На правах рукописи

Вялых Александр Сергеевич

МОДЕЛИ И АЛГОРИТМЫ АНАЛИЗА И ПРОГНОЗИРОВАНИЯ НАДЕЖНОСТИ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ В УСЛОВИЯХ КОНФЛИКТНЫХ ВЗАИМОДЕЙСТВИЙ

Специальность 05.13.17 – «Теоретические основы информатики»

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

кандидата технических наук

Воронеж – 2014

Работа выполнена в ФГБОУ ВПО «Воронежский государственный университет»

Научный руководитель:	доктор технических наук, профессор Сирота Александр Анатольевич
Официальные оппоненты:	Душкин Александр Викторович, доктор технических наук, доцент, Воронежский институт ФСИН России, начальник кафедры управления и информационно-технического обеспечения
	Толстых Николай Николаевич, доктор технических наук, профессор, ОАО «Концерн «Созвездие», начальник службы
Ведущая организация:	Научно-исследовательский центр ракетно-космических систем «4 ЦНИИ Минобороны России»

Защита состоится «25» июня 2014 г. в 17 часов на заседании диссертационного совета Д 212.038.24 при ФГБОУ ВПО «Воронежский государственный университет» по адресу: 394006, г. Воронеж, Университетская пл., 1, ауд. 226.

С диссертацией можно ознакомиться в библиотеке и на сайте ФГБОУ ВПО «Воронежский государственный университет», http://www.science.vsu.ru.

Автореферат разослан «___» мая 2014 г.

Ученый секретарь
диссертационного совета  Воронина Ирина Евгеньевна

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Усложнение процессов, реализуемых в современных информационных структурах и системах (ИС), развитие используемых в них информационных технологий требуют новых подходов к анализу и прогнозированию надежности использования программного обеспечения (ПО). Под надежностью использования ПО ИС в работе понимается сохранение работоспособности ИС и всех выполняемых ПО функций в условиях наличия внутренних дефектов (ошибок программного обеспечения). При этом в данной работе рассматриваются классы дефектов, наличие которых может быть использовано внешними источниками и привести к отказам в работе ИС, т.е., в конечном счете, оказать влияние на ее надежность. Такие дефекты в данной работе определяются как уязвимости ПО, использование которых приводит к нарушению доступности и/или целостности информации. Попытка источника негативных воздействий (ИНВ), используя подобные дефекты, воздействовать на ИС с одной стороны, а ИС противостоять данной попытке с другой, рассматривается как конфликтное взаимодействие.

Количество уязвимостей, обнаруживаемых в ПО, с каждым годом возрастает. Возрастает также время их устранения, растет число эксплойтов (программ, использующих их для негативного воздействия на ИС). Соответственно, возрастают совокупные материальные, репутационные и иные потери. В связи с этим повышаются требования к степени обоснованности оценок надежности использования ПО, что в свою очередь, предполагает решение научной задачи разработки адекватных моделей и методов оценки надежности использования ПО в ИС, имеющих внутренние дефекты (уязвимости) и функционирующих в условиях конфликтных взаимодействий. Разработка данных методов ведется уже достаточно давно, в том числе, в работах И.И. Застрожнова, В.В. Липаева, А.Ю. Щеглова, O.H. Alhazmi, S. Frei, Y.K. Malaiya, J.D. Musa, A. Ozment, M.L. Shooman. Тем не менее, подходы, существующие на данный момент, обладают рядом недостатков и ограничений. Подходы, используемые в государственном регулировании вопросов надежности использования информационных технологий в рамках действующих систем на территории Российской Федерации, не учитывают как динамику уязвимостей в информационных системах, так и динамику преднамеренного негативного воздействия (НВ) на информационные системы. Те же подходы (не закрепленные в государственных нормативных документах), которые учитывают данные динамические процессы, моделируют их без учета ряда важных факторов (например, жизненного цикла уязвимостей ПО и различных возможностей их использования сторонами в процессе развития конфликта), которые проявляются именно в условиях конфликтного взаимодействия. В связи с этим, с одной стороны, остается открытым вопрос об оценке параметров, характеризующих эти процессы, то есть не ясно, каким образом с помощью этих подходов численно оценить надежность конкретных использования информационных технологий и систем, а, с другой стороны, не ясно, насколько данные методы адекватны практике реальных ситуаций.

В качестве универсальной синтетической методологии исследований в сфере надежности информационных систем и технологий целесообразно рассматривать методы математического и компьютерного моделирования динамики изменения состояний информационных процессов и систем, опирающиеся на концептуальные модели конфликтных взаимодействий и позволяющие учитывать все наиболее значимые факторы таких взаимодействий.

Таким образом, тема диссертации, посвященная разработке моделей и алгоритмов анализа и прогнозирования надежности использования программного обеспечения информационных систем в условиях конфликтных взаимодействий, представляется актуальной.

Тема входит в план научно-исследовательских работ ВГУ по кафедре технологий обработки и защиты информации и непосредственно связана с научным на-

правлением Воронежского государственного университета «Математическое моделирование, программное и информационное обеспечение, методы вычислительной и прикладной математики и их применение к фундаментальным и прикладным исследованиям в естественных науках».

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

- разработка и анализ моделей информационных процессов и структур (п. 2 паспорта специальности);

- 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 (п. 11 паспорта специальности).

Объектом исследования выступают динамические процессы, влияющие на надежность использования ПО в ИС: процесс динамики выявления и устранения уязвимостей в ИС и процесс конфликтного взаимодействия ИС и источника негативных воздействий.

Предметом исследования является математическое и алгоритмическое обес-печение моделирования процессов, влияющих на надежность использования ПО в ИС, и оценки данных характеристик.

Цель и задачи исследования. Целью исследования является повышение степени обоснованности оценки надежности использования программного обеспечения информационных систем в условиях конфликтных взаимодействий. Для достижения цели в работе рассматриваются и решаются следующие задачи:

1. Анализ наиболее важных факторов, влияющих на надежность использования ПО в ИС, определение основных требований к разрабатываемым алгоритмам и моделям анализа надежности использования ПО в ИС в условиях конфликтных взаимодействий, анализ современных подходов к оценке надежности использования ПО в ИС на предмет учета данных факторов и требований.

