УДК 004.05

Ю.Л. Поночовный[1], В.С. Харченко[2], Т.П. Межиборец[1], К.А. Ревенко[1], К.А. Шуст[1]

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

ПРИМЕНЕНИЕ ДИСКРЕТНЫХ ЗАКОНОВ РАСПРЕДЕЛЕНИЯ В МОДЕЛИ ДОСТУПНОСТИ ИНФОРМАЦИОННОГО РЕСУРСА С ПРОФИЛАКТИЧЕСКИМИ МЕРАМИ АУДИТА БЕЗОПАСНОСТИ

Рассматриваются компьютерные методы оценки доступности информационного ресурса с профилактическими мерами аудитов безопасности. Предлагаются элементы инструментально-ориентированной методики рационального функционирования ресурса в условиях проведения последовательных атак на уязвимости конфигурации службы DNS, а также периодических профилактических мероприятий (аудита безопасности программных средств) по обнаружению и устранению уязвимостей с последующим их устранением без изменения программного кода или с помощью патчеризации. Для моделирования используется программный комплекс MATLAB.

Ключевые слова: *модель доступности, информационный ресурс, профилактики аудита безопасности, дискретный закон распределения.*

Введение

Информационная безопасность является одной из важных составляющих глобальной безопасности. В процессе глобализации, в условиях построения информационного общества роль информационной безопасности усиливается и, наоборот, глобальные процессы влияют на информационную безопасность и взаимосвязанную с ней экономическую, национальную и глобальную. Особенности неограниченного и неконтролируемого воздействия, несанкционированного доступа, а также возникновения компьютерных вирусов и других угроз, вызывают необходимость в обеспечении информационной безопасности. 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 профилактик аудита безопасности не должно снижать доступность ресурса. Это требование обосновывает необходимость разработки и исследования соответствующих моделей доступности.

В [3, 4] рассмотрены модели функционирования информационных ресурсов на основе аппарата многофрагментного моделирования, позволяющие учесть влияние уязвимостей и профилактик аудита безопасности на доступность системы. В разработанных моделях для описания процесса выявления уязвимостей используется геометрическое распределение. Этот вариант является частным случаем моделирования процесса выявления уязвимостей и требует детализации допущений модели.

Постановка задачи исследования. Целью данного исследования является анализ применимости дискретных законов распределения вероятности выявления j уязвимостей в ходе профилактики в модели доступности информационного ресурса с учетом атак на его сервисы. В статье рассматривается архитектура информационного ресурса, которая включает взаимодействующие сервисы DNS, DHCP и маршрутизации (Route). В качестве базовых рассматриваются биномиальное, геометрическое, гипергеометрическое распределения дискретных случайных величин и закон редких явлений (Пуассона).

Математическая модель доступности информационного ресурса

Представленная модель доступности описывает периодические профилактические мероприятия аудита безопасности по обнаружению и устранению уязвимостей и допускает устранение обнаруженной в ходе атаки уязвимости без изменения программного кода (λ_{DNS}=const). Размеченный орграф для системы с тремя уязвимостями представлен на рис. 1, согласно которому изначально информационный ресурс функционирует в условиях проявления отказов и восстановления служб DNS, DHCP и маршрутизации (Route). После проведения атаки на службу DNS (переход в состояние S_5 с интенсивностью d1dns*laatdns) система теряет работоспособность, но может ее восстановить путем перезапуска без устранения неисправности с условной интенсивностью (1–d2p)*murecovery, или с устранением уязвимости с условной интенсивностью d2p*murecovery. С некоторой периодичностью в системе проводятся профилактиче-

ские мероприятия (состояние S_4) в результате которых может быть обнаружено и устранено от 0 до n_v уязвимостей. После проявления и устранения всех уязвимостей система продолжает функционировать в условиях проявления отказов и восстановления ее служб (состояния $S_n \ldots S_{n+3}$).

