Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК_____

Каленик

Кристина Геннадьевна

Методы защиты информационной системы нечёткого описания спецификации

АВТОРЕФЕРАТ

на соискание степени магистра технических наук

по специальности 1-98 80 01 Методы и системы защиты,

информационная безопасность

Научный руководитель

Новиков В.И.

Кандидат т.н., доцент

Минск, 2015

ВВЕДЕНИЕ

Ввиду высокой интеграции информационных технологий во всех приложениях приходится все больше полагаться на надежность программных и аппаратных средств. Некорректная работа программного обеспечения может стать причиной многих проблем, таких как нарушение информационной безопасности, финансовые потери, потери ресурсов (клиентов, времени) и даже привести к травмам и летальному исходу.

Тестирование представляет собой один из возможных способ оценки качества программного обеспечения в терминах найденных дефектов. В соответствии со стандартом ISO 9126 принято следующее определение тестирования.

Тестирование – это наблюдение за функционированием ПО в специфических условиях с целью определения степени соответствия ПО требованиям к нему.

При переходе к современным методологиям разработки ПО тестирование ориентируется в первую очередь на оценку качества с помощью следующих методов:

- проверка соответствия требованиям, указанным в техническом задании;
- проверка выполнения основных предположений и требований на конкретных примерах;
- выявление и документирование дефектов качества;
- составление общих рекомендаций относительно качества.

Сегодня тестирование рассматривается как деятельность, которую необходимо проводить на протяжении всего процесса разработки и сопровождения и является важной частью конструирования программных продуктов. Действительно, планирование тестирования должно начинаться на ранних стадиях работы с требованиями, необходимо систематически и

постоянно развивать и уточнять планы тестов и соответствующие процедуры тестирования. Даже сами по себе сценарии тестирования оказываются очень полезными для тех, кто занимается проектированием, позволяя выделять те аспекты требований, которые могут неоднозначно интерпретироваться или даже быть противоречивыми.

Должным образом разработанная модель тестирования уменьшает общий уровень риска в системе. Для принятия решения о достаточном объеме тестирования необходимо принимать во внимание не только проектные ограничения, но и уровень рисков.

Процесс тестирование состоит не только из выполнения различных вариантов использования, но и из планирования, управления, выбора тестовых условий, проектирования и разработки тестовых сценариев, проверка результатов выполнения, оценки критериев выхода, составление отчетов и анализ полученных данных.

Работы по проектированию модели тестирования на раннем этапе жизненного цикла программного обеспечения могут предотвратить попадание дефекта в код.

Основными задачами анализа и проектирования тестов являются:

- Рецензирование базиса тестирования и оценка его тестируемости.
- Расстановка приоритетов тестирования.
- Определение необходимых условий тестирования.
- Определение и установка необходимой инфраструктуры и инструментов.
- Установление соответствия между базисом тестирования и тестовыми сценариями.

Так как проектные ограничения играют существенную роль в определении объемов тестирования, при проектировании модели тестирования необходимо четко расставлять приоритеты тестирования тех или иных областей.

В зависимости от вида тестирования приоритеты могут быть расставлены различным образом; при этом следует определить критические, важные, средние и маловажные области. После определения областей необходимо выполнить детализацию, т.е. определить конкретные варианты использования (тестовые сценарии) функционала той или иной области.

Для сложных систем при условии нечеткого описания спецификации даже в одной выделенной области количество тестовых сценариев, как правило, достаточно велико и для их наилучшей организации необходимо прибегать к вероятностному анализу.

В таких условиях оценка параметров СЗИ должна вычисляться с использованием не одной математической модели, а согласованного семейства моделей, адаптивно конструирующихся одна из другой и, таким образом, непрерывно совершенствующихся на основе оптимального выбора исходных данных.

При разработке оптимальных методов защиты исходными должны явиться следующие два положения:

– выбор математически продуктивного критерия оптимальности в соответствии с архитектурой системы защиты и технологией обработки информации в ИС;

– четкая математическая формулировка задачи, учитывающая все априорные сведения и позволяющая решить ее в соответствии с принятым критерием.

