**УДК 004.05**

*Овчаренко А.І., студент,*
*Данілейко В.С., студентка,*
*Кулинич І.О., студент*
*Полтавський національний технічний*
*університет імені Юрія Кондратюка*

# МОДЕЛЬ ГОТОВНОСТІ ДВОХРІВНЕВИХ АРХІТЕКТУР ВЕБ-РЕСУРСУ З ВРАХУВАННЯМ АТАК НА ВРАЗЛИВОСТІ ЙОГО КОМПОНЕНТ

***Анотація**. У статті розглянуто вплив факторів інформаційної безпеки на функціонування веб-ресурсу з дворівневою архітектурою. Розглянуто модель готовності веб-ресурсу, її стани та можливі переходи між ними. Досліджено вплив параметру інтенсивності профілактик на показник готовності та поведінку його зміни з часом. Запропоновано рекомендації щодо встановлення певних границь зміни інтенсивності профілактик.*

***Ключові слова:** веб-ресурс, атака, модель готовності*

## Вступ

Інформаційна безпека є однією з важливих складових глобальної безпеки. В умовах побудови інформаційного суспільства роль інформаційної безпеки посилюється і, навпаки, глобальні процеси впливають на інформаційну безпеку і взаємопов'язану з нею економічну, національну і глобальну. Особливості необмеженого і неконтрольованого впливу, несанкціонованого доступу, а також виникнення комп'ютерних вірусів і інших погроз, викликають необхідність в забезпеченні інформаційної безпеки. В даний час розроблені інструментальні засоби, призначені для автоматизації та профілактики пошуку вразливостей програм.

В [1,2] виконаний аналіз життєвого циклу вразливостей, що обґрунтовує необхідність проведення регулярних профілактик аудиту безпеки для виявлення нових і неліквідованих вразливостей веб-ресурсу. З іншого боку, проведення профілактик аудиту безпеки не повинно знижувати доступність ресурсу. Ця вимога обґрунтовує необхідність розробки і дослідження відповідних моделей готовності.

В [3,4] розглянуті моделі функціонування інформаційних та веб-ресурсів на основі апарату багатофрагментного моделювання, що дозволяють врахувати вплив вразливостей і профілактик аудиту безпеки на готовність системи.

## Марковська модель готовності веб-ресурсу

Представлена модель готовності описує періодичні профілактичні заходи аудиту безпеки з виявлення й усунення вразливостей і допускає усунення виявленої в ході атаки уразливості без зміни програмного коду ($\lambda f = const$). Розмічений орграф для системи з трьома уразливостями представлений на рис.1.

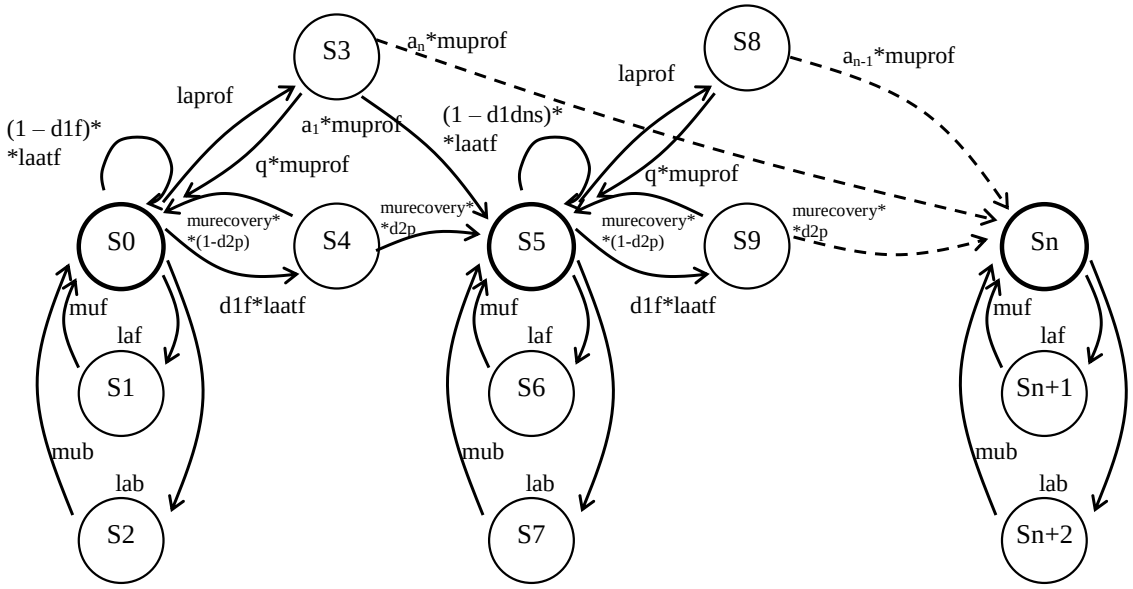


*Рис.1. Розмічений граф станів і переходів моделі готовності веб-ресурсу з дворівневою архітектурою*

Згідно графа на рис.1, спочатку інформаційний ресурс функціонує в умовах прояву відмов і відновлення служб FrontEnd та BackEnd. Після проведення атаки на службу FrontEnd (перехід в стан S4 з інтенсивністю d1f*laatf) система втрачає працездатність, але може її відновити шляхом перезапуску без усунення несправності з умовної інтенсивністю (1-d2p)*murecovery, або з усуненням уразливості з умовної інтенсивністю d2p * murecovery. З певною періодичністю в системі проводяться профілактичні заходи (стан S3) в результаті яких може бути виявлено та усунуто від 0 до nv вразливостей. Після прояву і усунення всіх вразливостей система продовжує функціонувати в умовах прояву відмов і відновлення її служб (стани Sn ... Sn+2). Так як при профілактиці можливе виявлення і усунення не тільки однієї, а й кількох вразливостей з множини [1 ... nv], то необхідно ввести параметр αj ймовірності виявлення j (j = [1 ... nv]) вразливостей.

