть при обработке крайних случаев. Например, если программа должна обрабатывать числа от 1 до 100, то тестирование граничных значений включает проверку для 1, 100 и значений рядом с ними.

2. Методы белого ящика

Методы белого ящика основаны на анализе внутренней структуры программы. Этот подход позволяет проверить правильность работы программы на основе ее кода и алгоритмов. [2] Вот некоторые методы белого ящика:

- Тестирование покрытия кода

Этот метод основан на измерении покрытия кода тестами. Цель состоит в том, чтобы проверить, насколько хорошо тесты охватывают код программы. Популярные метрики покрытия кода включают покрытие строк, покрытие ветвей и покрытие условий.

- Тестирование путей выполнения

Этот метод направлен на проверку всех возможных путей выполнения в программе. Пути выполнения представляют собой последовательности операций и условий, которые могут быть выполнены программой. Тестирование путей выполнения позволяет выявить ошибки, связанные с неправильной логикой программы или недостаточным покрытием различных сценариев.

3. Автоматизированное тестирование

Автоматизированное тестирование является методом, который использует программные инструменты и скрипты для выполнения тестов. Это позволяет повторно использовать тесты, ускоряет процесс тестирования и уменьшает вероятность человеческих ошибок. [3] Автоматизированное тестирование может быть применено как к методам черного ящика, так и к методам белого ящика.

Планирование и организация тестирования

Эффективное тестирование программного обеспечения требует хорошо спланированного и организованного подхода. Вот некоторые важные аспекты планирования и организации тестирования:

*Определение целей тестирования**:*** Первым шагом является определение целей тестирования. Что именно вы хотите проверить и какие аспекты программы требуют особого внимания? Цели тестирования могут включать проверку функциональности, производительности, безопасности и других аспектов программы.

Создание тестовых планов и сценариев: На основе целей тестирования необходимо разработать тестовые планы и сценарии. Тестовый план описывает общую стратегию тестирования, включая ресурсы, расписание и ожидаемые результаты. Сценарии тестирования представляют собой конкретные шаги и данные, которые будут использованы для тестирования программы.

Выбор подходящих методов тестирования: Исходя из целей тестирования и характеристик программы, выберите подходящие методы тестирования. Комбинируйте методы черного ящика и белого ящика, используйте тестирование граничных значений и тестирование покрытия кода в зависимости от требований проекта.

Использование автоматизированного тестирования: В случае, если это возможно, рекомендуется использовать автоматизированное тестирование. Это позволяет повторно использовать тесты, автоматизировать выполнение тестовых сценариев и ускорить процесс тестирования. Существуют различные инструменты и фреймворки для автоматизации тестирования, которые могут быть адаптированы под ваши потребности.

Управление тестовыми данными: Тестирование требует разнообразных тестовых данных, которые должны быть правильно управляемыми. Создайте наборы тестовых данных, которые покрывают различные сценарии и граничные случаи. Обратите внимание на конфиденциальность и безопасность данных, особенно если ваши тестовые данные содержат конфиденциальную информацию.

*Анализ и отчетность результатов**:*** После выполнения тестов необходимо проанализировать результаты и составить отчеты. Зафиксируйте найденные ошибки и дефекты, оцените покрытие кода и выполнение тестовых сценариев. Отчеты о тестировании помогут команде разработки понять текущее состояние программы и принять меры для устранения проблем.

Заключение:

Создание надежных тестов программного обеспечения - это сложный и ответственный процесс, который требует внимательного планирования и организации. Комбинация методов черного ящика и белого ящика, таких как тестирование эквивалентных классов, тестирование граничных значений, тестирование покрытия кода и тестирование путей выполнения, позволяет достичь более полного покрытия различных аспектов программы.

