УДК 681.321+004.519.217

В.С. Харченко[1], Аль-Судани Мустафа Кахтан Абдулмунем[1], Ю.Л. Поночовный[1,2]

[1] *Национальный аэрокосмический университет им. Н.Е. Жуковского "ХАИ", Харьков*
[2] *Полтавский национальный технический университет им. Ю. Кондратюка, Полтава*

МАРКОВСКИЕ МОДЕЛИ ГОТОВНОСТИ ИНФОРМАЦИОННО-УПРАВЛЯЮЩЕЙ СИСТЕМЫ «УМНОГО» ДОМА ПРИ РАЗДЕЛЬНОМ И ОБЩЕМ ОБСЛУЖИВАНИИ ПО НАДЕЖНОСТИ И БЕЗОПАСНОСТИ

В статье рассмотрены вопросы построения марковских моделей и оценки готовности информационно-управляющей системы «умного» дома (smart building automation system, BAS). Определено, что причинами отказов и недоступности компонент архитектуры BAS могут быть как внутрисистемные, так и внешние факторы, среди которых выделены программные дефекты и уязвимости. Последние рассматриваются как элементы двух непересекающихся множеств. Детально проанализированы модели архитектуры BAS с программными дефектами и атакуемыми уязвимостями без процедур обслуживания, с общим и раздельным обслуживанием по надежности (дефекты) и безопасности (уязвимости). Сформулированы рекомендации по выбору стратегий и параметров обслуживания.

Ключевые слова: *информационно-управляющая система, умный дом, программные дефекты и уязвимости, готовность, надежность, безопасность, стратегии обслуживания, марковские модели*

Введение

Развитие технологий виртуализации и создания сред облачных вычислений обусловливают появление новых вариантов архитектуры ИТ-систем, которую необходимо учитывать при оценке и обеспечении качества современных компьютерных систем и сервисов, к которым относятся системы «умный дом». При этом динамический характер процессов информационного взаимодействия существенно усложняет возможности оперативной оценки надежности и доступности программных и инфраструктурных ресурсов, предоставляемых в режиме удаленного доступа [1].

Совокупность подсистем «умных» домов, выполняющих информационные и управляющие функции, рассматривается как система автоматизации здания – жилища, офисного или иного сооружения (building automation system, BAS) [2]. Компоненты BAS могут быть спроектированы с использованием различной элементной базы, включая реализацию управляющих функций нижнего уровня на FPGA-платформе. Архитектура BAS «умного» дома согласно [2] включает урони FPGA, баз данных, и беспроводных коммуникаций (Wireless Unite). Применение на каждом из этих уровней архитектуры программных средств с возможностью их модификации усложняет процесс оценивания и прогнозирования готовности системы, особенно для корпоративных решений. Учитывая критичность последствий отказов системы, обусловленных как отказами программно-аппаратных компонент вследствие их физических и проектных дефектов (фактор надежности), так и атаками на уязвимости (фактор информационной безопасности) BAS [3], необходимо обосновать стратегии и параметры обслуживания и восстановления, включая модификацию программных средств с учетом этих двух факторов. Одним из ключевых вопросов разработки таких стратегий является вопрос их раздельной или общей реализации с учетом факторов надежности и безопасности [3, 4].

Модификация программных средств вследствие устранения проектных дефектов, патчеризации уязвимостей приводит к изменению параметров потоков отказов и восстановлений системы. Для исследования систем с изменяемыми параметрами предпочтительно применение аппарата марковских и полумарковских процессов [4, 5]. В [6] развит системный поход к построению многофрагментных моделей, а в [5] разработаны модели, в которых учитываются факторы надежности и безопасности для веб-систем. Однако в известных работах не исследовано влияние разных стратегий обслуживания по этим факторам. Поэтому **целью данной статьи** является разработка и анализ моделей готовности BAS при проведении общего и раздельного обслуживания с учетом поэтапного устранения программных дефектов и уязвимостей.

1. Выбор марковских моделей для исследования архитектуры BAS

В процессе исследования процедур планирования и проведения обслуживания программных компонент архитектуры BAS важным этапом является получение количественных значений вероятностных составляющих их готовности. Применение аппарата марковского моделирования связано с определенным набором ограничений [5,7], не позволяющим построить и применить единую унифицированную

модель. Выходом является построение комплекса моделей, в котором каждая модель позволяет получить однообразные результирующие показатели, по которым удобно проводить сравнение и поиск оптимальных решений.

Основным аспектом моделирования функционирования программных компонент архитектуры BAS являются учет проявления и устранения ограниченных множеств программных дефектов и уязвимостей, причем данные множества рассматриваются как непересекающиеся.