2. Разработка моделей функционирования информационных структур и систем при наличии внутренних уязвимостей, влияющих на надежность использования ПО.

3. Разработка алгоритмов и моделей оценки надежности использования ПО в ИС в условиях конфликтных взаимодействий, учитывающих наиболее важные факторы и соответствующих основным требованиям, определенным в ходе анализа.

Методы проведения исследования. При решении поставленных в диссертации задач использовались модели и методы теории массового обслуживания, математический аппарат цепей Маркова, аппарат искусственных нейронных сетей, а также технологии компьютерного имитационного моделирования.

Основные результаты, выносимые на защиту, и их научная новизна. На защиту выносятся следующие результаты, впервые достаточно подробно развитые или полученные в диссертации:

1. Двухэтапный нейросетевой алгоритм статистического анализа и прогнозирования нестационарных временных последовательностей, используемый для оценки динамики обнаружения дефектов (уязвимостей) программного обеспечения.

2. Математические модели динамики изменения состояний программного обеспечения с учетом возможных уязвимостей и общий алгоритм оценки надежности использования программного обеспечения.

3. Объектно-ориентированные и математические модели оценки надежности использования программного обеспечения информационных систем в динамике конфликтного взаимодействия.

4. Компьютерные имитационные модели использования программного обеспечения информационных систем в динамике конфликтного взаимодействия с коалицией внешних источников.

Научная новизна полученных результатов определяется следующим:

1. Разработанный двухэтапный нейросетевой алгоритм статистического анализа и прогнозирования нестационарных временных последовательностей, используемый для оценки интенсивности обнаружения уязвимостей ПО, отличается применением на первом этапе специальной процедуры интерполяции экспериментальных данных в виде разложения по радиально-базисным функциям с нахождением коэффициентов разложения с использованием метода регуляризации, а на втором этапе – процедуры прогнозирования на основе комитета нейронных сетей (многослойных персептронов), обученных по интерполированным данным.

2. Предложенные математические модели и общий алгоритм оценки надежности использования ПО, основанные на представлении процесса появления и устранения уязвимостей как процесса функционирования системы массового обслуживания, отличаются учетом зависимостей интенсивности обнаружения уязвимостей от времени, полученных по данным прогноза, учетом временных характеристик закрытия уязвимостей, а также характера действий производителя ПО и администратора информационной системы и реальных данных, которые могут быть получены из открытых источников.

3. Разработанные объектно-ориентированные и математические модели оценки надежности использования ПО информационных систем в условиях конфликтного взаимодействия в виде цепи Маркова с непрерывным временем, отличаются введением пространства состояний, учитывающих динамику обнаружения и закрытия уязвимостей и основные этапы организации негативного воздействия в дуэльных ситуациях, что позволяет повысить обоснованность оценки надежности использования программного обеспечения информационных систем в условиях конфликтных взаимодействий.

4. Предложенные компьютерные имитационные модели использования программного обеспечения информационных систем отличаются использованием формализма гибридных автоматов (карт состояний Харела) для исследования ситуативных изменений в динамике конфликтного взаимодействия, позволяют рассматривать ситуации без ограничений на характер распределения времени переходов между состояниями ПО информационной системы и для произвольной коалиции источников внешних воздействий, что дает возможность оценки надежности использования программного обеспечения в ситуациях конфликтного взаимодействия любого вида.

Достоверность результатов работы. Результаты исследований, сформулированные в диссертации, получены на основе корректного использования взаимно дополняющих друг друга теоретических и экспериментальных (имитационное моделирование, обработка данных реальной статистики уязвимостей программного обеспечения) методов исследований. Их достоверность также определяется совпадением результатов, полученных различными методами, между собой, а, в ряде частных случаев, с известными, наглядной физической трактовкой установленных закономерностей и соотношений.

Теоретическая и практическая значимость работы. Теоретическая значимость работы определяется тем, что полученные модели и алгоритмы отвечают потребностям важного направления – развития методов анализа и прогноза надежности использования программного обеспечения информационных систем в условиях конфликтных взаимодействий. Одним из достоинств разработанных моделей и алгоритмов является их достаточно простая адаптация к новым вариантам конфликтных ситуаций, а также к более глубокому учету процессов функционирования информационных систем. Следовательно, данные модели и алгоритмы могут быть использованы как основа для последующих исследований в области надежности использования программного обеспечения информационных структур и систем различного типа.

Практическая значимость диссертации заключается в том, что разработаны алгоритмы и реализующее их программное обеспечение, позволяющие: сформировать рекомендации в политике обеспечения надежности использования программного обеспечения реальных информационных структур и систем; оценить материальные и иные риски, которым может подвергнуться информационные структуры и системы, а также выработать предложения по их уменьшению; более рационально распределить финансовые и иные ресурсы при поддержке существующего и разработке нового программного обеспечения.

Реализация научных результатов. Полученные в диссертации результаты 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.

Личный вклад автора. Основные результаты по теме диссертации получены лично автором. В совместных работах соавторам принадлежит постановка задачи и определение направления исследований, автору – проведение рассуждений, необходимых для решения поставленных задач, разработка концептуальных, математических и имитационных моделей информационных процессов, обоснование и разработка алгоритмов анализа данных, вывод формул для оценки вероятностных характеристик надежности информационных технологий, а также анализ и интерпретация полученных результатов.

Публикации. По теме диссертации опубликовано 11 работ, из них 4 работы – в изданиях, рекомендованных ВАК для публикации результатов диссертационных работ.

Апробация работы. Основные положения диссертационной работы докладывались и обсуждались: на XII, XIII, XIV Международных научно-технических конференциях «Кибернетика и высокие технологии XXI века» (Воронеж) в 2011, 2012 и 2013 годах; на XI, XII, XIII Международных конференциях «Информатика: проблемы, методология, технологии» (Воронеж) в 2011, 2012 и 2013 годах; на X Международной научно-технической конференции «Физика и технические приложения волновых процессов» (Самара) в 2011 году.

