УДК 004.05

Ю.Л. Поночовный[1], А.В. Боярчук[2], В.С. Харченко[2]

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

МОДЕЛИ ГОТОВНОСТИ ВЕБ-СИСТЕМЫ С УЧЕТОМ ПРОГРАММНЫХ ОТКАЗОВ И АТАК НА УЯЗВИМОСТИ КОНФИГУРАЦИИ СЛУЖБЫ DNS

В статье рассмотрены вопросы оценки непрерывности функционирования веб-систем. Определено, что причинами недоступности их сервисных услуг могут быть как внутрисистемные, так и внешние факторы, среди которых выделены атаки на уязвимости серверной части. Разработаны три марковские модели функционирования веб-системы в условиях проявления программных дефектов и выполнения атак на уязвимости служб DNS, DHCP и Route. При построении моделей учтено устранение уязвимостей программного кода в процессе эксплуатации системы. По результатам моделирования сделаны выводы о влиянии вероятности выявления и устранения уязвимостей и скорости восстановления системы на поведение функции готовности. Для моделирования используется программный комплекс MATLAB.

Ключевые слова: *модель готовности, сервис-ориентированная веб-система, уязвимости доступности.*

Введение

Информационная безопасность является одной из важных составляющих глобальной безопасности. Успешный запуск и эксплуатация веб-систем возможен только при условии окупаемости затрат на их функционирование и положительной прибыли. При этом точка окупаемости достигается после введения системы в эксплуатацию, а при неправильной оценке рисков вообще может быть не достигнута. В настоящее время разработаны инструментальные средства, предназначенные для автоматизации и профилактики поиска уязвимостей программ.

В [1, 2] выполнен анализ жизненного цикла уязвимостей, обосновывающий необходимость проведения регулярных профилактик аудита безопасности для выявления новых и неустраненных уязвимостей информационного ресурса. С другой стороны, проведение аудита безопасности не должно снижать готовность и доступность ресурса. Это требование обосновывает необходимость разработки и исследования соответствующих моделей веб-систем.

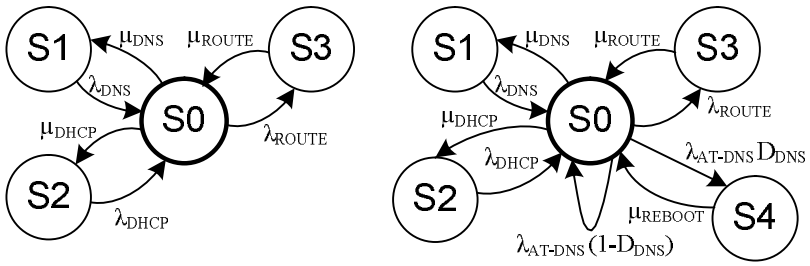
Однако, большинство известных моделей атак, угроз и инцидентов имеют вероятностный характер оценки рисков. Лишь в некоторых источниках указывается на возможность моделирования веб-систем с помощью полумарковских процессов [3] и аппарата сетей Петри [4]. В [5] рассмотрены модели функционирования информационных ресурсов на основе многофрагментного моделирования, позволяющие учесть влияние уязвимостей и профилактик аудита безопасности на доступность системы.

Целью данного исследования является разработка марковских моделей готовности веб-систем с учетом атак и исследование влияния входных параметров модели на функцию готовности. В статье рассматривается архитектура информационного ресурса, которая включает взаимодействующие сервисы DNS, DHCP и маршрутизации (Route).

Модели без устранения уязвимостей при атаках на службу DNS

В качестве базовой модели рассматривается модель идеальной веб-системы без атак, в которой протекают процессы отказов и восстановлений ПС соответствующих сетевых служб (МА1). Результирующие характеристики такой модели зачастую выставляются представителями хост-компаний как значения готовности или аптайма площадок размещения веб-сервисов [6]. Размеченный граф состояний и переходов такой модели показан на рис. 1, а. Он включает исходное работоспособное состояние S0 и неработоспособные состояния S1, S2 и S3 [7]. Переходы в неработоспособные состояния взвешены соответствующими интенсивностями отказов λ_{DNS}, λ_{DHCP} и λ_{ROUTE}. Возврат в работоспособное состояние осуществляется после восстановления служб с интенсивностями μ_{DNS}, μ_{DHCP} и μ_{ROUTE}.

