

УДК 004.5

МПК 6 G11

№ держреєстрації 0113U001104.

Інв. №

Національна академія наук України
Інститут проблем реєстрації інформації
(ІПРІ НАН України)

03113, м. Київ, вул. М. Шпака, 2; тел. (044) 456 83 89;
E-mail: vvp@ipri.kiev.ua

ЗАТВЕРДЖУЮ
Директор ІПРІ НАН України
академік НАН України
_____ В.В. Петров
2015.12.31

ЗВІТ
ПРО НАУКОВО-ДОСЛІДНУ РОБОТУ
«Розробити та дослідити методи забезпечення живучості комп'ютерних
інформаційних мереж для високотехнологічних об'єктів»
(Шифр «КІМ –2013»)
(заключний)

Науковий керівник НДР
завідуючий відділом
д-р техн. наук, професор

_____ О.Г.Додонов
2015.12.31

2015.12.31

Рукопис закінчено 14 грудня 2015 року. Результати роботи розглянуті та схвалені Вченою Радою ІПРІ НАН України, протокол № 18 від 15.12.2015.

Всі примірники звіту ідентичні за змістом

РЕФЕРАТ

Звіт про НДР (заклуч.): 442с., 42 рис., 8 табл., 202 джерел, 4 додатка.

Тема: «Розробити та дослідити методи забезпечення живучості комп'ютерних інформаційних мереж для високотехнологічних об'єктів» (Шифр «КІМ –2013»).

Державний реєстраційний номер теми: 0113U001104.

Об'єкт дослідження: методи забезпечення живучості комп'ютерних інформаційних мереж.

Мета роботи: розробка та дослідження методів забезпечення живучості, моделювання деструктивних впливів, відновлення інформаційних структур та збереження інформаційного ресурсу, організацію процесів протидії спрямованим деструктивним впливам.

Методи дослідження: методи математичного та імітаційного моделювання, теорії ймовірностей, теорії графів і складних мереж.

Основні результати:

1. Досліджені особливості структурної організації комп'ютерних інформаційних мереж (КІМ) високотехнологічних об'єктів, визначені параметри, що впливають на їх функціонування і можуть бути використані для розробки математичних моделей оцінки властивостей КІМ, методів та відповідних методик реконструкції або відновлення втрачених інформаційних структур та ресурсів. Запропоновано класифікацію можливих деструктивних впливів та показників якості функціонування КІМ. Досліджено моделі деструктивних впливів, відновлення інформаційних структур, збереження інформаційного ресурсу та організацію процесів протидії спрямованим деструктивним впливам.

2. Досліджено сценарний підхід до забезпечення протидії деструктивним впливам на КІМ, в рамках якого враховано властивості і показники живучості КІМ, запропоновано механізми протидії деструктивним впливам, забезпечення живучості, інформаційної безпеки КІМ. Запропоновано підхід до розгляду КІМ як «інформаційної резервації», згідно з яким у якості критеріїв «інформаційної резервації» можуть розглядатися параметри динаміки інформаційних потоків у межах КІМ, та побудовано комп'ютерну імітаційну модель динаміки інформаційних потоків у межах «інформаційної резервації».

3. Розроблено метод та відповідна методика реконструкції інформаційних структур у КІМ ВТО, що зазнали часткового руйнування, або відновлення втрачених інформаційних структур та ресурсів; методи підвищення живучості компонент КІМ спеціального призначення; Розроблено та розглянуто критерії і моделі оцінки рівней живучості КІМ; методи та методики підвищення структурної живучості КІМ; методика оцінки живучості мережі з точки зору її структурної вразливості та функціональності. Розглянуто також математичний апарат для моделювання поширення зовнішніх впливів по структурі мережі.

Результати, отримані при виконанні НДР, мають скласти теоретичну базу для створення комп'ютерних мереж з заданим рівнем живучості, дозволять зменшити рівень вразливості КІМ ВТО, забезпечити виконання критичних інформаційних процесів при наявності деструктивних впливів у КІМ та зовнішньому середовищі.

БЕЗПЕКА, ДЕСТРУКТИВНІ ВПЛИВИ, ЖИВУЧІСТЬ, ІНФОРМАЦІЙНА СТРУКТУРА, ІНФОРМАЦІЯ, МЕРЕЖА, МОДЕЛЬ, МЕТОД, ОЦІНКА, ПАРАМЕТР.

Умови отримання звіту: за договором.

93113, м. Київ, вул. М. Шпака, 2, ІПРІ НАН України.

