Міністерство освіти і науки України
Державний ВНЗ «Національний гірничий університет»

Факультет інформаційних технологій
(факультет)

Кафедра програмного забезпечення комп'ютерних систем
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА
дипломної роботи

магістра
(назва освітньо-кваліфікаційного рівня)

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

спеціальність *122 Комп'ютерні науки*
(код і назва спеціальності)

спеціалізація *Інформаційні управляючі системи та технології*
(назва спеціалізації)

освітній рівень *магістр*
(назва освітнього рівня)

кваліфікація *інженер з комп'ютерних систем*
(назва кваліфікації)

на тему: *Моделі та алгоритми виявлення та попередження розподілених атак на прикладі порталу «Затребувана освіта»*

Виконавець:
студент *2* **курсу , групи** *122м-16-1*

(підпис) *Булгаков М.О.* (прізвище та ініціали)

Керівники	Посада, прізвище, ініціали	Оцінка	Підпис
проекту	*проф. Корнієнко В.І.*		
розділів:			
Спеціальний	*проф. Корнієнко В.І.*		
Економічний	*доц. Касьяненко Л.В.*		

Рецензент			

Нормоконтроль	*доц. Коротенко Л.М.*		

Дніпропетровськ
2018

Міністерство освіти і науки України
Державний вищий навчальний заклад
«Національний гірничий університет»

ЗАТВЕРДЖЕНО:
завідувач кафедри

програмного забезпечення комп'ютерних систем
(повна назва)

_____ І.М. Удовик
(підпис) (прізвище, ініціали)

« » _____ 20 ____ року

ЗАВДАННЯ
на виконання кваліфікаційної роботи магістра

спеціальності *122 Комп'ютерні науки*
(код і назва спеціальності)

студенту *122м-16-1* *Булгаков М.О.*
(група) (прізвище та ініціали)

Тема дипломної роботи Моделі та алгоритми виявлення та попередження розподілених атак на прикладі порталу «Затребувана освіта»

1 ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Наказ ректора Державного ВНЗ «НГУ» від 26.*12.2017 р.* № 2127-*л*

2 МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень – результати моделювання розподіленої атаки.
Предмет досліджень – виявлення та попередження розподілених атак.
Мета НДР – розробка алгоритму знаходження розподілених атак.
Вихідні дані для проведення роботи – поведінка системи під час розподіленої DoS-атаки.

3 ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна результатів, що очікуються, полягає у новому методі виявлення та попередження розподілених атак на основі самоподібності системи.
Практична цінність результатів полягає у можливості розробки більш продвинутого прикладного рішення по запобіганю розподілених атак.

4 ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Результи повині відповідати вигомогам стандарту NIST «Internet Infrastructure Protection», «Integration of IDPS Technologies»

5 ЕТАПИ ВИКОНАННЯ РОБІТ

Найменування етапів робіт	**Строки виконання робіт (початок-кінець)**
Дослідження існуючих рішень по виявленню та попередженню розподілених атак	12.09.2017 – 22.10.2017
Побудова модлі розподіленої атаки на прикладі порталу «Затребувана освіта»	23.10.2017 – 03.11.2017
Дослідження результатів розподіленої атаки та виявлення закономірностей у поведінці системи під час атаки	04.11.2017 – 12.12.2017
Дослідження існуючих рішень по виявленню та попередженню розподілених атак	12.09.2017 – 22.10.2017

6 РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект від реалізації результатів роботи очікується позитивним завдяки можливості впровадження більш надійної системи запобігання розподіленим атакам.

Соціальний ефект від реалізації результатів роботи очікується позитивним завдяки поліпшенню роботи порталів та систем завдяки підвищенню їх рівня відмовостійкості.

7 ДОДАТКОВІ ВИМОГИ

Відповідність оформлення:

1. ДСТУ 3008-95. Документація. Звіти у сфері науки і техніки. Структура і правила оформлення.

Завдання видав _____ *Корнієнко В.І.*
(підпис) (прізвище, ініціали)

Завдання прийняв до виконання _____ *Булгаков М.О.*
(підпис) (прізвище, ініціали)

Дата видачі завдання: *12.09.2017р.*

Термін подання дипломного проекту до ДЕК _____

Реферат

Пояснительная записка: 76 стр., 23 рис., 8 табл., 3 приложения, 50 источников.

Объект исследования: распределенные атаки на компьютерные системы на примере сайта «Востребованное образование»

Цель магистерской работы: нахождения критериев в поведении компьютерной системы для раннего обнаружения распределенной атаки

Методы исследования: Разработка и анализ математической модели распределенной атаки

Научная новизна полученных результатов состоит в новом способе определения распределенной атаки на компьютерную систему на основе самоподобия системы

Практическое значение работы заключается в возможности разработки прикладного ПО на основе результатов анализа математической модели.

Область применения: системы предупреждения и предотвращения распределенных атак на компьютерные системы.

Значение работы и выводы. Работа способствует значительному развитию в такой непростой теме как нахождение и предупреждение об распределенных атаках и имеет полное право из стадии анализа и концепции перерасти в прикладное ПО.

Прогнозы по развитию исследований. Прогнозы являются положительным, так как в силу хаотичности поведения трафика(TCP, UDP и так далее) возможен анализ и нахождение новых, дополнительных факторов для определения распределенных атак.

В разделе «Экономика» описаны маркетинговые исследования и приведен социальный экономический эффект от данной работы.

Список ключевых слов: РАСПРЕДЕЛЕННЫЕ АТАКИ, DoS-атаки, ОТКАЗОУСТОЙЧИВОСТЬ, САМОПОДОБИЕ СИСТЕМЫ, КОМПЬЮТЕРНАЯ СИСТЕМА

Реферат

Пояснювальна записка: 76 стор., 23 рис., 8 табл., 3 додатки, 50 джерел.

Об’єкт досліджень: розподілені атаки на комп'ютерні системи на прикладі сайту «Затребувана освіта»

Мета дипломного проекту: знаходження критеріїв в поведінці комп'ютерної системи для раннього виявлення розподіленої атаки

Методи дослідження: Розробка і аналіз математичної моделі розподіленої атаки

Научна новизна отриманих результатів полягає в новому способі визначення розподіленої атаки на комп'ютерну систему на основі самоподібності системи

Практичне значення роботи полягає в можливості розробки прикладного ПЗ на основі результатів аналізу математичної моделі.

Область застосування: системи попередження і запобігання розподілених атак на комп'ютерні системи.

Значення роботи і висновки. Робота сприяє значному розвитку в такій непростій темі як знаходження і попередження про розподілених атаках і має повне право з стадії аналізу і концепції перерости в прикладне ПО.

Прогнози щодо розвитку досліджень. Прогнози є позитивним, так як в силу хаотичності поведінки трафіку (TCP, UDP і так далі) може бути аналіз і знаходження нових, додаткових факторів для визначення розподілених атак.

У розділі «Економіка» описані маркетингові дослідження і наведено соціальний економічний ефект від даної роботи.

Список ключових слів: РОЗПОДІЛЕНІ АТАКИ, DoS-АТАКИ, ВІДМОВОСТІЙКІСТЬ, САМОПОДІБНІСТЬ СИСТЕМИ, КОМП'ЮТЕРНА СИСТЕМА

The abstract

Explanatory note: 76 pages, 23 figures, 8 tables, 3 annexes, 50 sources

Object of the research: distributed attacks on computer systems on the example of the site "Demand for education"

The purpose of the master's work: finding criteria in the behavior of a computer system for early detection of a distributed attack

Research methods: Development and analysis of the mathematical model of distributed attack

The scientific novelty of the results is a new method for determining a distributed attack on a computer system based on the self-similarity of the system

The practical importance of the work lies in the possibility of developing application software based on the results of analysis of the mathematical model.

Scope: systems for preventing and preventing distributed attacks on computer systems.

The meaning of the work and conclusions. The work contributes to significant development in such a difficult topic as finding and warning about distributed attacks and has every right from the analysis stage and the concept to grow into application software.

Forecasts for the development of research. The forecasts are positive, because due to the chaotic behavior of the traffic (TCP, UDP and so on), it is possible to analyze and find new, additional factors for determining distributed attacks.

In the section "Economics", marketing research is described and the social economic effect of this work is shown.

List of keywords: DISTRIBUTED ATTACKS, DoS-attacks, SELF-ADVANCED SYSTEMS, COMPUTER SYSTEM

Зміст

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ЕОМ – Електронна обчислювальна машина

ЄРК – Європейська рамка кваліфікацій

ЗУН – Знання, уміння та навички

НРК – Національна рамка кваліфікацій

ПЗ – Програмнезабезпечення

СРК – Секторальна рамка кваліфікацій

ТЗ – Технічне завдання

ВСТУП

Теперішній час характеризується значним зростанням соціальної та економічної діяльності. Наслідком і необхідною умовою даних процесів стає швидке збільшення обсягу соціальної та економічної (виробничої) інформації, ускладнення обчислювальної та телекомунікаційної інфраструктури оброблюваних даних. При цьому обґрунтованість і оперативність прийнятих рішень стає все більш залежними від якості інформаційного забезпечення даних процесів. На даний момент наука має в своєму розпорядженні істотні можливості в області автоматизованої обробки масових даних статистики, заснованими, наприклад, на засобах теорії розпізнавання образів, кластерного аналізу, дискримінантного аналізу та ін., але проблема якості інформації продовжує залишатися відкритою.

Забезпечення доступності інформаційних ресурсів і процесів в ІТКМ, в першу чергу, пов'язують із завданням виявлення і «парирування» інформаційних атак на доступність. Незважаючи на високу активність в дослідженнях, на сьогодні немає єдиної теорії виявлення такого типу атак. Тому формальні методи виявлення атак опрацьовані недостатньо для широкого використання в реальних системах. Методи виявлення, які використовуються сьогодні в комерційних і некомерційних системах виявлення вторгнень, можна визначити як евристичні. Вони все використовують деякі апріорні припущення про те, що є атака, яка поведінка об'єкта в мережі можна вважати нормальним.

Комерційні системи здебільшого використовують евристичний метод виявлення, заснований на експертному підході, коли система аналізує спостерігається поведінка об'єктів в мережі на основі існуючої в неї бази описів відомих атак. Ці описи будуються на основі знань експертів. Для експериментальних систем характерне використання формалізованих методів виявлення атак, які використовують формальну модель атаки і намагаються наблизити процес її виявлення до повної автоматизації.

У даній дипломній роботі розглядаються питання, пов'язані із забезпеченням доступності інформаційних ресурсів і процесів в ІТКМ. Аналізуються інформаційні атаки на доступність. На основі гіпотези, що самоподобна і персистентність мережевого трафіку викликана атакою на доступність, розробляються моделі і процедури аналізу TCP-трафіку на основі теорії хаосу, пропонується методика раннього виявлення інформаційної атаки, досліджується адекватність запропонованих моделей.

РОЗДІЛ 1.
АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАВДАННЯ

1.1. Сутність і основні характеристики DoS-атак в контексті порталу

DDoS - це скорочення англійського виразу Distributed Denial of Service, що перекладається як «розподілена атака типу« відмова в обслуговуванні »». Це означає відмову від обслуговування мережевого ресурсу в результаті численних розподілених (тобто відбуваються з різних точок інтернет-доступу) запитів. Відмінність DoS-атаки (Denial of Service - «відмова від обслуговування») від DDos полягає в тому, що в цьому випадку перевантаження відбувається в результаті запитів з якогось певного інтернет-вузла.

Виділимо два методи виявлення DoS-атак - аналіз інформаційного мережевого потоку і аналіз журналів реєстрації операційної систе-ми або додатків. Перший підхід до виявлення атак є більш ефективним з причини реагування в реальному масштабі часу. Тому основні дослідження в даний моменбт спрямовані на раз-робітку способів і процедур виявлення атак в мережевому трафіку. Тут основним завданням є ідентифікація шкідливого трафіку. Більшість атак в даний час важко відрізнити від звичайних дій користувачів, в той же час, зворотне твердження так само справедливо - найчастіше діяльність користувачів викликає ефекти, ідентичні ефекту від проведення розподіленої атаки відмови в обслуговуванні.

З позиції всіх способів аналізу мережевого трафіку атака визначається як неприродне і помітна зміна статистичних властивостей досліджуваного трафіку. Хоча автори даних способів і декларують успішні результати у виявленні деяких типів атак на доступність, мають місце суттєві проблеми:

Проблема варіювання умов тестування. Більшість способів виявлення розроблені і вивчені комплексно. Проведення комплексних досліджень

ускладнене і вимагає великих тимчасових витрат. Розглянуті способи не беруть до виду широке коло умов: варіювання параметрів мереж, динаміки атак і т.п .;

Проблема оцінки природної мережевої активності. Виявлення атак прив'язане до статистичних властивостях природною мережевої активності. Моделі атаки, що використовуються в розглянутих підходах, складають малу частину від загального числа можливих атак. А такі характеристики як збільшення обсягу трафіку і розподіл адрес джерел трафіку вже застаріли, вони були властиві раннім реалізаціям DoS-атак**.**

Секторальна рамка кваліфікацій повинна визначати, структурувати і класифікувати кваліфікації бакалаврів і магістрів основних освітніх програм конкретних напрямів підготовки, які працюють у відповідних професійних областях.

При розробці необхідно врахувати і основні принципи Болонського процесу, і особливості сфери праці і освіти України, відображені в ряді документів і в результатах деяких проектів.

Одним з основних інструментів Болонського процесу є Європейська рамка кваліфікацій (ЄРК), схвалена Європейським Парламентом 23 квітня 2008 року, з метою «...забезпечення прозорості, порівнянності, співставності і визнання кваліфікацій і дипломів і свідоцтв про освіту з метою розвитку академічної та трудової мобільності громадян на європейському континенті». З появою ЄРК національні системи кваліфікацій, що включають національні та галузеві рамки кваліфікацій, отримали можливість зіставлення професійних кваліфікацій.

Аналіз галузевих рамок кваліфікацій, їх місця і ролі в національну систему кваліфікацій дозволив зробити деякі висновки, які необхідно врахувати при розробці секторальної рамки кваліфікацій за напрямами підготовки:

Деякі галузеві кваліфікаційні рамки, по суті, є каталогами детальних описів кваліфікацій, що дозволяють виробляти оцінювання та сертифікацію фахівців. Кваліфікації пов'язані з рівнями національної рамки кваліфікацій і з

профілями посад, поширених в галузі. До таких рамок можна віднести, рамки фахівців перукарського бізнесу;

Інші галузеві кваліфікаційні рамки, також пов'язані з рівнями національної рамки кваліфікацій та профілями сектора, містять рамкові опису компетенцій працівників і, перш за все, призначені для використання вирішення завдань ринку праці. Такі рамки компетенцій служать надійними орієнтирами, що дозволяють описати результати навчання в термінах очікування роботодавців за частиною характеристик успішного виконання робіт в певному контексті робочого простору. Такі рамки надають можливості для гнучкого формування профілів посад динамічно змінюються секторів, наприклад, інформаційних технологій.

Призначення секторальної рамки кваліфікацій

СРК покликана забезпечити простоту і ясність зв'язків між різними кваліфікаціями в рамках напряму підготовки.

СРК призначена для різних груп користувачів (об'єднань роботодавців, органів управління освітою, підприємств, освітніх організацій, громадян) і дозволяє:

- формувати загальну стратегію розвитку ринку праці і системи освіти по конкретному напрямку підготовки, в тому числі, планувати різні траєкторії освіти, що ведуть до отримання конкретної кваліфікації, підвищення кваліфікаційного рівня, кар'єрного росту;
- формувати велику академічну і трудову мобільність, в т.ч. міжнародну;
- розробляти освітні програми за профілями напрямків з урахуванням вимог роботодавців;
- описувати з єдиних позицій вимоги до кваліфікації працівників і випускників при розробці професійних і освітніх стандартів, програм професійної освіти;

- розробляти процедури оцінки результатів освіти і сертифікації кваліфікацій, формувати систему сертифікатів.

СРК у відповідність з НРК може містити конкретне число ієрархічно вибудуваних кваліфікаційних рівнів, що відповідають різним рівням освіти, наприклад:

1 рівень – початкова загальна освіта,

2 рівень – основна загальна освіта,

3-4 рівні – початкова професійна освіта,

5 рівень – середня професійна освіта,

6 рівень – бакалаврат,

7 рівень – магістратура,

8 рівень – програми підготовки науково-педагогічних кадрів в аспірантурі (ад'юнктурі), програми ординатури, програми асистентури-стажування.

При необхідності всередині кваліфікаційних рівнів можуть виділятися підрівні, що відображають специфіку напряму підготовки.

СРК утворюють представлені в формі таблиці характеристики (дескриптори) кваліфікаційних рівнів та підрівнів, розкриваються через основні показники підготовки до професійної діяльності – результати навчання: знання, вміння, загальні компетенції.

Дані показники безпосередньо пов'язані і визначаються дескрипторами НРК: широта повноважень і відповідальність, складність і наукоємність діяльності (табл.1.1).

Таблиця 1.1.

Взаємозв'язок результатів навчання і дескрипторів НРК

Дескриптор НРК	**Зміст**	**Результати навчання**
Широта повноважень і відповідальність	Визначає загальну компетенцію працівника і пов'язаний з масштабом діяльності, ціною можливої	Загальні компетенции

Дескриптор НРК	Зміст	Результати навчання
	помилки, її соціальними, екологічними, економічними і т. п. наслідками, а також з повнотою реалізації в професійній діяльності основних функцій керівництва	
Складність діяльності	Визначає вимоги до умінь і залежить від ряду особливостей професійної діяльності: - множинності (варіативності) способів вирішення професійних завдань, необхідність вибору або розробки цих способів; - ступеня невизначеності робочої ситуації і непередбачуваності її розвитку	Характер вмінь
Наукоємність діяльності	Визначає вимоги до знань, що використовуються у професійній діяльності, залежить від: - обсягу і складності використовуваної інформації; - інноваційності застосовуваних знань; - ступеня їх абстрактності (співвідношення теоретичних і практичних знань)	Характер знань

Ступінь прояву показника «Знання» (перехід від одного рівня кваліфікації до іншого) може бути пов'язана зі зміною одного (будь-якого) зі складових показника, двох або трьох (табл. 1.2).

