УДК 681.321

АЛАА МОХАММЕД АБДУЛ-ХАДИ, Ю.Л. ПОНОЧОВНЫЙ, В.С. ХАРЧЕНКО

Национальный аэрокосмический университет им. Н.Е. Жуковского "ХАИ", Украина

РАЗРАБОТКА БАЗОВЫХ МАРКОВСКИХ МОДЕЛЕЙ ДЛЯ ИССЛЕДОВАНИЯ ГОТОВНОСТИ КОММЕРЧЕСКИХ ВЕБ-СЕРВИСОВ

В статье рассмотрены вопросы оценки непрерывности функционирования коммерческих веб-сервисов. Определено, что причинами недоступности сервисных услуг могут быть как внутрисистемные, так и внешние факторы, среди которых выделены уязвимости серверной части. Проанализированы системы метрик уязвимостей и сделаны выводы о возможности выделения подмножеств уязвимостей, влияющих на доступность системы и ее элементов; при этом они характеризуются критерием severity, характеризующем успешность возможной атаки на уязвимость. Разработаны два вида марковских моделей функционирования веб-сервиса в условиях проявления внутрисистемных неисправностей и выполнения атак на уязвимости служб DNS, DHCP и Route.

Ключевые слова: *доступность, готовность, availability, коммерческий веб-сервис, метрики уязвимостей, марковские модели.*

Введение

Стремительное развитие коммерческих веб-приложений и сервисов обуславливает жесткие условия конкуренции в данном бизнес-сегменте. Известно, что количество коммерческих веб-сервисов в украинском сегменте Интерента за последние 9 лет увеличилось в 8 раз [1], только за 2012 год к 1642 магазинам, зарегистрированным в процессинговом центре (UPC) [2] подключилось еще 406 новых сайтов; за последние 4 года количество покупок в интернет-магазинах увеличилось в 4 раза [3], а количество операций, совершенных держателями карт eCommerceConnect UPC в интернет-магазинах за 2012 год выросло на 81% [2]; оборот интернет-торговли из 100 млн долл. в 2005 г. увеличился до 1 млрд долл. в 2011 г. Согласно доступных аналитических прогнозов [4] до 2015 г. ожидается рост доли интернет-магазинов до 20-25% и рост количества онлайн-магазинов в городах меньше 500 тыс. жителей.

В условиях жесткой конкуренции к современному коммерческому веб-сервису выдвигаются высокие требования как к непрерывности функционирования, так и к высокой динамике развития.

В международной практике требования к непрерывности функционирования регламентированы в группе стандартов Business Continuity Management (управление непрерывностью бизнеса) [4]. Следует отметить, что с 2004 года Business Continuity включает такие элементы, как процесс управления информационной безопасностью и анализ рисков [5].

Согласно исследований [6], причинами отказов веб-сервисов могут быть как внутрисистемные (дефекты аппаратных и ошибки программных средств, ошибки обслуживающего персонала), так и внешние факторы (стихийные бедствия, хакерские атаки и др.). Следует отметить, что для оценки непрерывности функционирования системы с учетом внутренних факторов используются модели готовности [7].

С точки зрения пользователя веб-сервис представляет собой некий «черный ящик», выполняющий определенные функции сервисного характера. При этом пользователя, как правило, не интересуют причины простоев веб-сервиса, они только формируют мнение о качестве его работы. С другой стороны, в стандартах по непрерывности бизнеса [4] качество работы веб-сервиса также оценивается общим временем простоев и недоступности сервисных функций.

В силу высоких требований к динамичности развития, современные веб-сервисы допускают запуск и использование их на начальном этапе с определенной долей ошибок и уязвимостей (сначала важна работоспособность функционала, приносящего прибыль). В дальнейшем с некоторой периодичностью проводятся итерационные работы по выявлению и устранению дефектов, ошибок и уязвимостей [8].

Постановка задачи исследования

Как правило, решение о вводе веб-сервиса в эксплуатацию, а также последующая интенсивность выявления и устранения дефектов, ошибок и уязвимостей, определяются исходя из личного опыта менед-

жеров проектов или же методом абстрактных экспертных оценок. Между тем, даже для средних коммерческих веб-сервисов успешность их развития и стабильность дохода напрямую зависят от правильного расчета затрат на работы по обслуживанию, тестированию отказоустойчивости и безопасности и устранению выявленных изъянов.