В процессе создания оптимального метода защиты ИС неизбежно возникает задача коррекции требований к системе защиты. Трудность ее решения заключается в том, что возникают неопределенности не стохастического характера, определяемые:

– наличием целенаправленного противодействия со стороны противоборствующей системы, способы действий которой неизвестны исследователю;

– недостаточной изученностью некоторых явлений, сопровождавших процесс функционирования систем защиты;

– нечетким представлением цели операции, приводящей к неоднозначной трактовке соответствия реального результата операции требуемому.

Целью данной работой является разработка методов тестирования и защиты информационных систем в условиях нечёткого описания спецификаций.

Для достижения этой цели в рамках работы решаются следующие задачи:

1. Проведение анализа стратегий тестирования и защиты информационных систем в условиях нечёткого описания спецификаций.
2. Изучение методологии сбора и анализа требований при формулировании спецификации.
3. Изучение методов формализации требований.
4. Создание методов тестирования и защиты информационной системы.
5. Сформулировать выводы и определить пути дальнейших исследований.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Целью данной работы является разработка методов тестирования и защиты информационных систем в условиях нечёткого описания спецификаций. Для достижения этой цели в рамках работы решаются следующие задачи:

1. Проведение анализа стратегий тестирования и защиты информационных систем в условиях нечёткого описания спецификаций.
2. Изучение методологии сбора и анализа требований при формулировании спецификации.
3. Изучение методов формализации требований.
4. Создание методов тестирования и защиты информационной системы.
5. Сформулировать выводы и определить пути дальнейших исследований.

Моделирование процесса тестирования, на сегодняшний день, является неотъемлемой частью проектирования и тестирования сложных систем. Должным образом разработанная модель тестирования уменьшает общий уровень риска в системе. Трудность исследования вопросов обеспечения безопасности информационных технологий усугубляется большой неопределённостью требований к ИС. Теоретические основы построения оптимальных систем защиты исключительно сложны и, несмотря на интенсивность исследований в этой предметной области, ещё далеки от совершенства. Некорректная работа программного обеспечения может стать причиной многих проблем, таких как финансовые потери, потери ресурсов (клиентов, времени) и даже привести к травмам и летальному исходу.

В рамках исследовательской работы разработан и применен алгоритм построения модели тестирования, а также на примерах рассмотрены методы выбора рационального варианта защиты системы на основе экспертной информации.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Общий объем магистерской диссертации составляет 87 страниц, включая 10 иллюстраций, 4 таблицы, библиографический список из 27 наименований, 8 приложения. Работа состоит из общей характеристики, введения, пяти глав, заключения и приложений.

Во введении отмечены актуальность темы исследования, цель и задачи дипломной работы.

В первой главе рассматриваются подходы и стратегии тестирования информационных систем: аналитические, методические, динамические, эвристические, регрессионные и подходы, основанные на моделях.

Вторая глава посвящается одному из самых важных этапов в разработке программного продукта – сбору и анализу бизнес требований. Выделены наиболее важные этапы сбора бизнес требований. Приведены методы и подходы к детализации и анализу уже собранных требований, систематизации и избавления от дублируемых данных, детализированию составленного списка требований.

Третья глава описывает формализацию требований с использованием модели взаимодействия с пользователем, диаграмм вариантов использования (UML) и применением прототипов.

Указаны основные пункты технического задания по проекту. Описано применение диаграммы активности, конечных автоматов, диаграммы последовательностей и их текстовых аналогов для описания сложных потоков выполнения.

В четвёртой главе описывается создание метода тестирования ИС на основании сбора и анализа требований. Для построения модели тестирования, основанной на требованиях, приведено выделение критических функции, определение цикломатической сложности, оценка вероятности возникновения ошибок в ветвях программного продукта.