Таблиця 1.2.

Опис знань за рівнями

Рівень	**Характеристика знань**
1	Базові загальні знання, отримані в процесі інструктажу або навчання на робочому місці
2	Знання, отримані в процесі професійної підготовки і самостійно
3	Практико-орієнтовані професійні знання, отримані в процесі професійної підготовки і самостійно
4	Знання для здійснення діяльності на основі практичного досвіду, отримані в процесі професійної освіти і самостійно
5	Професійні (практичні і теоретичні) знання і практичний досвід (або широкий діапазон теоретичних і практичних знань у професійній області) Самостійний пошук інформації, необхідний для вирішення професійних завдань
6	Діяльність, що вимагає синтезу спеціальних (теоретичних і практичних) знань (в тому числі інноваційних) і практичного досвіду Самостійний пошук, аналіз і оцінка професійної інформації
7	Синтез професійних або наукових знань (в тому числі і інноваційних) і досвіду в певній галузі і / або на стику областей Оцінка і відбір професійної інформації. Створення нових знань прикладного характеру в певній галузі. Визначення джерел та пошук інформації, необхідної для розвитку діяльності
8	Знання на самому передовому рівні в галузі науки і професійної

Рівень	Характеристика знань
	діяльності Використання спеціальних знань для критичного аналізу, оцінки і синтезу нових складних ідей, які знаходяться на самому передовому рубежі даної області. Оцінка і відбір інформації, необхідної для розвитку діяльності Розширення або переосмислення існуючих знань і / або професійної практики в рамках конкретної області або на стику областей Демонстрація здатності стійкого інтересу до розробки нових ідей або процесів і високого рівня розуміння процесів навчання Методологічні знання в області інноваційно-професійної діяльності

Ступінь прояву показника «Уміння і навички» (перехід від одного рівня кваліфікації до іншого) може бути пов'язана як зі зміною одного (будь-якого) зі складових показника, так і обох (табл. 1.3).

Таблиця 1.3.

Опис вмінь за рівнями

Рівень	Характеристика вмінь та навичок
1	Виконання стандартних практичних завдань певною ситуації Корекція дій відповідно до умов робочої ситуації
2	Рішення стандартних і однотипних практичних завдань Вибір способу дій по заданому інструкціями алгоритму Корекція дій відповідно до умов робочої ситуації
3	Рішення стандартних і простих однотипних практичних завдань Вибір способів дій з відомих на основі знань і практичного досвіду

Рівень	Характеристика вмінь та навичок
	Корекція діяльності з урахуванням отриманих результатів
4	Рішення різних типів практичних завдань, що вимагають самостійного аналізу робочої ситуації і її передбачуваних змін Вибір технологічних шляхів здійснення діяльності Поточний і підсумковий контроль, оцінка і корекція діяльності
5	Рішення практичних завдань, які передбачають розширення засобів вирішення і їх вибір Творчий підхід або вміння і навички самостійної розробки і висунення різних, в тому числі альтернативних варіантів вирішення професійних проблем із застосуванням теоретичних і практичних знань Поточний і підсумковий контроль, оцінка і корекція діяльності
6	Рішення проблем технологічного або методичного характеру, які стосуються певної галузі знань, які передбачають вибір і різноманіття способів вирішення Розробка, впровадження, контроль, оцінка і корекція компонентів технологічного процесу Вміння і навички здійснення науково-дослідної та інноваційної діяльності з розвитку нового знання і процедур інтеграції знань різних областей, правильного та логічного оформлення своїх думок в письмовій та усній формі, застосування на практиці теоретичних знань в конкретній галузі
7	Рішення проблем технологічного або методичного характеру, що вимагають розробки нових підходів, використання різноманітних методів (в тому числі і інноваційних) Корекція діяльності підрозділу чи організації Вміння і навички наукового обґрунтування постановки цілей і вибору

Рівень	Характеристика вмінь та навичок
	методів і засобів їх досягнення
8	Дослідження, розробка, реалізація і адаптація проектів, які призводять до накопичення нових знань і нових рішень Найбільш просунуті і спеціалізовані навички та вміння, включаючи синтез і оцінку, необхідні для вирішення критичних проблем в дослідженні і / або нововведенні і дозволяють переглядати і оновлювати існуюче знання або професійну практику Здатність брати участь в усній або письмовій формі в фахових дискусіях, а також публікація вихідних результатів досліджень в міжнародних академічних виданнях (може сприяти на науковому та професійному рівні технічного, громадському і культурному прогресу суспільства) Вміння генерувати ідеї, прогнозувати результати інноваційної діяльності, здійснювати широкомасштабні зміни в професійній і соціальній сфері, керувати складними виробничими та науковими процесами

Показник «Особистісні та професійні компетенції» (табл. 1.4) визначає загальну компетенцію працівника і має три основних ступеня прояву:

- діяльність під керівництвом;
- самостійна виконавська діяльність;
- керівництво іншими.

Таблиця 1.4.

Опис загальних компетенцій за рівнями

Рівень	**Характеристика особистісних та професійних компетенцій**
1	Індивідуальна відповідальність Дії під безпосереднім керівництвом
2	Індивідуальна відповідальність Діяльність під керівництвом з певним ступенем самостійності
3	Індивідуальна відповідальність за виконання завдань Виконавська діяльність, що включає планування діяльності, виходячи з поставленого завдання
4	Виконавська діяльність: визначення завдань і планування діяльності з урахуванням поставленої мети Керівництво роботою інших з прийняттям часткової відповідальності за результат їх дій Відповідальність за власне навчання та навчання інших
5	Керівництво співробітниками (групою) з прийняттям відповідальності за результат їх дій на конкретній ділянці технологічного процесу Здатність самостійно управляти і контролювати процес трудової і навчальної діяльності в рамках стратегії, політики і цілей організації, обговорювати проблеми, аргументувати висновки і грамотно оперувати інформацією
6	Керівництво співробітниками (групою) з прийняттям відповідальності за результат на конкретній ділянці технологічного процесу або на рівні підрозділу Узгодження робіт на дорученій ділянці з діяльністю інших ділянок Здатність до творчості у професійній діяльності, ініціативи в управлінні, приймати відповідальність за розвиток професійного знання

Рівень	Характеристика особистісних та професійних компетенцій
	і за результати професійної діяльності
7	Керівництво діяльністю співробітників (групи) з прийняттям відповідальності за результат на рівні підрозділу або організації Визначення стратегії діяльності підрозділу чи організації Здатність визначати стратегію, керувати процесами і діяльності, приймати рішення і нести відповідальність на рівні підрозділів інституційних структур
8	Визначення стратегії, управління процесами і діяльністю (в тому числі інноваційної) з прийняттям рішення і відповідальності на рівні великих інституційних структур Визначення стратегії, управління складними соціальними, виробничими, науковими процесами. Відповідальність за результат в масштабі галузі, країни, на міжнародному рівні Демонстрація значних лідерських якостей, інноваційності та самостійності в трудовій та навчальній діяльності в нових контекстах, які потребують вирішення проблем, пов'язаних безліччю взаємопов'язаних факторів Критичний аналіз, оцінка і сінтезнових і складних ідей і прийняття стратегічних рішень на підставі цих процесів Демонстрація досвіду операционального взаємодії зі здатністю прийняття стратегічних рішень в складному оточенні Авторитетне спілкування в рамках критичного діалогу з рівними по статусу фахівцями

Структура секторальної рамки кваліфікацій

СРК складається з наступних елементів:

1) найменування напряму (профілю) підготовки;

2) найменування області і видів професійної діяльності;
3) кваліфікаційні рівні та підрівні;
4) дескриптори СРК для конкретного кваліфікаційного рівня:
   - основні показники професійної діяльності, що відповідають кожному кваліфікаційним рівнем / подуровню СРК – результати навчання (знання, вміння, загальні компетенції);
   - додаткові показники професійної діяльності;
   - шляхи досягнення кваліфікації відповідного рівня / підрівні - наводяться відомості про шляхи досягнення кваліфікації, уточнюючі шлях досягнення кваліфікації відповідного рівня;
   - основні види трудової діяльності – наводиться перелік видів трудової діяльності відповідно до кваліфікаційними підрівнями СРК, що виділяються;
   - рекомендовані найменування посад для виділених видів трудової діяльності.

1.2. Результати навчання як основні дескриптори секторальних рамок кваліфікацій

У європейському програмному документі (Європейські кваліфікаційні рамки для безперервної освіти) дається таке визначення: «результати навчання означають констатацію того, що учень знає, розуміє і вміє робити по завершенні процесу навчання, вони визначаються в термінах знань, умінь і компетенцій». Відобразимо в схемі трактування понять «компетенція», «знання» і «вміння і навички» згідно з документом «Європейські кваліфікаційні рамки для безперервної освіти» (рис. 1.1).

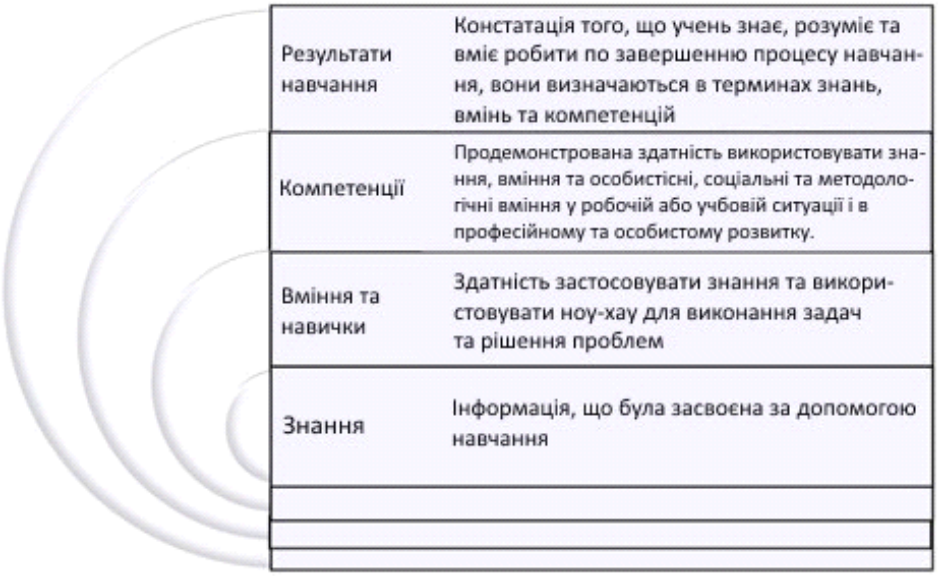


Рис. 1.1. Поняття «знання», «вміння і навички», «компетенції» і «результати навчання» в документі «Європейські кваліфікаційні рамки для безперервної освіти»

Таким чином, в основі виявлення і оцінки результатів навчання лежить проблема виявлення і оцінки знань, умінь і навичок, як основних їх складових. При уявній простоті понять «знання», «вміння і навички» спроби їх осмислення заводять у глухий кут багатьох фахівців, так як вони використовуються для опису різних явищ дійсності. З одного боку, знання, вміння і навички (ЗВН) - це ті сліди в пам'яті, той досвід, який формується у студентів в педагогічному процесі і є найважливішим показником його результату. З іншого боку, перш ніж стати результатами навчання, навчальних досягнень проходять через всі компоненти дидактичної системи, відображаються в її цілі, зміст, методи, засоби, знаннях, уміннях і навичках викладача.

У вітчизняній педагогіці система наукових знань, умінь і навичок традиційно розглядалася в контексті змісту освіти, яке найбільш повно розкривається в програмах, підручниках та навчальних посібниках. Відповідно і самі знання, вміння і навички аналізувалися переважно як основа змісту освіти. Такий підхід був простий і зручний, так як можна було говорити про те, що повинно бути, про ту інформацію, яку навчається повинен засвоїти, про тих уміннях і навичках, які повинні бути сформовані. В цьому випадку в зміст

освіти включалися і необхідні (на думку розробників змісту) наукові та міждисциплінарні знання, і досвід здійснення відомих способів діяльності, і досвід здійснення емоційно-ціннісних відносин. У цьому випадку зміст освіти формувалося з надлишком.

Сьогодні в умовах інформаційного вибуху більшість вчених і практиків розуміють, що неможливо вмістити в освітні програми та курси все важливе і можливий зміст. Треба вичленити ті необхідні і достатні для фахівця знання, вміння і навички, при яких він може успішно здійснювати професійну діяльність.

Повертаючись до визначень використовуваних термінів, засвоєна інформація - це та, що зберігається в пам'яті. Але, на жаль, чи, на щастя, пам'ять людини - не книжкова шафа і не файлове сховище і все, що там відбувається - це різного роду процеси. Пам'ять - це процеси запам'ятовування, збереження, відтворення, а також забування. Ми не можемо «прочитати» то, що зберігається в пам'яті людини, але ми можемо судити про знання, які він засвоїв в процесі їх впізнавання або відтворення. При цьому пам'ять буває не тільки словесна і логічна, але і образна (зорова, слухова, тактильна, нюхова і смакова), емоційна (пам'ять на почуття), моторна (пам'ять на рухи).

Уміння - освоєний суб'єктом спосіб виконання діяльності. У діяльності людини психологи виділяють дві форми: зовнішню практичну діяльність і внутрішню діяльність, яка має принципово ту ж будову, при цьому дії проводяться не з матеріальними предметами, а з їх образами, а замість реального продукту виходить уявний результат. Внутрішні дії готують зовнішні дії, економлять зусилля, даючи можливість вибрати потрібну дію, допомагають уникнути грубих помилок. Ю. Б. Гіппенрейтер у своїй роботі наводить такий приклад внутрішньої діяльності: Н. збирається повісити книжкові полиці і «прикидає», де і як їх розташувати. Оцінивши один варіант, він від нього відмовляється, переходить до іншого, третього варіанту, нарешті, вибирає найбільш підходяще, на його погляд, місце. Причому за весь час він жодного разу «Не ворухнув пальцем», тобто не справив жодного практичного дії.

До внутрішніх умінь віднесемо володіння способами здійснення розумових дій і операцій (порівняння, аналіз, синтез, внутрішня мова і ін.), А до зовнішніх - володіння способами здійснення зовнішніх або практичних дій.

Звичка - доведене до автоматизму вміння. Будь-який новий спосіб дії, протікаючи спочатку як деякий самостійне, розгорнуте і свідома дія, потім в результаті багаторазових повторень може здійснюватися вже в якості автоматично виконуваного компонента. Ю.Б. Гіппенрейтер стверджує, що навички - процеси, які пройшли через свідомість і перестали усвідомлюватися, вони лежать в основі розвитку всіх наших умінь, знань і здібностей. Людина набуває майстерність шляхом просування від простих дій до складних, завдяки передачі на неусвідомлювані рівні дій вже освоєних. Завдяки формуванню навички досягається двоякий ефект: по-перше, дія починає здійснюватися швидко і точно; по-друге, відбувається вивільнення свідомості, яке може бути направлено на виконання більш складної дії.

Для виявлення знань, умінь і навичок розроблено велику кількість методів.

Один з найбільш доступних і найстаріших методів - це спостереження. Воно дозволяє проаналізувати і оцінити процес виконання які навчаються дії або діяльності. Одним з недоліків методу є можливість впливу суб'єкта спостереження на його результати. Для підвищення об'єктивності результатів спостереження необхідно розробити комплекс матеріалів для спостереження, докладно описати: мета, спостерігаються ознаки або характеристики діяльності, параметри опису даних ознак, спосіб фіксації спостережуваних явищ або ознак і ін. для зручності спостерігає складається карта спостереження або таблиця. Спостереження може використовуватися, коли студент виконує завдання на практиці, стажуванні, в умовах реального виробництва або в умовах, наближених до реальних (у віртуальних світах, тренажерному залі і ін.)

Опитувальні методи бувають усні (усне опитування, бесіда, інтерв'ю) та письмові (письмове опитування, анкетування, тестування). Як правило, усні опитування індивідуальні, а письмові - фронтальні.

Усне опитування - один з найбільш поширених методів контролю у вищій школі, більшість іспитів і заліків проводиться у формі опитування, співбесіди по заздалегідь підготовленим темам або проблем. Перевагою цього методу є гнучкість, можливість задати додаткові питання, зрозуміти глибину знань того, хто навчається. Істотним недоліком знову є суб'єктивність висновків про рівень навченості студента. Щоб отримати об'єктивні результати за допомогою цього методу, необхідна система критеріїв і показників, відкрита і зрозуміла як викладачеві, так і учневі.

Тест - (від англ. Test - випробування, дослідження) - стандартизована процедура вимірювання. Дуже популярний на даний момент метод контролю результатів навчання, один з найбільш об'єктивних. Тестом не може бути випадковий набір завдань, тест повинен бути надійним (стійкість результатів тестування), дійсним (відповідати цілям діагностики).

Анкетування - метод, який дозволяє зібрати інформацію про таких важко стандартизовані результати навчання, як відношення до освітньої установи, майбутньої професії і т.п. Відкриті, що вимагають розгорнутої відповіді, питання дозволяють зібрати різнопланову інформацію.

Вивчення результатів діяльності також є ефективним методом. Розроблена студентом комп'ютерна програма, виконаний проект, портфоліо, створений макет, реальний об'єкт, і т.д., все може характеризувати результати навчання. Для аналізу і оцінки цих робіт викладачами та учнями розробляються методики оцінки, які включають критерії та параметри.

Проаналізуємо найбільш відомі підходи до оцінки результатів навчання. Одним з найвідоміших варіантів класифікації педагогічних цілей, а відповідно і підходом до оцінки результатів є Таксономія Блума. Він запропонував ієрархічний список когнітивних процесів: знання, розуміння, застосування, аналіз, синтез, оцінка. Цей список зручний для формулювання цілей і завдань конкретної навчальної програми або заняття, однак, він не може виступати в якості вимірювальної шкали для результатів навчання, навіть номінальної шкали. Ми не можемо розбити всі результати навчання, користуючись цим

списком на непересічні класи (наприклад, аналіз, синтез і оцінка служать ознаками розуміння навчаються матеріалу і т.д.).