Второй аспект – проведение обслуживания, в процессе которого вероятно выявление и устранение как дефектов, так и уязвимостей. Процедуры обслуживания могут проводиться на протяжении всего жизненного цикла BAS, или ограничиваться определенным количеством процедур.

Третий аспект – состав мероприятий обслуживания: они могут быть направлены только на выявление программных дефектов, либо только на выявление уязвимостей, либо содержать общий комплекс мер по выявлению и дефектов, так и уязвимостей. Множество базовых моделей систематизировано в табл. 1. Далее исследованы первые три модели BAS.

2. Базовая модель готовности архитектуры BAS с учетом программных дефектов и уязвимостей (MBAS1)

Базовая модель описывает процессы проявления и устранения программных дефектов и уязвимостей как разделенные потоки случайных событий. Исходное количество дефектов (Nd) и уязвимостей (Nv) являются входными параметрами модели. Также входными параметрами являются обычные для всех марковских моделей интенсивности случайных потоков событий. В статье рассматривается пример архитектуры BAS, которая на момент ввода в эксплуатацию содержит два программных дефекта и две уязвимости. На рис. 1 представлен ее размеченный граф.

Таблица 1

Множество базовых моделей BAS

Обозначение модели	Количество дефектов	Количество уязвимостей	Количество обслуживаний	Вид обслуживания
MBAS1	0..Nd	0..Nv	0	-
MBAS2	0..Nd	0..Nv	∞	общее
MBAS3	0..Nd	0..Nv	∞	раздельное
MBAS4	0..Nd	0..Nv	0..Np	общее
MBAS5	0..Nd	0..Nv	0..Ndp, 0..Ndv	раздельное

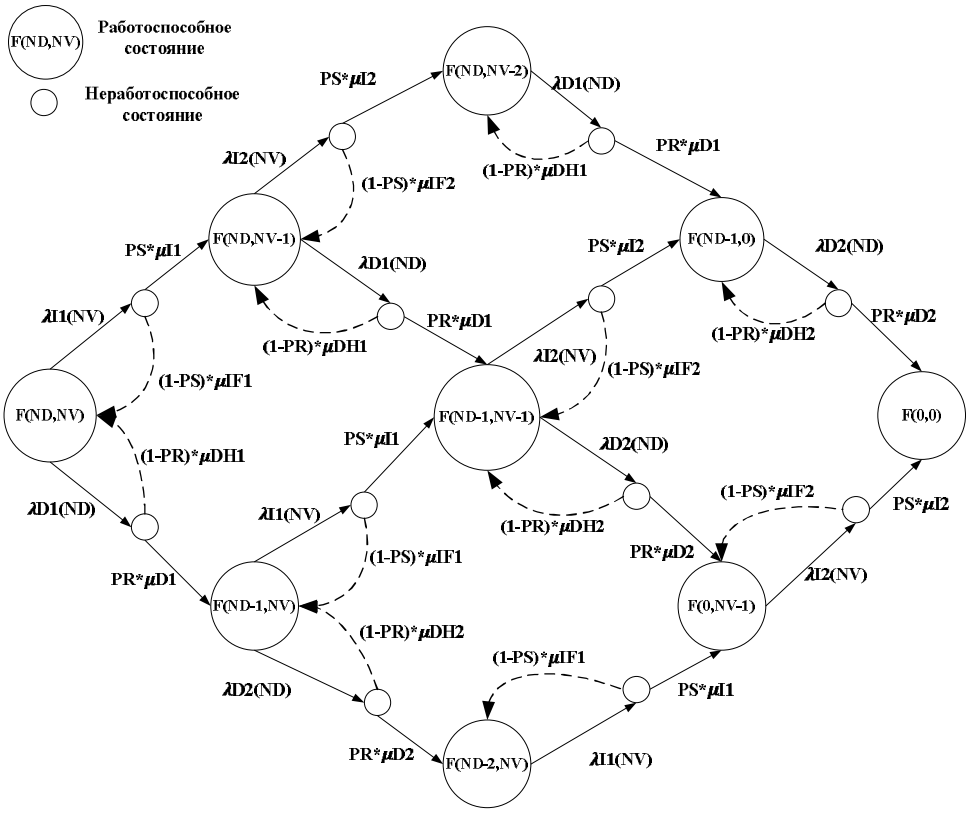


Рис. 1. Размеченный граф базовой модели MBAS1
с учетом проявления и устранения программных дефектов и уязвимостей

Основными являются допущения о простейших потоках отказов и восстановлений, изменяющих состояния системы. После проявления дефекта (или уязвимости) система с вероятностью PR (PS) прекращает работу до их полного устранения. С вероятностью 1–PR (для дефектов) или 1–PS (для уязвимостей) система возвращается в предыдущее работоспособное состояние через рестарт программы. В ходе устранения новые дефекты и уязвимости не вносятся. По мере проявления дефекты и уязвимости постепенно устраняются. Далее в работе рассматривается частный случай функционирования BAS, когда после проявления дефекта или уязвимости система останавливается до их полного устранения (то есть PR=1 и PS=1).