Структура и объем работы. Диссертация состоит из введения, четырех разделов, заключения и списка литературы из 94 наименований. Объем диссертации составляет 167 страниц, включая 157 страниц основного текста, содержащего 56 рисунков, и 10 страниц списка литературы.

СОДЕРЖАНИЕ РАБОТЫ

Во введении к диссертации обоснована актуальность темы, сформулированы цель и задачи работы, ее научная новизна, практическая значимость полученных результатов и положения, выносимые на защиту.

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

Во второй главе дается описание разработанного двухэтапного нейросетевого алгоритма статистического анализа и прогнозирования нестационарных временных последовательностей, используемого для прогнозирования интенсивности обнаруже-

ния уязвимостей в ПО. Обосновывается преимущество его прогностических способностей по отношению к существующим аналитическим моделям обнаружения уязвимостей. Для прогноза использовались данные по дефектам ПО (уязвимостям), использование которых позволяет нарушить доступность и/или целостность информации при наличии внешних воздействий в операционных системах Windows XP, Windows Vista и Windows Server 2003 из National Vulnerability Database (минимальная выборка данных составляла 36 месяцев).

На первом этапе осуществляется предварительная обработка данных о ранее обнаруженных уязвимостях, полученных, как правило, в моменты времени $t^{(1)},...,t^{(P)}$ с различными интервалами. Соответствующая процедура обработки должна обеспечить их сглаживание и интерполяцию для представления в виде непрерывной функциональной зависимости от времени. При проведении предварительной обработки предложено осуществлять восстановление зависимости в виде взвешенной суммы радиально-базисных функций

$$F(t) = \sum_{i=1}^{K} w_i \varphi_i(t) = w^T \varphi(t), \qquad (1)$$

где $\varphi_i(t)$ – i-я радиально-базисная функция; w_i – соответствующий весовой коэффициент этой функции; K – количество используемых функций.

При вычислении коэффициентов ряда проводилось решение переопределенной системы линейных уравнений

$$Gw = d, \;\; G = \left\| g_{p,i} \right\|, \;\; g_{p,i} = \left\| \varphi_i\left(t^{(p)}\right) \right\|, \;\; p = \overline{1,P}, \;\; i = \overline{1,K}, \;\; K < P \qquad (2)$$

где G – матрица Грина, являющаяся в данном случае прямоугольной; $d = \left(d^{(1)},...,d^{(P)}\right)^T$ – целевой вектор, определяемый из исходного множества аппроксимируемых данных; P - число моментов времени, для которых проводится обработка данных. Решение системы уравнений (2) с использованием метода регуляризации выглядит следующим образом:

$$w = w^{(a)} + \left(G^T G + \alpha I\right)^{-1} G^T \left(d - G w^{(a)}\right), \qquad (3)$$

где $w^{(a)}$ – априорное решение; α – параметр регуляризации, который выбирается одним из стандартных методов; I – единичная матрица размера $K \times K$. В качестве априорного решения предложено использовать зависимости, получаемые на основе аналитических моделей обнаружения уязвимостей (логистическая модель Алхазми-Малаийа или линейная модель Рескорлы).

На втором этапе обработки осуществляется прогнозирование сглаженных и интерполированных данных с использованием комитета из 10 искусственных двухслойных нейронных сетей прямого распространения с сигмоидной функцией активации в виде гиперболического тангенса для 1-го слоя и линейной функции активации для 2-го слоя. Для построения прогнозирующего алгоритма проводилось обучение каждой нейронной сети при помощи функции, которая модифицирует веса и смещения в соответствии с методом шкалированных связанных градиентов, обеспечивающее восстановление нелинейной авторегрессионной зависимости разницы между очередным (прогнозируемым) значением и предыдущим значением анализируемого процесса от Nu предшествующих значений. В качестве итогового результата прогноза бралось среднее значение между прогнозами 10 нейронных сетей.

Результаты сравнения показывают, что прогноз динамики обнаружения уязвимостей (дефектов ПО) для операционных систем семейства Windows с использованием нейронной сети без учета априорного решения в среднем на 2% точнее, чем

прогноз при помощи линейной модели Рескорлы и логистической модели Алхазми-Малаийа, а прогноз с использованием нейронной сети с учетом априорного решения в среднем на 10% точнее, чем прогноз при помощи этих моделей. В отдельных точках повышение точности прогноза может составлять 70%.

Далее во 2-й главе приводится описание разработанной модели динамики дефектов ПО (уязвимостей), использование которых позволяет нарушить доступность и/или целостность информации при наличии внешних воздействий в программах, установленных в ИС. Для оценки числа уязвимостей в программе, аналогично модели, представленной в работах А.Ю. Щеглова, предлагается представить процесс появления новых уязвимостей и их устранения как процесс функционирования системы массового обслуживания (СМО). Отличительной особенностью используемой в работе модели является то, что на вход СМО поступает нестационарный пуассоновский поток заявок (уязвимостей) с интенсивностью $\lambda(t)$, зависящей от времени t и прогнозируемой на основе описанного выше алгоритма (поток уязвимостей - нестационарный пуассоновский, так как фактически он представляет собой сумму порядка 100÷1000 независимых нестационарных потоков с приблизительно одинаковой интенсивностью, порождаемых ИНВ и специалистами, занимающимися поиском новых уязвимостей). Кроме того, вводится коэффициент работы системного администратора k, позволяющий учесть его действия по устранению уязвимостей в программе ($k=0$ – программа не обновляется; $0<k<1$ – программа обновляется несвоевременно; $k=1$ – программа обновляется своевременно; $k>1$ – программа обновляется своевременно и системный администратор разрабатывает собственные решения по устранению уязвимостей). Соответственно, время обслуживания заявки (устранения уязвимости), имеет экспоненциальное распределение с интенсивностью $\mu = k/T_в$, где $T_в$ - среднее время создания вендором обновления программы, закрывающего уязвимость после ее обнаружения. Предполагается, что работа над устранением каждой уязвимости начинается сразу же после ее обнаружения, соответственно, СМО имеет бесконечное число каналов обслуживания. Тогда среднестатистическое число уязвимостей в программе на момент времени t при $k>0$ рассчитывается по формуле

$$N_{ср}(t) = \frac{T_в e^{-t}}{k}\left(\lambda(t) + \int_0^t \lambda(\tau) e^{\tau} d\tau \right), \qquad (4)$$