Беспалько В. П. у своїй роботі виділяє чотири ключові точки, де відбувається, на його погляд, якісна зміна рівня володіння учням вихідною інформацією. Ці точки, на думку автора, диференціюють майстерність оволодіння діяльністю учням в ході навчання і розглядаються як чотири рівні майстерності (досягнення, компетенції) учня для оцінки його досвіду (рис. 1.2).

Інтерес представляє і підхід В. П. Симонова, який виділяє п'ять послідовних показників, які складають ідеальну модель навченості: розрізнення, запам'ятовування, розуміння, елементарні вміння і навички, перенесення (складні вміння і навички).

Рис 1.2. Логічна структура класифікації рівнів засвоєння

Існує підхід, в якому враховані недоліки і переваги описаних вище підходів. Поділ на рівні багато в чому є умовним, так як знання, вміння і навички ми можемо розділити тільки в теорії, на практиці ж судити про знання суб'єкта можна, аналізуючи його діяльність або результати цієї діяльності, а й діяльність відбувається на основі певної інформації вже наявної в пам'яті. Можна виділити чотири групи результатів навчання: впізнавання, розуміння, відтворення, інновації (табл. 1.5).

Таблиця 1.5.

Поділ результатів навчання на групи

№	Групи результатів навчання	Конкретні дії, що дозволяють виявити і оцінити результати навчання
1	Впізнавання	Впізнання сприйманого об'єкта як такого, який вже відомий по минулому досвіду Виконує тестові завдання на вибір вірних відповідей із запропонованих, завдання на відповідності та ін.
2	Відтворення	Відтворює терміни, конкретні факти, відтворення, методи і процедури, основні поняття, правила і принципи, руху, дії, виконує тестові завдання з коротким вільною відповіддю (словосполучення або число)
3	Розуміння	Здійснює з вивченим матеріалом дії: аналіз, синтез, порівняння, узагальнення, конкретизація, абстрагування та ін. Багато ці дії можуть бути як розумовими (проходити у внутрішньому плані), так і зовнішніми (практичними, тобто об'єкти розбираються на складові, збираються з частин і т.д.) Виконує завдання з розгорнутою вільним відповіддю: словесне обгрунтування, математичний висновок, есе, докази, викладення власної позиції та ін.
4	Інновації	Створює нове знання, вдосконалює діяльність Проектна, дослідницька робота, творчість

Для кожної групи можуть бути розроблені контрольно-вимірювальні матеріали для виявлення відносного показника якості дозволяє зіставляти і порівнювати успіхи різних учнів або одного і того ж учня в різні періоди

навчання.

1.3. Принципи і послідовність розробки секторальної рамки кваліфікацій

СРК розробляється на основі національної рамки кваліфікацій та професійних стандартів з урахуванням наступних принципів:

- відображення пріоритетів напряму підготовки з урахуванням стратегічних цілей розвитку і бізнес-інтересів компаній;
- спадкоємність і безперервність розвитку кваліфікаційних рівнів від нижчого до вищого відповідно рівнями освіти;
- прозорість опису кваліфікаційних рівнів для всіх користувачів;
- відповідність ієрархії кваліфікаційних рівнів структурі європейської та національних освітніх системах поділу праці;

Розробка рамок кваліфікацій здійснюється в наступній послідовності:

- структурне проектування і попереднє заповнення рамок кваліфікацій;
- актуалізація рамок кваліфікацій з уточненням їх змісту.

Структурне проектування повинно проводитися зверху вниз за ієрархією рамок кваліфікацій, як це показано на рисунку 1.3.

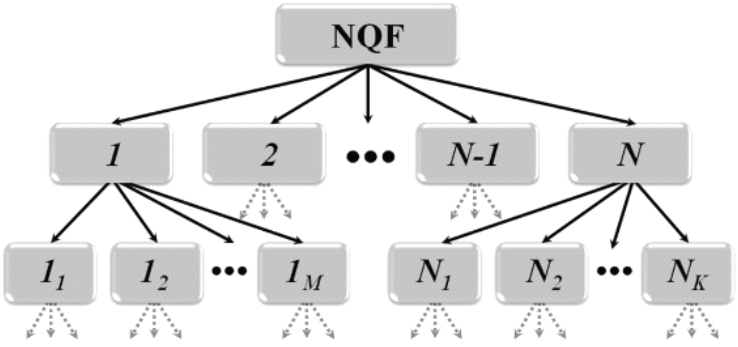


Рис. 1.3. Структурне проектування рамок кваліфікацій

На даному етапі задається структура ієрархії і структури рамок кваліфікацій всіх ступенів з додаванням відповідних додаткових полів. При заповненні змісту рамок кваліфікацій в якості вихідних матеріалів повинні використовуватися зміст рамки кваліфікацій, під яким в ієрархії знаходиться

проектована рамка, а також всі доступні нормативні документи і бази даних, які містять в тій чи іншій формі результати навчання, придатні для даної щаблі. В якості таких джерел можуть розглядатися професійні стандарти, описи трудових функцій, бази даних вакансій і т.д. При цьому широта і повнота використання вихідних матеріалів багато в чому визначатимуть якість проектованої рамки кваліфікацій, тобто ступінь її відповідності реальної ситуації на потенційному ринку праці.

Структурний проектування повинно проводитися не дуже часто, як правило, у випадках кардинальних структурних змін в національній освітній системі. Незначні зміни в структурі можуть, звичайно, проводитися досить часто, але це скоріше за все можна віднести до доопрацювання, а не проектування рамок кваліфікацій. В даному випадку можна говорити про якийсь процесі конкретизації результатів навчання зверху вниз по ієрархії рамок кваліфікацій.

Актуалізація рамок повинна проводитися знизу вгору по ієрархії рамок кваліфікацій, як це показано на рисунку 1.4.

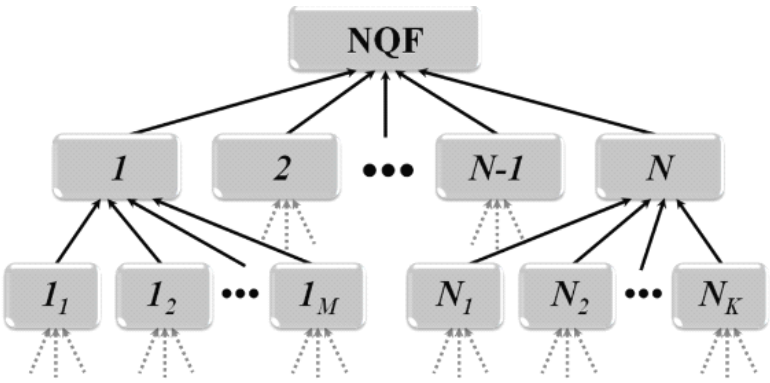


Рис. 1.4. Актуалізація рамок кваліфікацій

На даному етапі зміст рамок кваліфікацій має уточнюватися на основі аналізу думок всіх, зацікавлених в якості освіти, сторін, залучення нових (оновлених) нормативних документів і баз даних, а також змісту актуалізованих рамок, які в ієрархії знаходяться під актуалізується рамкою. Актуалізація рамок кваліфікацій повинна проводитися досить часто з тим, щоб поточне утримання рамок кваліфікацій максимально відповідало реальної ситуації на потенційному

ринку праці. В даному випадку можна говорити про процес узагальнення результатів навчання від низу до верху по ієрархії рамок кваліфікацій.

З інформаційної точки зору актуалізація може розглядатися як процес послідовного наближення (простої ітерації) до оптимальних рамкам кваліфікацій. Збіжність подібної послідовної оптимізації не складно довести формально на основі теорії динамічного програмування. Іншими словами в будь-якому випадку в процесі послідовних актуалізацій будуть отримані рамки кваліфікацій, максимально відповідають реальній ситуації на потенційному ринку праці. При цьому формально кажучи, якість і широта охоплення вихідних матеріалів на етапі структурного проектування будуть впливати лише на кількість ітерацій, необхідних для досягнення локального оптимуму.

Однією з найважливіших складових процесу актуалізації рамок кваліфікацій є вибір списку зацікавлених сторін для отримання від них необхідної зворотного зв'язку. Аналіз процесів управління якістю навчальної діяльності передових університетів дозволяє зробити висновок, що, як показано на рисунку 1.5, з точки зору вдосконалення освітніх програм та забезпечення якості найбільш важливими зацікавленими сторонами є:

- потенційні роботодавці;
- недавні випускники;
- викладачі;
- студенти.

Всі перераховані зацікавлені сторони досить тісно взаємодіють, маючи одну загальну глобальну мету – забезпечення високої якості освіти. При цьому перші дві з перерахованих є зовнішніми зацікавленими сторонами, які в першу чергу стурбовані тим, що викладається в університетах, тобто в структурі освітніх програм і, як наслідок, в результатах навчання. Разом з тим, останні дві в списку є внутрішніми зацікавленими сторонами, які в першу чергу стурбовані тим, як здійснюється процес навчання (як постачальників або одержувачів знань, умінь і навичок), тобто в використані принципи, методиках і інструментах. Безсумнівно, з точки зору забезпечення затребуваності

випускників на ринку праці максимальний інтерес представляють запити і вимоги роботодавців.

В якості засобів отримання зворотного зв'язку від зацікавлених сторін можна розглядати індивідуальні та групові інтерв'ю, фокус групи, спільні обговорення і т.д. Однак, в більшості випадків, особливо при подальшій комп'ютерній обробці отриманої інформації, найбільш ефективними представляються електронні форми анкетування.

В цілому можна відзначити, що такий підхід до розробки рамок кваліфікацій допускає використання самих різних методик заповнення змісту на етапі структурного проектування, а також різних технологій отримання зворотного зв'язку від зацікавлених сторін на етапі актуалізації. Більш того, для окремих рамок кваліфікацій можуть використовуватися специфічні методики і технології.

РОЗДІЛ 2.
ОПИС ВЕБ-ДОДАТКА, ЩО РОЗРОБЛЯЄТЬСЯ («ЗАТРЕБУВАНА ОСВІТА»)

2.1. Призначення розробки

Основною метою розроблюємого веб-додатка є об'єднання систем освіти країн СНД і Європи і визначення відповідностей між ними. На даному сайті користувачі матимуть можливість отримувати різну корисну інформацію про освітню діяльність: наприклад, роботодавці – про зміст актуальних програм навчання в університетах, а студенти – про можливі професіях і трудових функціях, властивих цих професій, і не тільки в рамках своєї країни, а та інших країн. Така інформація є необхідною для розуміння особливостей працевлаштування за кордоном.

Неймовірно корисну функцію веб-додатка також виконує динамічноадаптуючийся опитувальний модуль. Він дозволяє користувачам сайту користуватися пошуком голосування відповідно їх сфері діяльності. На основі результатів голосувань будується статистика, як наприклад: які професії є найбільш популярними або затребуваними на думку користувачів. До того ж результати опитувань можуть принести величезну користь різним учасникам освітньої діяльності, так як з їх допомогою університети, наприклад, мають можливістьспостерігати за тим, які спеціальності найбільш цікаві абітурієнтам або якими знаннями, вміннями і навичками, а також компетенціями необхідно володіти співробітнику на думку роботодавця і коригувати свої навчальні програми; студенти ж, володіючи такою інформацією, будуть знати, що конкретно їм необхідно вивчити для отримання бажаної роботи. Характерною рисою опитувального модуля є те, що опитування для конкретного користувача генеруються в залежності від його типу (професіонал ринку праці, професіонал сфери освіти, методист, студент і зацікавлений). Наприклад, якщо користувач є абітурієнтом (зацікавленим), то йому пропонується голосування за інтересуючи його спеціальності.

2.2. Опис бази даних

Зберігання сутностей і атрибутів компетентнісних моделей різних країн в єдиній базі даних повинне ґрунтуватися на принципах динамічності і масштабованості. Оскільки сутності можуть мати різну безліч атрибутів, а кількість кваліфікаційних рамок і їх дескрипторів варіюється від країни до країни (те ж стосується, наприклад, категорій в класифікаторі професій), система повинна пропонувати мінімум обмежень по конфігурації національних рамок. База даних повинна наслідувати загальну логіку систем освіти багатьох країн, що дозволить адаптувати національні вимоги під загальну схему, відповідно оптимізувавши роботу з програмною частиною.

Таблиця 2.1.

Імена таблиць у БД

Назва таблиці у БД	**Сутність**
Country	Країна
User	Користувач
ChangebleObjects	Змінні об’єкти
User_Rate	Рейтинг користувачів
Rate	Рейтинг
Rate_OccupationDescriptors	Рейтинг дескрипторів професій
OccupationDescriptors	Дескриптори професій
Rate_Descriptors	Рейтинг дескрипторів
DescriptorType	Типи дескрипторів
OccupationCategory	Категорії професій
OccupationalStandard	Професійний стандарт
Transversal_skills/competences	Поперічні навички/компетенції
Job-specific_skills/competences	Специфічні робочі навички/компетенції
DescriptorsContent	Вміст дескрипторів

Назва таблиці у БД	**Сутність**
Skills	Навички (вміння)
Descriptors	Дескриптори
EducationalLevel	Освітній рівень
Competences	Компетенції
KnowledgeSectors	Галузі знань
Discipline	Дисципліни
SectorHierarchy	Ієрархія галузі
Rate_Discipline	Рейтинг дисциплін
Cycle	Цикл
CompetenceDescriptors	Дескриптори компетенцій
SkillsDescriptors	Дескриптори вмінь
Occupations	Професій
Qualifications	Кваліфікації
Descriptions	Описання
Framework	Рамки

Основні таблиці БД:

- Framework – таблиця з записами про всі існуючі рамки; містить спеціальний ідентифікатор з текстовим ім'ям рамки.
- Descriptors – таблиця, в якій зберігаються записи про такі дескриптори рамок як знання, вміння і так далі.
- DescriptorsContent – таблиця з записами про вміст дескрипторів.
- EducationalLevel – таблиця з записами про рівні освіти.
- KnowledgeSectors – таблиця, в якій зберігаються записи про галузі знань з їх кодами і назвами.
- OccupationCategory – таблиця, в якій зберігаються записи про категорії професій.

- OccupationalStandard – таблиця, в якій зберігаються записи про професійні стандарти.
- OccupationDescriptors – таблиця з записами про дескриптори професій.

Для уніфікації даних, що відносяться до різних національних систем, передбачено створення таблиці ієрархії кваліфікаційних рамок, яка пов'язана з рівнем доступу користувачів. На рис. 2.1 представлено відповідність кваліфікаційних рамок і наборів дескрипторів, їх описів (в окремій таблиці з урахуванням рівня освіти і відповідних навичок).

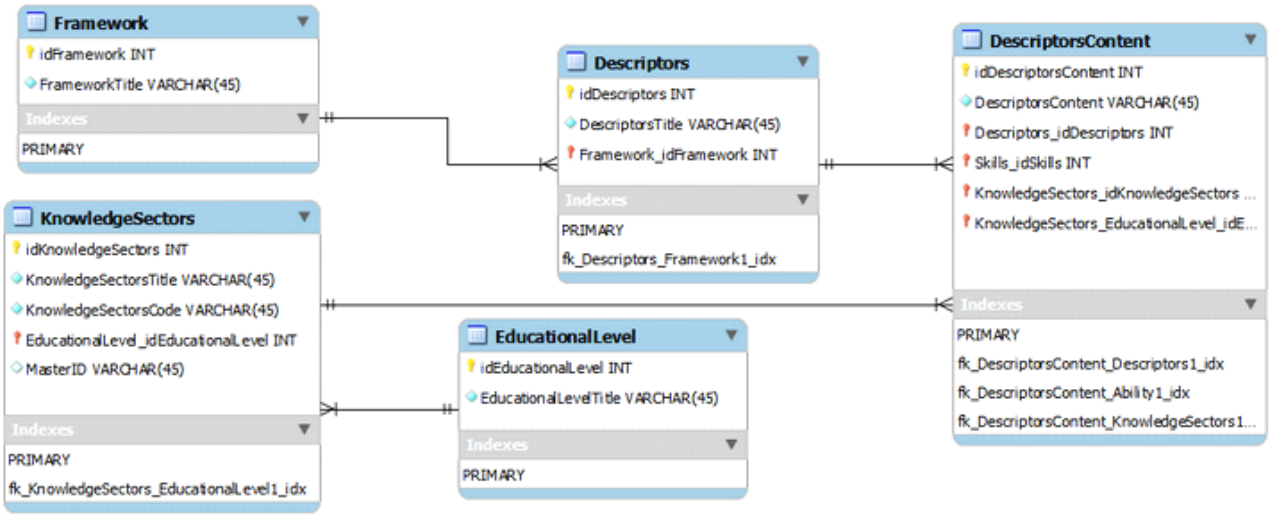


Рис. 2.1. Загальна модель кваліфікаційних рамок

При додаванні країн-учасниць необхідний облік можливості реєстрації шаблону незаповненою бази даних, а також визначення структури шаблонів.

Також необхідно передбачити можливість обліку користувачів з різними правами доступу для внесення змін тільки в певні таблиці для певних країн. Категорії користувачів (рис. 2.2) повинні ділитися на звичайних користувачів без права на зміни, користувачів з обмеженими правами - можливістю редагувати освітні дескриптори, рамку, яка безпосередньо до них відноситься, і на користувачів з розширеними правами доступу - правом редагування однієї або кількох інших рамок професійного стандарту. Право доступу буде

змінюватися в залежності від значення полів CanManage і IsVerified. За замовчуванням їх значення будуть false. Залежно від запиту користувача, адміністратор зможе змінити їх або ж залишити початкове значення.