Работоспособные состояния на рис.1 показаны большими окружностями с указанием в них количества дефектов и уязвимостей; неработоспособные состояния показаны малыми окружностями без подписей.

В исходном состоянии F(Nd,Nv) система содержит 2 программных дефекта и 2 уязвимости.

Проявление программных дефектов на графе проиллюстрировано диагональными переходами со смещением вниз (взвешенными интенсивностями λDi(Nd)), а уязвимостей – диагональными переходами со смещением вверх (взвешенными интенсивностями λIj(Nv)). После проявления уязвимостей выполняется их устранение с интенсивностями PS*μIj, соответственно, устранение программных дефектов производится с интенсивностями PR*μDi. После устранения всех дефектов и уязвимостей система переходит в состояние F(0,0). Рестарт программного обеспечения проиллюстрирован переходами из неработоспособных состояний, взвешенными интенсивностями (1–PR)*μDHi и (1–PS)*μIFi. В последующем эти переходы не рассматриваются так как при PR=1 и PS=1 их интенсивности приравниваются к нулю.

3. Модель готовности BAS с учетом проведения общего обслуживания (MBAS2)

Модель является расширением базовой и включает дополнительные состояния, которые позволяют моделировать проведение процедур обслуживания. Размеченный граф модели показан на рис. 2.