Вторая модель (МА2) описывает функционирование веб-системы в условиях проведения одной атаки на службу DNS с перезапуском системы после удачной атаки без устранения уязвимости. Граф модели показан на рис. 1, б. Изначально веб-система функционирует в условиях проявления отказов и восстановления служб DNS, DHCP и Route. Атаки на службу DNS характеризуются интенсивностью laatdns и критичностью D_{DNS}. Поэтому в модели применен возврат в состояние S0 с интенсивностью $(1-D_{DNS})*\lambda_{AT\text{-}DNS}$. После проведения атаки (переход в состояние S4 с интенсивностью $D_{DNS}*\lambda_{AT\text{-}DNS}$) система теряет работоспособность. После перезапуска восстанавливает ее с интенсивностью μ_{REBOOT}.



а б

Рис. 1. Размеченные графы моделей веб-системы
без атак МА1 (а) и с перезапуском после атаки МА2 (б)

Модель готовности при устранении уязвимостей службы DNS

Данная модель (МА3) описывает функционирование веб-системы в условиях проведения атак на уязвимости службы DNS с последующим их устранением. Так как устранение уязвимостей возможно только при изменении программного кода, то изменяется параметр потока отказов службы DNS (λ_{DNS}= λ_{DNS}–$\Delta\lambda_{DNS}$). В модели МА3 рассматривается устранение уязвимости только после ее проявления (после удачной атаки на нее) путем разработки и установки патча.

После успешной атаки возможны два независимых варианта развития событий. Первый - запускаются процедуры поиска и устранения уязвимости и система переходит в состояние патчеризации S5. Второй - существует вероятность необнаружения уязвимости, поэтому система из состояния S4 может вернуться в S0 без устранения уязвимости и быть снова атакованной. Для оценки вероятности обнаружения и устранения уязвимости вводится дополнительный параметр D_P.

Согласно рис. 2 изначально веб-система функционирует в условиях проявления отказов и восстановления служб DNS, DHCP и ROUTE. После проведения атаки на службу DNS (переход в состояние S4 с интенсивностью D_{DNS}*$\lambda_{AT\text{-}DNS}$) система теряет работоспособность. После проявления, уязвимость может быть устранена с вероятностью D_P (система остается в состоянии S4 с интенсивностью D_P*μ_{REBOOT} и далее переходит в состояние S5 с интенсивностью λ_{PATCH}). Или система с интенсивностью $(1–D_P)$*μ_{REBOOT} вернется в исходное состояние без устранения уязвимости. После проявления и устранения всех уязвимостей система продолжает функционировать в условиях проявления отказов и восстановления ее служб (состояния Sn…Sn+3).