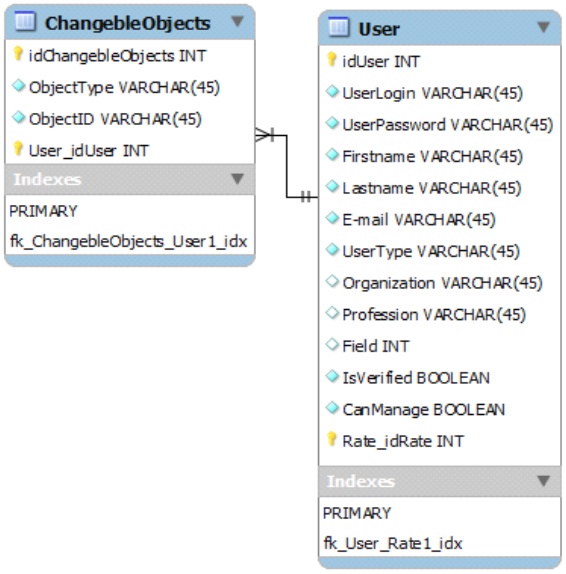


Рис. 2.2. Фрагмент моделі БД, що демонструє користувачів і об'єкти, які можуть бути ними змінені

Для уніфікації системи передбачається створення таблиці змінюваних об'єктів, яка пов'язана з рівнем доступу користувачів.

Прив'язка таблиць Країна-Користувач і уніфікація загального вигляду системи має забезпечити створення повноцінної бази всіх учасників, швидкий обмін досвідом з розробки кваліфікаційних рамок, професійних стандартів та освітніх дескрипторів.

Для кожної країни має бути вказано ім'я сервера, мова і користувачі бази.

З кожним користувачем слід пов'язати (рис. 2.2) індивідуальні дані ідентифікації, особисту інформацію, атрибути, що характеризують відношення / доступ цього користувача до тих чи інших напрямках освіти або сферами економічної діяльності.

На рис. 2.1 представлена частина бази даних, що дозволяє зберігати всі дані, необхідні з позицій освіти для розробки кваліфікаційних рамок. У

таблиці Framework пропонується зберігати всі кваліфікаційні рамки (національні, секторальні, субрамкі). Для кожної кваліфікаційної рамки існує свій набір дескрипторів в пов’язаній таблиці Descriptors, а зміст кожного дескриптора - в DescriptorsContent. Це важливий поділ для масштабованості системи, оскільки кожна країна-учасник має своє власне бачення на критерії для кваліфікаційних рамок, їх назви і кількість.

Наповнення рамок залежить від галузі знань (KnowledgeSectors). Кожна країна має свою ієрархічну структуру галузі знань, тому в таблиці KnowledgeSectors поле MasterID дозволяє її зберегти і створити єдину динамічну мультинаціональної систему. Сектор знання і його рівень залежить від рівня освіти (EducationalLevel).

Ми пропонуємо через опис дескрипторів пов'язувати загальну базу освітніх рамок з освітніми дескрипторами, унікальними для кожної з країн.

У випадку України зв'язок грунтується на наповненні рамок спеціальностей (галузевих субрамок) через дескриптори «вміння». Саме ці вміння будуть набуватися при вивченні тієї чи іншої дисципліни, тому подібний зв'язок таблиць цілком виправданений. Подібний прийом демонструє можливості динамічного підходу до використання пропонованої структури бази даних, яку можна гнучко конфігурувати під безліч національних систем.

Як приклад розглянемо модель бази даних, яка застосовується для опису освітніх дескрипторів України (рис. 2.3).

Список дисциплін міститься в таблиці Discipline з інформацією про назву дисципліни, її шифр, тривалість академічних годин, кількість нарахованих кредитів. Вона пов'язана з освітнім циклом (Cycle) і компетенціями, що придбані при вивченні дисципліни. У кожної компетенції є кілька дескрипторів (наприклад, типова задача діяльності, її вид і клас). Ці дані містяться в таблиці CompetenceDescriptors.

Рис. 2.3. Модель українських освітніх дескрипторів

Кожній компетенції відповідає певний набір навичок і умінь (Skills). Вони можуть мати ряд дескрипторів, який буде зберігатися в таблиці SkillsDescriptors.

Як згадувалося раніше, зв'язок рамок і освітніх дескрипторів в пропонованій базі здійснюється через вміння і навички, оскільки вміння, придбані при вивченні дисципліни, збігаються з вмістом дескрипторів кваліфікаційних рамок.

Класифікатор професій (рис. 2.4) являє собою ієрархічну структуру. Всі назви рівнів категорій професій будуть знаходитися в таблиці OccupationCategory. Оскільки в різних країнах класифікатори професій можуть значно відрізнятися, розподіл за категоріями пропонується здійснювати за допомогою додаткового поля MasterCategoryID. Кожній категорії буде віднесено назву, унікальний шифр і опис.

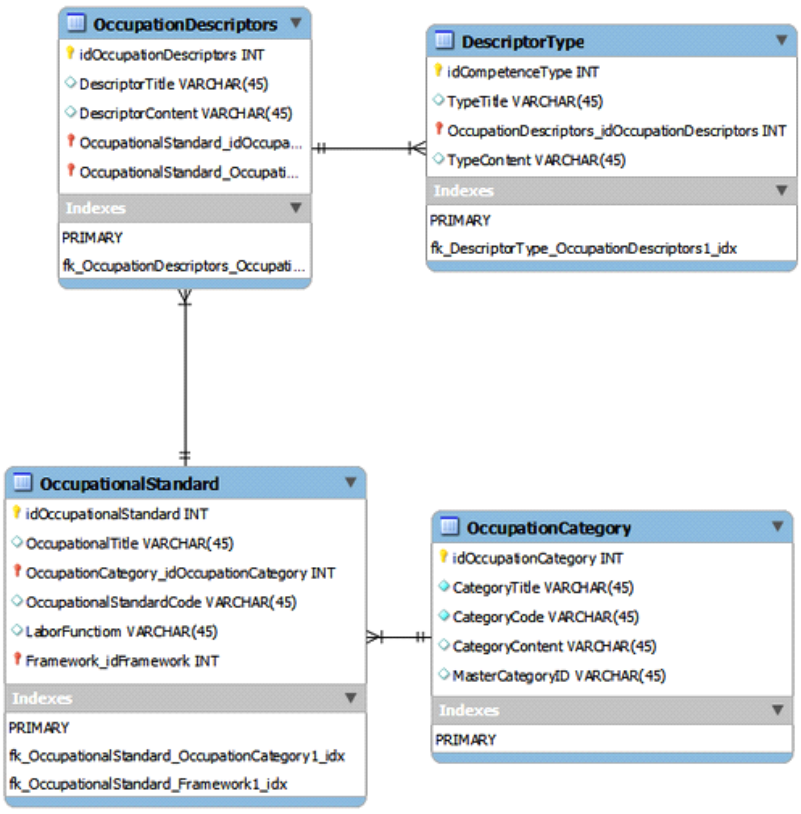


Рис. 2.4. Модель класифікаторів професій

Кожен професійний стандарт (OccupationalStandard) включає в себе назву професійної роботи, її шифр і трудові функції. У разі відповідності кількох трудових функцій одній роботі остання буде дублюватися зі зміною тільки в поле LaborFunction.

Дескриптори професійного стандарту і їх опис містяться в таблиці OccupationDescriptors і можуть мати певний тип. Дані про тип зберігаються в таблиці DescriptorType. Але оскільки тип дескриптора - необов'язковий параметр, то він може приймати значення NULL.

Зв'язок між професійними дескрипторами і кваліфікаційними рамками буде здійснюватися через прив'язку конкретних професій (OccupationalStandard) безпосередньо до рівня освіти (EducationalLevel) і побічно до сектору знань (KnowledgeSectors).

Для порівняння і допомоги в проектуванні кваліфікаційних рамок країн-партнерів, користувачам пропонується можливість аналізу рамок Європи, зокрема бази даних ESCO. Вони зберігаються в окремих таблицях (рис. 2.5) і мають прив'язку до рівня освіти. Європейська система являє собою зв'язок між

кваліфікацією освіти, навичками / компетенціями (які в свою чергу поділяються на Job-spesific і Transversal) і спеціальностями. Кожна з цих сутностей є ієрархічно структурованою. Поле MasterID реалізує це на технічному рівні.

Європейська система дозволяє робити вибірку компетенцій, які набуваються при певній кваліфікації, а також показує, які навички і компетенції необхідні для роботи на конкретній спеціальності.

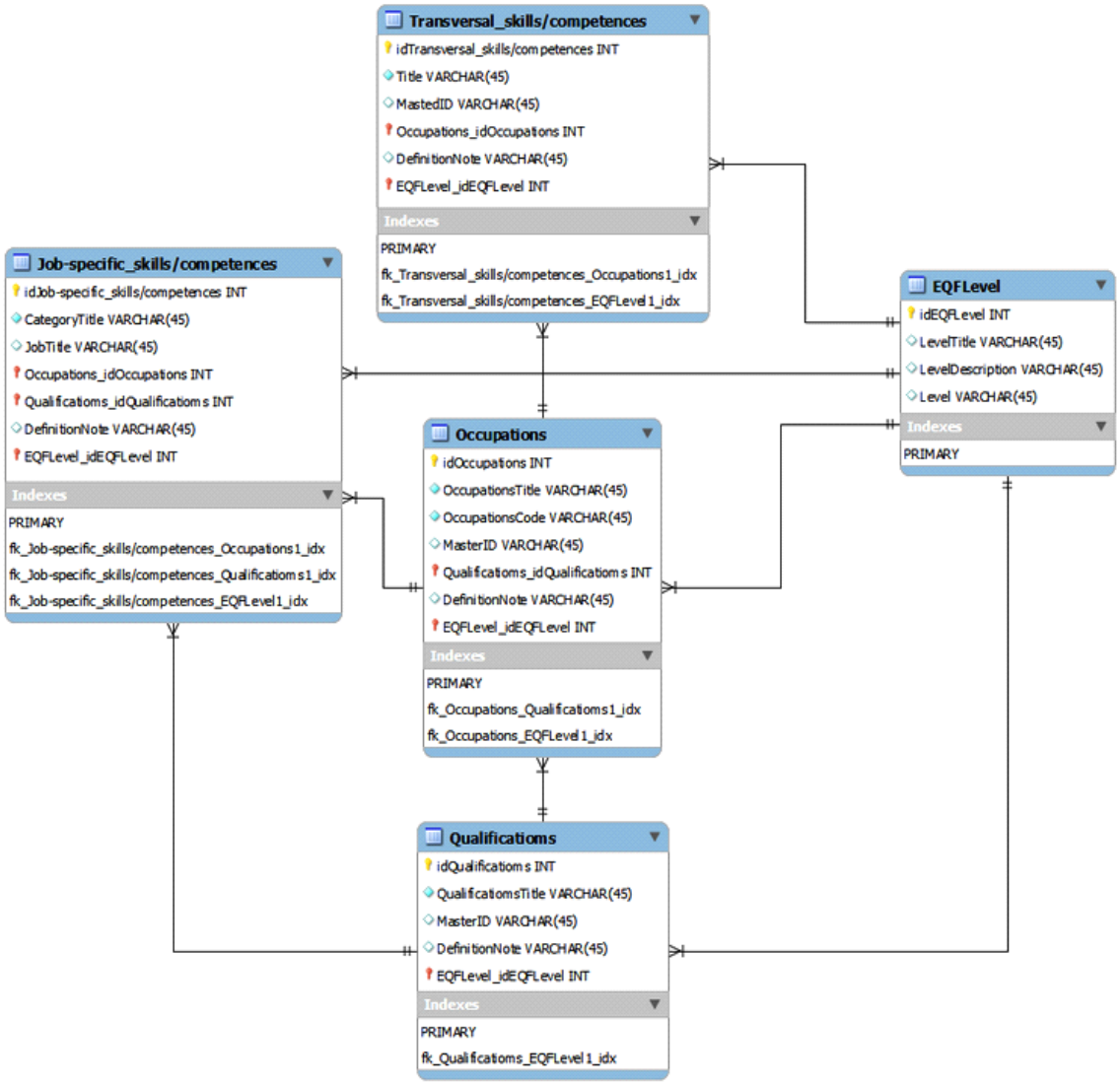


Рис. 2.5. Європейські навички, компетенції, кваліфікації і професії

Залежно від зазначеної інформації при реєстрації, кожному користувачеві буде надана можливість взяти участь в опитуванні по певним категоріям. Розглянемо відповідні таблиці баз даних, які відповідали поставленим вище завданням. Структура такої частини БД представлена на рис. 2.6. Так, в таблиці

Rate могла б зберігатися інформація за всіма опитуваннями з прив'язкою до кожного користувача. Вона повинна містити ID об'єкта, його ім'я і рейтинг.

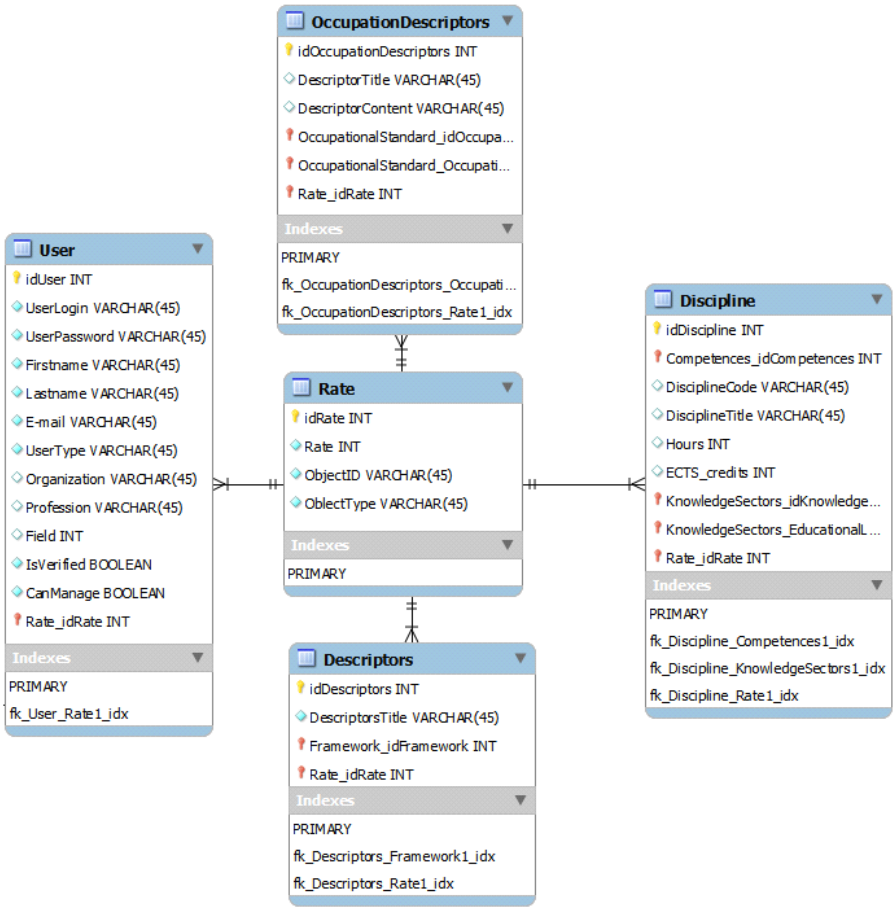


Рис. 2.6. Рейтингова система оцінювання.

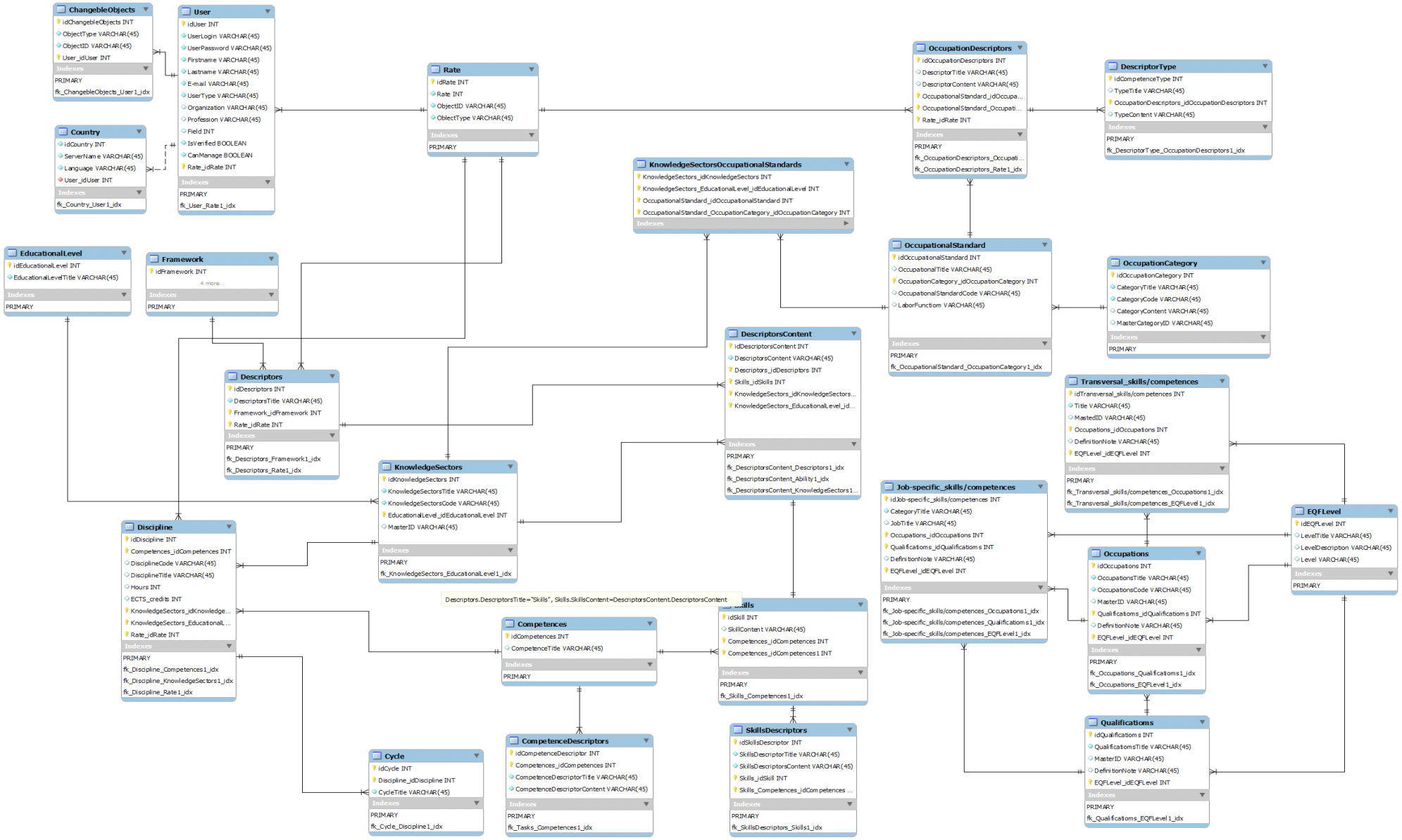


Рис. 2.7. Фізична модель бази даних веб-додатку, що розробляється

РОЗДІЛ 3.
МОДЕЛІ ТА АЛГОРИТМИ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ РОЗПОДІЛЕНИХ АТАК

3.1. Визначення DDoS-атаки

DDoS - це скорочення англійського виразу Distributed Denial of Service, що перекладається на російську мову як «розподілена атака типу« відмова в обслуговуванні »». Це означає відмову від обслуговування мережевого ресурсу в результаті численних розподілених (тобто відбуваються з різних точок інтернет-доступу) запитів. Відмінність DoS-атаки (Denial of Service - «відмова від обслуговування») від DDos полягає в тому, що в цьому випадку перевантаження відбувається в результаті запитів з якогось певного інтернет-вузла.