а при $k=0$ - по формуле

$$N_{ср}(t) = \int_0^t \lambda(\tau) d\tau \ . \qquad (5)$$

Вероятность отсутствия в программе уязвимостей в момент времени t равна

$$P_0(t) = e^{-N_{ср}(t)} . \qquad (6)$$

Приводится описание разработанных математических моделей функционирования ИС. Модель ИС без средств защиты информации (СЗИ) отображена на рисунке 1, здесь $\lambda^{(m)}(t)$ – интенсивность обнаружения уязвимостей в m-й программе, $k^{(m)}$ – коэффициент, характеризующий обслуживание системным администратором m-й программы, $T_в^{(m)}$ - среднее время создания вендором патча, закрывающего уязвимость после ее обнаружения в m-й программе, а M - общее число программ.

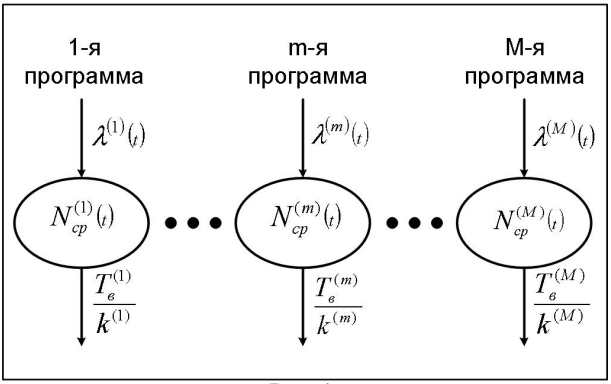

Рис. 1.

В этом случае среднестатистическое число уязвимостей в ИС будет определяться как сумма среднестатистического числа уязвимостей в каждой программе

$$N_{cp}(t)=\sum_{m=1}^{M}N_{cp}^{(m)}\ ,\ N_{cp}^{(m)}(t)=\frac{T_в^{(m)}e^{-t}}{k^{(m)}}\left(\lambda^{(m)}(t)+\int_0^t\lambda^{(m)}(\tau)e^{\tau}d\tau\right), \qquad (7)$$

Вероятность отсутствия в ИС уязвимостей может быть рассчитана по формуле (6), если вместо среднего числа уязвимостей в конкретной программе ((4) или (5)) в нее подставить среднее число уязвимостей в ИС (7).

В простейшем случае, когда уязвимости каждой программы могут быть использованы непосредственно для негативного воздействия на ИС, потенциальная вероятность того, что работоспособность данной ИС в данный момент времени не может быть нарушена ИНВ (далее вероятность надежности ИС), совпадает с вероятностью отсутствия в ИС уязвимостей (в данном случае не имеет значения, является ли ИНВ внешним или внутренним)

$$P_{над}(t)=P_0(t)\ . \qquad (8)$$

Возможны другие варианты организации ИС, когда в ней установлено специальное ПО, защищающее ее от непосредственного негативного воздействия внешнего источника, в этом случае вероятность надежности данной ИС для данного момента времени по отношению к внешнему ИНВ будет рассчитываться по следующей формуле:

$$P_{над}(t)=P_0^{(СЗИ)}(t)+P_0^{(ПО)}(t)(1-P_0^{(СЗИ)}(t))\ , \qquad (9)$$

где $P_0^{(СЗИ)}$ - вероятность отсутствия уязвимостей в СЗИ, а $P_0^{(ПО)}$ - вероятность отсутствия уязвимостей в остальном ПО, установленном в ИС.

Таким образом, полученные модели позволяют, в отличие от известных, учесть зависимость интенсивности обнаружения уязвимостей в ПО от времени, зависимость интенсивности закрытия уязвимостей в ПО от качества работы системного администратора и структурные характеристики ИС (наличие различных программ, наличие СЗИ и их конфигурации и т.п.).

В конце 2-й главы представлен общий алгоритм анализа вероятностных характеристик надежности использования программного обеспечения информационной системы в условиях негативных воздействий (рис. 2), основанный на совокупности представленных моделей и алгоритмов. При этом характер негативного воздействия (преднамеренное или непреднамеренное) не учитывается.

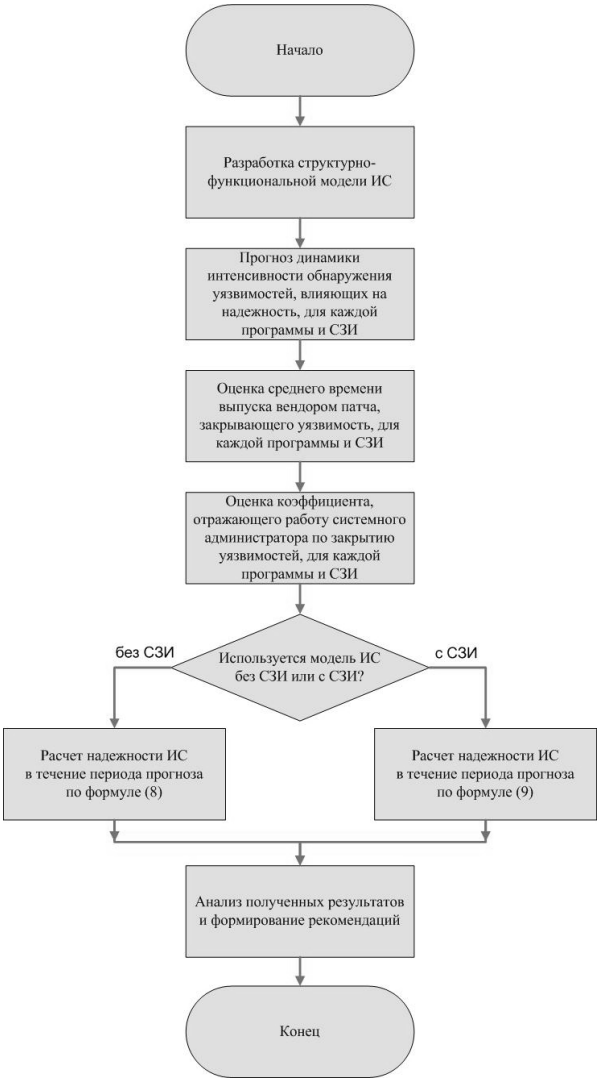

Рис. 2.