## Дослідження результатів моделювання

Рішення системи рівнянь Колмогорова було виконано в системі Matlab за допомогою методу ode15s для тимчасового інтервалу [0 ... 50000] годин.

Для моделі готовності досліджено вплив параметру laprof на характер поведінки і значення функції готовності. Значення параметру взяті з множини [4.57e-2 4.57e-3 4.57e-4 4.57e-5 4.57e-6] 1/годин. Для дослідження впливу зазначеного параметра була розроблена спеціальна циклічна програмна конструкція. Результати моделювання у вигляді графічних залежностей показані на рис.2.

Поведінка функції готовності при зміні інтенсивності проведення профілактик має наступний характер: з одного боку, чим рідше проводяться профілактики, тим вище мінімум функції готовності на початковому етапі функціонування; з іншого боку - чим частіше проводяться профілактики, тим швидше функція готовності перейде в усталений режим. З рис.2 видно, що мінімум функції готовності можна підвищити до сталого значення Pg = 0.9888 при занадто затяжних профілактиках.

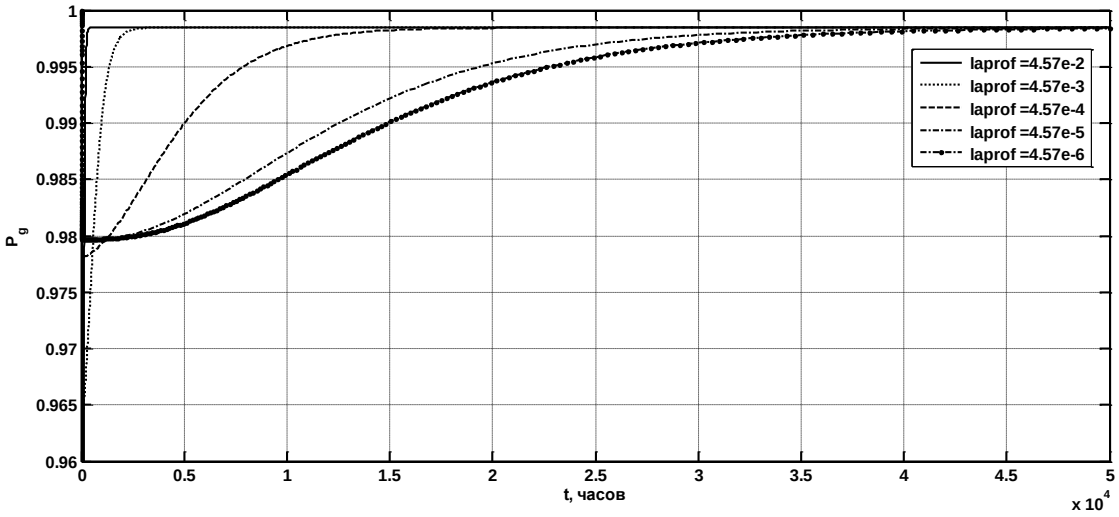


*Рис.2. Графіки зміни функції готовності моделі веб-ресурсу для різної інтенсивності проведення профілактик*

## Висновок

У статті запропоновані елементи методики побудови марковських моделей оцінки готовності веб-ресурсу з урахуванням атак на вразливості його сервісів. Обґрунтовано можливість застосування дискретних законів розподілу при моделюванні виявлення вразливостей в ході профілактик аудиту безпеки.

Результати моделювання показують, що при прийнятих значеннях вхідних даних система з профілактиками, які виявляють декілька вразливостей, забезпечує перехід функції готовності в сталий стан за більш короткий період.

Подальші дослідження слід спрямувати на розробку інтегрованих стратегій обслуговування веб-ресурсів з урахуванням апаратних, програмних засобів і політики інформаційної безпеки.

## Посилання

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. 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.*

**Authors:**
Ovcharenko Andrey Ivanovich, Danileiko Victoria Sergeevna, Kulinich Igor Alekseevich

**MODEL OF AVAILABILITY UNIFORM WEB RESOURCE ARCHITECTURE WITH ATTACK ON VULNERABILITIES HIS COMPONENT**

**Abstract**. The article considers the influence of information security factors on the functioning of a web resource with two-tier architecture. The model of availability of a web resource, its states and possible transitions between them is considered. The influence of the parameter of intensity of preventive measures on the availability index and the behavior of its change over time is investigated. Recommendations on the establishment of certain limits of change in the intensity of prevention are suggested.

**Keywords:** web resource, attack, availability model.

**Авторы**:
Овчаренко Андрей Иванович, Данилейко Виктория Сергеевна, Кулинич Игорь Алексеевич

**МОДЕЛЬ ГОТОВНОСТИ ДВУХУРОВНЕВОЙ АРХИТЕКТУРЫ ВЕБ-РЕСУРСОВ С УЧЕТОМ АТАК НА УЯЗВИМОСТИ КОМПОНЕНТ**

**Аннотация**. В статье рассмотрено влияние факторов информационной безопасности на функционирование веб-ресурса с двухуровневой архитектурой. Рассмотрена модель готовности веб-ресурса, ее состояния и возможные переходы между ними. Исследовано влияние параметра интенсивности профилактик на показатель готовности и поведение его изменения со временем. Предложены рекомендации по установлению определенных границ изменения интенсивности профилактик.

**Ключевые слова**: веб-ресурс, атака, модель готовности