У разі набагато більш складною і досконалою DDos-атаки може бути повністю порушена робота будь-якого ресурсу - від невеликого інформаційного сайту до великого інтернет-магазину або поштового сервера. Під час атаки на сервер сайту-жертви надходять мільйони запитів від користувачів, що призводить до його перевантаження і, відповідно, недоступності. Не встигаючи обробляти величезну кількість запитів, сервер спочатку починає просто гальмувати, а потім і зовсім припиняє роботу. Запити найчастіше носять хитромудрий і безглуздий характер, що ще більше ускладнює роботу сервера.

Основна складність для власників сайтів полягає в тому, що величезна частина методів боротьби з DDos практично неефективні, адже запити надходять з різних сторін, і перекрити будь-який вузол, з якого надходять запити (як у випадку в Dos-атаками), недостатньо. Зазвичай атака проводиться за допомогою вірусних троянських програм, які залучають до цього процесу мільйони користувачів без їх на те згоди і повідомлення. Трояни заражають недостатньо захищені комп'ютери і можуть досить довгий час діяти, взагалі

ніяк себе не виявляючи. Зона охоплення таким чином стає неймовірно широкою, а запити можуть йти з самих різних сторін світу.

Заражені комп'ютери нерідко називають «зомбі», оскільки вони діють по чужому наказу. Комп'ютер може бути заражений через браузери при відвідуванні різних заражених сайтів, при отриманні пошти або при установці неліцензійного програмного забезпечення. Зомбі часто невидимі фаєрволлу або не відрізняються від реального користувача, що також ускладнює боротьбу з ними.

Вперше про DDos-атаки стало відомо в 1996 році, проте серйозну проблему вони почали представляти через три роки, коли хакерам вдалося вивести з ладу сайти таких компаній як Amazon, Yahoo, CNN, eBay і деяких інших. На сьогоднішній день замовити таку атаку досить просто і відносно недорого. І першими в зоні ризику опиняються бізнесмени, яких досить легко вивести з гри таким чином.

Зрозуміло, загибель корпоративного сайту - подія неприємне. Однак воно стає повністю катастрофічним, якщо від роботи порталу безпосередньо залежить прибуток компанії або якщо атака відбувається під час проведення грамотної, продуманої, добре спланованою і оплаченої інтернет-кампанії з просування і розкручування.

Не застраховані від DDos-атак і приватні особи, останнім часом набув поширення такий варіант помсти. Добре відомі і ідеологічні атаки, спрямовані на неправильні з точки зору організаторів атак ресурси. Відомі й випадки вимагання з боку самих хакерів, які вимагають грошей за припинення подібних атак, проте, зі зрозумілих причин, це не частий варіант розвитку подій, оскільки виконавці вважають за краще не виявляти себе.

В даний час найчастіше під час проведення атаки використовується трирівнева структура. Верхній рівень займає керуючий комп'ютер (або кілька комп'ютерів), з якого подаються керуючі сигнали - в тому числі і про початок

атаки. Наступними в ряду йдуть керуючі консолі, через які сигнали розподіляються по мільйонам комп'ютерів користувачів. Саме ці, що знаходяться в самому низу виконавці і відправляють запити на інтернет-сайті, який є метою злочинців. Простежити зворотний зв'язок неможливо, максимум можна обчислити одну з керуючих консолей, які також вважаються постраждалими від атаки.

Складністю у виявленні злочинців є і вільне поширення в мережі програм для проведення атак. Спочатку подібне програмне забезпечення розроблялося для виявлення ступеня стійкості мережі до зовнішніх навантажень. Однак за роки воно зазнало серйозних змін, було сформовано і вдосконалено кілька видів атак, які до того ж можуть поєднуватися, варіюватися і видозмінюватися. Саме тому захист від DDos-атак повинна бути професійною, постійною і оновлюваної.

3.2. Методи виявлення атак

Формальні методи виявлення і передбачення атак (в першу чергу DoS-атак) практично відсутні для широкого використання в реальних системах. В даний час серед фахівців склалося чітке переконання в тому, що аналіз інформаційного мережевого потоку є найбільш ефективним методом виявлення аномального поведінки розподіленої інформаційно-телекомунікаційній системі (ІТКМ) через його великий інформативності і потенційної можливості реагування в реальному масштабі часу. Тому найбільш перспективні дослідження в даний момент спрямовані на розробку способів і процедур виявлення атак, основою яких є вивчення впливу шкідливого впливу на характеристики мережевого трафіку.

В якості теоретичної бази в основному застосовується методологія та прикладні результати теорії систем масового обслуговування (теорії черг). Протягом десятиліть аналіз черг грунтувався на припущенні про відповідність типу трафіку розподілу Пуассона. Однак результати ряду досліджень показали, що в окремих випадках трафік є за своєю природою самоподібним (self-similar),

або фрактальним. При такому трафіку системні характеристики не підпорядковується формулами аналізу черг, а мають місце великі затримки і зниження пропускної здатності. Ці результати були підтверджені на трафіках самих різних типів. У своїй роботі «The chaotic nature of TCP congestion control» Верес показав, що виникаючи скупчення пакетів TCP-трафіку поводяться як хаотичні. В даному випадку під хаосом розуміється складна поведінка, мінлива у часі, викликана взаємним впливом потоків TCP-трафіку. Така поведінка трафіку чутлива до найменших збурень, незважаючи на те, що описується простими і детерминистическими рівняннями. Розгляд TCP-трафіку з позицій теорії хаосу дає можливість враховувати кореляції потоків і надає ту ж складну картину мережі, яка спостерігається і в реальності.

В даний час достовірно невідомо, що в точності викликає хаотична поведінка TCP-трафіку, відповідно невідомо як дана модель може бути застосовна в загальному випадку. Зокрема, дослідження в [24] вказують на те, що хаотичність спостерігалася в мережах, де ймовірність втрати пакетів становила значно більше 1%, і спостерігався наростаючий процес відстрочки передачі (цілком ймовірно, що дана мережа була під DoS-атакою).

У розділі на основі гіпотези, що самоподобна і персистентність мережевого трафіку викликана DoS-атакою, розробляються моделі і процедури аналізу TCP-трафіку на основі теорії хаосу, пропонується методика раннього виявлення інформаційної атаки, досліджується адекватність запропонованих моделей.

3.3. Математична модель самоподібного процесу

3.3.1. Неперервний самоподібний процес

Процес X (t) вважається статистично самоподібним з параметром , якщо для будь-якого позитивного числа a, процеси і матимуть ідентичні розподілення, тобто матимуть однакові статистичні властивості для всіх позитивних цілих n:

•

Ставлення ^ (~ D) позначає асимптотическое рівність в сенсі розподілення. Практично статистична самоподобна має на увазі, що виконуються наступні умови [24]:

- середнє ; (3.2)
- дисперсія ; (3.3)
- автокореляція . (3.4)

H – параметр Херста (Hurst), показує «ступінь» самоподібності. Значення H = 0,5 показує відсутність самоподібності, а великі значення H (близькі до 1) показують велику ступінь самоподібності або тривалої залежності (long-range dependence, LRD) в процесі. Це означає, що якщо LRD-процес має тенденцію до збільшення (або зменшення) в минулому, то з великою ймовірністю він буде матимуть тенденцію до збільшення (або зменшення) в майбутньому.

3.3.2. Дискретний самоподібний процес

Розглянемо тимчасової процес і визначимо інший часовий процес шляхом усереднення оригінального тимчасового процесу на непересічні сусідами блоки довжиною m як

(3.5)

представляє в цьому випадку найбільше можливе для процесу дозвіл. Наступні еволюції процесу можуть бути отримані шляхом m-усереднення процесу , наприклад:

Процес є менш деталізованою копією процесу . У разі, якщо статистичні властивості (середнє, дисперсія) зберігаються при усередненні, тоді процес є самоподібним.

Існує два класи самоподібних процесів: так звані точно самоподібні і асимптотично самоподібні процеси. Процес X называется точно самоподобным с параметром β (0 < β < 1) якщо для виповнюэться такі умови:

– дисперсія визначається наступним чином:

; (3.6)

– функція автокореляції

. (3.7)

Параметр β связан с параметром Херста H відношенням

. (3.8)

Процес X називається асимптотично самоподібним, якщо для великих k дисперсія визначається як , а функція автокореляції при .

Є спостереження, що для обох класів самоподібних процесів дисперсія меншується набагато повільніше, ніж при в порівнянні зі стохастичними процесами, де дисперсія зменшується пропорційно и наближається до 0 при .

Найбільш точним властивістю самоподібних процесів є те, що функція автокореляції не вироджується при , на відміну від випадкових процесів, де при .

3.4. Математична модель DDoS-атаки

Для моделювання припустимо, що атакуючий вузол має вхідний канал з пропускною спроможністю C біт/с, а прикордонний маршрутизатор - вхідний буфер розміром B біт. Ситуація атаки може бути симульована за допомогою моделі статистичного мультиплексування трафіку від N атакуючих вузлів, які можуть перебувати в двох станах: відсилання пакетів (ON-стан) і бездіяльності (OFF-стан).

Позначимо періоди часу (в секундах) функціонування і бездіяльності як t1 = i t2 = відповідно. Якщо джерело є активним (ON-стан), то він генерує r пакетів в секунду. Розмір посилається пакета в бітах позначимо як L, а обсяг отриманих пакетів в момент часу t як Q(t).

Тоді ймовірність перевантаження буфера може бути апроксимована формулою:

, (3.17)

де

. (3.18)

Щоб викликати перевантаження каналу передачі, атакуючому необхідно вибрати такі параметри атаки, щоб значення було близько до нуля або негативне. Тому число вузлів для здійснення атаки має задовольняти нерівності

(3.19)

Назвемо коефіцієнтом зайнятості джерела трафіку ставлення тривалості відсилання пакетів джерелом до всього періоду функціонування і бездіяльності

(3.20)

Тоді нерівність, що обмежує кількість атакуючих вузлів, можна виразити як . У типових ICMP-flood атаках атакуючі вузли постійно знаходяться в ON-стані, направляючи паразитний трафік жертві. У цьому випадку коефіцієнт і нерівність для кількості атакуючих вузлів спрощується до .

Щоб атака стала важко розпізнавана, зловмисник маскує її під звичайне перевантаження в мережі. Для цього йому потрібно підібрати досить малі значення для параметрів і . Так, якщо зловмисник вибере значення і пак/с, а метою атаки є сервер з каналом пропускною спроможністю C = 10 Мбіт / с, то знадобиться атакуючих вузлів для проведення атаки.

Крім того, зловмисник може виконувати кілька процесів на кожному з вузлів атаки, а ті, використовуючи фіктивні адреси відправників, зможуть виступати для атакуючого як різні джерела трафіку. Таким чином, здійснити розподілену DoS-атаку, маскуючи її під природні перевантаження каналу, досить реально.

Зроблені висновки можна узагальнити і на різні типи джерел атаки. Нехай у атакуючого є M різних типів атакуючих вузлів. Тоді атакуючий повинен так підібрати параметри атаки, щоб виконувалося співвідношення

. (3.20)

Маючи в своєму розпорядженні достатню кількість N підконтрольних вузлів, зловмисник може генерувати трафік, який не викликає підозр і аналогічний трафіку від звичайного користувача. На підставі деякої зібраної статистики про динаміку стану мережі (наприклад, рівні втрат пакетів) - процесі – можна дати оцінку майбутнім станам системи, що вивчається.

3.5. Опис системи, що моделюється

Одним з поширених методів проведення DDoS-атаки є перевантаження вхідного каналу жертви. Атакуючі вузли намагаються завантажити всю смугу пропускання каналу пакетами з даними, що не несуть ніякого сенсу, з підставним адресою відправника. Прикладом такої атаки є ICMP-flood атака.

Наша модель буде описувати систему, що складається з N обчислювальних машин (ОМ) - джерел TCP-трафіку, з'єднаних з маршрутизатором (В), який в свою чергу з'єднаний з сервером - метою атаки.

На рис. 4.1 представлена топологія модельованої системи. Кожна ОМ працює по протоколу TCP NewReno (дана модифікація використовується в більшості систем). Відсилаємий трафік від джерел будегенеруватися FTP-додатками. У моделі = 1 Мбіт / с; відсилання пакетів (ON-стан) - , бездіяльність (OFF-стан) -; кожен з атакуючих вузлів з'єднаний з маршрутизатором каналом = 10 Мбіт / с (i = 1..N).

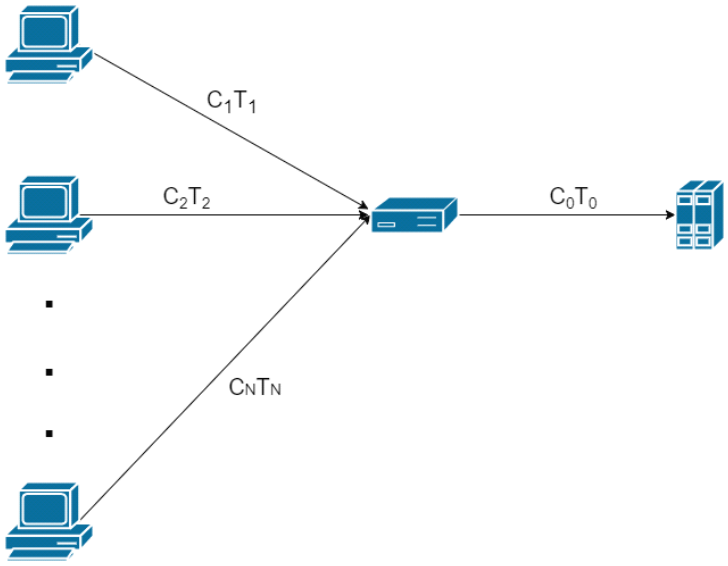


Рис. 4.1. Топологія моделюючої системи

Розмір переданого файлу 10 Кбайт (типовий для трафіку FTP-додатків), значення параметра розподілу дорівнює 1,2. Для моделювання розглянутої мережі зручно скористатися існуючим ПЗ. Найбільш відповідною програмою тут є NetworkSimulator, оскільки вона надає можливість провести імітаційне

моделювання поведінки транспортних і прикладних протоколів. Програма надає опис вузлів мережі, завданняїх характеристик, характеристик каналівпередачі, що зв'язують вузли між собою. ПЗ NetworkSimulator (NS) реалізує всі модифікації протоколу TCP (Vegas, Tahoe, Reno, NewReno), а також протокол UDP. За допомогою скриптового мови TCL можна розробити свій протокол мережевої взаємодії.

Результати моделювання

Моделювання проводилося протягом 2000 секунд. Процес починає передачу в моменти часу t_1 = 0,072 с і t_2 = 0,0669 с відповідно. Синтезованийтрафік, якийпоказуєзавантаження каналу передачі між сервером і маршрутизатором двома потоками TCP-з'єднань, зображений на рис. 4.2.

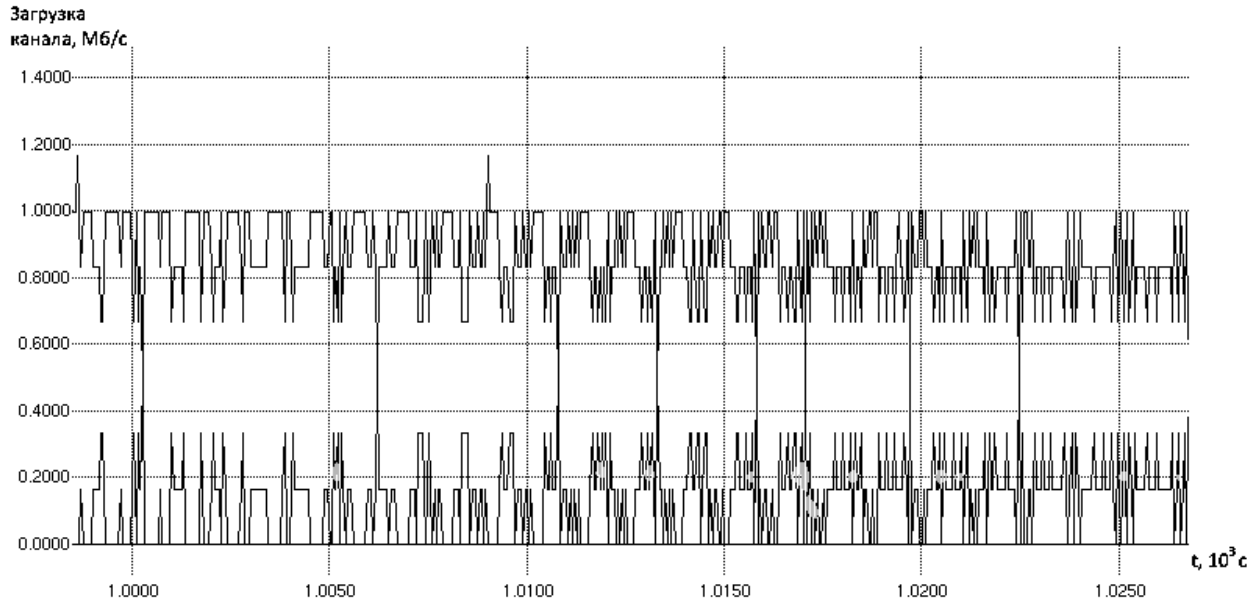


Рис. 4.2. Завантаження каналу передачі між сервером і маршрутизатором двома потоками TCP-з'єднань

На рис. 4.3 зображена динаміка зміни значення вікон контролю перевантаження кожного з TCP-з'єднань. Як видно з графіка, протягом 300 з вікна перевантаження TCP-з'єднань адаптувалися до наданого каналу передачі, після чого перейшли в більш-менш стабільну фазу передачі.