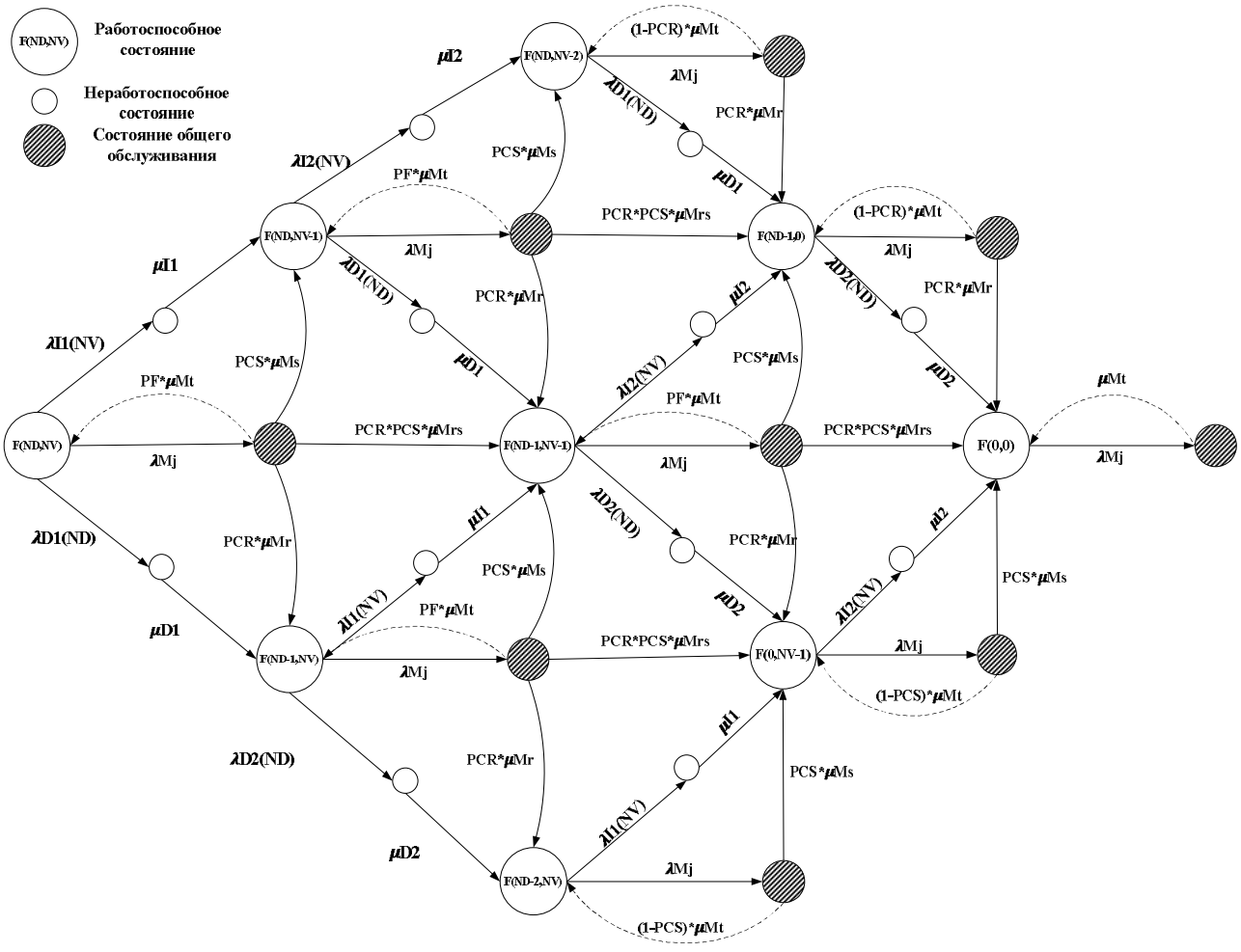


Рис. 2. Размеченный граф модели MBAS2 с учетом общего обслуживания

Помимо перечисленных выше допущений, в модели MBAS2 принято, что в ходе общего обслуживания возможно обнаружение и устранение одного программного дефекта или одной уязвимости.

Состояния, моделирующие процедуры обобщенного обслуживания показаны заштрихованными окружностями. Переходы в состояния обслуживания выполняются из работоспособных состояний с интенсивностью λMj (интенсивность обслуживания). В процессе проведения мероприятий обслуживания выявление программного дефекта происходит с вероятностью PCR, выявление уязвимости – с вероятностью PCS. Одновременное выявление уязвимости и программного дефекта происходит с вероятностью PCR*PCS. Вероятность необнаружения дефектов и уязвимостей PF дополняет предыдущие события до полной группы:

$$PF+PCS+PCR+PCS*PCR=1.$$

Таким образом, из состояния обслуживания возможны четыре перехода:

а) в случае обнаружения уязвимости с вероятностью PCS выполняется переход по стрелке вертикально вверх, взвешенный интенсивностью PCS*μMs, где μMs – величина, обратная среднему времени выявления и устранения уязвимости, μMs=1/(TdetV+TremV);

б) в случае обнаружения программного дефекта с вероятностью PCR выполняется переход по стрелке вертикально вниз, взвешенный интенсивностью PCR*μMr, где μMr – величина, обратная среднему времени выявления и устранения дефекта, μMr=1/(TdetD+TremD);

в) в случае обнаружения программного дефекта и уязвимости с вероятностью PCS*PCR выполняется переход по стрелке вправо, взвешенный интенсивностью PCS*PCR*μMrs, где μMrs – величина, обратная среднему времени выявления и устранения дефекта и уязвимости, μMrs=μMr*μMs/(μMr+μMs);

г) в случае необнаружения дефекта и уязвимости с вероятностью PF выполняется возвратный переход в предыдущее работоспособное состояние (влево), взвешенный интенсивностью PF*μMt, где μMt – величина, обратная среднему времени проведения обслуживания, $\mu Mr=1/T_M$.

Следует отметить, что в данной модели рассматриваются операции обслуживания, не предусматривающие прогнозирование количества дефектов и уязвимостей. Поэтому, после устранения всех уязвимостей переходы из состояний обслуживания, моделирующие необнаружение дефекта взвешены не с вероятностью PF, а с параметром (1–PCR)*μMt. Аналогично переходы, моделирующие необнаружение уязвимости после устранения всех программных дефектов, взвешены параметром (1–PCS)*μMt. Крайнее правое состояние, в котором моделируется обслуживание системы без дефектов и уязвимостей имеет соответственно переход, взвешенный параметром μMt.

4. Модель готовности BAS с учетом проведения раздельного обслуживания (MBAS3)

Модель также является расширенной по отношению к базовой и включает дополнительные состояния процедур раздельного обслуживания. В отличие от предыдущей модели, количество состояний обслуживания увеличено вдвое, так как рассматриваются процедуры обслуживания, целью которых является выявление только программных дефектов, и напротив, только уязвимостей. Размеченный граф модели показан на рис. 3.

Состояния, моделирующие процедуры раздельного обслуживания, показаны окружностями с различной штриховой заливкой. Переходы в состояния обслуживания выполняются из работоспособных состояний: в состояния обслуживания по уязвимостям – с интенсивностью обслуживания λMs, в состояния обслуживания по программным дефектам – с интенсивностью λMr. Так как рассматривается раздельное обслуживание, то образуются две полных группы событий: выявление уязвимости в процессе обслуживания с вероятностью PCS и невыявление уязвимости с вероятностью (1–PCS); выявление программного дефекта в процессе обслуживания с вероятностью PCR и невыявление дефекта с вероятностью (1–PCR).