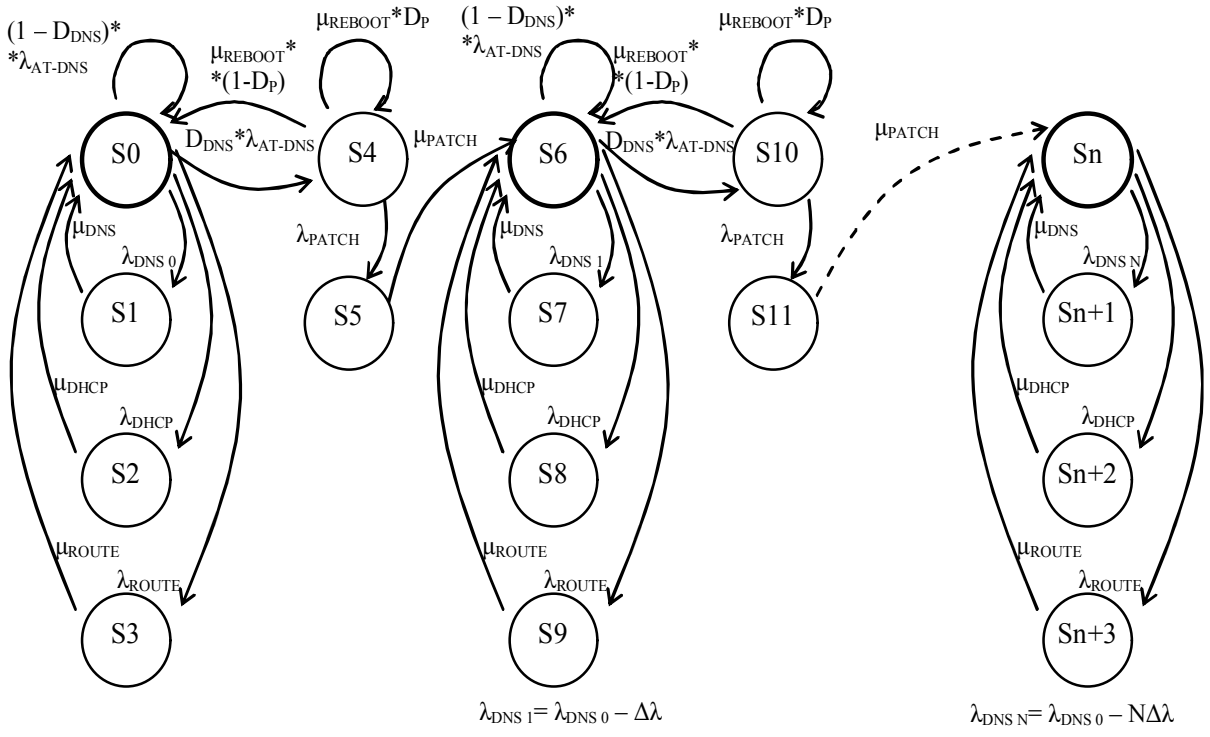


Рис. 2. Размеченный граф модели готовности веб-системы
с устранением уязвимостей (МА3)

Сравнение результатов моделирования

Результаты моделей МА1-МА3 получены при значениях входных параметров из табл. 1.

Таблица 1

Значения входных параметров моделей

Имя	Значение	Ед.измерения
ladns	3e-5	1/час
ladhcp	1.5e-5	1/час
laroute	5e-4	1/час
mudns	0.67	1/час
mudhcp	1	1/час
muroute	0.33	1/час
laatdns	6.279e-3	1/час
ddns	0.77	
dp	0.5	
mureboot	0.5	1/час
murecovery	0.33	1/час
deltaldns	4e-6	1/час
lapath	0.0104	1/час
mupath	0.33	1/час

Решение СДУ Колмогорова было выполнено в системе Matlab с помощью метода ode15s для временного интервала [0…5000] часов.

На рис. 3 представлены результаты сравнения разработанных моделей.

При принятых значениях входных параметров, функция готовности модели МА1 принимает устоявшееся значение A = 0,99844 в течение первых 20 часов функционирования.

Этот же уровень примерно через 45000 часов достигнет функция готовности системы с устранением уязвимостей (МА3).

Если уязвимости не устранять, а ограничиться только перезапуском, то готовность веб-системы уменьшиться до устоявшегося значения в 0,9888 (МА2).

Минимум функции готовности модели МА3 располагается ниже устоявшегося значения функции готовности МА2, так как для поиска и устранения уязвимости требуется больше времени, чем для перезапуска системы ($\mu_{RECOVERY}$=0.33 < μ_{EBOOT}=0.5).

Дальнейший интерес представляет исследование влияния отдельных параметров на характер поведения и значения функции готовности.

Для модели МА3 были отобраны следующие параметры (табл. 2):

Таблица 2

Значения переменных параметров модели МА3

Имя	Значения	Ед.измерения
dp	[0 0.1 0.2 0.5 0.7 1]	
lapath	[1 .1 .01 .005 .001]	1/час
mupath	[0.05 0.1 0.5 1 2]	1/час