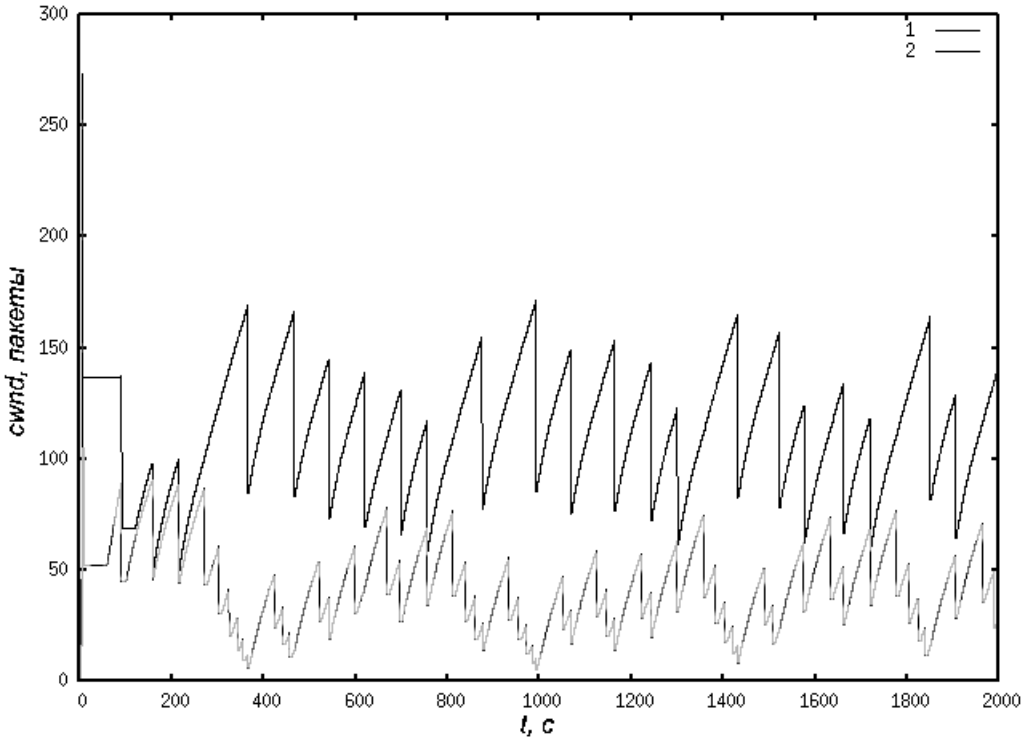


Рис. 4.3. Зміна величини вікон перевантаження TCP-з'єднань

На графіку видно, що коливання 1-ого та 2-ого з'єднань слідують одному і тому ж сценарію: підйом - алгоритм уникнення затору, після слід втрата пакета і повернення - зниження вікна контролю перевантаження.

Розглянемо докладніше один з інтервалів (рис. 4.4).

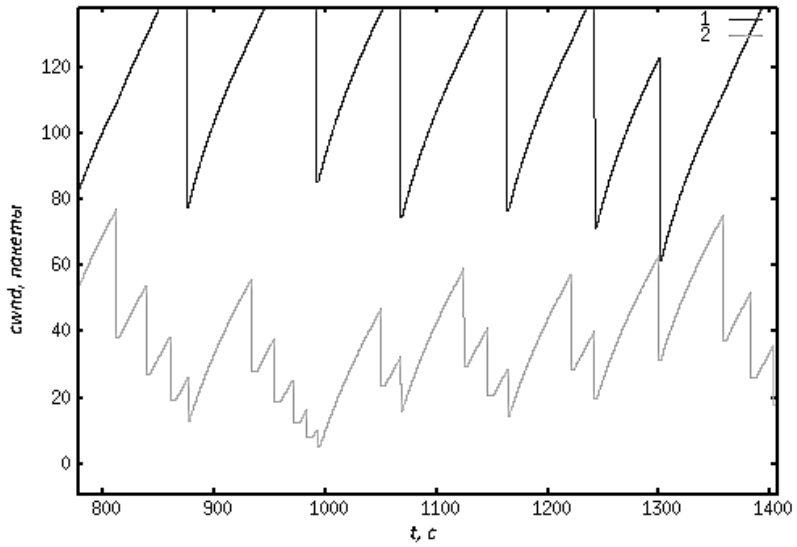


Рис. 4.4. Інтервал графіка вікон перевантаження з 800 по 1400 с.

У момент часу t_1 = 932,17 с. друга ОМ виявляє втрату пакета при передачі, в цей час вікно контролю перевантаження мало значення cwnd = 55,9293. Відповідно до специфікації протоколу TCP версії NewReno після детектування

втрати пакета передаюча сторона повинна зменшити поріг розгону ssthresh і вікно cwnd в два рази, що і спостерігається на графіку (значення cwnd падає з 55,9293 до 27,964).

Після цього передача поновлюється відразу в режимі уникнення затору: клієнт працює в режимі швидкого надолуження. При цьому значення cwnd зросте на 1 за час повного оберту пакета RTT, але до 952-ій секунді відбувається чергова втрата пакета, тим самим починаючи процес швидкого надолуження заново.

Параметри модельованої системи можна розглядати не тільки в залежності від часу. Побудуємо траєкторію системи в фазовому просторі. Фазовий простір - багатовимірний простір, де кожна з вимірювань являє собою значення однієї із системних змінних. Таким чином, кожна точка в цьому просторі представляє універсальний стан розглянутої системи.

Зобразивши еволюцію системи в даному просторі, отримуємо (так як система детермінована), що якщо система повернеться в одну з вже побудованих точок, то в подальшому вона повторить вже відображене безліч станів, і в підсумку вийде замкнутий цикл. Виходить, що якщо система періодична, то її траєкторією є замкнутий цикл, і навпаки.

Досліджувана система може мати досить велику кількість змінних: кількість переданих пакетів, значення порогів розгону кожного із з'єднань, значення вікон прийому і контролю перевантаження та ін.

Однак якщо траєкторія системи в фазовому просторі замкнута, то також замкнута буде її проекція в просторі з іншою кількістю системних змінних.

Побудуємо проекцію фазового простору на площину, де кожному з вимірів буде відповідати розмір вікна перевантаження одного з TCP-з'єднань (рис. 4.5).

При побудові зображення не враховувався період до 300-ої секунди (т. зв. перехідний процес). Розмірність зображеного на мал. 4.5 об'єкта подрібнена. Щоб визначити її значення скористаємося клітинним методом.

У клітинному методі область, яка містить фрактальний об'єкт, розбивається на клітини (коробки), в двовимірному випадку це - квадрати, зі стороною L.

Потім підраховується число клітин, необхідних для покриття всього фрактала. Такий підрахунок здійснюється для декількох розмірів боку клітини.

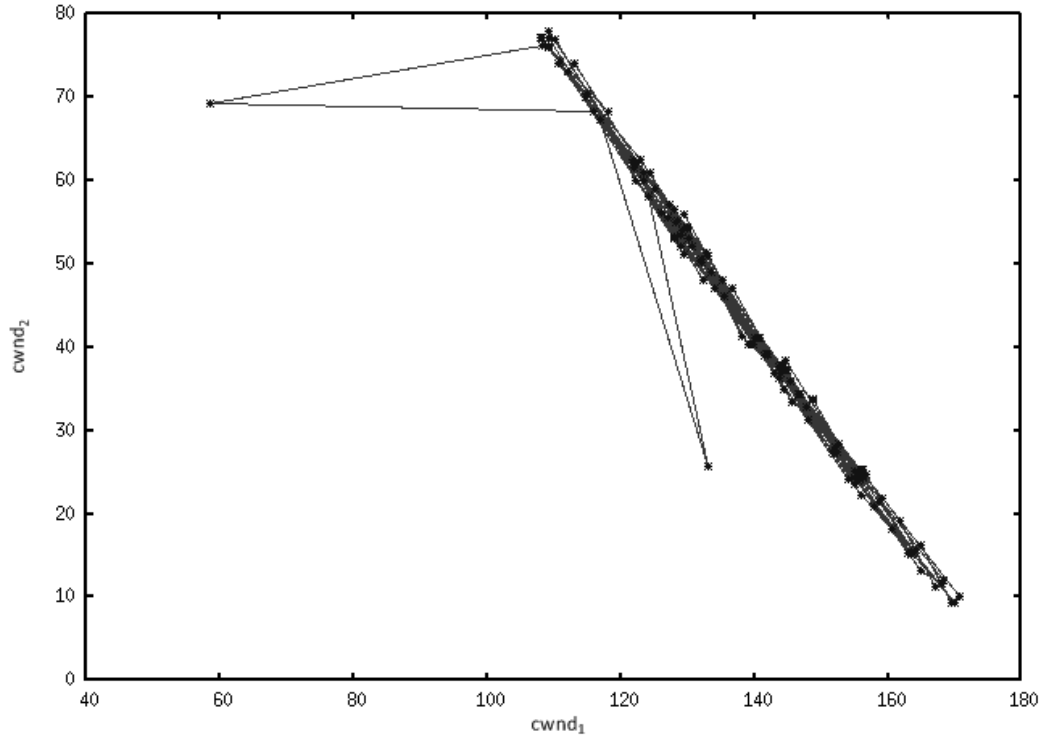


Рис. 4.5. Проекція фазового простору

Програма обчислення розмірності Мінковського для нашої системи видає такі результати (рис. 4.6):

0,01 N:135	0,58 N:104	7 N:24	26 N:8
0,04 N:135	0,61 N:107	8 N:19	27 N:7
0,07 N:133	0,64 N:104	9 N:17	28 N:7
0,1 N:128	0,67 N:104	10 N:16	29 N:6
0,13 N:121	0,7 N:102	11 N:15	30 N:6
0,16 N:124	0,73 N:107	12 N:14	31 N:6
0,19 N:119	0,76 N:99	13 N:12	32 N:7
0,22 N:122	0,79 N:99	14 N:13	33 N:6
0,25 N:120	0,82 N:92	15 N:12	34 N:6
0,28 N:115	0,85 N:102	16 N:10	35 N:7
0,31 N:112	0,88 N:97	17 N:10	36 N:6
0,34 N:116	0,91 N:101	18 N:11	37 N:6
0,37 N:116	0,94 N:95	19 N:10	38 N:6
0,4 N:117	0,97 N:94	20 N:8	39 N:5

Рис. 4.6. Фрагмент результатів програми обчислення розмірності Мінковського

Тут перше число - довжина сторони клітки L, друге – кількість клітин, що покривають фрактал - N. У висновку програми видно, що ні завжди клітини з

меншим розміром оптимальніше охоплюють об'єкт. Це обумовлюється тим, що в вживаному алгоритмі клітини слідують один за одним, не вирівнюючись щодо кордонів об'єкта. Цей момент був би суттєвий при одиничному вимірі розмірності.

Отриману ламану аппроксимуємо прямою (на рис. 4.7 вона позначена точками), яка задається рівнянням, де d - фрактальна розмірність, C - деяка константа.

Звідси розмірність можна обчислити як

Так як , то формулу для обчислення розмірності перепишемо як, і d тут - кут нахилу апроксимуючої прямої. Таким чином, отримуємо d = 0,8625.

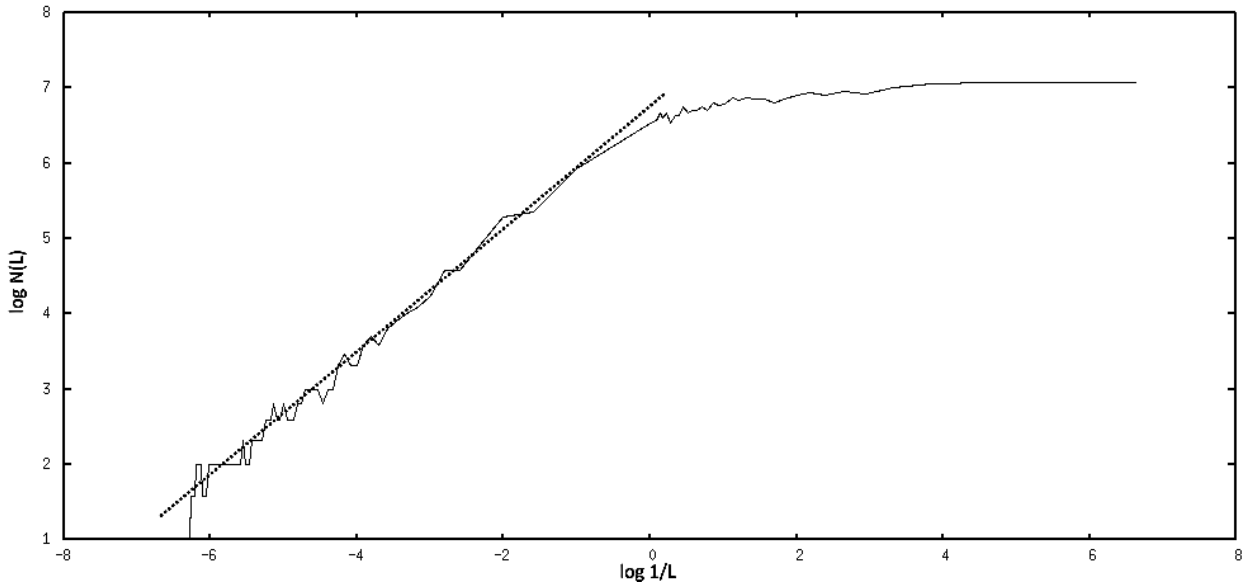


Рис. 4.7. Обчислення розмірності Мінковського

Чутливість до атакуючого впливу

Покажемо, що розглянута система має значну залежність від атакуючого впливу, яке в даному випадку є зміна початкових умов. Тобто навіть при незначній зміні вхідних параметрів вже через деякий час характеристики зміненої системи матимуть значну відмінність від вихідних, що і є одним з головних ознак хаотичної системи.

Експеримент полягав в тому, що програмним шляхом було внесено зміну до модель: на 300-ій с. вікно одного з TCP-з'єднань було збільшено на 1 пакет.

Динаміка зміни вікон перевантаження для даного випадку наведена на рис. 4.8. До 300-ою с. TCP-сесії поводяться однаково, значення вікон перевантаження збігаються, але після внесення змін картина змінюється. На рис. 4.9 представлена різниця значень вікон контролю перевантаження для кожної сесії.

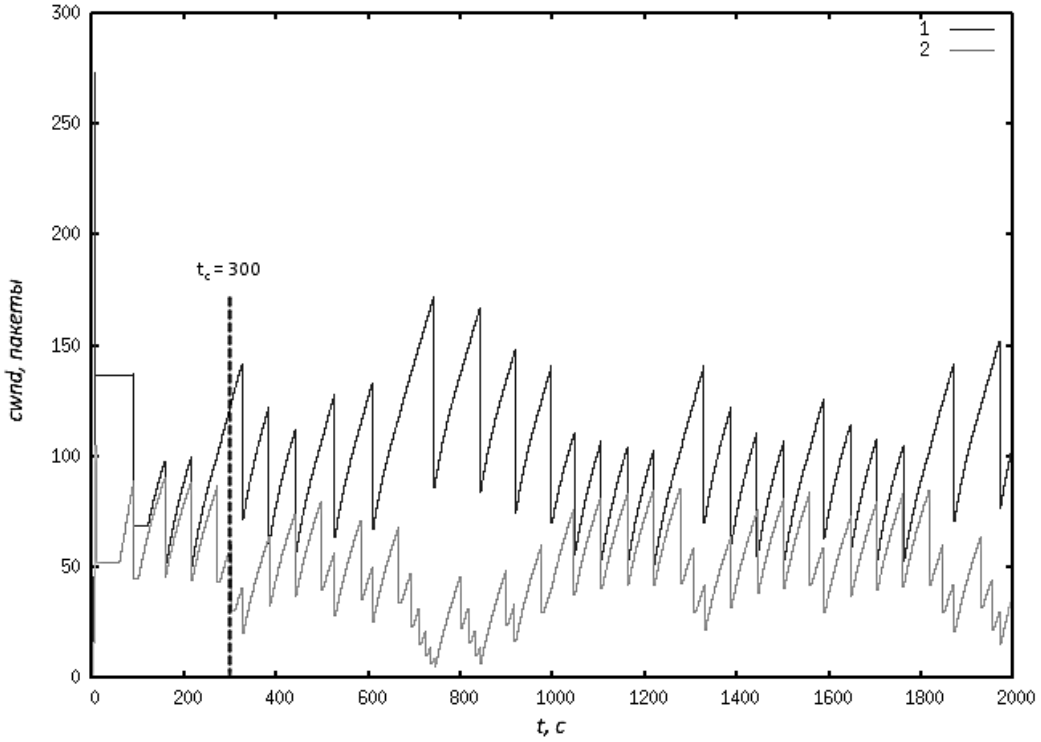


Рис. 4.8. Динаміка зміни вікон контролю перевантаження зі зміненими вхідними даними

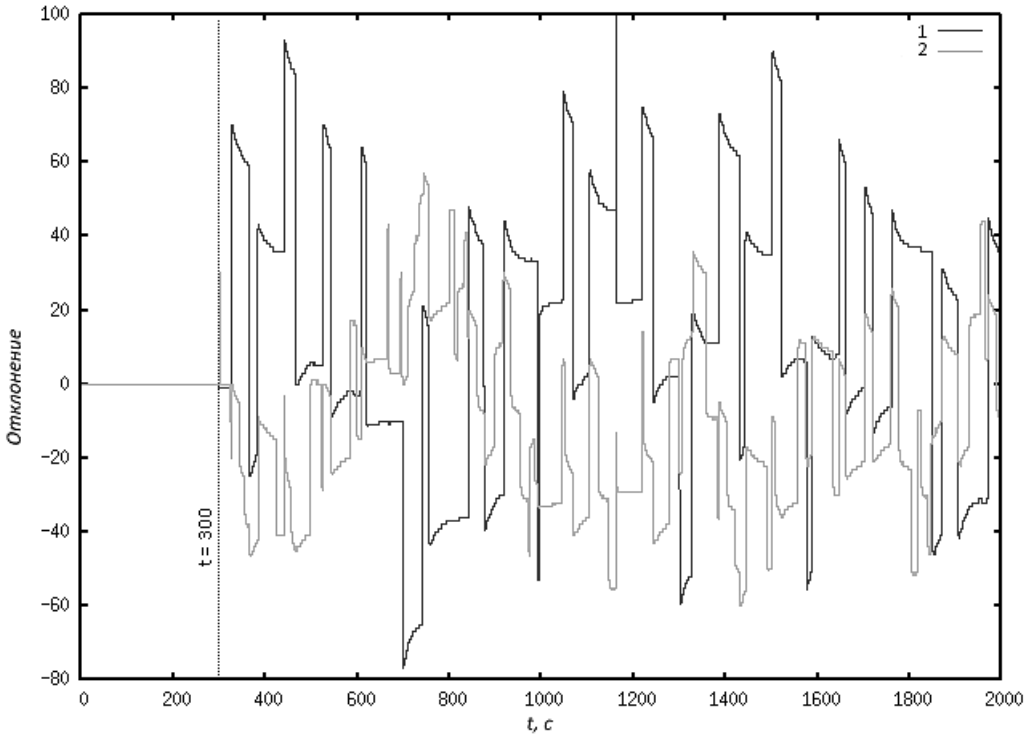


Рис. 4.9. Різниця значень вікон контролю перевантаження

Покажемо, що дана система функціонує в режимі детермінованого хаосу. Для цього необхідно обчислити показник Ляпунова – ступінь експоненціального роз бігання траєкторій системи. Показник Ляпунова є коефіцієнтом розтягування системи

,

де ξ – відстань між двома точками траєкторії в початковий момент часу t_0;

- час, за який системи розбігаються на відстань.

