Экз.№1

УТВЕРЖДАЮ

Начальник 4 Центрального
научно-исследовательского института
Министерства обороны
Российской Федерации

Таразевич С.Е.

«29» 05 2014г.

ОТЗЫВ

ведущей организации

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»

Интенсивное развитие индустрии разработки программного обеспечения и его приложения в различных отраслях человеческой жизнедеятельности обусловливает актуальность исследований по проблемам оценивания влияния программного обеспечения (ПО) на надежность информационных систем (ИС), в которых оно применено. Названное свойство в значительной мере зависит от наличия в программных продуктах особого класса дефектов (уязвимостей), которые могут быть использованы для реализации негативных воздействий на ИС с целью нарушить их работоспособность. В рецензируемой работе отмечается, что в научной литературе недостаточно полно исследованы модели функционирования ИС, которые учитывали бы процесс появления и устранения уязвимостей в применяемом ПО. При решении задачи оценки надежности использования ПО специалисты преимущественно рассматривали динамику ошибок (дефектов) в ПО, но не ставили вопрос о том, каким образом данные ошибки могут проявиться в условиях внешних негативных

воздействий. Так, в работах, в той или иной степени затрагивающих данный вопрос, возможности использования внешних негативных воздействий с целью нарушить работоспособность программного обеспечения ИС оцениваются без учёта влияния интенсивности открытия новых уязвимостей, оперативности их нейтрализации, продолжительности процессов подготовки и реализации негативного воздействия. Добавим, что существующие методики применяют в основном экспертные методы оценивания, а это снижает доверие к получаемым результатам. Диссертационная работа Вялых А.С. в известной мере лишена отмеченных недостатков, направлена на разработку моделей и алгоритмов анализа и прогнозирования надежности применения программного обеспечения информационных систем, учитывает особенности их функционирования в условиях внешних негативных воздействий и представляется актуальной.

Тема диссертации непосредственно связана с научно-исследовательскими и опытно-конструкторскими работами, выполняемыми в высших учебных заведениях и научно-исследовательских организациях РФ.

Диссертационная работа содержит введение, четыре главы основного текста, заключение и список литературы. Во введении обоснована актуальность работы, ясно сформулированы цель и задачи исследования, научная новизна и практическая значимость работы.

Новизна основных научных результаты работы определяется следующим.

1. Разработан двухэтапный нейросетевой алгоритм прогнозирования интенсивности обнаружения уязвимостей программного обеспечения, отличающийся тем, что на первом этапе в нем используется специальная процедура интерполяции экспериментальных данных в виде разложения по радиально-базисным функциям с нахождением коэффициентов разложения на основе использования метода регуляризации, что дает возможность учета в качестве априорного решения аналитических моделей обнаружения уязвимостей, а на втором этапе – процедуры прогнозирования на основе комитета, состоящего из нескольких нейронных сетей (многослойных персептронов), обученных по интерполированным данным. В качестве априорного решения при проведении регуляризации предложено использовать зависимости, получаемые на основе аналитических моделей обнаружения уязвимостей (логистическая модель Алхазми-Малаийа или линейная модель

Рескорлы). На основе данного алгоритма проведены исследования качества прогноза динамики обнаружения уязвимостей (дефектов ПО) для операционных систем семейства Windows и показано преимущество предложенного решения перед известными.

2. Предложены математические модели и общий алгоритм оценки надежности использования ПО, базирующиеся на прогнозировании изменения интенсивности появления уязвимостей и представлении процесса выявления и устранения уязвимостей в ПО как процесса функционирования системы массового обслуживания. Основное отличие этих моделей состоит в том, что 1) на единой методической основе обеспечивается учет зависимостей интенсивности обнаружения уязвимостей от времени, оперативности «закрытия» уязвимостей, определяемых характером действий производителя ПО и администратора ИС, а также 2)в расчетах применяются конкретные статистические данные, опубликованные в открытых источниках.

3. Разработаны объектно-ориентированные и математические модели оценки надежности использования программного обеспечения информационных систем в условиях конфликтных взаимодействий, основанные на представлении процессов негативного воздействия и «закрытия» уязвимостей ПО в виде цепи Маркова с непрерывным временем, отличающиеся учетом динамики обнаружения и устранения уязвимостей и основных этапов воздействия внешнего источника негативного воздействия в дуэльных ситуациях.

4. Предложены компьютерные имитационные модели использования ПО информационных систем, отличающиеся использованием карт состояний Харела, что позволяет рассматривать ситуации конфликтного взаимодействия без ограничений на характер законов распределения времени переходов между состояниями ПО информационной системы и для произвольного числа участников конфликта. Это позволило на единой методической основе рассматривать различные варианты конфликтных взаимодействий ИС и источника негативных воздействий. Источником негативного воздействия может быть злоумышленник или независимый тестировщик системы, а также пользователь, совершающий ошибки в процессе работы системы или действующий в нештатном режиме.

Приведенные в работе выводы следует признать научно обоснованными. Их обоснованность и достоверность подтверждается 1)применением взаимно дополняющих, друг друга теоретических и экспериментальных методов исследований, 2)совпадением результатов, полученных различными методами, 3)наглядной физической трактовкой результатов оценки надежности эксплуатируемых ИС. Солидные публикации в научной печати и материалах международных и всероссийских конференций подтверждают корректность выводов и правильность полученных в диссертации результатов.

При проведении исследований автор показал уверенное владение теорией массового обслуживания, математическим аппаратом цепей Маркова, аппаратом применения искусственных нейронных сетей, а также технологиями компьютерного имитационного моделирования.