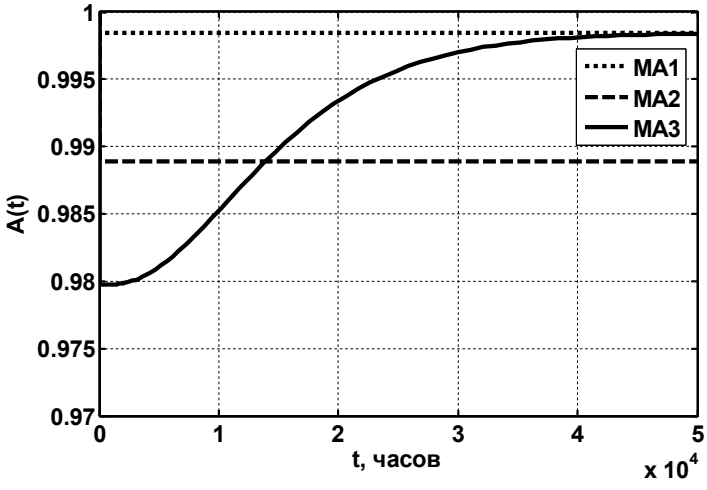
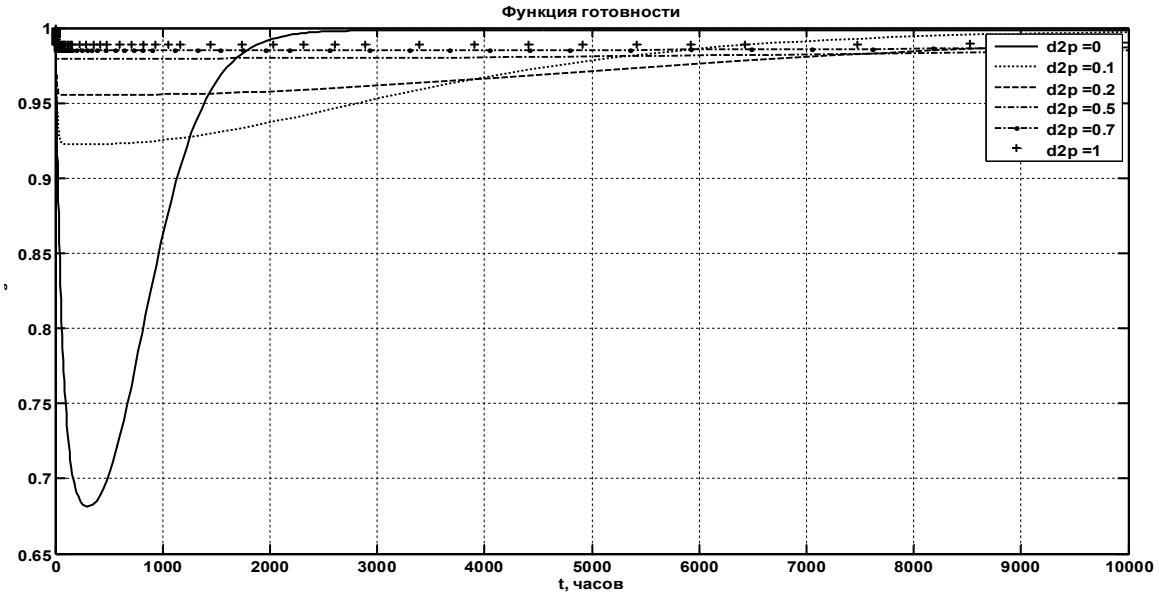
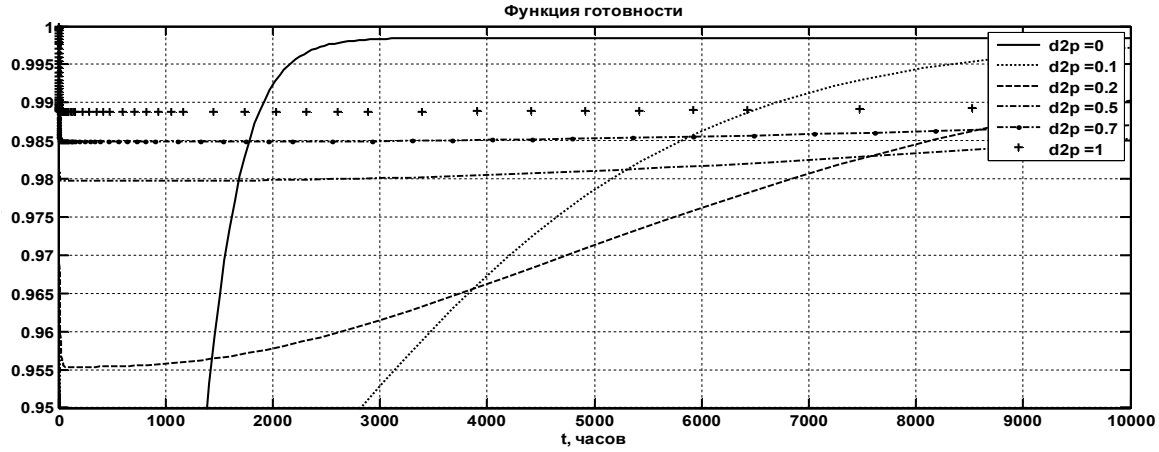