Евклідова відстань обчислюється за такою формулою

,

де – вікно перевантаження 1-го TCP-з'єднання в момент часу t в першому випадку;

- вікно перевантаження 2-го TCP-з'єднання в момент часу t в другій системі зі зміненими вхідними даними.

У нашому експерименті $\xi = 1$ і покладемо $\Delta t = 50$. Відстань між двома станами системи за час $\Delta t = 10$.

.

Показник Ляпунова

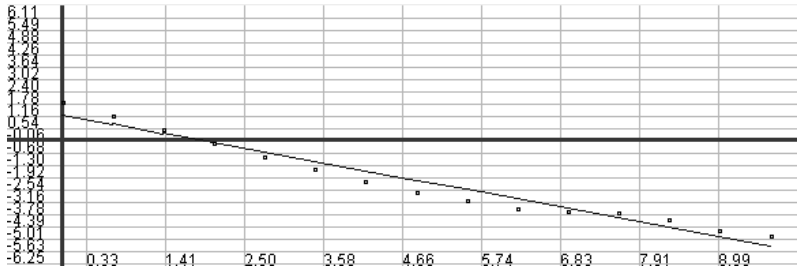
.

Таким чином, відмінність в двохсистемах наростає кожну секунду зі швидкістю .

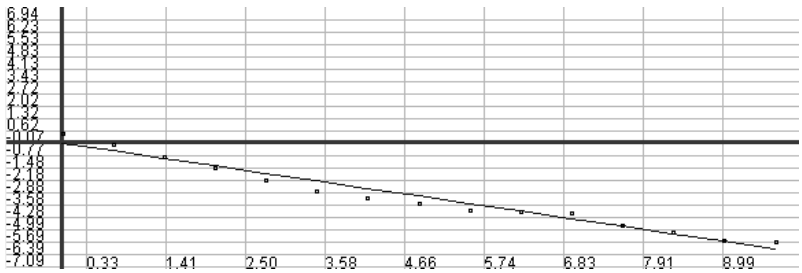
Той факт, що розмірність системи (d = 0,8625) є дробовим числом і показник Ляпунова позитивний, дозволяє говорити про те, що аттрактор даної системи є дивним.

Самоподібність системи

Обчислимо параметр Херста для нашої системи. Важливо отримати значення параметра для того, щоб визначити, чи є спостережуваний процес персистентний, тобто має пам'ять. Для обчислення параметра Херста були отримані значення пропускної здатності окремо для кожного TCP-з'єднання і агрегованого трафіку. Обчислення вироблялося в програмі SELFIS за двома методами: метод агрегированої дисперсії (AVM) і метод R / S-статистики (нормованого розмаху). Результати обчислень наведені на рис. 4.10 - 4.12.

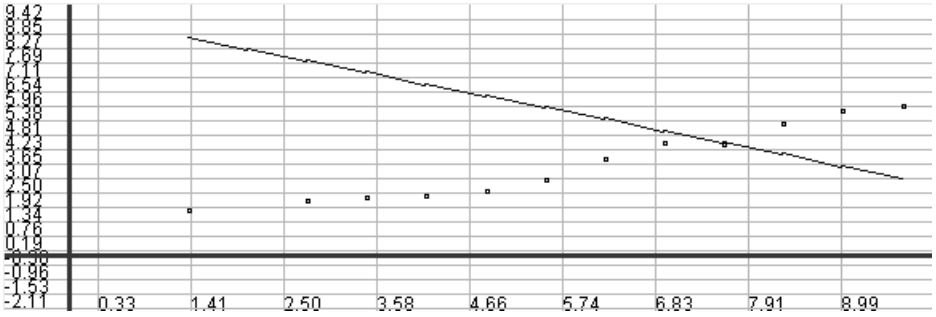


а (*AVM; H* = 0,66)

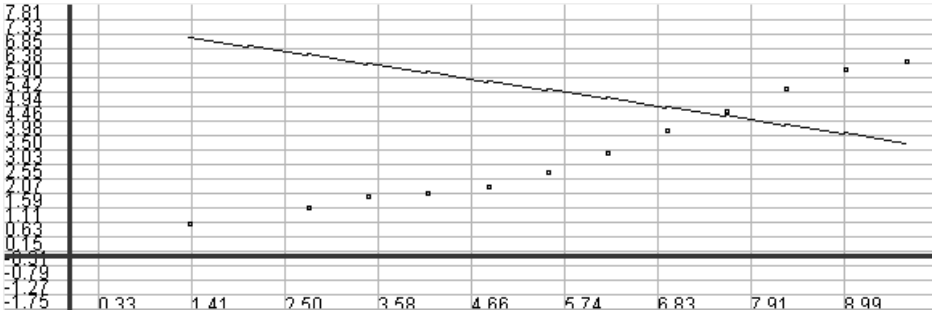


б (*R/S; H* = 0,673)

Рис. 4.10. Визначення параметра Херста для 1-го з'єднання

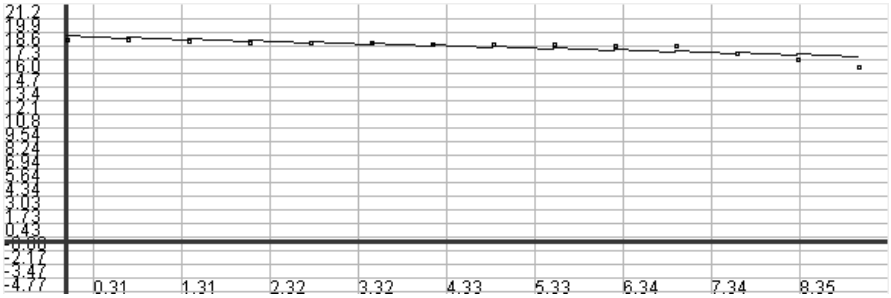


а (*AVM*; $H = 0{,}691$)



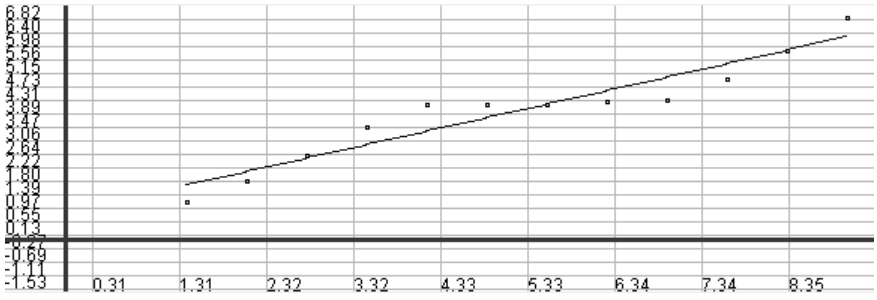
б (*R/S;* $H = 0{,}515$)

Рис. 4.11. Визначення параметра Херста для 2-го з'єднання



а (*AVM;* $H = 0{,}888$)

Рис. 4.12. Визначення параметра Херста для 3-го з'єднання (початок)



б (*R/S;* $H = 0{,}605$)

Рис. 4.12. Визначення параметра Херста для 3-го з'єднання (закінчення)

Як видно з малюнків вище для всіх розглянутих трафіків параметр Херста перевищує 0,5, що говорить про те, що система є персистентною і

самоподобною. Близькість параметра Херста до 1 для агрегованого трафіку вказує на те, що система має тривалу пам'ять (LRD).

Таким чином, у цьому розділі розроблена математична модель, на основі який був визначений параметр Херста для комп’ютерної системи під час розподіленої атаки. Високий показник цього параметра(більше 0.5) вказує на самоподібність системи, що характеризуэ системи під розподіленою атакою.

РОЗДІЛ 4.
ЕКОНОМІЧНА ЧАСТИНА

4.1. Маркетингові дослідження ринку збуту розробленого продукту

На основі аналізу системних характеристик і процесів інформаційно-телекомунікаційних систем, а також можливостей (активності) зловмисника в рамках дипломної роботи розроблена та проаналізована математична модель розподіленої DoS-атаки на комп'ютерну систему дозволяє виконувати аналітичне дослідження процесів розподіленого інформаційного впливу на інформаційно-телекомунікаційну систему і розраховувати можливе перевантаження такої системи на основі експериментально проведених дослідів на предмет поведінки комп'ютерної мережі в системи під час розподілених DoS-атак. Результати цих дослідів описують поведінку пакетів у протоколі TCPпід час розподілених DoS-атак, виявляють закономірності у навантажені комп'ютерної мережі.

Модель може сприяти розробці прикладних рішень щодо усунення досліджуваної розподіленої DoS-атаки на ранньому етапі. У ході маркетингового дослідження аналізувалися готові рішення на ринку безпеки інформаційно-телекомунікаційних систем, проте найпопулярніші представники мали певні недоліки.

Сервіс CloudFlare, один із лідерів в усунені розподілених DoS-атак на інформаційно-телекомунікаційні системи, в своїй основі представляє проміжний сервіс між користувачем та системою. При звертанні до системи відбувається перевірка на перевищення ліміту запитів за певний час від користувача. У разі наявності перевищення ліміту CloudFlare зберігає IP-адресу порушника в загальну базу CloudFlare на деякий період часу, тим саме інша клієнт-система може уникнути DoS-атаки цього правопорушника, так як він був знайдений раніше у ході DoS-атаки на іншу клієнт-систему. У такого рішення є ряд недоліків:

- Пряма залежність ефективності запобігання DoS-атакам від кількості клієнтів. Тобто при зменшенні кількості клієнтів сервісу CloudFlare падає ефективність так званого «обміну знаннями» на предмет IP-адресів правопорушників.
- Система передбачає наявність бази даних порушників, яка була створена і заповнена на основі проведених раніше DoS-атак. Таким чином, перші атаки від невідомих зловмисників будуть вдалими до перевищення ліміту запитів від користувачів і зберігання IP-адресу порушника в базу даних.
- Сервіс CloudFlare не має відношення до інфраструктури інформаційно-телекомунікаційної системи, що вона обслуговує, таким чином комунікація між сервісом та системою виконується через звичайні інтернет-мережі, що збільшує час відгуку системи на запит користувача.

Іншим рішенням на ринку сервісів усунення розподілених DoS-атак є сервіс OVH, який у технологічному плані уявляє з себе додатковий сервіс, який валідує запити від користувача на предмет розподілених DoS-атак. Сервіс є частиною інфраструктури інформаційно-телекомунікаційної системи, на які ідуть запити. Така реалізація сприяє більш швидкому відгуку системи на запити користувача, проте через це база даних правопорушників не ділиться поміж іншими клієнтами сервісу і є відносно невеликою. Недоліки невеликої бази даних сервіс компенсує тим, що не бере гроші за невдале усунення DoS-атак, після чого зберігає учасників DoS-атаки в базу даних порушників для подальшого успішного усунення таких атак.

Усі ці рішення мають загальні недоліки, які полягають у тому, що спочатку деяка частина DoS-атак повинна пройти успішно, після чого учасники таких DoS-атак зберігаються у базах даних для подальшої ідентифікації вже відомих порушників серед користувачів системи.

У свою чергу результати аналізу роботи математичної моделі можуть використовуватися для розробки прикладного рішення, яке буде усувати DoS-

атаки, аналізуючи запити до інформаційно-телекомунікаційних систем у режимі реального часу, зменшуючи ймовірність перевантаження систему при розподіленій DoS-атаці, що, в свою чергу, зменшує ризик матеріальних і репутаційних збитків для підприємств, що володіють цими системами. Головною перевагою такого рішення буде автономність і незалежність від кількості відомих учасників DoS-атак, адже аналіз комп'ютерної мережі виконується на основі поведінки трафіку TCP-пакетів, а не від кількості запитів від користувача за певний час.

4.2. Оцінка економічної ефективності впровадження продукту

Не є можливим розрахувати економічну ефективність впровадження програмного забезпечення, бо в ході виконання дипломної роботи програмне забезпечення не розроблювалось. Але є можливість виокремити соціальну ефективність представленого продукту. Впровадження продукту може дозволити отримати такий соціальний ефект:

- посприяти розробці прикладних нових рішень щодо усунення DoS-атак;
- зменшити матеріальні та репутаційні збитки на підприємствах, які мають сервера для роботи з клієнтами;
- посприяти розробці прикладних рішень щодо усунення DDoS-атак;
- збільшення аптайму сервера.

Висновки

Підбиваючи підсумки, у цій роботі розроблена математична модель, яка дозволить по результатам дослідження розробити більш інтелектуальну систему виявлення розподілених DoS-атак, що є важливою складовою у нинішній час розвитку підприємств, бізнес яких покладається на безперебійну роботу своїх інформаційно-телекомунікаційних систем.

ВИСНОВКИ

Забезпечення відмовостійкості ІТКС є гострою проблемою в даний момент. Представники недобросовісної конкуренції у сфері інформаційних технологій часто намагаються отримати конкурентну перевагу за рахунок використання розподілених DoS-атак.

У даній дипломній роботі була розроблена математична модель, на основі якої булиз роблені аналізи і висновки, що дозволяють визначати розподілені DoS-атаки на ранньому етапі.

Практична значимість даної роботи полягає у можливості розробки прикладного рішення на основі досліджень математичної моделі, що дозволить з'явитися більш продвинутим рішенням у сфері інформаційної безпеки.

Дослідження проводилося за допомогоюмо програмування Python і стандартних бібліотек цієї мови.

В економічному розділі дипломної роботи описані маркетингові дослідження і економічний ефект даної роботи.

Наукова новизна даної дипломної роботи полягає у відкриті нового способу виявлення розподілених атак шляхом визначення само подібності трафіку в комп’ютерній системі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Разработка секторальных рамок квалификаций: методология и практика [Текст] : монография / Под. общ. ред. Е.А. Митрофановой, В.Я. Афанасьева, С.В. Чернышенко; Государственный университет управления. – М. : Издательский дом ГУУ, 2015. – 234 с.
2. Кэти Сьерра, Берт Бейтс. Изучаем Java, 2-е изд. – М. : Эксмо, 2012 – 718 с.
3. Герберт Шилдт. Java. Полное руководство, 8-е изд. – М. : И.Д. Вильямс, 2012 – 1104 с.
4. PostgreSQL: Documentation (Электрон. ресурс) / Спосіб доступу: URL: https://www.postgresql.org/docs/
5. Java – Википедия (Электрон. ресурс) / Спосіб доступу: URL: https://ru.wikipedia.org/wiki/Java
6. JSP – Википедия (Электрон. ресурс) / Спосіб доступу: URL: https://ru.wikipedia.org/wiki/JSP
7. PostgreSQL – Википедия (Электрон. ресурс) / Спосіб доступу: URL: https://ru.wikipedia.org/wiki/PostgreSQL
8. Принципы построения секторальной рамки ИТ-квалификации – 93evn513.pdf (Электрон. ресурс) / Спосіб доступу: URL: http://naukovedenie.ru/PDF/93evn513.pdf
9. Golovach Courses – YouTube (Электрон. ресурс) / Спосіб доступу: URL: https://www.youtube.com/channel/UCuIctN7x71qam9K_ZxS1W2A
10. Онлайн уроки по Java – YouTube (Электрон. ресурс) / Спосіб доступу: URL: https://www.youtube.com/channel/UCdXqgQdGW5go6nkkBbUVSMA
11. Yakov Fain – YouTube (Электрон. ресурс) / Спосіб доступу: URL: https://www.youtube.com/user/yfain/videos

12. Spring Framework – Википедия (Электрон. ресурс) / Спосіб доступу: URL: https://ru.wikipedia.org/wiki/Spring_Framework

13. Объектно-ориентированное проектирование (Электрон. ресурс) / Спосіб доступу: URL: http://www.poisk-ru.ru/s7237t2.html

14. К. Уоллс. Spring в действии. – М. : ДМК Пресс, 2013. – 752 с.

