ОТЗЫВ

официального оппонента доктора технических наук, доцента ФКОУ ВПО Воронежский институт ФСИН России Душкина Александра Викторовича на диссертацию Вялых Александра Сергеевича «Модели и алгоритмы анализа и прогнозирования надежности использования программного обеспечения информационных систем в условиях конфликтных взаимодействий», представленную на соискание ученой степени кандидата технических наук по специальности 05.13.17 – «Теоретические основы информатики»

Актуальность темы

Задачи анализа и прогнозирования надежности использования программного обеспечения имеют большое значение для организации стабильного функционирования информационных систем, использующихся во всех областях человеческой жизнедеятельности. В то же время, существующие алгоритмы и модели оценки надежности программного обеспечения информационных систем не в полной мере учитывают факторы, влияющие на работоспособность информационных систем в условиях конфликтных взаимодействий.

Большинство из существующих моделей оценки надежности программного обеспечения, рассматривая динамику появления и устранения ошибок в программном обеспечении, не выделяют ошибки, за счет которых возможно осуществление преднамеренного негативного воздействия. Они не рассматривают такой важный параметр уязвимости, как наличие информации о ее существовании и характеристиках. Если уязвимость неизвестна, то ей нельзя воспользоваться для негативного воздействия, в то время как любая другая ошибка в программном обеспечении, даже не будучи известной, может привести к нарушениям в его работе. В соответствии с такими моделями при устранении ошибок из программного обеспечения его надежность должна возрастать. Однако, на практике в условиях конфликтных взаимодействий с ростом времени эксплуатации программного обеспечения его надежность, как правило, падает, так как с ростом срока эксплуатации программы и соответственно ее популярности увеличивается средняя скорость открытия в ней новых уязвимостей, в то время как средняя скорость их устранения может оставаться неизменной и при окончании поддержки программного продукта разработчиками снижается до нуля.

В силу изложенного, тема диссертационной работы Вялых А.С., направленная на разработку моделей и алгоритмов анализа и прогнозирования надежности использования программного обеспечения в условиях конфликтных взаимодействий, является актуальной.

Степень обоснованности научных положений, выводов и рекомендаций

Полученные в диссертации теоретические и практические результаты и выводы обоснованы с позиций методологии исследования, основанной на корректном использовании взаимно дополняющих друг друга теоретических и экспериментальных (имитационное моделирование, обработка данных реальной статистики уязвимостей программного обеспечения) методов исследований.

Общая оценка работы

Диссертация состоит из введения, четырех разделов, заключения и списка литературы, включающего 94 наименования. Объем диссертации составляет 167 страниц, включая 157 страниц основного текста и 10 страниц списка литературы.

В первой главе диссертации дается общая характеристика условий функционирования современных информационных систем и технологий в условиях преднамеренных негативных воздействий, определяются наиболее важные факторы, влияющие на надежность использования ПО в ИС в условиях конфликтных взаимодействий, а также основные требования к алгоритмам и моделям анализа надежности использования ПО в ИС в данных условиях и проводится анализ современных подходов к оценке надежности использования ПО в ИС на предмет учета данных факторов и требований. На основе полученных результатов разрабатывается технологическая схема построения моделей и алгоритмов анализа и прогнозирования надежности использования ПО в ИС в условиях внутренних уязвимостей (дефектов) и преднамеренных негативных воздействий.

Во второй главе дается описание разработанного нейросетевого алгоритма прогнозирования интенсивности обнаружения уязвимостей (дефектов) в ПО, обосновывается преимущество его прогностических способностей над существующими аналитическими моделями обнаружения уязвимостей, описываются разработанные математическая модель динамики уязвимостей (дефектов) в ПО, а также математические модели функционирования

информационной системы в условиях конфликтных взаимодействий. Приводится общий алгоритм анализа вероятностных характеристик надежности использования ПО в ИС без учета характера негативных воздействий, основанный на ранее полученном нейросетевом алгоритме прогноза интенсивности обнаружения уязвимостей в ИС и математических моделях динамики уязвимостей в ПО и функционирования ИС в целом.

В третьей главе описываются разработанные объектно-ориентированные модели конфликтного взаимодействия ИС и источника негативных воздействий, использующие аппарат языка UML, математические модели конфликтного взаимодействия ИС и ИНВ на основе цепей Маркова и компьютерные имитационные модели конфликтного взаимодействия ИС и ИНВ, реализованные в интегрированной среде Matlab+Simulink+Stateflow, а также общий алгоритм анализа вероятностных характеристик надежности использования ПО в ИС в условиях преднамеренных негативных воздействий, использующий данные модели и результаты, полученные во 2-й главе.