Рис. 3. Графики функции готовности моделей МА1, МА2 и МА3

Для исследования влияния указанных параметров были разработаны специальные циклические программные конструкции Matlab. Временной интервал исследования увеличен до [0…15000] часов. Результаты моделирования в виде графических зависимостей показаны на рис.4 – 6. Графики на рис. 4 иллюстрируют поведение функции готовности при различной вероятности обнаружения атаки D_P. При нулевой вероятности система вырождается (показывает те же результаты) в модель МА2 для значения μ_{EBOOT} = 0.33, а при D_P = 1 показывает минимальное время перехода в устоявшийся режим.



а



б

Рис. 4. Графики функции готовности модели МАЗ при различной вероятности устранения неисправности D_P на временном масштабе [0…10000] (а) и с укрупненным масштабом (б)

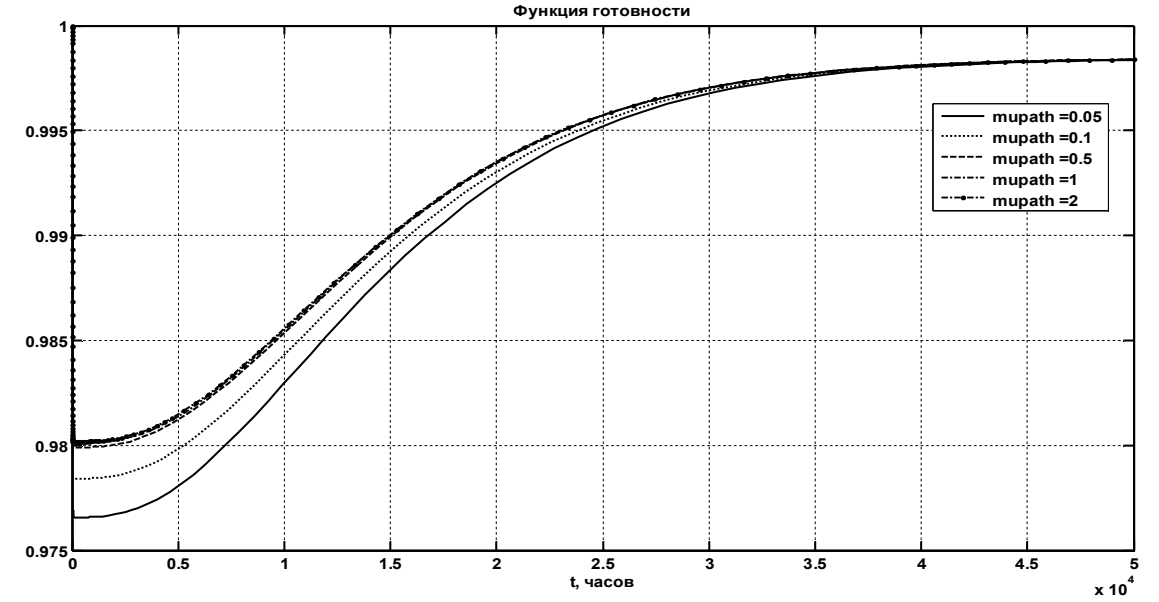
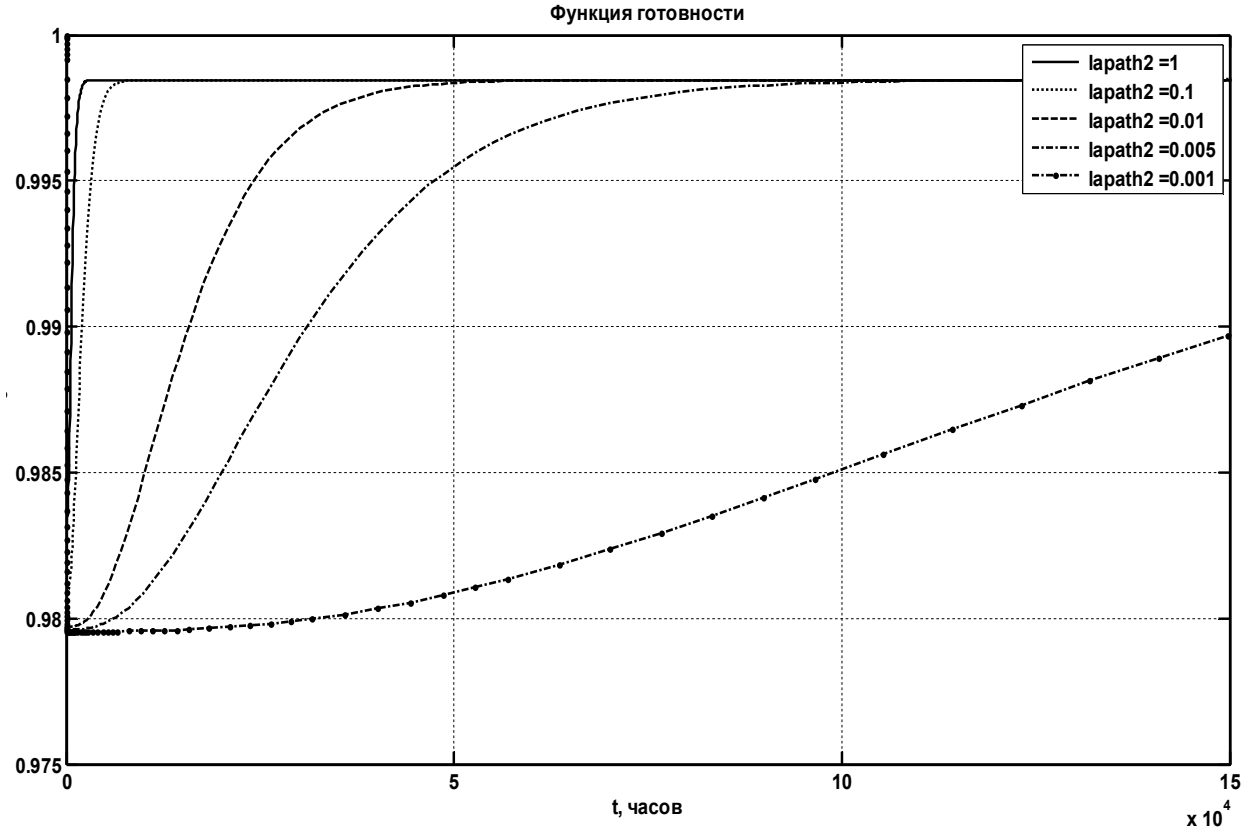
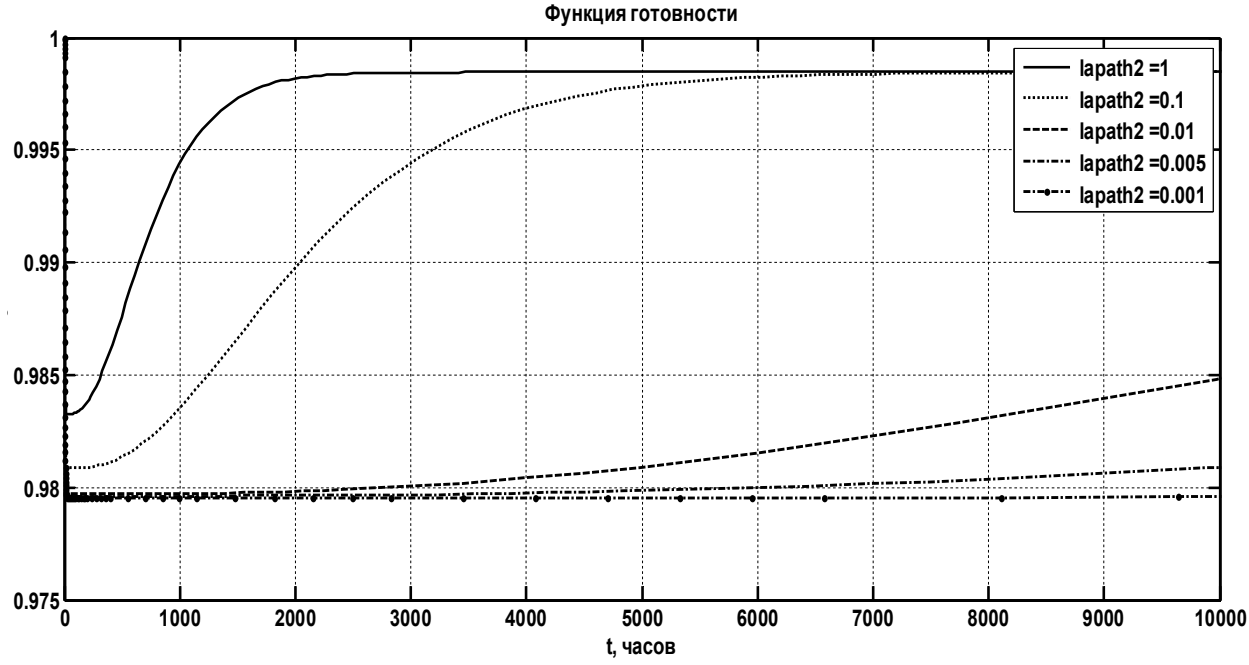