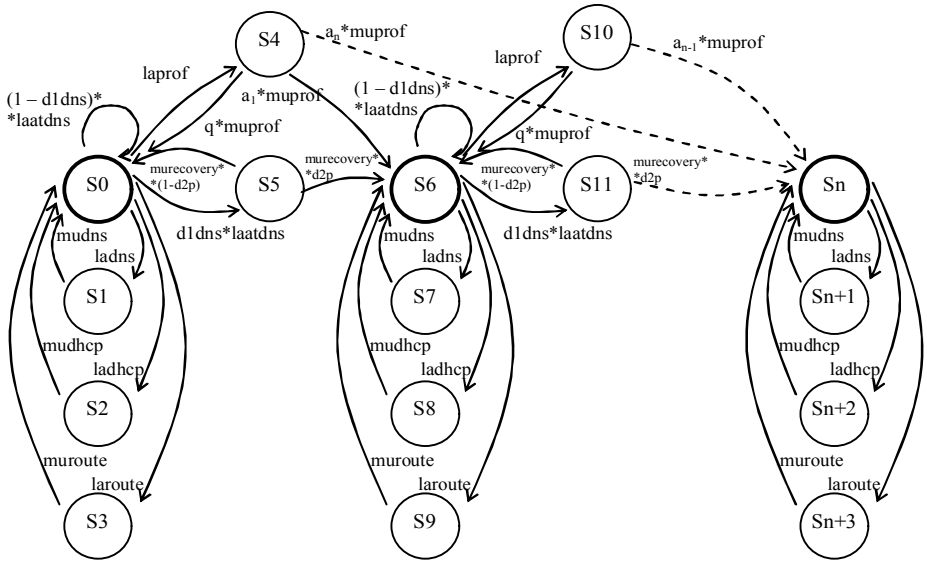

Рис. 1. Размеченный граф состояний и переходов модели доступности информационного ресурса

Так как при профилактике возможно обнаружение и устранение не только одной, но и нескольких уязвимостей из множества $[1 \ldots n_v]$, то необходимо ввести параметр α_j вероятности обнаружения j ($j \in [1 \ldots n_v]$) уязвимостей. Очевидно, что $\sum \alpha_j = 1$, а значения $\alpha_1, \alpha_2, \ldots \alpha_j, \ldots \alpha_{nv}$ имеют дискретный закон распределения. Для расчетов в работе принят геометрический закон распределения коэффициентов α_j с параметрами по умолчанию: p=0.7 (вероятность выявления одной уязвимости) и q=1–p=0.3.

Тогда для соблюдения равенства $\sum \alpha_j = 1$ значения коэффициентов α_j будут рассчитываться по формулам из табл. 1.

Таблица 1

Вероятности обнаружения j-уязвимостей

j	1	2	3	…	nv–1	nv
α_j	p	q*p	q^2*p	…	q^{nv-2}*p	1-$\sum\alpha_j$

Выбор дискретного закона распределения вероятности выявления j-уязвимостей

В рассмотренной модели доступности был использован геометрический закон распределения дискретной случайной величины. Согласно [5] область применения этого закона ограничивается условием независимости испытаний. Следовательно область применения модели доступности с геометрическим законом распределения дискретной случайной величины – проведение профилактик аудита безопасности, при которых события выявления j-уязвимостей не зависят друг от друга. Такой случай характерен для информационных ресурсов, собранных из компонент различных производителей. Профилактики аудита безопасности таких компонент выполняются несколькими независимыми командами. Также для выполнения требования $\sum \alpha_j \approx 1$ накладывается дополнительное ограничение $p*n_v>5$. Возможны и другие варианты проведения проверок и выявления уязвимостей, которым будут соответствовать другие законы распределения. Рассмотрим их применимость в разработанной модели доступности.