Для иллюстрации плана и графика работ по рассматриваемому проекту были разработаны две диаграммы Ганта: план тестирования программного продукта на основе анализа требований и критический путь проведения тестов.

В последней, пятой главе, разобраны существующие методы решения многокритериальных задач для выбора рационального варианта защиты ИС в условиях нечётко описанной спецификации. Всё множество методов было разделено на три группы:

- метод главного показателя;
- метод результирующего показателя;
- лексикографические методы.

Были описаны методы выбора варианта защиты ИС при разных условиях соотношения важности требований:

- при равной важности собранных требований;
- при различной важности собранных требований.

Дополнительно был рассмотрен выбор варианта защиты ИС нечёткого описания спецификации по аддитивному критерию и лексикографическим методом.

В заключении даны общие выводы по работе и предложения. Приведён список работ, опубликованных по теме магистерской диссертации.

ЗАКЛЮЧЕНИЕ

Тестирование, сбор, анализ и формализация требований – неотъемлемые этапы разработки надёжного программного продукта. В зависимости от выбранной методологии управления проектом эти этапы имеют ту или форму, содержание и продолжительность относительно друг друга. Однако, какая бы методология не применялась – очевидна тесная связь и зависимость всех этапов создания ПО.

В процессе работы над данной темой были изучены основные подходы, применяемые для выбора стратегии тестировании, отмечены достоинства и недостатки каждого из подходов и сделан вывод о необходимости интеграции подходов основанных на рисках и требованиях. Изучены методы и подходы к сбору и анализу требований, рассмотрены принципы и инструменты их формализации. Были сделаны выводы о причинах важности этого этапа при подготовке к реализации ПО и возможных способах упорядочивания собранных артефактов. Достигнута цель, поставленная для данной работы, а именно - разработка методов тестирования и защиты информационных систем в условиях нечёткого описания спецификаций.

Определена методология выявления критических функций для построения критического пути тестирования. На основе построенного графа функций была вычислена величина цикломатической сложности критического пути тестирования. Проведена вероятностная оценка возникновения ошибки в ветвях. На основании полученных результатов было выполнено постарение диаграммы Ганта процесса тестирования. Рассмотрены методы выбора варианта рациональной защиты ИС.

Оценка параметров защиты в условиях высокой степени неопределённости условий должны вычисляться с использованием не одной математической модели, а согласованного семейства моделей, адаптивно конструирующихся одна из другой и, таким образом, непрерывно совершенствующихся на основе оптимального выбора исходных данных.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

По теме магистерской диссертации были опубликованы следующие работы:

1. Использование электронной цифровой подписи для защиты сообщений / К.Г. Каленик // Материалы XVIII Международной научно-практической конференции «Современные средства связи»: тезисы доклада – Минск: ВГКС, 15-16 октября 2013, – С. 198-199.

2. SQL-инъекции: методы проверки и защиты ресурса / В.И. Новиков, К.Г. Каленик // Материалы XIX Международной научно-практической конференции «Современные средства связи»: тезисы доклада – Минск: ВГКС, 14-15 октября 2014, – С. 173-175.

3. Выбор стратегии тестирования на ранних этапах разработки в условиях нечёткой спецификации / В.И. Новиков, К.Г. Каленик // Материалы XIX Международной научно-практической конференции «Современные средства связи»: тезисы доклада – Минск: ВГКС, 14-15 октября 2014, – С. 175-176.

4. Межсайтовая атака с внедрением сценария / В.И. Новиков, К.Г. Каленик // Материалы 51-й научной конференции аспирантов, магистрантов и студентов «Телекоммуникационные системы и сети»: тезисы доклада – Минск: БГУИР, 13-17 апреля 2015, – С36

5. Модель тестирования в условиях нечеткого описания спецификаций / К.Г. Каленик. // Материалы XIII Белорусско-Российской научно-технической конференции «Технические средства защиты информации»: тезисы доклада – Минск: БГУИР, 4-5 июня 2015, – С. 67.