В третьей главе для оценки надежности использования ПО ИС на основе единой методологии рассматриваются четыре варианта конфликтных взаимодействий ИС и ИНВ (взаимодействие ИС без СЗИ с одним ИНВ, взаимодействие ИС с СЗИ с одним ИНВ, взаимодействие ИС без СЗИ с коалицией ИНВ без инсайдера, взаимодействие ИС без СЗИ с коалицией ИНВ с инсайдером, поставляющим информацию о ПО коалиции ИНВ). Источником негативного воздействия может быть злоумышленник или независимый тестировщик системы, а также пользователь, совершающий ошибки в процессе работы системы и действующий в нештатном режиме.

В рамках развиваемого в диссертации подхода для каждого из этих вариантов создается сначала концептуальная объектно-ориентированная модель, описывающая

основные состояния сторон и переходы между ними, далее на ее основе – математическая модель, использующая вероятностные описания динамики конфликта и, наконец, компьютерная имитационная модель, реализованная в интегрированной среде Matlab+Simulink+Stateflow, обеспечивающая наиболее адекватный учет исходных концептуальных и функциональных объектных представлений с использованием формализма гибридных автоматов (карты Харела).

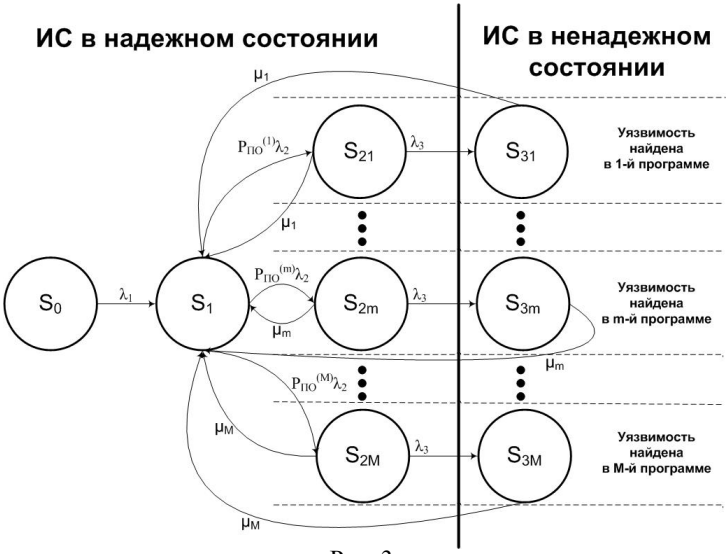

Рис. 3.

Пример одной из разработанных математических моделей конфликтного взаимодействия, основанной на представлении процесса смены состояний объединенной системы ИС – ИНВ в виде цепи Маркова с непрерывным временем с конечным числом состояний представлен на рис. 3. Времена переходов между состояниями описываются экспоненциальным законом распределения. Узлы цепи соответствуют следующим состояниям объединенной системы ИС – ИНВ: S_0 – у ИНВ отсутствует какая-либо информация об ИС; S_1 – у ИНВ есть информация о ПО ИС; S_{2m} – у ИНВ есть информация о ПО ИС и об одной уязвимости в ПО, где m - номер программы, в котором была найдена уязвимость ($m \in 1..M$), а M – количество программ в ИС; S_{3m} ($m \in 1...M$) – у ИНВ есть информация о ПО ИС, об одной уязвимости в ПО, а также о способе использования этой уязвимости для осуществления НВ на ИС. Вероятности нахождения в указанных состояниях обозначаются соответственно $P_0, P_1, P_{21}, ..., P_{2m}, ..., P_{2M}, P_{31}, ..., P_{3m}, ..., P_{3M}$. При этом часть выделенных состояний ($S_0, S_1, S_{21}, ..., S_{2m}, ..., S_{2M}$) агрегируются в состояние *«ИС в надежном состоянии»*, а состояния ($S_{31}, ..., S_{3m}, ..., S_{3M}$) - в состояние *«ИС в ненадежном состоянии»*. Полученная цепь Маркова описывается начальным вектором вероятностей состояний $P(0) = \begin{bmatrix} 1 & 0 & ... & 0 \end{bmatrix}^T$ и переходной матрицей

$$P_{пер}(t)=\exp(Qt),\ Q=\begin{bmatrix} -\frac{1}{T_{по}} & \frac{1}{T_{по}} & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & -\sum_{m=1}^{M}\frac{N_{ср\_конф}^{(m)}}{T_{уязв}} & \frac{N_{ср\_конф}^{(1)}}{T_{уязв}} & \dots & \frac{N_{ср\_конф}^{(M)}}{T_{уязв}} & 0 & \dots & 0 \\ 0 & \frac{2k^{(1)}}{T_{в}^{(1)}} & -\left(\frac{2k^{(1)}}{T_{в}^{(1)}}+\frac{1}{T_{нв}}\right) & \dots & 0 & \frac{1}{T_{нв}} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \frac{2k^{(M)}}{T_{в}^{(M)}} & 0 & \dots & -\left(\frac{2k^{(M)}}{T_{в}^{(M)}}+\frac{1}{T_{нв}}\right) & 0 & \dots & \frac{1}{T_{нв}} \\ 0 & \frac{2k^{(1)}}{T_{в}^{(1)}} & 0 & \dots & 0 & -\frac{2k^{(1)}}{T_{в}^{(1)}} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \frac{2k^{(M)}}{T_{в}^{(M)}} & 0 & \dots & 0 & 0 & \dots & -\frac{2k^{(M)}}{T_{в}^{(M)}} \end{bmatrix}, \quad (10)$$