Из каждого состояния обслуживания по уязвимостям выполняются два перехода: первый – с интенсивностью PCS*μMs моделирует выявление и устранение уязвимости при обслуживании, второй – с интенсивностью (1–PCS)*μMt моделирует проведение обслуживания без выявления уязвимости. В случае устранения всех уязвимостей переход из состояния обслуживания взвешен интенсивностью μMt. Аналогично происходит моделирование переходов из состояний обслуживания по программным дефектам. Переходы с интенсивностью PCR*μMr моделируют выявление и устранение программного дефекта при обслуживании, переходы с интенсивностью (1–PCR)*μMt моделируют проведение обслуживания без выявления дефектов. В случае устранения всех дефектов переходы из состояния обслуживания взвешены интенсивностью μMt.

5. Обоснование входных данных и сравнение результатов моделирования

Временные интервалы проведения общего и раздельного обслуживаний включают периоды тестирования, устранения обнаруженных дефектов и уязвимостей и верификации модифицированного программного обеспечения. Процедуры поиска дефектов и уязвимостей отличаются как по составу, так и по длительности, а их полнота определяет соответствующие вероятности PCS и PCR.

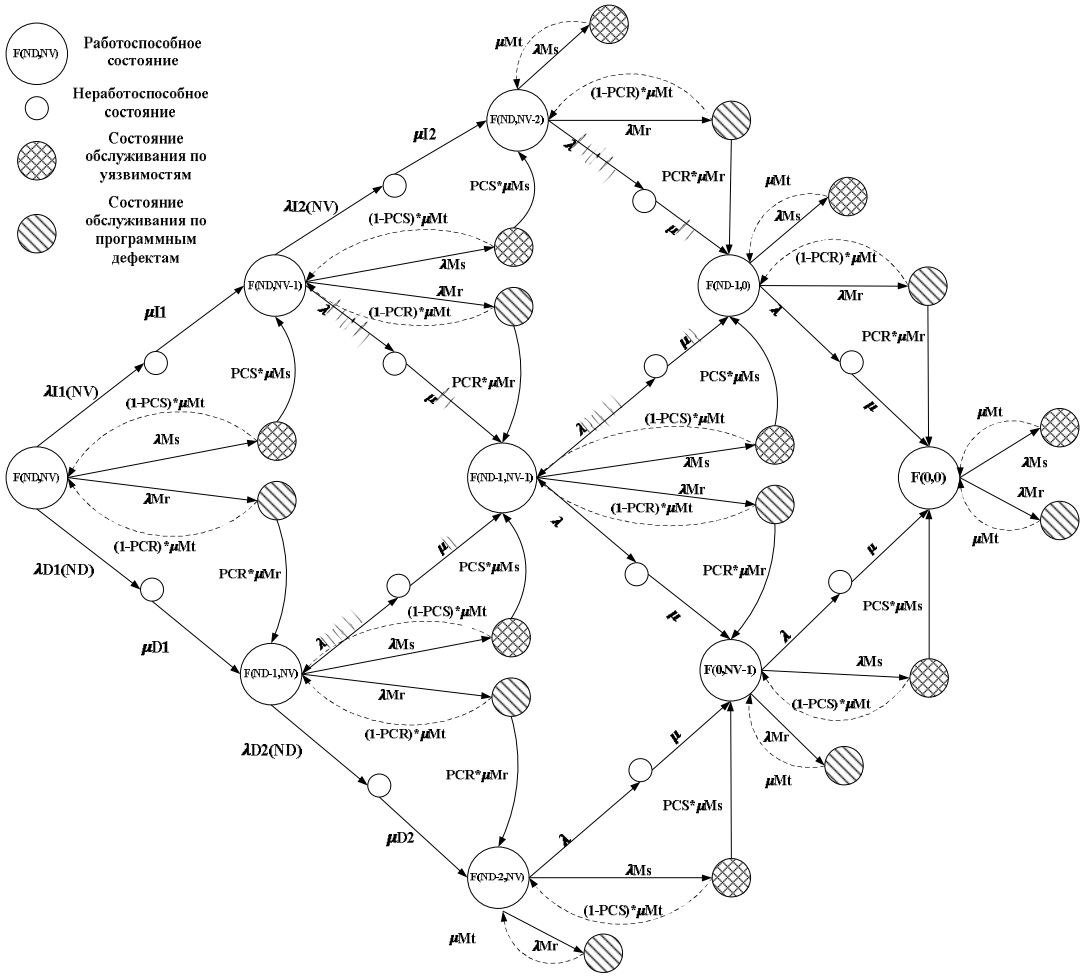


Рис. 3. Размеченный граф модели MBAS3
с учетом разделенного обслуживания по уязвимостям и программным дефектам

В ходе исследований приняты следующие значения входных параметров (табл. 2). Для исследования моделей были разработаны программные конструкции в системе Matlab.

