

МОДЕЛЬ ТЕСТУВАННЯ ЗАСТОСУНКІВ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ

Браїла І. В., Дяченко В. О., Міхаль О. П.

Харківський національний університет радіоелектроніки, Харків, Україна

Потреба в комплексному та систематизованому багатогранному підході до тестування застосунків для мобільних пристроїв зростає разом із тим, як мобільні застосунки стають ще більш складними.

Метою доповіді є аналіз моделей тестування застосунків для мобільних пристроїв.

Проведено огляд методів тестування програмного забезпечення на метарівні. Для цього дослідження цільовою мобільною платформою була обрана Apple iOS. Досліджено аспекти, які впливають на функціональне тестування застосунків iOS зокрема та мобільних – загалом. У роботі також розкриваються можливості безпеки, якими часто нехтують при виході на ринок. Також розглянуті інструменти автоматизації тестування мобільного інтерфейсу користувача. Особлива увага приділена можливостям та обмеженням Apple UIAutomation. Ще одним важливим питанням, яке розглянуто, була тактика тестування застосунків.

Тактика тестування може відрізнитися залежно від фази проекту та інших мінливих обставин середовища. Вона повинна відповідати стратегії тестування.

Таким чином, тактика часто обирається в статичних межах шкал впливу. Для виконання цілей мікротестування слід обрати відповідні підходи, методи та прийоми тестування, які мають бути відображені в плані тестування. Тестові артефакти (наприклад, тестові приклади, набори тестів, матриця відстеження, тестові дані тощо), які будуть створені в процесі тестування, також повинні бути зазначені в плані тестування. Проведено структурування методів тестування за підходами чорного та білого ящиків [1]. Межі підходу до тестування сірого ящика є досить неоднозначними, а методи та прийоми цього підходу ще формально не описані в теорії тестування. Останнім розглянутим питанням є безпека застосунків.

Механізмами забезпечення безпеки є використання захищених мережевих протоколів, шифрування бази даних і блокування даних програми. Іншою частиною функціонального тестування безпеки є перевірка та усунення залишків розробки та тестування в продуктивній збірці програми. Прикладами залишків є файли налаштувань і код, який зчитує їх або виконує дію на основі значення налаштування.

Список літератури

1. Луиза Тамре. Введение в тестирование программного обеспечения / Вильямс, 2018. 600 с.