На данный момент складывается ситуация, когда с одной стороны, к системе выдвигаются требования к ограниченному времени простоя, с другой стороны только модели готовности позволяют априорно оценить этот показатель исходя из известных входных параметров; моделей, позволяющих оценить априорно длительность недоступности сервиса нет.

Поэтому целью данной статьи является разработка базовых марковских моделей для априорной оценки времени недоступности коммерческого веб-сервиса с учетом особенностей существующих систем класификации и метрик уязвимости.

Сравнительный анализ стандартов, определений, показателей и свойств готовности и доступности

Свойства готовности и доступности веб-сервиса как информационной системы участвуют в определяющей иерархии комплексного свойства гарантоспособности (dependability). Так как они имеют идентичное обозначение на английском языке (availability), то в русскоязычных руководящих документах при их переводе встречаются определенные коллизии [9]. Поэтому в данной статье вначале рассмотрены определяющие составные элементы каждого из свойств, представленные в табл. 1.

Таблица 1

Сравнительный анализ свойств готовности и доступности

№ п/п	Характеристики свойства «готовность»	Характеристики свойства «доступность»
1	Готовность – свойство объекта быть в состоянии выполнять требуемую функцию при заданных условиях в данный момент времени или в течение заданного интервала времени при условии обеспечения необходимыми внешними ресурсами [6,9].	Доступность - состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие право доступа, могут реализовывать их беспрепятственно [10]
2	Готовность является одним из свойств, составляющих понятия «надежность» и «гарантоспособность» (dependability)	Доступность является одним из свойств, составляющих категорию «безопасность информации (данных)», которая также есть составляющей понятия «гарантоспособность» (dependability)
3	Обеспечение готовности осуществляется за счет повышения: безотказности (reliability), ремонтопригодности (maintainability) обеспеченности технического обслуживания и ремонта (maintenance support)	Основными методами обеспечения доступности информации (данных) являются: использование систем бесперебойного питания, резервирования и дублирования мощностей, разработки и внедрения планов непрерывности бизнес-процессов [4].
4	Показателями готовности являются: коэффициент готовности $K_г = (T – t_п \Sigma) /T$ коэффициент простоя $K_п= t_п \Sigma/T$ (где $t_п$ – суммарная длительность простоев системы за время эксплуатации T)	Показателем доступности является суммарное время доступности серверных услуг на протяжении всего периода эксплуатации системы
5	Причины отказов – дефекты АС, ошибки (дефекты) ПС, ошибки обслуживающего персонала	Причины отказов – уязвимости серверной части системы
6	Модели оценки – марковские и многофрагментные [7]	–

Анализ систем классификации и метрик уязвимостей информационных систем

На сегодня существует несколько систем классификаций уязвимостей (vulnerabilities), которые активно используются в образовательных и технологических процессах. Одной из самых известных и наиболее полной является CVE (Common Vulnerabilities and Exposures), которая курируется компанией NCSD (National Cyber Security Division). Полностью CVE размещена на сервере Национальной Базы Уязвимостей США (NVD - nvd.nist.gov) или на официальном сайте (cve.mitre.org/data/downloads). На момент издания статьи база CVE включала 55235 записей. Для сравнения, популярная в рунете база уязвимостей securitylab.ru/vulnerability включает 27389 записей.

Каждая уязвимость в базе CVE имеет как минимум четыре атрибута:

- уникальный идентификатор (например, CVE-2013-0125);

- короткая общая информация об уязвимости, в каких продуктах она обнаружена (Summary);

- дата публикации (Published);

- уровень серьезности (CVSS Severity);

а также другие атрибуты, доступные при детализации конкретной уязвимости на отдельной веб-странице. Среди дополнительных атрибутов можно выделить «Vulnerability Type», который использует классификатор из словаря CWE (Common Weakness Enumeration), а также базовую метрику (CVSS Base Score) – параметр, который рассчитывается по специальной формуле исходя из экспертных оценок отдельных метрик AccessComplexity, Authentication, AccessVector, ConfImpact, IntegImpact, AvailImpact. Кроме базовой, используются также комплексные метрики CVSS Temporal Equation (TemporalScore) и CVSS Environmental Equation (EnvironmentalScore).

Следует отметить, что метрика, связанная с доступностью (AvailImpact, AvailabilityImpact) принимает значения «none» (0), «partial» (0.275) и «complete» (0.66). Исходя из классификаторов уязвимостей базы NVD, можно выделить подмножества уязвимостей по виду приложения и по влиянию на доступность. Также очевидно, что не все уязвимости могут гарантированно (со 100% вероятностью) вывести систему из строя (из доступа).