На рис. 4 показаны размеченные графы моделей, построенные с помощью модифицированной функции grPlot [8]. На графах работоспособные состояния показаны черными окружностями с порядковой нумерацией от 0 до 8.

Таблица 2

Значения входных параметров моделей готовности

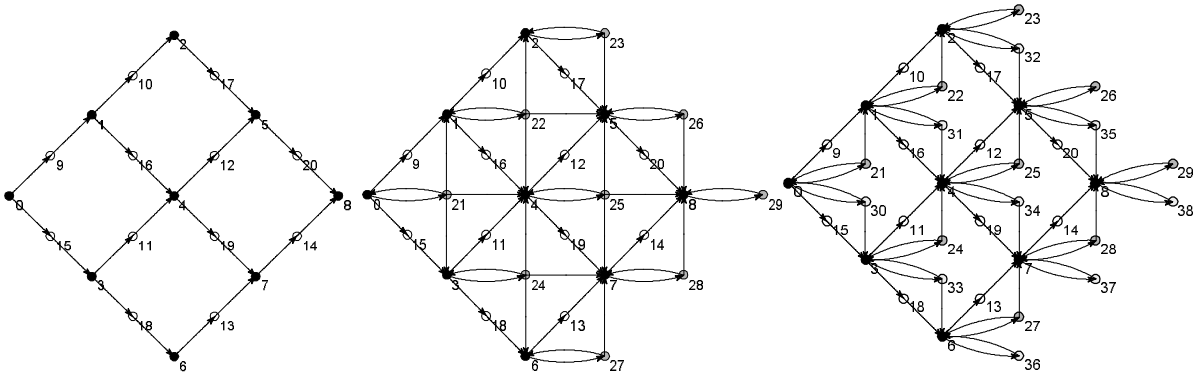
Входной параметр	Значение
λD1, λD2	5e-4, 4.5e-4 (1/час)
λI1, λI2	3e-3, 3.5e-3 (1/час)
μD1, μD2	0.5, 0.4 (1/час)
μI1, μI2	0.45, 0.34 (1/час)
λMj	1e-3 (1/час)
λMs	5e-3 (1/час)
λMr	1e-3 (1/час)
μMt	0.4 (1/час)
μMs	0.2 (1/час)
μMr	0.3 (1/час)
PCS	0.4
PCR	0.2

Для построения матрицы системы дифференциальных уравнений Колмогорова-Чепмена используется функция matrixA [9]. Для решения системы дифференциальных уравнений применен встроенный решатель Matlab ode15s. Функция готовности определяется как:

$$A(t) = \sum_{i=0}^{8} P_i(t). \qquad (1)$$

Результаты моделирования показаны на рис. 5. Графики моделей имеют одинаковый характер изменения функции готовности. На первом этапе готовность системы снижается до минимума, далее она асимптотически стремится к устоявшемуся значению. Таким образом, при дальнейшем анализе результатов необходимо учитывать три параметра:

- значение минимума функции готовности $A_{MBAS\,i}$min (для модели MBAS1 – 0.9919, для модели MBAS2 – 0.9886, для модели MBAS3 – 0.9758);
- значение функции готовности в устоявшемся режиме $A_{MBAS\,i}$const (для модели MBAS1 – 1, для модели MBAS2 – 0.9975, для модели MBAS3 – 0.9852);
- временной интервал перехода функции готовности в устоявшийся режим $T_{MBAS\,i}$const (для модели MBAS1 – 8246.5 часов, для модели MBAS2 – 5252.6 часов, для модели MBAS3 – 5303.3 часов).



MBAS1 MBAS2 MBAS3

Рис. 4. Орграфы моделей готовности архитектуры BAS с двумя программными дефектами и двумя уязвимостями, построенные с помощью функции grPlot