Рис. 5. Графики функции готовности модели МАЗ при различной скорости установки патча на временном отрезке [0…150000]



а



б

Рис. 6. Графики функции готовности модели МАЗ при различных интенсивностях разработки патча на временных отрезках [0…150000] (а) и [0…10000] (б)

Таким образом, значения параметра D_P существенно влияют на величину минимума функции готовности и на длительность периода ее перехода в устоявшийся режим. Анализ графиков на рис. 5 показывает, что значение параметра μ_{PATH} влияет на величину минимума функции готовности. Так, при μ_{PATH}=2 (1/час) минимум функции готовности составит 0,981 в точке t=23 часов; а при μ_{PATH}=0.05 (1/час) минимум функции готовности составит 0,977 в точке t=36 часов.

Также значение параметра μ_{PATH} не влияет на максимальное значение функции готовности в установившемся режиме Pg=0,99844.

Анализ графиков на рис.6 показывает, что значение параметра λ_{PATH} (скорость разработки патча после проявления уязвимости) для модели МА3 существенно влияет на длительность периода перехода функции готовности в стационарный режим; влияние на минимум функции готовности не так выражено.

Так, при λ_{PATH} =1 (1/час) минимум функции готовности составит 0,983 в точке t=22 часа; а при λ_{PATH}=0.005 (1/час) минимум функции готовности составит 0,979 в точке t=11 часов.

Также значение параметра λ_{PATH} не влияет на максимальное значение функции готовности в установившемся режиме.

Выводы

Анализ результатов моделирования готовности веб-системы с учетом атак на компоненты и устранения уязвимостей конфигурации показал, что: для ускорения перехода функции готовности в стационарное состояние следует повышать вероятность выявления и устранения уязвимостей после атак на них; в начальный период эксплуатации минимум функции готовности системы будет зависеть от параметров λ_{PATH} и μ_{PATH} (чем быстрее будет разработан патч и система восстановится после атаки, тем выше минимум функции готовности).

Дальнейшие исследования следует направить на разработку интегрированных стратегий обслуживания веб-систем с учетом аппаратных, программных средств и политики безопасности; оценку влияния на готовность веб-систем других видов уязвимостей [8]; анализ гибких стратегий обслуживания и обновления облачных ИТ-инфраструктур.