Биномиальный закон (распределение Бернулли) описывает случай повторного выявления событий в группе (с возвратом). Соответственно он применим для случаев, когда программный модуль (сервис) с выявленной уязвимостью в пределах одной профилактики не останавливается, а продолжает проверяться для выявления дополнительных уязвимостей. Такой вариант профилактик возможен на начальном этапе эксплуатации системы при возможности проведения длительных профилактик с простоем информационного ресурса. Также на начальном этапе эксплуатации вероятность выявления уязвимости в системе высока p>0.1.

Закон Пуассона (закон редких явлений) является частным случаем биномиального закона [5] и применим для этапа эксплуатации информационного ресурса, когда легковыявляемые уязвимости устранены и вероятность выявления уязвимости p<0.1.

Применение равномерного закона распределения не представляется возможным, так как сложно привести практический пример равновероятного одновременного обнаружения одной, двух, трех и более уязвимостей в системе, состоящей из разных сервисов.

Гипергеометрический закон распределения применим для профилактик, жестко ограниченных временем проведения, когда за одну профилактику возможно проверить только часть программных мо-

дулей. Также следует отметить, что параметрами этого закона выступают не вероятность выявления одной уязвимости p, а общее количество программных модулей N_m и количество модулей, проверяемых при одной профилактике m. В табл. 2 обобщена информация об использовании дискретных законов распределения в модели доступности информационного ресурса.

Таблица 2

Применимость дискретных законов распределения в модели доступности информационного ресурса

№	Закон распределения	Выражение для α_j	Вариант применения
1	Биномиальный	$\alpha_j = C_{nv}^{\ j} * p^j * q^{nv-j}$; $q=1-p$; $p>0.1$	Сервис с выявленной уязвимостью в пределах одной профилактики не останавливается, а продолжает проверяться для выявления дополнительных уязвимостей, вероятность выявления уязвимости высока
2	Пуассона	$\alpha_j = (p*n_v)^j/(e^j*j!)$; $q=1-p$; $p*n_v<1$, $p<0.1$	Легковыявляемые уязвимости устранены и вероятность выявления уязвимости низка, невыявленных уязвимостей много
3	Геометрический	$\alpha_j = q^{j-1}*p$; $q=1-p$; $p*n_v>5$	Проведение профилактик отдельных модулей информационного ресурса независимыми командами
4	Гипергеометрический	$\alpha_j = [C_m^{\ j} * C_{Nm-m}^{\ nv-j}]/C_{Nm}^{\ nv}$; $Nm>m\geq n_v$	Профилактики жестко ограниченны временем проведения, за одну профилактику возможно проверить только часть программных модулей

Параметризация модели доступности и анализ результатов моделирования

Исходные данные (значения входных параметров) для построения модели доступности информационного ресурса представлены в табл. 3, согласно [4]. Так как рассматриваемые модели представляют собой программные конструкции среды Mathlab, то в данной таблице введены и в дальнейшем будут использованы символьные обозначения входных параметров.

На рис. 2 представлены результаты расчета модели доступности для различных законов распределения. Очевидно, что для случаев применения биномиального и гипергеометрического закона событие вероятного устранения всех невыявленных уязвимостей наступает раньше. Это объясняется тем, что при значениях параметров p=0.7, Nm=300 и m=100, принятых при расчетах модели, наиболее вероятно выявление нескольких уязвимостей в ходе одной профилактики. В случае применения закона редких явлений при p=0.01 устранение всех уязвимостей происходит в более поздний срок (после 8000 часов эксплуатации).

Выводы

В статье предложены элементы методики построения марковских моделей оценки доступности информационного ресурса с учетом атак на уязвимости его сервисов. Обоснована применимость дискретных законов распределения при моделировании выявления уязвимостей в ходе профилактик аудита безопасности, в частности, проанализированы варианты применения законов Пуассона, геометрического, биномиального и гипергеометрического.