Теоретическая и практическая ценность диссертации определяется возможностью применения развитого в диссертации методического аппарата для научных исследований в области надежности и безопасности применения программного обеспечения в информационных системах, учитывающих динамику конфликтных взаимодействий с различными внешними источниками. Полученные модели и алгоритмы обработки информации могут быть применены при анализе и прогнозировании надежности использования программного обеспечения в современных информационных системах, а также при разработке теоретических и практических рекомендаций проектировщикам перспективных систем.

В частности, пользователи информационных систем смогут выявить «слабые места» в политике обеспечения надежности ИС, а разработчики ПО - оценить надежность применения их продуктов, более рационально распределить свои ресурсы при поддержке эксплуатируемого и разработке нового ПО. Организации, осуществляющие аттестацию информационных систем и сертификацию программного обеспечения, смогут точнее оценить реальные процессы функционирования информационных систем в условиях конфликтных взаимодействий и выработать на основе разработанных моделей и алгоритмов новую методологию, более полно учитывающую данные процессы.

Реализация результатов диссертации и рекомендации по их дальнейшему использованию. Результаты, полученные в диссертации, реализованы в департаменте связи и массовых коммуникаций Воронежской области при оценке надежности работы удостоверяющего центра правительства Воронежской области, а также в Воронежском государственном университете при выполнении исследований по гранту РФФИ в рамках научного проекта № 13-01-97507 р_центр_а.

В дальнейшем, результаты, полученные в диссертации, целесообразно использовать в организациях, занимающихся научными и прикладными исследованиями в области надежности программного обеспечения и информационных систем, а также разработкой моделей и алгоритмов оценки надежности программного обеспечения, таких как Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Военно-космическая академия им. А.Ф. Можайского, Институт проблем информатики РАН, Институт программных систем им. А.К. Айламазяна РАН, Институт систем информатики им. А.П. Ершова СО РАН, а также в организациях - заказчиках информационных систем.

Результаты работы целесообразно использовать в учебном процессе подготовки бакалавров, магистров и специалистов соответствующих специальностей и направлений в Воронежском государственном университете и других вузах.

Следует отметить достаточно полную апробацию основных результатов диссертационной работы и достаточный уровень публикаций. По теме диссертации опубликовано 11 научных работ, причем 4 из них – в журналах, рекомендованных ВАК для публикации результатов диссертационных работ.

Автореферат также достаточно полно отражает содержание диссертационной работы.

По диссертации необходимо сделать следующие замечания:

1. Сравнение нейросетевого алгоритма прогноза обнаружения уязвимостей и аналитических моделей обнаружения уязвимостей проведено только по операционным системам семейства Windows, тогда как для более

полных оценок необходимо рассмотреть данные по другим операционным системам, а также по различным видам программного обеспечения.

2. В модели динамики уязвимостей в программном обеспечении не учитывается возможность обнаружение уязвимостей, которые впоследствии не устраняются разработчиками программного обеспечения и системными администраторами. В этих случаях результаты оценок при использовании разработанных моделей окажутся не в полной мере достоверными.

3. Автор дал ссылки на источники статистики по уязвимостям программного обеспечения, но не раскрыл в диссертации механизм, при помощи которого он вычисляет количество уязвимостей, обнаруженных в программе за месяц, и среднее время устранения уязвимости из программы.

4. Не рассмотрен вариант действия системного администратора, при котором дефекты программного обеспечения не устраняются, а проводится его замена на другое аналогичного назначения.

5. В диссертационной работе рассмотрен только один из вариантов стратегии поведения источника негативных воздействий. Однако источник негативных воздействий может не ограничиться нахождением одной уязвимости в программном обеспечении информационной системы, а постарается найти их как можно больше, с тем чтобы по очереди пытаться использовать каждую.

6. Автор предложил качественную порядковую шкалу оценивания действий системного администратора ИС. «Деления» такой шкалы представляют собой словесные характеристики действий последнего. Последующая «арифметизация» качественной шкалы, т.е. переход к количественной оценочной шкале, не обосновывается.

7. Введённое автором словосочетание «вероятность надёжности» представляется неудачным.

Сделанные замечания не отменяют общую положительную оценку работы.

Вывод. Диссертация Вялых А.С. является законченной научно-квалификационной работой, содержит новые результаты в области исследования надежности использования программного обеспечения и удовлетворяет требованиям ВАК, предъявляемым к кандидатским диссертациям. Автор диссертации, Вялых Александр Сергеевич, заслуживает

присуждения ученой степени кандидата технических наук по специальности 05.13.17 – «Теоретические основы информатики».

Диссертация и отзыв рассмотрены на научно-техническом семинаре управления 4 ЦНИИ Минобороны России, протокол №5 от 19.05.14г.

Главный научный сотрудник управления
4 Центрального научно-исследовательского
института Министерства обороны
Российской Федерации
кандидат технических наук,
доцент Половников Алексей Юрьевич

Старший научный сотрудник
4 Центрального научно-исследовательского
института Министерства обороны
Российской Федерации
кандидат технических наук,
старший научный сотрудник Живов Анатолий Дмитриевич

Научный сотрудник
4 Центрального научно-исследовательского
института Министерства обороны
Российской Федерации
кандидат технических наук Зорин Виктор Игоревич

Подписи Половникова А.Ю., Живова А.Д. и Зорина В.И. заверяю.

Секретарь учёного совета
4 Центрального научно-исследовательского
института Министерства обороны
Российской Федерации
кандидат технических наук,
старший научный сотрудник Бордюков Михаил Михайлович

«29» мая 2014г.

Адрес: 141090, Московская обл., г. Юбилейный, ул. Тихонравова, д.29.
Тел.: 8 495 515 0155, 8 495 515 1188. Факс: 8 495 515 8285.