где Q - матрица интенсивностей переходов между состояниями цепи; t - текущее время, отсчитываемое от начала конфликта; $T_{по}$ – среднее время, требующееся ИНВ для нахождения информации о ПО ИС; $N_{ср\_конф}^{(m)}$ - среднеарифметическое среднестатистического числа уязвимостей $N_{ср}^{(m)}(t)$, находящихся в m-й программе за все время конфликта; $T_{уязв}$ – среднее время, требующееся ИНВ для нахождения информации о всех уязвимостях в ПО ИС; $T_{нв}$ – среднее время, требующееся ИНВ для нахождения информации о способе использования уязвимости в ПО ИС для НВ на ИС; $T_{в}^{(m)}$ – среднее время, которое требуется вендору m-й программы для создания патча или временного решения, закрывающих уязвимость с момента ее обнаружения; $k^{(m)}$ – коэффициент, отражающий работу системного администратора по устранению уязвимостей из m-й программы.

Вероятность нахождения ИС в надежном состоянии за все время конфликтного взаимодействия рассчитывается по формуле

$$P_{нах\_над\_конф}=\int_{0}^{T_{\text{конф}}}\left(1-\sum_{m=1}^{M}\left(P(0)P_{пер}(t)\right)_{3m}\right)dt \Big/ T_{\text{конф}}, \quad (11)$$

где $T_{конф}$ - время длительности конфликта.

Для реализации компьютерных имитационных моделей конфликта ИС и ИНВ использовался формализм гибридных автоматов (карт состояний Харела) и возможности, которые для этих целей предоставляет интегрированная среда MATLAB + Simulink + Stateflow. Конфликтное взаимодействие ИС – ИНВ в терминах среды MATLAB + Simulink + Stateflow можно описать при помощи SF-модели. На рис. 4 представлен пример построения такой модели для рассмотренной выше ситуации. Модель состоит из 3-х параллельно функционирующих объектов (*«Sysadmin»* и *«IS»* с одной стороны, *«IPNV»* с другой стороны), в которых размещены карты состояний Харела, описывающие возможные значения учитываемых факторов и поведение (в зависимости от этих значений) всех участников взаимодействия. Каждый объект может находиться в нескольких состояниях. Переходы между состояниями осуществляются либо по истечению случайных промежутков времени с произвольным законом распределения, либо при возникновении события, сгенерированного другим объектом (за счет этого происходит взаимодействие объектов).

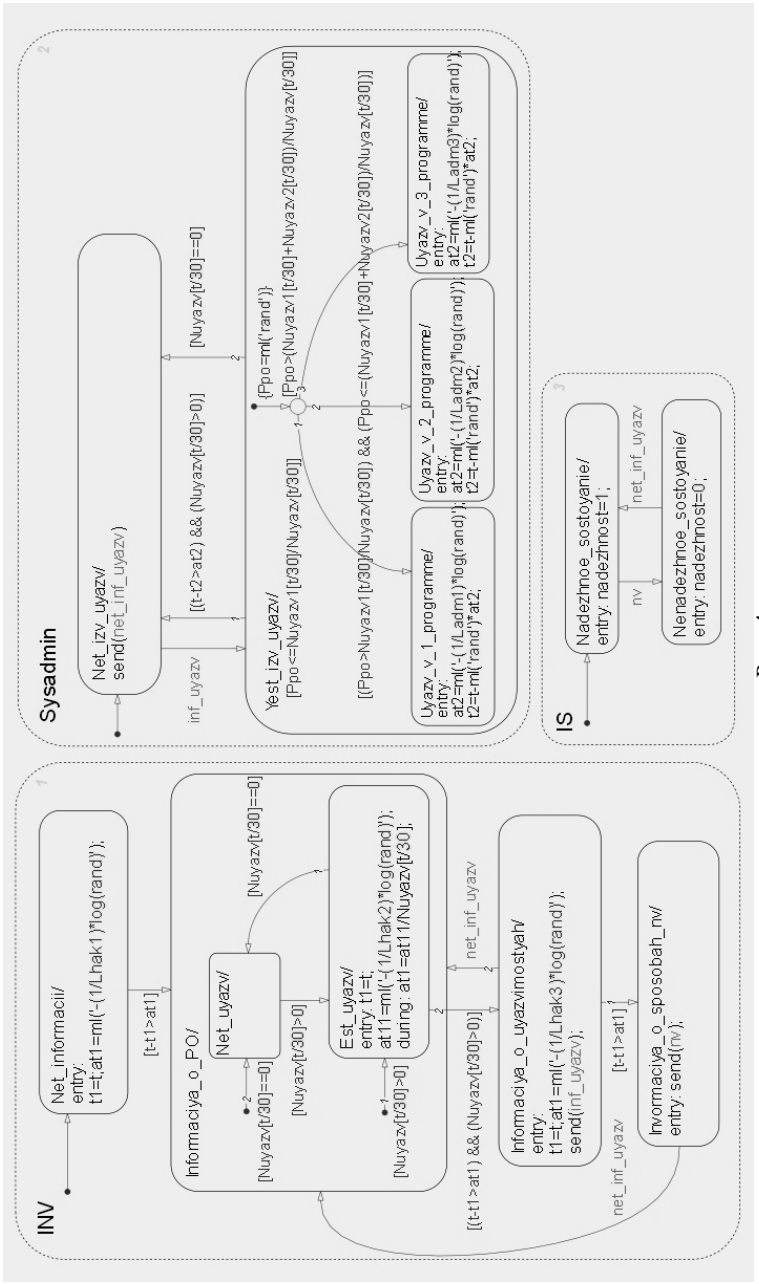
INV
Net_informacii/
entry:
t1=t;at1=ml('-(1/Lhak1)*log(rand)');
[t-t1>at1]
Informaciya_o_PO/
Net_uyazv/
[Nuyazv[t/30]==0]
[Nuyazv[t/30]>0]
[Nuyazv[t/30]==0]
Est_uyazv/
entry: t1=t;
at11=ml('-(1/Lhak2)*log(rand)');
during: at1=at11/Nuyazv[t/30];
[Nuyazv[t/30]>0]
net_inf_uyazv
[(t-t1>at1) && (Nuyazv[t/30]>0)]
Informaciya_o_uyazvimostyah/
entry:
t1=t;at1=ml('-(1/Lhak3)*log(rand)');
send(inf_uyazv);
net_inf_uyazv
[t-t1>at1]
Invormaciya_o_sposobah_nv/
entry: send(nv);
Sysadmin
Net_izv_uyazv/
send(net_inf_uyazv)
inf_uyazv
[(t-t2>at2) && (Nuyazv[t/30]>0)]
[Nuyazv[t/30]==0]
Yest_izv_uyazv/
[Ppo<=Nuyazv1[t/30])/Nuyazv[t/30]]
{Ppo=ml('rand')}
[Ppo>(Nuyazv1[t/30]+Nuyazv2[t/30])/Nuyazv[t/30]]
[(Ppo>Nuyazv1[t/30])/Nuyazv[t/30]) && (Ppo<=(Nuyazv1[t/30]+Nuyazv2[t/30])/Nuyazv[t/30])]
Uyazv_v_1_programme/
entry;
at2=ml('-(1/Ladm1)*log(rand)');
t2=t-ml('rand')*at2;
Uyazv_v_2_programme/
entry;
at2=ml('-(1/Ladm2)*log(rand)');
t2=t-ml('rand')*at2;
Uyazv_v_3_programme/
entry;
at2=ml('-(1/Ladm3)*log(rand)');
t2=t-ml('rand')*at2;
IS
Nadezhnoe_sostoyanie/
entry: nadezhnost=1;
nv
net_inf_uyazv
Nenadezhnoe_sostoyanie/
entry: nadezhnost=0;