Здесь заключается одно из существенных отличий уязвимостей от внутрисистемных дефектов и ошибок, которые выводят систему (или ее компонент) из строя со 100-% вероятностью.

Структурная схема надежности (готовности) веб-сервиса

Веб-сервис, как сложная многоуровневая и распределенная система может быть представлена с помощью схем различного уровня вложенности. В данной статье принято решение ограничится на начальном этапе трехэлементной структурной схемой надежности (готовности) веб-сервиса (ССН), описывающей взаимодействие основных служб: присвоения IP-адресов (DHCP), маршрутизации IP-пакетов (Route) и поддержки прямого и обратного преобразования текстовых адресов URL в IP-адреса (DNS). Такое решение обусловлено тем, что согласно классификаторам CVE можно выделить подмножества уязвимостей указанных служб.

Неработоспособность любой из перечисленных служб повлечет за собой отказ в обслуживании клиента. На основании этого, ССН будет включать три последовательных элемента, каждый из которых характеризует исправность перечисленных трех служб (рис. 2).

Естественно, что эту ССН можно детализировать, так как каждая служба, во-первых, реализована как клиент-серверная распределенная структура (соответственно ей присущи отказы и восстановления клиентской и серверной сторон), а во-вторых, построена на основе аппаратно-программных обслуживаемых комплексов (соответственно ей присущи отказы аппаратных и программных средств); но эти вопросы выходят за рамки исследований данной статьи.

Рис. 2. Структурная схема надежности (готовности) служб поддержки веб-сервиса

Граф состояний и переходов с учетом ССН будет включать одно исправное состояние и три неработоспособных (рис. 3). В последующем этот граф рассматривается как структурный фрагмент моделей с учетом атак на веб-сервис и обозначается восьмиугольной условной фигурой. При построении марковских моделей оценивания времени недоступности веб-сервиса использованы следующие понятия.

Уязвимость – изъян системы (преимущественно программного характера), который можно использовать для ограничения доступности сервисов;

Атака – событие, определяемое временем использования уязвимости;

Патч – совокупность мероприятий, устраняющих уязвимость в системе.

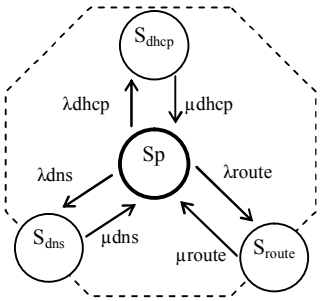

Рис. 3. Размеченный граф функционирования служб поддержки веб-сервиса

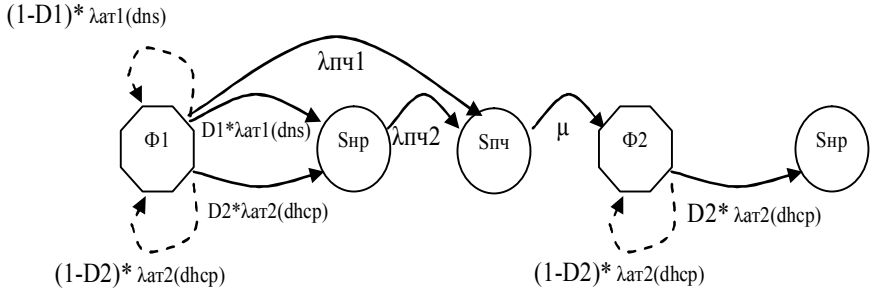

Рис. 4. Вариант марковской модели двух атак на информационную систему

Далее рассмотрены возможные варианты построения марковских моделей для оценки влияния уязвимостей на непрерывность функционирования информационной системы.

Марковская модель функционирования веб-сервиса с учетом влияния критичности уязвимостей на интенсивность перехода в неработоспособное состояние

Данная модель предусматривает аналогию атак на уязвимости с моделями проявления скрытых отказов [11]. Размеченный граф состояний и переходов модели представлен на рис.4. При построении графа модели рассматривалось функционирование информационной системы под воздействием двух разнородных атак на доступность (атака на DNS и атака на DHCP). Каждая из атак характеризуется своей интенсивностью и уровнем критичности (Severity).

При этом уровень критичности атаки определяет интенсивность перехода системы в неработоспособное состояние как произведение ожидаемой интенсивности атаки на ее severity D*λ. Устранение уязвимости характеризуется состоянием Sпч, в модели рассматривается как периодическое проведение патч-менеджмента с интенсивностью λпч1, так и применение патчей после проведения атаки с интенсивностью λпч2.