Четвертая глава посвящена практическому применению результатов диссертационной работы, а именно, в ней на основе предложенных моделей и алгоритмов оценки надежности ПО выполнены исследования для базовых элементов типовой ИС удостоверяющего центра и типовой ИС пользователя удостоверяющего центра и предложены рекомендации для повышения их надежности.

Оценка новизны и достоверности результатов

Научные результаты, представленные Вялых А.С. в диссертационной работе, являются новыми.

Научная новизна диссертационного исследования заключается в следующем:

1. Рассмотрены вопросы прогнозирования интенсивности обнаружения новых уязвимостей в программном обеспечении. Предложен новый двухэтапный алгоритм, позволяющий в среднем увеличить точность прогноза на 10%. Повышение точности было достигнуто за счет использования в качестве априорного решения при сглаживании и интерполяции исходных данных (первый этап алгоритма) уже существующих аналитических моделей обнаружения уязвимостей, а при прогнозировании (второй этап алгоритма) – комитета нейронных сетей, обученных на уже обработанных данных.

2. Разработаны модели динамики открытия и устранения уязвимостей в отдельных программах и в программном обеспечении информационной системы в целом. Данные модели основаны на применении теории массового обслуживания и позволяют учесть зависимость скорости открытия новых уязвимостей от времени (то есть в полной мере использовать существующую статистику и возможности прогноза), скорость выпуска разработчиками обновлений программного обеспечения, уровень работы системного администратора по устранению уязвимостей из программного обеспечения (установки обновлений и разработки собственных решений), а также наличие в информационной системе средств защиты информации. Эти модели могут использоваться как отдельно для оценки надежности использования программного обеспечения информационной системы в условиях конфликтных взаимодействий, так и для расчета среднего числа известных уязвимостей в каждой отдельной программе и в информационной системе в целом за определенные промежутки времени, что может быть применено в более сложных моделях, учитывающих особенности конкретного негативного воздействия.

3. Предложены математические модели конфликта информационной системы и источника (группы источников) негативных воздействий, основанные на применении цепей Маркова. Данные модели учитывают среднее число известных уязвимостей в системе за время конфликта, наличие в информационной системе средств защиты информации, этапы негативного воздействия, априорные знания источника негативного воздействия об информационной системе и его способности (категорию). Данные модели вместе с моделями динамики уязвимостей в программном обеспечении информационных систем позволяют для конечных вычислений использовать статистические данные, опубликованные в открытых источниках, и прогноз, основанный на этих данных.

4. Разработаны компьютерные имитационные модели конфликта информационной системы и источника (группы источников) негативных воздействий, использующие формализм гибридных автоматов (карты Харела). Преимущества данных моделей перед математическими заключаются в том, что они учитывают зависимость среднего числа известных уязвимостей в информационной системе от времени, допускают произвольный характер переходов между состояниями сторон конфликта и позволяют рассматривать

конфликтные ситуации с любыми вариантами отношений между источниками негативных воздействий.

Достоверность научных положений, выдвинутых в работе, подтверждается их понятной физической трактовкой, результатами применения взаимно дополняющих теоретических и экспериментальных методов исследования, их согласованностью, совпадением в ряде случаев с известными результатами. В работе автор использовал аппарат теории вероятностей и математической статистики, модели и методы теории систем массового обслуживания, математический аппарат цепей Маркова, аппарат искусственных нейронных сетей, а также технологии компьютерного имитационного моделирования.

Основные результаты работы представлены, обсуждены и опубликованы в виде тезисов на 7 Международных научно-практических конференциях

По теме диссертационного исследования автором опубликовано 11 работ, в том числе 4 статьи в изданиях, рекомендованных ВАК при Минобрнауки России.

Текст диссертации, несмотря на незначительные стилистические погрешности, изложен логично, грамотным языком. Ссылки на литературные источники, которыми пользовался автор, приведены корректно.

Автореферат диссертации соответствует основным положениям диссертации и в полной мере отражает решённые автором задачи, методологию исследования и полученные результаты.

Теоретическая и практическая значимость работы

Теоретическая значимость диссертации заключается в том, что разработанные модели и алгоритмы могут служить основой для будущих исследований в области надежности использования программного обеспечения. На их основе могут быть разработаны новые модели и алгоритмы, более подробно учитывающие специфику построения оцениваемой информационной системы и возможные действия конфликтующих сторон. Кроме того, с помощью данных моделей и алгоритмов может быть теоретически оценено влияние различных факторов на работоспособность информационных систем.

Практическая значимость диссертации определяется возможностью использования предложенных моделей и алгоритмов для оценки надежности информационных систем различных частных компаний и государственных

учреждений, для планирования разработчиками программного обеспечения распределения ресурсов между созданием новых программ и поддержкой старых, совершенствования методологии аттестации информационных систем и сертификации программного обеспечения.