Рис. 4.

Объектно-ориентированные, математические и имитационные модели для остальных 3-х рассматриваемых случаев конфликта строятся аналогичным образом. При сравнении имитационных и математических моделей для всех случаев (расчет вероятности надежности и вероятности нахождения ИС в надежном состоянии) было выявлено, что разница в результатах применения различных типов моделей в случае конфликта ИС без СЗИ с одним ИНВ, в случае конфликта ИС с СЗИ с одним ИНВ и в случае конфликта ИС без СЗИ с коалицией ИНВ без инсайдера составила до 8%, а в случае конфликта ИС без СЗИ с коалицией ИНВ при наличии инсайдера до 20%. То есть при относительно грубой оценке надежности использования ПО в ИС в условиях внутренних уязвимостей (дефектов ПО) в большинстве случаев (кроме последнего) имитационные модели конфликта могут быть заменены математическими, при более точной оценке возможность применения математической модели вместо имитационной может быть обоснована или наоборот отвергнута, исходя из оценки рисков, к которым может привести однократное успешное негативное воздействие на ИС и нахождение ИС в ненадежном состоянии. Принципиальная же разница между данными моделями заключается в том, что компьютерные имитационные модели, в отличие от математических, учитывают зависимость среднестатистического числа уязвимостей в ИС от времени (в математических моделях используется значение данной величины, усредненное по времени конфликта), допускают произвольный характер переходов между состояниями сторон (при использовании математической модели вероятности переходов между состояниями имеют показательный закон распределения), позволяют рассматривать конфликтные ситуации с любыми вариантами отношений между ИНВ и рассчитать дополнительные величины, характеризующие надежность ИС (например, количество возможных успешных НВ на ИС).

В четвертой главе диссертации на основе предложенных моделей и алгоритмов оценки надежности использования ПО выполнены исследования для базовых элементов типовой ИС удостоверяющего центра (УЦ) (сервер публикации отозванных сертификатов, центр регистрации) и типовой ИС пользователя и даны рекомендации для повышения их надежности. Ниже на рисунке 5 приведены графики прогноза вероятности нахождения типового сервера публикации отозванных сертификатов в надежном состоянии на период с сентября 2013 года по февраль 2014 года в зависимости от коэффициента работы системного администратора для 4-х категорий ИНВ (с ростом категории ИНВ уменьшается время каждого этапа преднамеренного НВ).

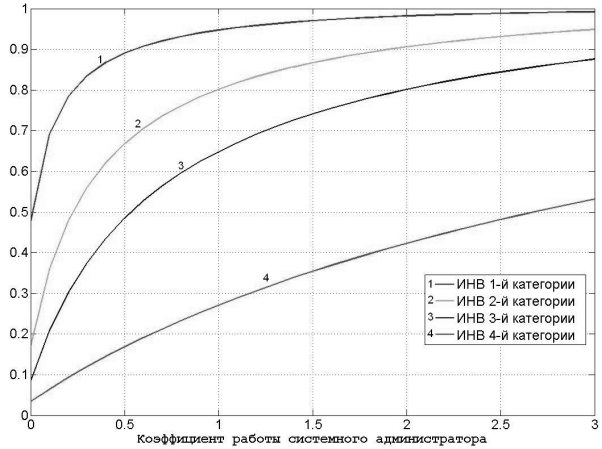

Рис. 5.

В ходе выполненного анализа показано, что наиболее ненадежным звеном системы документооборота с использованием электронной подписи являются ИС пользователей УЦ (работа ИС может быть нарушена в 90% случаев и более в зависимости от категории ИНВ, пытающегося оказать НВ на ИС, но при этом вся система сохраняет свою работоспособность). В УЦ наиболее ненадежным звеном является сервер публикации отозванных сертификатов, и, более того, нарушение его работоспособности является наиболее критичным для системы электронного документооборота в целом. Для повышения

его надежности предлагается применять дополнительные меры по защите доступности и целостности публикуемой УЦ информации. Центр регистрации УЦ является ненадежным в случае, если открыт протокол https доступа к его сервису IIS (Internet Information Services), при этом при использовании IIS 6-й версии (Windows Server 2003) его надежность существенно (до 7×10^7 раз) меньше, чем при использовании IIS 7-й версии (Windows Server 2008). Для повышения надежности центра регистрации предлагается закрыть доступ к IIS из незащищенных сетей.