Список литературы

1. Красов А. В. и др. Способы коммутации пакетов в сетях CISCO//Материалы Всероссийской научно-практической конференции" Национальная безопасность России: актуальные аспекты" ГНИИ" Нацразвитие". Июль 2018. – 2018. – С. 31-35.
2. Красов А. В. и др. Программная реализация средств предотвращений вторжений и аномалий сетевой инфраструктуры.
3. Сахаров Д. В. и др. Использование математических методов прогнозирования для оценки нагрузки на вычислительную мощность IOT-сети//Научно-аналитический

журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». – 2020. – №. 2. – С. 86-94.
4. Гельфанд А. М. Способы выбора стегоконтейнеров для передачи данных//Региональная информатика и информационная безопасность. – 2020. – С. 260-262.
5. Волкогонов В. Н. и др. Анализ безопасности wi-fi сетей//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 270-275.
6. Бударный Г. С. и др. Разновидности нарушений безопасности и типовые атаки на операционную систему//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 406-411.
7. Небаева К. А. Разработка необнаруживаемых стегосистем для каналов с шумом //СПб.: СПбГУТ. – 2014. – Т. 176.
8. Ахрамеева К. А. и др. Анализ средств обмена скрытыми данными злоумышленниками в сети интернет посредством методов стеганографии //Телекоммуникации. – 2020. – №. 8. – С. 14-20.
9. Березина Е. О., Виткова Л. А., Ахрамеева К. А. Классификация угроз информационной безопасности в сетях IOT//Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 2. – С. 11-18.
10. Бирих Э. В., Ферапонтова С. С. К вопросу об аудите персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). – 2018. – С. 111-114.
11. Бирих Э. В. и др. Исследование вопросов повышения уровня защищенности органов исполнительной власти //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). – 2018. – С. 107-110.

References

1. Krasov A. V. et al. Methods of Packet Switching in CISCO Networks // Proceedings of the All-Russian Scientific and Practical Conference "National Security of Russia: Actual Aspects" of the State Research Institute "National Development". July 2018. – 2018. p. 31-35.
2. Krasov, A. V., et al. Software Implementation of Intrusion and Anomaly Prevention Tools for Network Infrastructure.
3. Sakharov, D. V., et al. Ispol'zovanie matematicheskikh metody prognozirovanii dlya otsenki naload na vychuchutel'nuyu vozdushnosti IOT-neti [Use of mathematical methods of forecasting for assessing the load on the computing power of the IOT network]. – 2020. – №. 2. p. 86-94.
4. Gelfand A. M. Methods of Choosing Stegocontainers for Data Transfer//Regional Informatics and Information Security. – 2020. p. 260-262.
5. Volkogonov V. N. et al. Analysis of the security of wi-fi networks // Actual problems of infotelecommunications in science and education (APINO 2019). – 2019. p. 270-275.
6. Budarny, G. S., et al. Varieties of Security Violations and Typical Attacks on the Operating System//Actual Problems of Infotelecommunications in Science and Education (APINO, 2022). – 2022. p. 406-411.
7. Nebaeva K. A. Development of undetectable stegosystems for channels with noise. – 2014. – T. 176.

8. Akhrameeva K. A. et al. Analysis of the means of exchanging hidden data by intruders on the Internet through steganography methods. – 2020. – №. 8. p. 14-20.
9. Berezina E. O., Vitkova L. A., Akhrameeva K. A. Classification of Information Security Threats in IOT Networks. Series 1: Natural and Technical Sciences. – 2020. – №. 2. p. 11-18.
10. Birikh E. V., Ferapontova S. S. On the Issue of Personal Data Audit//Actual Problems of Infotelecommunications in Science and Education (APINO 2018). – 2018. p. 111-114.
11. Birikh E. V. et al. Issledovanie voprosy povysheniya urovannosti zashchnosti organov executive vlasti [Study of issues of increasing the level of protection of executive authorities]//Aktual'nye problemy infotelekomtelekomatsii v nauke i obrazovaniya (APINO, 2018). – 2018. p. 107-110.