Результаты работы целесообразно использовать в организациях, требующих передачи большого объема информационных потоков.

Недостатки диссертации

1. Диссертация переполнена аббревиатурами, в том числе не являющимися общепринятыми. Это затрудняет понимание диссертации. Целесообразно было бы включить в диссертацию список использованных аббревиатур.

2. Первая глава диссертации содержит, наряду с информацией, непосредственно относящейся к существу диссертационного исследования, и явно лишнюю информацию, которую можно убрать без ущерба для понимания диссертации. Такой лишней информацией является, например, описание рынков уязвимостей, так как в дальнейшем соискатель не проводит экономических исследований.

3. В разработанных моделях не определена требуемая точность учитываемых исходных данных и ее влияние на конечный результат.

4. В диссертационной работе недостаточно подробно описаны ограничения классических подходов к определению надежности использования программного обеспечения информационных систем в условиях конфликтных взаимодействий.

5. В работе отсутствуют детальные пояснения по исходной статистике и критериям, положенным в основу выбора параметров источника негативного воздействия.

6. Формула (2.15) на стр. 63 диссертации верна только в том случае, когда отсутствие уязвимостей в СЗИ и отсутствие уязвимостей в остальном ПО, установленном в ИС, являются независимыми случайными событиями. Данное утверждение неочевидно, так как теоретически возможна ситуация, когда какие-либо уязвимости в СЗИ могут быть родственны каким-либо уязвимостям в остальном ПО. Но соискатель вообще не приводит обоснования верности формулы (2.15).

7. В таблице 2.11 на стр. 65 диссертации приводятся значения средней вероятности надежности ИС за 12 лет, вычисленные по формулам (2.14) и (2.15). Но эти формулы предназначены для расчета вероятности надежности ИС в заданный момент времени, а не для расчета средней вероятности надёжности ИС за заданный промежуток времени.

8. На стр. 84 диссертации вводится формула (3.14). На той же странице написано, что вероятность нахождения ИС в надежном состоянии на n-м шаге конфликта находится по этой формуле, но в этой формуле n вообще не фигурирует. Далее на той же странице написано: «Вероятность нахождения ИС в надежном состоянии за все время конфликта будет равна среднему арифметическому между вероятностями нахождения ИС в надежном состоянии на каждом шаге конфликта», после чего приводится формула (3.15), в которой осуществляется не суммирование по шагам n конфликта, а интегрирование по времени t.

9. Диссертационная работа содержит умеренное количество опечаток и стилистических неточностей.

Заключение

Отмеченные недостатки не снижают научной ценности и общей положительной оценки оппонируемой работы.

Диссертационная работа Вялых Александра Сергеевича является завершённой научно-квалификационной работой, в которой на основании выполненного автором исследования, решена актуальная научная задача, имеющая существенное значение в области оценки надежности использования программного обеспечения

Диссертация соответствует специальности 05.13.17 – «Теоретические основы информатики» по следующим областям исследований:

- п. 2 – разработка и анализ моделей информационных процессов и структур;

- п. 11 – разработка методов обеспечения высоконадежной обработки информации и обеспечения помехоустойчивости информационных коммуникаций для целей передачи, хранения и защиты информации; разработка основ теории надежности и безопасности использования информационных технологий.

Диссертационная работа Вялых А.С. «Модели и алгоритмы анализа и прогнозирования надежности использования программного обеспечения информационных систем в условиях конфликтных взаимодействий» соответствует требованиям пункта 9 «Положения о порядке присуждения учёных степеней и присвоения учёных званий» ВАК при Минобрнауки России, предъявляемым к диссертационным работам.

В целом диссертация обладает научной новизной, практической и теоретической значимостью, соответствует критериям, установленным в «Положения о порядке присуждения учёных степеней и присвоения учёных званий» ВАК при Минобрнауки России, а потому её автор, Вялых Александр Сергеевич, заслуживает присуждения учёной степени кандидата технических наук по научной специальности 05.13.17 – «Теоретические основы информатики».

Официальный оппонент
начальник кафедры управления и информационно-технического обеспечения
ФКОУ ВПО Воронежский институт ФСИН России
доктор технических наук, доцент
Александр Викторович Душкин
«3» 06 2014 года

Адрес: 394072, г. Воронеж, ул. Иркутская 1а.
Тел. (473) 260-68-19
e-mail: a_dushkin@mail.ru

Подпись Душкина А.В. заверяю.
Начальник отдела кадров и работы с личным составом
ФКОУ ВПО Воронежский институт ФСИН России
А.А. Шкуменов