Таблица 3

Вероятности обнаружения j-уязвимостей

№	Параметр	Обозначение	Значение	Ед.изм.
1.	Интенсивность проявления дефектов ПС службы DNS	ladns	3e-5	1/□□□
2.	Интенсивность проявления дефектов ПС службы DHCP	ladhcp	1.5e-5	1/час
3.	Интенсивность проявления дефектов ПС службы Route	laroute	5e-4	1/час
4.	Интенсивность восстановления службы DNS	mudns	0.67	1/час
5.	Интенсивность восстановления службы DHCP	mudhcp	1	1/час
6.	Интенсивность восстановления службы Route	muroute	0.33	1/час
7.	Интенсивность атак на доступность службы DNS	laatdns	6.3e-3	1/час
8.	Критичность атак на доступность службы DNS	d1dns	0.77	
9.	Интенсивность перезапуска службы после атаки на доступность	mureboot	0.5	1/час
10.	Интенсивность восстановления службы с устранением уязвимости	murecovery	0.22	1/час
11.	Интенсивность проведения профилактик аудита безопасности	laprof	4.5e-4	1/час
12.	Интенсивность восстановления после профилактик аудита безопасности	muprof	0.5	1/час
13.	Вероятность перезапуска с устранением уязвимости	d2p	0.5	
14.	Вероятность устранения уязвимости при проведении профилактики (для биномиального и геометрического распределения)	p ($p=\alpha_1$)	0.7	
15.	Вероятность устранения уязвимости при проведении профилактики (для распределения Пуассона)	p ($p=\alpha_1$)	0.01	
16.	Общее количество программных модулей N_m	Nm	300	
17.	Количество модулей, проверяемых при одной профилактике m	m	100	
18.	Количество невыявленных уязвимостей на начальном этапе	nv	10	

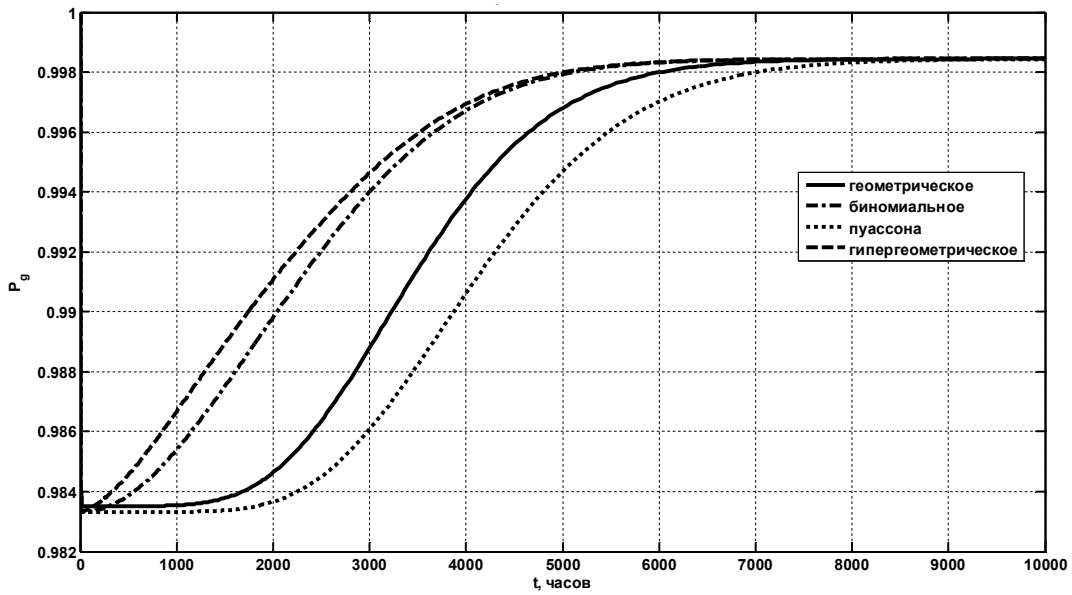

Рис. 2. Сравнение результирующих функций модели доступности при различных законах распределения вероятности выявления j уязвимостей при профилактике

Результаты моделирования показывают, что при принятых значениях входных данных система с профилактиками, выявляющими несколько уязвимостей, обеспечивает переход функции готовности в устоявшееся состояние за более короткий период.