ЗМІСТ

ЗАТВЕРДЖУЮ.....	1
ПЕРЕЛІК СКОРОЧЕНЬ.....	7
ВСТУП.....	8
1. ДОСЛІДЖЕННЯ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ МЕРЕЖ ВИСОКОТЕХНОЛОГІЧНИХ ОБ'ЄКТІВ.....	11
1.1. Поняття складних комп'ютерних мереж.....	11
1.2. Основні визначення і властивості КІМ ВТО.....	15
1.2.1 Призначення та характеристики комп'ютерних мереж.....	17
1.2.2 Властивості корпоративних комп'ютерних інформаційних мереж.....	17
1.2.3. Основні властивості та характеристики сучасних КІМ.....	22
1.2.4 Властивості комп'ютерних інформаційних систем (мереж).....	44
1.2.5 Основні функції, реалізовані комп'ютерними мережами ВТО.....	49
1.2.6 Класифікації комп'ютерних мереж.....	50
1.3. Моделі побудови КІМ ВТО.....	52
1.3.1 Моделювання і аналіз комп'ютерних мереж.....	52
1.3.2. Дослідження моделей КІМ з ненадійними системами.....	60
1.3.3. Формалізований апарат структурно графових об'єктів як засоб побудови моделей для дослідження живучості комп'ютерних мереж.....	65
2. ЖИВУЧІСТЬ КІМ ВТО.....	80
2.1. Основні визначення.....	80
2. Віді живучості. Аналіз і оцінка живучості.....	80
2.2.1. Функціональна живучість.....	81
2.2.2. Структурна живучість.....	86
2.2.3. Інформаційна живучість КІМ.....	88
2.2.4 Живучість корпоративних інформаційно-аналітичних систем.....	89
2.2.5. Задача забезпечення живучості корпоративної КІМ при частковому руйнуванні каналів зв'язку.....	104
2.2.6. Методологічні аспекти вибору компонентів корпоративної КІМ с урахуванням критерію живучості.....	116
2.3 Критерії оцінки рівней живучості КІМ ВТО.....	126
2.4 Критерії і моделі оцінки живучості комп'ютерної системи.....	137
2.4.1 Моделі для дослідження живучості КС.....	141
2.4.2. Побудова моделей аналізу живучості розподілених мережевих структур.....	143
3. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ СТВОРЕННЯ КІМ ВТО.....	148
3.1 Методи підвищення структурної живучості КІМ.....	148
3.1.1. Метод підвищення структурної живучості КІМ шляхом реконфігурації мережі.....	148
3.1.2. Метод оцінки та підвищення структурної живучості КІМ.....	155
3.1.3. Загальна методологія багатокритеріальної оптимізації при проектуванні мережі в умовах суперечливих вимог.....	161
3.2. Методика оцінки живучості КІМ спеціального призначення.....	165
3.3. Зворотна задача структурної живучості систем.....	182
3.4 Сценарний підхід до забезпечення заданого рівня живучості КІМ...188	188
3.5. Підхід до оцінки рівня живучості складних систем в умовах зовнішніх деструктивних впливів.....	204
4. ЖИВУЧІСТЬ ІНФОРМАЦІЇ В ІНТЕРНЕТІ.....	211
4.1. Механізми забезпечення живучості інформаційних об'єктів.....	211
4.2. Формальні моделі живучості інформаційних об'єктів.....	213
4.3. Цифрові сліди і тіні.....	216
4.4. Теоретико-ігровий підхід.....	219
5. ОЦІНКА ЖИВУЧОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ.....	228
5.1. Логіко-імовірнісні моделі оцінки живучості інформаційних систем	228
5.2. Оцінка живучості інформаційної системи за її станом.....	233
5.3. Оцінка живучості за результатами виконання завдання.....	238

5.4. Оцінка живучості за метою функціонування.....	239
6. БЕЗПЕКА КІМ ВТО.....	249
6.1. Математичні моделі безпеки.....	249
6.1.1. Моделі на основі дискретних компонент.....	250
6.1.2. Моделі на основі аналізу загроз системі.....	254
6.1.3. Моделі кінцевих станів.....	256
6.2. Моделі і політики інформаційної та кібербезпеки комп'ютерної інформаційної мережі ВТО.....	265
6.3. Загрози і деструктивні впливи на КІМ ВТО.....	273
6.3.1 Безпека обміну інформацією в комп'ютерних мережах.....	284
6.3.2 Основні поняття та визначення.....	286
6.3.3 Модель мережевої безпеки.....	287
6.3.4 Сервіси безпеки.....	294
6.3.5 Механізми безпеки.....	295
6.3.6 Модель мережевої взаємодії.....	296
6.3.7 Модель безпеки інформаційної системи.....	297
6.3.8 Графове представлення комп'ютерної мережі зі взаємновпливаючими засобами захисту інформації і засобами дії.....	298
6.3.9 Аналіз інструментальних засобів оцінки ризиків витоку інформації в комп'ютерній мережі.....	303
6.4 Забезпечення безпеки ресурсів глобальної мережі Internet.....	312
6.5. Методика аналізу захищеності корпоративних інформаційних систем та мереж.....	331
6.6 Сценарії протидії деструктивним впливам на КІМ ВТО.....	339
6.6.1 Актуальність проблеми.....	339
6.6.2 Проблема інформаційного вторгнення в КІМ із застосуванням інформаційної зброї.....	342
6.6.3 Технологія виявлення атак.....	344
6.6.4 Системи виявлення атак.....	347
6.6.5 Методи реагування.....	350
6.6.6 Підходи до організації протидії деструктивним впливам на КІМ ВТО.....	351
6.6.7 Сценарій протидії на деструктивні впливи на КІМ ВТО.....	352
6.6.8 Принципи попередження деструктивних впливів на КІМ ВТО.....	354
6.7. Метод оцінки рівня захисту інформації від несанкціонованого доступу в комп'ютерних мережах.....	356
ВИСНОВКИ.....	367
ВИКОРИСТАНА ЛІТЕРАТУРА.....	376
ДОДАТОК А.....	396
ДОДАТОК Б.....	410
ДОДАТОК В.....	419
ДОДАТОК Г.....	435