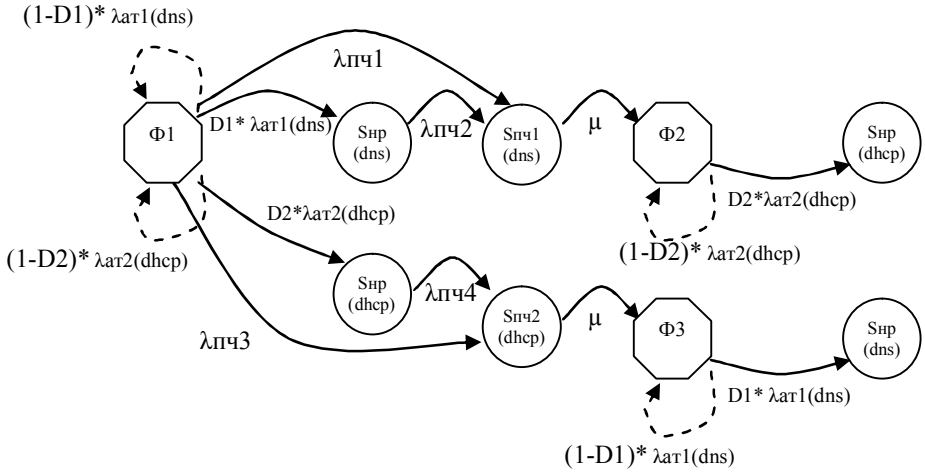

Рис. 5. Вариант марковской модели двух атак на информационную систему с разделенными состояниями патчеризации служб DNS и DHCP

Для упрощения графа, комбинация из 4-х состояний (рис.3) заменена условной фигурой Ф (восьмиугольник), обозначающей фрагмент состояний. Так как после патчеризации изменяются параметры системы, то из состояния Sпч система переходит в новый фрагмент Ф2.

Однако, разнородность служб DNS и DHCP обуславливает различные состояния и параметры наложения патчей. Размеченный граф марковской модели, учитывающей эту особенность представлен на рис.5.

Суть состояний фрагментов модели на рис.5 следующая.

Фрагмент Ф1: начальный фрагмент, система функционирует при условии отказов и восстановлений по внутренним причинам.

Фрагмент Ф2: после проведения патчеризации устранены уязвимости службы DNS, система функционирует при условии отказов и восстановлений по внутренним причинам.

Фрагмент Ф3: после проведения патчеризации устранены уязвимости службы DHCP, система функционирует при условии отказов и восстановлений по внутренним причинам.

Марковская модель функционирования веб-сервиса с учетом влияния критичности уязвимостей на вероятность работоспособных состояний

Для данной модели характерно применение «условно-вероятных» состояний, заключенных внутри фрагментов (восьмиугольников). Размеченный граф модели представлен на рис. 6. Рассмотрим суть фрагментов модели (рис. 6) более детально.

Фрагмент Ф1: начальный фрагмент, система функционирует при условии отказов и восстановлений по внутренним причинам. Фрагмент Ф2: на систему осуществлена атака на службу DNS с уровнем серьезности D1. Система продолжает функционировать в условиях отказов и восстановлений по внутренним причинам, однако вероятность ее исправного состояния уменьшается в 1-D1 раз. Фрагмент Ф3: на систему осуществлена атака на службу DHCP с уровнем серьезности D2. Система продолжает функционировать в условиях отказов и восстановлений по внутренним причинам, однако вероятность ее исправного состояния уменьшается в 1-D2 раз.