В заключении сделаны общие выводы и сформулированы основные результаты, которые сводятся к следующему:

1. Разработан двухэтапный нейросетевой алгоритм статистического анализа и прогнозирования нестационарных временных последовательностей, позволяющий повысить точность прогноза интенсивности обнаружения уязвимостей программного обеспечения по сравнению с известными.

2. Предложены математические модели динамики состояний программ и информационной системы в целом с учетом возможных уязвимостей и общий алгоритм оценки надежности использования программного обеспечения, учитывающие зависимости интенсивности обнаружения уязвимостей от времени, временных характеристик закрытия уязвимостей от работы производителя ПО и администратора информационной системы, что позволяет повысить степень обоснованности получаемых оценок.

3. Разработаны объектно-ориентированные и математические модели использования информационных технологий и информационной системы в целом в динамике конфликтного взаимодействия, обеспечивающие оценку надежности в дуэльных ситуациях при выполнении ограничения в виде пуассоновского характера потоков, описывающих переходы между состояниями информационной системы и источника внешних воздействий.

4. Предложены компьютерные имитационные модели использования информационных технологий и информационной системы в целом в динамике конфликтного взаимодействия, основанные на применении формализма гибридных автоматов Харела, обеспечивающие оценку надежности информационных систем в условиях воздействия коалиции внешних источников при произвольных характере статистики переходов между состояниями информационной системы и количестве источников внешних воздействий.

5. Даны практические рекомендации относительно использования базовых элементов типовой ИС удостоверяющего центра и типовой ИС пользователя, обеспечивающие повышение надежности использования устанавливаемого типового программного обеспечения.

6. В целом разработанные алгоритмы и модели оценки надежности использования ПО в ИС: позволяют учитывать прогноз будущего состояния информационной системы; используют данные, которые могут быть получены из открытых источников и статистики, опубликованной в сети Интернет; достаточно просто могут быть модифицированы под конкретные условия функционирования исследуемых информационных процессов и систем.

Основные публикации по теме диссертации

1. Вялых, А.С. Оценка уязвимости информационной системы на основе ситуационной модели динамики конфликта / А.С. Вялых, С.А. Вялых, А.А. Сирота // Информационные технологии. - 2012. - № 9. - С. 16-21.

2. Вялых, А.С. Нейросетевой алгоритм обработки информации для прогнозирования надежности программного обеспечения / А.С. Вялых, С.А. Вялых, А.А. Сирота // Вестник Воронежского государственного ун-та. Серия: Системный анализ и информационные технологии. - 2013. - № 2. – С. 140-143.

3. Вялых, А.С. Динамика уязвимостей в современных защищенных информационных системах / А.С. Вялых, С.А. Вялых // Вестник Воронежского государственного ун-та. Серия: Системный анализ и информационные технологии. - 2011. - № 2. - С. 59-63.

4. Вялых, А.С. Оценка эффективности сигнатурных методов обнаружения вредоносных программ / А.С. Вялых, С.А. Вялых // Вестник Воронежского государственного ун-та. Серия: Системный анализ и информационные технологии. - 2011. - № 2. - С. 64-66.

5. Вялых, А.С. Оценка уязвимости современных информационных систем / А.С. Вялых, С.А. Вялых // Информатика : проблемы, методология, технологии : матер. XI Международ. науч. – метод. конф., Воронеж, 10-11 февр. 2011 г. – Воронеж : ИПЦ ВГУ, 2011. – Т. 1. – С. 168-172.

6. Вялых, А.С. Оценка эффективности обнаружения вредоносных программ / А.С. Вялых, С.А. Вялых // Информатика : проблемы, методология, технологии : матер. XI Международ. науч. – метод. конф., Воронеж, 10-11 февр. 2011 г. – Воронеж : ИПЦ ВГУ, 2011. – Т. 1. – С. 172-176.

7. Вялых, А.С. Оценка возможностей атаки на информационную систему / Вялых А.С., Вялых С.А. // Кибернетика и высокие технологии XXI века : матер. XII международ. науч.-тех. конф., Воронеж, 11-12 мая 2011 г. – Воронеж : ИПЦ ВГУ, 2011. – Т.1. – С. 91-96.

8. Сирота, А.А. Имитационная модель ситуационного конфликта информационной системы и злоумышленника / А.А. Сирота, А.С. Вялых, С.А. Вялых // Информатика : проблемы, методология, технологии : матер. XII Международ. науч. – метод. конф., Воронеж, 9-10 февр. 2012 г. – Воронеж : ИПЦ ВГУ, 2012. – Т. 1. – С. 359-361.

9. Вялых, А.С. Имитационная модель конфликта информационной системы и коалиции злоумышленников / А.С. Вялых, С.А. Вялых, А.А. Сирота // Кибернетика и высокие технологии XXI века : матер. XIII международ. науч.-тех. конф., Воронеж, 15-16 мая 2012 г. – Воронеж : НПФ «САКВОЕЕ» ООО, 2012. – Т.2. – С. 413-424.

10. Сирота, А.А. Прогнозирование динамики обнаружения уязвимостей программного обеспечения при помощи нейросетевых алгоритмов обработки информации / А.А. Сирота, А.С. Вялых, С.А. Вялых // Информатика : проблемы, методология, технологии : матер. XIII Международ. науч. – метод. конф., Воронеж, 7-8 февр. 2013 г. – Воронеж : ИПЦ ВГУ, 2013. – Т. 3. – С. 224-228.

11. Вялых, А.С. Использование нейросетевых алгоритмов обработки информации для прогнозирования динамики обнаружения уязвимостей в современном программном обеспечении / А.С. Вялых, С.А. Вялых, А.А. Сирота // Кибернетика и высокие технологии XXI века : матер. XIV международ. науч.-тех. конф., Воронеж, 14-15 мая 2013 г. – Воронеж : НПФ «САКВОЕЕ» ООО, 2013. – Т.2. – С. 417-422.

Работы № 1–4 опубликованы в изданиях, соответствующих перечню ВАК РФ.