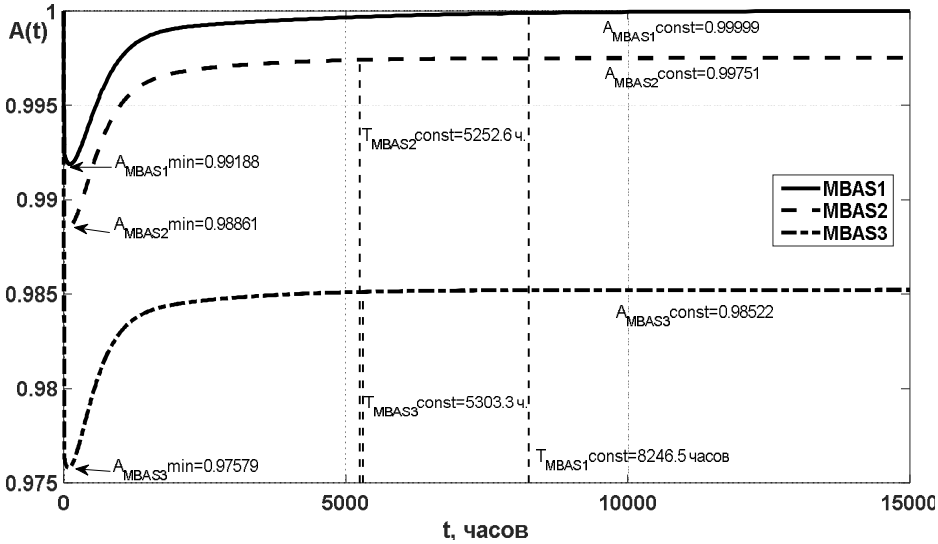


Рис. 5. Результаты моделирования готовности архитектуры BAS (результирующие показатели определены с погрешностью 10^{-4})

Как видно из графиков на рис.5, проведение мероприятий обслуживания снижает как установившееся значение функции готовности, так и ее минимум. В связи с принятыми допущениями об постепенном устранении дефектов и уязвимостей, готовность системы без обслуживания асимптотически стремится к единице. Для моделей с обслуживанием характерно стремление готовности к значению, определяемому крайним правым фрагментом, что для общего обслуживания составляет:

$$A_{MBAS\ 2}\text{const} = \mu Mt/(\lambda Mj+\mu Mt),$$

а для раздельного обслуживания составляет:

$$A_{MBAS\ 3}\text{const} = \mu Mt/(\lambda Mr+\lambda Ms+\mu Mt).$$

Этим можно объяснить выигрыш модели с общим обслуживанием по показателям минимума функции готовности (на 0.0128) и стационарного значения функции готовности (на 0.0123).

Проведение обслуживания позволяет в 1.57 раз ускорить выявление и устранение дефектов и уязвимостей. При этом разница показателей $T_{MBAS\ I}$ const для моделей с общим и раздельным обслуживанием несущественна (менее 1%). Но здесь необходимо учитывать фактор того, что на вход моделей MBAS2 и MBAS3 были поданы одинаковые значения вероятностей обнаружения и выявления дефектов и уязвимостей PCS и PCR. И если в модели MBAS3 PCS и PCR могут изменяться в диапазоне 0..1 одновременно, то в модели MBAS3 параметры PCS и PCR одновременно могут принимать максимальное значение 0.4142.

Выводы

В статье разработаны марковские модели готовности BAS с учетом внутрисистемных (дефекты аппаратных и программных средств) и внешних (атаки на уязвимости служб DNS и DHCP) факторов и проанализированы модели системы без процедур обслуживания, с общим и раздельным обслуживанием по дефектам и уязвимостям.

Результаты моделирования показали, что система без обслуживания обладает самыми высокими показателями готовности, при отсутствии дефектов и уязвимостей ее готовность асимптотически стремится к единице. С другой стороны системы с раз-

дельным и общим обслуживанием позволяют в 1.57 раз быстрее выявить и устранить дефекты и уязвимости.

Практический интерес представляют разработанные Matlab-программы, которые можно использовать в инженерной практике.

Дальнейшие исследования следует направить на:

- разработку и исследование марковских моделей и инструментальных средств оценки готовности архитектуры BAS с учетом ограниченного количества процедур обслуживания;

- исследование влияния входных параметров на результирующие показатели марковских моделей оценки готовности архитектуры BAS;

- разработку метода определения вида и оптимального количества процедур обслуживания для максимизации показателей готовности и минимизации периода устранения дефектов и уязвимостей.

Интересным решением могут быть адаптивные стратегии с изменяющимся режимом обслуживания по времени (комбинации моделей MBAS1-3).

Список литературы

1. Розрахунок показників безвідмовності для IT-систем з хмарною послугою NaaS / В.С. Харченко, Ю.Л. Поночовний, К.С. Вишвцева, К.Д. Безугла // Системи обробки інформації. – Х.: ХУПС, 2016. - Вип. 9. – С. 177-181.

2. Al-Sudani Mustafa Qahtan Abdulmunem. The method of IMECA-based security assessment: case study for building automation system / Mustafa Qahtan Abdulmunem Al-Sudani, Waleed Al-Khafaji Ahmed, V. S. Kharchenko // Системи обробки інформації. - 2016. - Вип. 1. - С. 138-144.

3. Granzer, W. Security in Networked Building Automation Systems. [Електронний ресурс]/W. Granzer, W. Kastner, N. Georg, F. Praus// ViennaUniversity of TechnologyInst. of Computer Aided Automation, Automation Systems GroupTreitlstraße 1-3, A-1040 Vienna, Austria. – Режим доступу: http://osgug.ucaiug.org/utilisec/embedded/ Shared %20Documents/Device%20Security/Epoch Inputs/ BAS%20 Security.pdf – 18.09.2016 г.