Список литературы

1. *Рекомендация МСЭ-Т X.1500. Методы обмена информацией о кибербезопасности. Женева, 2012. – 36 С.*
2. *Рекомендация МСЭ-Т X.1520. Общеизвестные уязвимости и незащищенность. Женева, 2012 г. – 22 С.*
3. *Gashi I. Uncertainty Explicit Assessment of Off-The-Shelf Software: A Bayesian Approach / I. Gashi, P. Popov, V. Stankovic // Elsevier Journal of Information and Software Technology, Elsevier, 51(2), 2009, pp.497–511.*
4. *Trivedi K.S. Dependability and security models / K.S.Trivedi, D.S. Kim, A.Roy, D. Medhi // In Proc. of the 7th Workshop on the Design of Reliable Communication Networks. – 2009. – pp.11-20.*
5. *Kharchenko V. Web Systems Availability Assessment Considering Attacks on Service Configuration Vulnerabilities/ Kharchenko V., Alaa Mohammed Abdul-Hadi, Boyarchuk A., Ponochovny Y. / Seria "Advances in Intelligent Systems and Computing", Vol.286, / W. Zamojski et al (edits), Springer International Publishing Switzerland, 2014. - pp.275-284.*
6. *Papazoglou M.P. Web Services: Principles and Technology / M.P. Papazoglou // Prentice Hall. – 2007. – vol. 21. – P. 139-145.*
7. *Алаа Мохаммед Абдул-Хади. Разработка базовых марковских моделей для исследования готовности коммерческих веб-сервисов / Алаа Мохаммед Абдул-Хади, Ю.Л. Поночовный, В.С. Харченко // Радіоелектронні і комп'ютерні системи. – 2013. – Вип. 5(64). – С. 186-191.*
8. *Fernandes S. Dependability assessment of virtualized networks. [Text] / Fernandes S. Tavares E., Santos M., Lira V., Maciel P. // In Proc. of the IEEE International Conference on Communications (ICC) – 2012. – pp.2711-2716.*

Поступила в редколлегию 22.04.2015

Рецензент: д-р техн. наук, проф. Б.М. Конорев, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.

МОДЕЛІ ГОТОВНОСТІ ВЕБ-СИСТЕМИ З УРАХУВАННЯМ ПРОГРАМНИХ ВІДМОВ І АТАК НА ВРАЗЛИВОСТІ КОНФІГУРАЦІЙ СЛУЖБ DNS

Ю.Л. Поночовний, А.В. Боярчук, В.С. Харченко

У статті розглянуті питання оцінки безперервності функціонування веб-систем. Визначено, що причинами недоступності їх сервісних послуг можуть бути як внутрішньосистемні, так і зовнішні фактори, серед яких виділено атаки на уразливості серверної частини. Розроблено три марковские моделі функціонування веб-системи в умовах прояву програмних дефектів та виконання атак на вразливості служб DNS, DHCP і Route. При побудові моделей враховано усунення вразливостей програмного коду в процесі експлуатації системи. За результатами моделювання зроблено висновки про вплив ймовірності виявлення та усунення вразливостей і швидкості відновлення системи на поведінку функції готовності. Для моделювання використовується програмний комплекс MATLAB.

Ключові слова: *модель готовності, сервіс-орієнтована веб-система, вразливості доступності.*

AVAILABILITY MODELS OF WEB-SYSTEM CONSIDERING SOFTWARE FAULTS AND ATTACKS ON THE CONFIGURATION VULNERABILITIES OF DNS

Y.L. Ponochovniy, A.V. Boyarchuk, V.S. Kharchenko

The paper assesses the continuity of web-systems up-state. It's determined that the reasons for the unavailability of services can be both intra and external factors, among which are the attacks on the server-side vulnerabilities. Three Markov's models of functioning web-based system considering software faults and execution of attacks on vulnerable services DNS, DHCP, and Route are developed. Eliminating configuration vulnerabilities during system operation is taken into account. The modeling outcomes allow concluding the effect of the probability of detecting and eliminating vulnerabilities, and speed recovery system on the behavior of readiness. Software package MATLAB is applied for service modeling.

Key words: *availability model, service-oriented web-system, the vulnerability of availability.*