15. Система управления базами данных – Википедия (Электрон. ресурс) / Спосіб доступу: URL: https://ru.wikipedia.org/wiki/Система_управления_базами_данных

16. Цикл и этапы разработки программного обеспечения – EDISON (Электрон. ресурс) / Спосіб доступу: URL: https://www.edsd.ru/ru/princypy/cikl_razrabotki_po

17. git за 100 минут – YouTube (Электрон. ресурс) / Спосіб доступу: URL: https://www.youtube.com/playlist?list=PLFEoX6sZK2G2BXRQYJ0VWq75sNxa-QRFe

18. Кларенс Хо, Роб Харроп. Spring 3 для профессионалов. – М. : Вильямс, 2013. – 880 с.

19. Maven Repository: Search/Browse/Explore (Электрон. ресурс) / Спосіб доступу: URL: http://mvnrepository.com/

20. Home: Java Platform, Enterprise Edition (Java EE) 7 Release 7 (Электрон. ресурс) / Спосіб доступу: URL: http://docs.oracle.com/javaee/7/index.html

21. The Java™ Tutorials (Электрон. ресурс) / Спосіб доступу: URL: https://docs.oracle.com/javase/tutorial/

22. Модели обеспечения достоверности и доступности информации в информационно-телекоммуникационных системах : монография / М. Ю. Монахов [и др.] ; Владим. гос. ун-т им. А. Г. и Н. Г. Сто-летовых. – Владимир : Изд-во ВлГУ, 2015. – 208 с.

23. Veres B.M., Kenesi Z., Molnar S., Vattay G. On the propagation of long-range dependence in the Internet // ACM SIGCOMM 2000, Stockholm, Sweden, 2000.

24. Что такое DDoS? (Электрон. ресурс) / Спосіб доступу: URL: http://ddos-protection.ru/chto-takoe-ddos

25. Методичні вказівки з виконання економічного розділу в дипломних проектах студентів спеціальності "Комп'ютерні системи " / Уклад. О.Г. Вагонова, Нікітіна О.Б. Н.Н. Романюк – Дніпропетровськ: Національний гірничий університет. – 2013. – 11 с.

26. Методичні рекомендації до виконання кваліфікаційних робіт магістрів галузі знань 12 «Інформаційні технології» спеціальності 122 «Комп'ютерні науки» / Л.М. Коротенко , О.С. Шевцова; Нац. гірн. ун-т. – Д : ДВНЗ НГУ, 2017. – 20 с.

27. Закон України «Про освіту» № 2145-19 (Электрон. ресурс) / Спосіб доступу: URL: http://zakon3.rada.gov.ua/laws/show/2145-19

28. Закон України «Про вищу освіту» № 1556-18 (Электрон. ресурс) / Спосіб доступу: URL: http://zakon5.rada.gov.ua/laws/show/en/1556-18

29. DDoS: ИТ-маньяки на острие атаки / Блог компании RUVDS.com / Хабрахабр (Электрон. ресурс) / Спосіб доступу: URL: https://habrahabr.ru/company/ruvds/blog/308764/

30. DDoS-атаки: нападение и защита / Блог компании RUVDS.com / Хабрахабр (Электрон. ресурс) / Спосіб доступу: URL: https://habrahabr.ru/company/ruvds/blog/321992/

31. Немного о типах DDoS-атак и методах защиты / Блог компании VAS Experts / Хабрахабр (Электрон. ресурс) / Спосіб доступу: URL: https://habrahabr.ru/company/vasexperts/blog/313562/

32. Особенности DDoS атак в беспроводных сетях (Электрон. ресурс) / Спосіб доступу: URL: https://cyberleninka.ru/article/n/osobennosti-ddos-atak-v-besprovodnyh-setyah

33. Методика и средства раннего выявления и противодействия угрозам нарушения информационной безопасности в результате ddos атак (Электрон. ресурс) / Спосіб доступу: URL: https://cyberleninka.ru/article/n/metodika-i-sredstva-rannego-vyyavleniya-i-protivodeystviya-ugrozam-narusheniya-informatsionnoy-bezopasnosti-v-rezultate-ddos-atak

34. Описание DDoS-атаки с помощью катастрофы «сборка» (Электрон. ресурс) / Спосіб доступу: URL: https://cyberleninka.ru/article/n/opisanie-ddos-ataki-s-pomoschyu-katastrofy-sborka

35. Задачи проектирования защиты web-сервера от атак типа ddos с применением аппарата нечеткой логики (Электрон. ресурс) / Спосіб доступу: URL: https://cyberleninka.ru/article/n/zadachi-proektirovaniya-zaschity-web-servera-ot-atak-tipa-ddos-s-primeneniem-apparata-nechetkoy-logiki

36. Проблемы и реализация комплекса мер безопасности компьютерных сетей (Электрон. ресурс) / Спосіб доступу: URL: https://cyberleninka.ru/article/n/problemy-i-realizatsiya-kompleksa-mer-bezopasnosti-kompyuternyh-setey

37. Разработка архитектуры системы обнаружения распределенных сетевых атак типа «Отказ в обслуживании» (Электрон. ресурс) / Спосіб доступу: URL: https://cyberleninka.ru/article/n/razrabotka-arhitektury-sistemy-obnaruzheniya-raspredelennyh-setevyh-atak-tipa-otkaz-v-obsluzhivanii

38. Современные методы распространения вирусов (Электрон. ресурс) / Спосіб доступу: URL: https://cyberleninka.ru/article/n/sovremennye-metody-rasprostraneniya-virusov

39. Современные проблемы безопасности корпоративных сетей (Электрон. ресурс) / Спосіб доступу: URL: https://cyberleninka.ru/article/n/sovremennye-problemy-bezopasnosti-korporativnyh-setey

40. Метод построения моделей информационных атак (Электрон. ресурс) / Спосіб доступу: URL: https://cyberleninka.ru/article/n/metod-postroeniya-modeley-informatsionnyh-atak

41. Киберпреступность как новая криминальная угроза (Электрон. ресурс) / Спосіб доступу: URL: https://cyberleninka.ru/article/n/kiberprestupnost-kak-novaya-kriminalnaya-ugroza

42. Киберпреступность как форма выражения криминального профессионализма (Электрон. ресурс) / Спосіб доступу: URL: https://cyberleninka.ru/article/n/kiberprestupnost-kak-forma-vyrazheniya-kriminalnogo-professionalizma

43. Анализ свойств самоподобия трафика веб-ресурса (Электрон. ресурс) / Спосіб доступу: URL: http://morozov.krc.karelia.ru/articles/kp/

44. Проблемы распределенных систем (Электрон. ресурс) / Спосіб доступу: URL: https://cyberleninka.ru/article/n/problemy-raspredelennyh-sistem

45. Veres B.M. The chaotic nature of TCP congestion control // IEEE INFOCOM'2000. 2000. (Электрон. ресурс) / Спосіб доступу: URL: http://www2.ensc.sfu.ca/~ljilja/ENSC835/Fall03/Assignments/papers/74.pdf

46. Ильницкий С.В. Работа сетевого сервера при самоподобной (self-similar) нагрузке. 2004. (Электрон. ресурс) / Спосіб доступу: URL: http://314159.ru/ilnickis/ilnickis1.pdf

47. Вредоносные программы в компьютерных сетях / Монахов Ю.М., Груздева Л.М., Монахов М.Ю. Владимир: Изд-во Владим. гос. ун-та. – 2010. – 96 с.

48. Модель распределенных атак в программно-конфигурируемых сетях связи (Электрон. ресурс) / Спосіб доступу: URL: https://cyberleninka.ru/article/n/model-raspredelennyh-atak-v-programmno-konfiguriruemyh-setyah-svyazi

49. Методология обнаружения вторжений (Электрон. ресурс) / Способ доступа: URL: https://cyberleninka.ru/article/n/metodologiya-obnaruzheniya-vtorzheniy

50. Обеспечение информационной безопасности компьютерных сетей на основе анализа сетевого трафика (Электрон. ресурс) / Спосіб доступу: URL: https://cyberleninka.ru/article/n/obespechenie-informatsionnoy-bezopasnosti-kompyuternyh-setey-na-osnove-analiza-setevogo-trafika

ДОДАТОК А

Текст програми

```
import app_manager
import ofp_event
import MAIN_DISPATCHER
import set_ev_cls
import ofproto_v1_0


class Cbench(app_manager.RyuApp):
    OFP_VERSIONS = [ofproto_v1_0.OFP_VERSION]

    def __init__(self, *args, **kwargs):
        super(Cbench, self).__init__(*args, **kwargs)

    @set_ev_cls(ofp_event.EventOFPPacketIn, MAIN_DISPATCHER)
    def packet_in_handler(self, ev):
        msg = ev.msg
        datapath = msg.datapath
        ofproto = datapath.ofproto

        match = datapath.ofproto_parser.OFPMatch(
            ofproto_v1_0.OFPFW_ALL, 0, 0, 0,
            0, 0, 0, 0, 0, 0, 0, 0, 0)

        mod = datapath.ofproto_parser.OFPFlowMod(
            datapath, match=match, cookie=0, command=ofproto.OFPFC_ADD,
            idle_timeout=0, hard_timeout=0,
            priority=ofproto.OFP_DEFAULT_PRIORITY,
            flags=0, actions=None)
        datapath.send_msg(mod)


import json

import ControllerBase
import Response
import route
import WSGIApplication
 app_manager
dpid as dpid_lib
import get_switch, get_link, get_host


class TopologyAPI(app_manager.RyuApp):
    _CONTEXTS = {
        'wsgi': WSGIApplication
    }

    def __init__(self, *args, **kwargs):
        super(TopologyAPI, self).__init__(*args, **kwargs)

        wsgi = kwargs['wsgi']
        wsgi.register(TopologyController, {'topology_api_app': self})
```

```
class TopologyController(ControllerBase):
    def __init__(self, req, link, data, **config):
        super(TopologyController, self).__init__(req, link, data, **config)
        self.topology_api_app = data['topology_api_app']

    @route('topology', '/v1.0/topology/switches',
           methods=['GET'])
    def list_switches(self, req, **kwargs):
        return self._switches(req, **kwargs)

    @route('topology', '/v1.0/topology/switches/{dpid}',
           methods=['GET'], requirements={'dpid': dpid_lib.DPID_PATTERN})
    def get_switch(self, req, **kwargs):
        return self._switches(req, **kwargs)

    @route('topology', '/v1.0/topology/links',
           methods=['GET'])
    def list_links(self, req, **kwargs):
        return self._links(req, **kwargs)

    @route('topology', '/v1.0/topology/links/{dpid}',
           methods=['GET'], requirements={'dpid': dpid_lib.DPID_PATTERN})
    def get_links(self, req, **kwargs):
        return self._links(req, **kwargs)

    @route('topology', '/v1.0/topology/hosts',
           methods=['GET'])
    def list_hosts(self, req, **kwargs):
        return self._hosts(req, **kwargs)

    @route('topology', '/v1.0/topology/hosts/{dpid}',
           methods=['GET'], requirements={'dpid': dpid_lib.DPID_PATTERN})
    def get_hosts(self, req, **kwargs):
        return self._hosts(req, **kwargs)

    def _switches(self, req, **kwargs):
        dpid = None
        if 'dpid' in kwargs:
            dpid = dpid_lib.str_to_dpid(kwargs['dpid'])
        switches = get_switch(self.topology_api_app, dpid)
        body = json.dumps([switch.to_dict() for switch in switches])
        return Response(content_type='application/json', body=body)

    def _links(self, req, **kwargs):
        dpid = None
        if 'dpid' in kwargs:
            dpid = dpid_lib.str_to_dpid(kwargs['dpid'])
        links = get_link(self.topology_api_app, dpid)
        body = json.dumps([link.to_dict() for link in links])
        return Response(content_type='application/json', body=body)

    def _hosts(self, req, **kwargs):
        dpid = None
        if 'dpid' in kwargs:
            dpid = dpid_lib.str_to_dpid(kwargs['dpid'])
        hosts = get_host(self.topology_api_app, dpid)
        body = json.dumps([host.to_dict() for host in hosts])
        return Response(content_type='application/json', body=body)


class SimpleSwitchSnort(app_manager.RyuApp):
    OFP_VERSIONS = [ofproto_v1_3.OFP_VERSION]
    _CONTEXTS = {'snortlib': snortlib.SnortLib}
```

```
def __init__(self, *args, **kwargs):
    super(SimpleSwitchSnort, self).__init__(*args, **kwargs)
    self.snort = kwargs['snortlib']
    self.snort_port = 3
    self.mac_to_port = {}

    socket_config = {'unixsock': True}

    self.snort.set_config(socket_config)
    self.snort.start_socket_server()

def packet_print(self, pkt):
    pkt = packet.Packet(array.array('B', pkt))

    eth = pkt.get_protocol(ethernet.ethernet)
    _ipv4 = pkt.get_protocol(ipv4.ipv4)
    _icmp = pkt.get_protocol(icmp.icmp)

    if _icmp:
        self.logger.info("%r", _icmp)

    if _ipv4:
        self.logger.info("%r", _ipv4)

    if eth:
        self.logger.info("%r", eth)

@set_ev_cls(snortlib.EventAlert, MAIN_DISPATCHER)
def _dump_alert(self, ev):
    msg = ev.msg

    print('alertmsg: %s' % ''.join(msg.alertmsg))

    self.packet_print(msg.pkt)

@set_ev_cls(ofp_event.EventOFPSwitchFeatures, CONFIG_DISPATCHER)
def switch_features_handler(self, ev):
    datapath = ev.msg.datapath
    ofproto = datapath.ofproto
    parser = datapath.ofproto_parser

    match = parser.OFPMatch()
    actions = [parser.OFPActionOutput(ofproto.OFPP_CONTROLLER,
                                      ofproto.OFPCML_NO_BUFFER)]
    self.add_flow(datapath, 0, match, actions)

def add_flow(self, datapath, priority, match, actions):
    ofproto = datapath.ofproto
    parser = datapath.ofproto_parser

    inst = [parser.OFPInstructionActions(ofproto.OFPIT_APPLY_ACTIONS,
                                         actions)]

    mod = parser.OFPFlowMod(datapath=datapath, priority=priority,
                            match=match, instructions=inst)
    datapath.send_msg(mod)

@set_ev_cls(ofp_event.EventOFPPacketIn, MAIN_DISPATCHER)
def _packet_in_handler(self, ev):
    msg = ev.msg
    datapath = msg.datapath
    ofproto = datapath.ofproto
    parser = datapath.ofproto_parser
```

```
in_port = msg.match['in_port']

pkt = packet.Packet(msg.data)
eth = pkt.get_protocols(ethernet.ethernet)[0]

dst = eth.dst
src = eth.src

dpid = datapath.id
self.mac_to_port.setdefault(dpid, {})

self.mac_to_port[dpid][src] = in_port

if dst in self.mac_to_port[dpid]:
    out_port = self.mac_to_port[dpid][dst]
else:
    out_port = ofproto.OFPP_FLOOD

actions = [parser.OFPActionOutput(out_port),
           parser.OFPActionOutput(self.snort_port)]

if out_port != ofproto.OFPP_FLOOD:
    match = parser.OFPMatch(in_port=in_port, eth_dst=dst)
    self.add_flow(datapath, 1, match, actions)

data = None
if msg.buffer_id == ofproto.OFP_NO_BUFFER:
    data = msg.data

out = parser.OFPPacketOut(datapath=datapath, buffer_id=msg.buffer_id,
                          in_port=in_port, actions=actions, data=data)
datapath.send_msg(out)
```

ДОДАТОК Б

ВІДГУК

на дипломну роботу магістра на тему:
«Моделі та алгоритмивиявлення та попередження розподілених атак на прикладі порталу «Затребувана освіта»

студента групи 122М-16-1 Булгакова Максима Олександровича

1. Мета дипломної роботи магістра полягає у побудові способу виявлення розподілених DoS-атак на основі побудованої математичної моделі комп’ютерної системи.
2. Актуальність цієї роботи обґрунтована важливістю захисту комп'ьютерних систем у наш час та значними недоліками у сучасних прикладних рішенях на цю тему.
3. Тема дипломної роботи безпосередньо пов'язана з об'єктом діяльності магістра спеціальності 122 «Комп'ютерні науки» – створення, дослідження і реалізація математичних моделей.
4. Наукова новизна полягає у побудові математичної моделі і виявлені розподілених атак через самоподібність системи.
5. Практична цінність дослідження полягає у можливості розробити прикладне рішеня по виявленню і усуненню розподілених атак використовуючи засоби більш високого рівня.
6. Оформлення дипломної роботи магістра виконано на сучасному рівні і відповідає вимогам, що пред'являються до робіт даної кваліфікації. Ступінь самостійності виконання досить висока.
7. Дипломна робота магістра в цілому заслуговує оцінки «відмінно», а студент Булгаков М.О. – присвоєння кваліфікації «інженер з комп’ютерних систем».

Керівник дипломної роботи
магістра, д.т.н.,
проф. кафедри ПЗКС В.І. Корнієнко

ДОДАТОК В

РЕЦЕНЗІЯ

на дипломну роботу магістра на тему:
«Моделі та алгоритмивиявлення та попередження розподілених атак на прикладі порталу «Затребувана освіта»

студента групи 122М-16-1 Булгакова Максима Олександровича

Під розподіленими атаками розуміються так звані Denial-of-service атаки, які полягають у нападі на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена.

У цій роботі було зроблене та досліджене моделюваня розподіленої атаки на прикладі порталу «Затребувана освіта». Результатом моделювання є аналіз поведінки комп’ютерної системи під час розподіленої атаки. Автор проводе аналіз поведінки комп’ютерної системи і доводить, що система перебуває у стані самоподібності під час розподілених атак. Це є досить надійною підставою для виявлення та попередження о розподілених атаках.

Тема дипломної роботи безпосередньо пов'язана з об'єктом діяльності магістра спеціальності 122 «Комп'ютерні науки» – створення, дослідження і реалізація математичних моделей.

Наукова новизна полягає у побудові математичної моделі і виявлені розподілених атак через самоподібність системи.

Беручи до уваги вище викладене, можна зробити висновок, що дана робота цілком відповідає вимогам, що пред'являються до кваліфікаційних робіт рівня магістра.

З огляду на наукову новизну і ступінь опрацювання компонентів даної роботи, в цілому автор заслуговує оцінки «відмінно».

Рецензент,