Дальнейшие исследования следует направить на разработку интегрированных стратегий обслуживания сервис-ориентированных информационных ресурсов с учетом аппаратных, программных средств и политики информационной безопасности. Кроме того, представляет интерес исследование целесообразности и вариантов проведения гибких стратегий обслуживания и обновления информационных Cloud-ресурсов

Список литературы

1. Рекомендация МСЭ-Т X.1500. Методы обмена информацией о кибербезопасности. Женева, 2012 г. – 36 с.

2. Рекомендация МСЭ-Т X.1520. Общеизвестные уязвимости и незащищенность. Женева, 2012 г. – 22 с.

3. Алаа Мохаммед Абдул-Хади. Разработка базовых марковских моделей для исследования готовности коммерческих веб-сервисов [Текст] / Алаа Мохаммед Абдул-Хади, Ю.Л. Поночовный, В.С. Харченко // Радіоелектронні і комп'ютерні системи. – 2013. – Вип. 5(64). – С. 186-191.

4. Web Systems Availability Assessment Considering Attacks on Service Configuration Vulnerabilities / V. Kharchenko, Alaa Mohammed Abdul-Hadi, A. Boyarchuk, Y. Ponochovny / Seria "Advances in Intelligent Systems and Computing", Vol.286, / W. Zamojski et al (edits), Springer International Publishing Switzerland, 2014. – P. 275-284.

5. Вентцель Е.С. Теория случайных процессов и ее инженерные приложения [Текст] / Е.С. Вентцель, Л.А. Овчаров – М.: Высш. школа, 2000. – 383 с.

Поступила в редакцию 20.10.2014

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

ЗАСТОСУВАННЯ ДИСКРЕТНИХ ЗАКОНІВ РОЗПОДІЛУ В МОДЕЛІ ДОСТУПНОСТІ ІНФОРМАЦІЙНОГО РЕСУРСУ З ПРОФІЛАКТИЧНИМИ ЗАХОДАМИ АУДИТА БЕЗПЕКИ

Ю.Л. Поночовний, В.С. Харченко, Т.П. Межиборець, К.А. Ревенко, К.А. Шуст

Розглядаються комп'ютерні методи оцінки доступності інформаційного ресурсу з профілактичними заходами аудитів безпеки. Пропонуються елементи інструментально-орієнтованої методики функціонування ресурсу в умовах проведення послідовних атак на уразливості конфігурації служби DNS, а також періодичних профілактичних заходів (аудиту безпеки програмних засобів) з виявлення й усунення вразливостей без зміни програмного коду або за допомогою патчерізації. Для моделювання використовується програмний комплекс MATLAB.

Ключові слова: *модель доступності, інформаційний ресурс, вразливості, аудит безпеки, дискретний закон розподілу.*

USING OF DISCRETE DISTRIBUTION LAWS IN ACCESSIBILITY MODELS OF INFORMATION RESOURCES WITH PREVENTIVE MEASURES OF SECURITY AUDIT

J.L. Ponochovny, V.S. Kharchenko, T.P. Mezhiborets, K.A. Revenco, K.A. Shust

Software-based methods of information resources accessibility assessment are applied taking into consideration preventive measures of security audits. The elements of the instrumental-oriented technique for rational functioning of the system in conditions of successive attacks on the service configuration DNS vulnerabilities and periodic preventive measures (particular, auditing of software security) to detect and correct vulnerabilities with their subsequent elimination without changing the code or using patches are suggested. The MATLAB is used to simulate behavior of the systems.

Keywords: *accessibility model, information resource, vulnerabilities, security audit, discrete distribution law.*