4. Trivedi K. S. Dependability and security models / K. S. Trivedi, D. S. Kim, A. Roy and D. Medhi // Design of Reliable Communication Networks, 2009. DRCN 2009. 7th International Workshop on, Washington, DC, 2009, pp. 11-20.

5. Абдул-Хади А.М. Разработка базовых марковских моделей для исследования готовности коммерческих веб-сервисов / А.М. Абдул-Хади, Ю.Л. Поночовный, В.С. Харченко // Радіоелектронні і комп'ютерні системи. - 2013. - № 5. - С. 186–191

6. Харченко В.С. Базовые многофрагментные макромодели оценки надежности отказоустойчивых компьютерных систем информационно-управляющих комплексов / В.С. Харченко, О.Н. Одарущенко, Е.Б. Одарущенко // Радіоелектронні і комп'ютерні системи. – 2006. – Вип. 5(17). – С. 62-70.

7 Боярчук А.В. Разработка и исследование базовых моделей отказоустойчивых Web-сервисов / А.В. Боярчук, Ю.Л. Поночовный, В.С.Харченко // Радиоэлектронные и компьютерные системы. – Х., ХАИ, 2010. – № 5(46). – С. 42-49.

8. Функция для рисования графов и орграфов средствами MATLAB [Электронный ресурс]. – Режим доступа: http://iglin.exponenta.ru/All/ grth/grPlot.html – 18.09.2016 г.

9. Vyacheslav S. Kharchenko. Availability Assessment of Information and Control Systems with Online Software Update and Verification / Vyacheslav S. Kharchenko, Yuriy Ponochovnyi, Artem Boyarchuk // Ermolayev, V., Mayr, H.C., Nikitchenko, M., Spivakovsky, A., Zholtkevych, G. (eds.): Information and Communication Technologies in Education, Research and Industrial Applications. Springer Verlag, Berilin-Heidelberg, CCIS Vol. 469, 2014. – P. 300-324.

Надійшла до редколегії 16.09.2015

Рецензент: д-р техн. наук, проф. Б.М. Конорєв, Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», Харків.

МАРКІВСЬКІ МОДЕЛІ ГОТОВНОСТІ ІНФОРМАЦІЙНО-УПРАВЛЯЮЧОЇ СИСТЕМИ «РОЗУМНОГО» БУДИНКУ ПРИ РОЗДІЛЬНОМУ І СПІЛЬНОМУ ОБСЛУГОВУВАННІ З НАДІЙНОСТІ ТА БЕЗПЕКИ

В.С. Харченко, Аль-Судані Мустафа Кахтан Абдулмунем, Ю.Л. Поночовний

У статті розглянуті питання побудови марківських моделей і оцінки готовності інформаційно-управляючої системи «розумного» будинку (smart building automation system, BAS). Визначено, що причинами відмов і недоступності компонент архітектури BAS можуть бути як внутрішньо системні, так і зовнішні фактори, серед яких виділені програмні дефекти і уразливості. Останні розглядаються як елементи двох непересічних множин. Детально проаналізовано моделі архітектури BAS з програмними дефектами і атакованими уразливими без процедур обслуговування, із спільним і роздільним обслуговуванням з надійності (дефекти) і безпеки (уразливості). Сформульовано рекомендації щодо вибору стратегій і параметрів обслуговування.

Ключові слова: *інформаційно-управляюча система, розумний будинок, програмні дефекти і уразливості, готовність, надійність, безпека, стратегії обслуговування, марківські моделі.*

MARKOV AVAILABILITY MODEL OF SMART BUILDING AUTOMATION SYSTEM WITH SEPARATE AND COMMON RELIABILITY-SECURITY RELATED MAINTENANCE

V.S. Kharchenko, Al-sudani Mustafa Qahtan Abdulmunem, Y.L. Ponochovnyi

The paper deals with development and research of Markov models of smart building automation systems (BAS). It has been taken into account that BAS failures can be caused by intra (reliability) and external (security) reasons including software faults and attacks on vulnerabilities. The sets of faults and vulnerabilities are considered as separated and disjoint ones. Markov models of BAS architecture with occurred software faults and attacked vulnerabilities considering three maintenance strategies are systemized and researched. These strategies are based on recovery without maintenance, maintenance with common and separate activities on reliability (faults) and vulnerabilities (security). Recommendations concerning choice of strategies and parameters of maintenance are suggested.

Keywords: *building automation system, availability, smart home, software faults and vulnerabilities, availability, reliability, security, maintenance strategy, Markov models.*