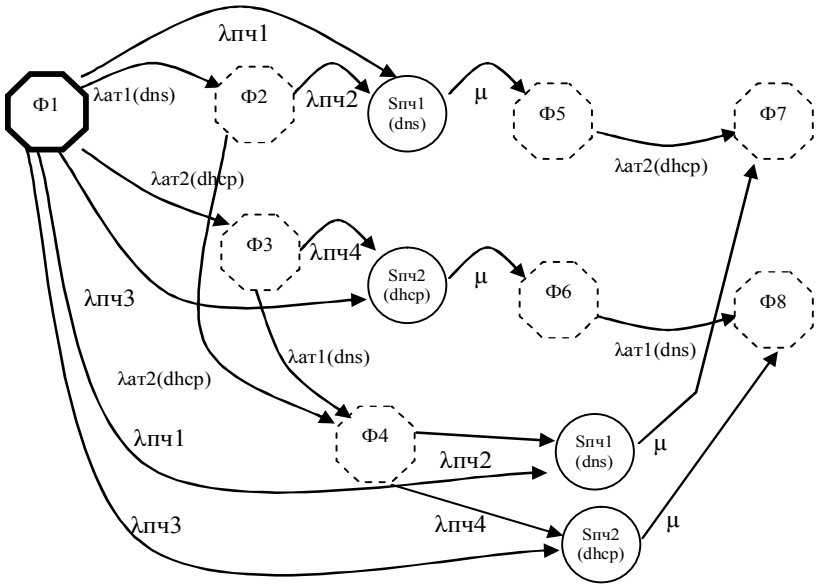

Рис. 6. Вариант марковской модели трех атак на информационную систему с использованием условно-вероятных состояний с разделенными состояниями патчеризации служб DNS и DHCP

Фрагмент Ф4: на систему осуществлены атаки на службу DHCP и на службу DNS. Система продолжает функционировать в условиях отказов и восстановлений по внутренним причинам, однако вероятность ее исправного состояния уменьшается в (1-D1*D2) раз. Фрагмент Ф5: после проведения патчеризации устранены уязвимости службы DNS, система функционирует при условии отказов и восстановлений по внутренним причинам. Фрагмент Ф6: после проведения патчеризации устранены уязвимости службы DHCP, система функционирует при условии отказов и восстановлений по внутренним причинам. Фрагмент Ф7: на систему осуществлена атака на службу DHCP с уровнем серьезности D2. Система продолжает функционировать в условиях отказов и восстановлений по внутренним причинам, однако вероятность ее исправного состояния уменьшается в 1-D2 раз. Фрагмент Ф8: на систему осуществлена атака на службу DNS с уровнем серьезности D1. Система продолжает функционировать в условиях отказов и восстановлений по внутренним причинам, однако вероятность ее исправного состояния уменьшается в 1-D1 раз.

Для определения коэффициента непрерывного функционирования (аналог коэффициента готовности) для модели на рис.6 необходимо:

- построить детальный граф состояний и переходов, раскрыв фрагменты Ф1-Ф8 на 4 состояния каждый;

- по детализированному графу построить систему дифференциальных уравнений Колмогорова;

- решить систему ДУ и определить вероятности нахождения системы в каждом состоянии;

- результирующий показатель – аналок коэффициента готовности определить по формуле:

$$A = P(Sp\text{-}ф1) + P(Sp\text{-}ф2) \times (1-D1) + P(Sp\text{-}ф3) \times \times (1-D2) + P(Sp\text{-}ф4) \times (1-D1*D2) + P(Sp\text{-}ф5) + + P(Sp\text{-}ф6) + P(Sp\text{-}ф7) \times (1-D2)) + P(Sp\text{-}ф8) \times (1-D1),$$

где P(Sp-ф1) – вероятность нахождения системы в работоспособном состоянии 1-го фрагмента.

Модели на рис. 5, 6 можно продолжить наращивать до полного устранения уязвимостей служб DHCP и DNS.

Выводы

В статье рассмотрены вопросы построения марковских моделей для оценки готовности коммерческого веб-сервиса с учетом внутрисистемных (дефекты аппаратных и программных средств) и внешних (атаки на уязвимости служб DNS и DHCP) факторов. Дальнейшие исследования следует направить на:

- разработку моделей и инструментальных средств формирования подмножеств уязвимостей по заданным признакам классификации, а также моделей оценивания интенсивности атак на уязвимости;

- исследование влияния входных параметров на результирующие показатели марковских моделей оценки непрерывности функционирования (готовности и доступности) веб-сервисов коммерческого применения.

Литература

1. Карпенко, О. Как развивается украинский рынок интернет-торговли [Электронный ресурс] / О. Карпенко. – Режим доступа к статье: ain.ua/ 2012/11/09/101611. – 11.01 2013 г.

2. Обороты украинских интернет-магазинов быстро растут [Электронный ресурс]. – Режим доступа: upc.ua/ru/news/1316.htm. – 11.01 2013 г.

3. Оборот интернет-торговли в Украине превысил $1 млрд. [Электронный ресурс]. – Режим доступа: seo-live.com/novosti-rinka/oborot-internet-torgovli-v-ukraine-previsil-1-mlrd. – 11.01 2013 г.

4. Мусатов, К. Непрерывность бизнеса. Подходы и решения [Электронный ресурс] / К. Муссатов. – Режим доступа к статье: www.jetinfo.ru/author/konstantin-musatov/nepreryvnost-biznesa-podkhody-i#AEN11

5. Справочник по информационной безопасности (Handbook of IT-Security), версия 2.2 [Текст]. – Главный информационный департамент Федеральной канцелярии Австрии.

6. Basic Concepts and Taxonomy of Dependable and Secure Computing [Text] / A. Avizienis, J.-C. Laprie, B.Randell, C.Landwehr // IEEE Transactions on Dependable and Secure Computing. –2004. – Vol. 1, № 1. – P. 11 – 33.

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

8. Статистика: Компании по всему миру подвергаются вирусным атакам каждые три минуты. [Электронный ресурс]. – Режим доступа: http://www.securitylab.ru/news/439232.php.

9. Нетес, В.А. Готовность и доступность – почувствуйте разницу [Текст] / В.А. Нетес // Вестник связи. – 2005. – № 3. – С. 43 – 49.

10. Рекомендации по стандартизации «Информационные технологии. Основные термины и определения в области технической защиты информации» [Текст] (Р 50.1.053-2005).

11. Засуха, С.А. Модель готовности двухканальной информационно-управляющей системы космического аппарата с оперативной верификацией программных средств [Текст] / С.А. Засуха, Ю.Л. Поночовный // Наука і техніка ПС ЗС України. – 2011. – Вип. 2 (6). – С. 144 – 149.

Поступила в редакцию 1.02.2013, рассмотрена на редколлегии 6.03.2013

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

РОЗРОБКА БАЗОВИХ МАРКІВСЬКИХ МОДЕЛЕЙ ДОСЛІДЖЕННЯ ГОТОВНОСТІ КОМЕРЦІЙНИХ ВЕБ-СЕРВІСІВ

А.М. Абдул-Хаді, Ю.Л. Поночовний,В.С. Харченко

У статті розглянуті питання оцінки безперервності функціонування комерційних веб-сервісів. Визначено, що причинами недоступності сервісних послуг можуть бути як внутрішньосистемні, так і зовнішні фактори, серед яких виділені вразливості серверної частини. Проаналізовано системи метрик вразливостей і зроблені висновки про можливість виділення підмножин вразливостей, що впливають на доступність системи та її елементів; при цьому вони характеризуються критерієм severity, що характеризує успішність можливої атаки на вразливість. Розроблено два види марківських моделей функціонування веб-сервісу в умовах прояву внутрішньосистемних несправностей та виконання атак на вразливості служб DNS, DHCP і Route.

Ключові слова: доступність, готовність, availability, комерційний веб-сервіс, метрики вразливостей, марківські моделі.

DEVELOPMENT OF BASIC MARKOV MODEL FOR RESEARCH OF COMMERCIAL WEB SERVICES AVAILABILITY

A.M. Abdul-Hadi, J.L. Ponochovny, V.S. Kharchenko

The problems of the operation and availability of commercial web services are analysed. It was determined that the reasons for unavailability of services can be both internal and external factors, including server-side vulnerabilities. The vulnerability metrics are analysed and some conclusions about the possibility of selecting subsets of vulnerabilities affecting the availability of the system and its elements are done, thus they are characterized by the criterion of severity, influencing on the success of a attack on the vulnarability. Two types of Markov models for describing of Web service in case of system component faults and execution of attacks on the vulnerabilities of DNS, DHCP and Route services are developed.

Key words: availability, commercial web service, metrics vulnerabilities, Markov models.

Абдул-Хади Алаа Мохаммед – аспирант кафедры компьютерных систем и сетей Национального аэрокосмического университета им. Н.Е. Жуковского «ХАИ», Харьков, Украина.

Поночовный Юрий Леонидович – канд. техн. наук, ст. науч. сотр., соискатель кафедры компьютерных систем и сетей Национального аэрокосмического университета им. Н.Е. Жуковского «ХАИ», Харьков, Украина. e-mail: pnch1@rambler.ru**.**

Харченко Вячеслав Сергеевич – заслуженный изобретатель Украины, д-р техн. наук, профессор, заведующий кафедрой компьютерных систем и сетей Национального аэрокосмического университета им. Н.Е. Жуковского «ХАИ», Харьков, Украина. e-mail: V.Kharchenko@khai.edu.