МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ОДЕСЬКА НАЦІОНАЛЬНА АКАДЕМІЯ ХАРЧОВИХ ТЕХНОЛОГІЙ

ІНСТИТУТ КОМП'ЮТЕРНИХ СИСТЕМ І ТЕХНОЛОГІЙ «ІНДУСТРІЯ 4.0» ІМ. П.Н. ПЛАТОНОВА

XII МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ І АВТОМАТИЗАЦІЯ – 2019

INFORMATION TECHNOLOGIES AND AUTOMATION– 2019

Збірник доповідей

Частина I

Одеса,
17-18 жовтня 2019

Секція 1

Наукові напрямки:

Комп'ютерні телекомунікаційні мережі та технології

Математичне моделювання та інформаційні технології

Список
скорочень організацій, представники яких взяли участь у конференції

Таблиця 1

Скорочення	Повна назва організації	Місто	Країна
BNTU	Belarusian National Technical University	Minsk	Belarus
CAFU	CRIAME of Armed Forces of Ukraine	Kyiv	Ukraine
DMTSAU	Dmutro Motornyi Tavria State Agrotechnological University	Melitopol	Україна
DNU	Vasyl' Stus Donetsk National University	Вінниця	Україна
EKSTU	East Kazakhstan State Technical University D. Serikbayev	Ust-Kamenogorsk	Kazakhstan
IAEl SB RAS	Institute of Automation and Electrometry of the Siberian Branch of the Russian Academy of Sciences	Novosibirsk	Russia
IRTC IT&S NAS AND MES	International Research and Training Center for Information Technologies and Systems of the National Academy of Sciences (NAS) of Ukraine and Ministry of Education and Science (MES) of Ukraine	Kyiv	Ukraine
KGES	Kharkiv general education school	Kharkov	Україна
LPNUU	Lviv Polytechnic National University	Lviv	Ukraine
NTU “KhPI”	National Technical University "Kharkiv Polytechnic Institute"	Kharkov	Україна
NTU «KPI»	National Technical University "Igor Sikorsky Kyiv Polytechnic Institute"	Kyiv	Ukraine
NU «OMA»	Національний університет «Одеська морська академія»	Одеса	Україна
NULESU	National University of Life and Environmental Sciences of Ukraine	Kyiv	Ukraine
NUOS	NATIONAL UNIVERSITY OF SHIPBUILDIN NAMED BY ADM. MAKAROV	Nikolaev	Ukraine
ONAFT	Odessa National Academy of Food Technologies	Odessa	Ukraine
ONU	Odessa I.I.Mechnikov National University	Odessa	Ukraine
SSU	Sukhumi State University	Sukhumi	Georgia
VNTU	Vinnytsia National Technical University	Vinnytsia	Ukraine
БНТУ	Белорусский национальный технический университет	Минск	Белоруссия
ВНТУ	Вінницький національний технічний університет	Вінниця	Україна
ДВНЗ «КНУ»	Державний вищий навчальний заклад «Криворізький національний університет»	Кривий Ріг	Україна
ДонНТУ	Донецький національний технічний університет	Покровськ	Україна
ІК НАН України	Інститут кібернетики імені В.М. Глушкова НАН України	Київ	Україна
НТУ «ХПІ»	Национальный технический университет "Харьковский политехнический институт"	Харків	Україна
НТУУ "КПІ"	Національний технічний університет «Київський політехнічний інститут» імені Ігоря Сікорського"	Київ	Україна
НУ «ЛП»	Національний університет «Львівська політехніка»	Львів	Україна
ОДАТРЯ	Одеська державна академія технічного регулювання та якості	Одеса	Україна

Продовження таблиці 1

Скорочення	Повна назва організації	Місто	Країна
ОНАЗ	Одеська національна Академія зв'язку ім. О.С. Попова	Одеса	Україна
ОНАПТ	Одесская национальная академия пищевых технологий	Одесса	Украина
ОНАХТ	Одеська національна академія піщевіх технологій	Одеса	Україна
ОНПУ	Одеський національний політехнічний університет	Одеса	Україна
ОНУ	Одеський національний університет імені І. І. Мечникова	Одеса	Україна
ОТК ОНАХТ	Одеський технічний коледж Одеської національної академії харчових технологій	Одеса	Україна
ПНПУ	Південноукраїнський національний педагогічний університет ім. К.Д. Ушинського	Одеса	Україна
ХНУРЕ	Харківський національний університет радіоелектроніки	Харків	Україна
ХРТК	Харківський радіотехнічний технікум	Харків	Україна
ЦНДІ ОВТ ЗС України	Центральний науково-дослідний інститут озброєння та військової техніки Збройних Сил України	Київ	Україна
ЮНПУ	Южноукраинский национальный педагогический университет им. К.Д.Ушинского	Одесса	Украина

ЗМІСТ

УДК 004.056.5(043.2)

КУЛЬЧИЦЬКИЙ О.С., ЛАДИГІНА О.А.
(ЦНТУ, Україна)

ОСОБЛИВОСТІ НАДІЙНОСТІ ТА ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ І МЕРЕЖАХ

Розглядаються особливості надійності комп'ютерних систем з відмовостійкістю, наведений принцип організації взаємодії моделей безпеки захисту роботи комп'ютерних систем та мереж. Запропоновано вирішення питання розширеного захисту мережі та підвищення ефективності роботи комп'ютеризованої системи.

Під телекомунікаційними технологіями розуміють передачу інформації, що заснована на використанні телекомунікаційних мереж, в склад яких входять об'єкти, які здійснюють функції перетворення та збереження продукту. До таких об'єктів підходять: телефонні, телевізійні та комп'ютерні мережі. Комп'ютерна мережа забезпечує обмін інформації на високій швидкості між двома або більше персональними комп'ютерами через кабельне або бездротове середовище.

Можливості комп'ютерних мереж можна перелічити безліч, але найголовніші – це швидкість (передача інформації на великі відстані, пошук будь-якої інформації і обмін інформацією в offline режимі) [1].

Використовуються комунікаційні мережі в таких спеціалізаціях як:

1. Сигналізація (короткі повідомлення).
2. Використання технічних ресурсів (периферійні пристрої та сховища даних).
3. Віддалене керування (моніторинг та виконання процесів).
4. Забезпечення надійності (резервування).

Крім явних переваг існування комп'ютерних мереж має і зворотну сторону. Відмова зв'язку або її деяких частин може мати сильні негативні наслідки. У зв'язку з цим проблема оцінки і забезпечення надійності мереж, а також захисту інформації в ній є актуальною. Це підтверджує аналіз застосування сучасних телекомунікаційних технологій, який свідчить про необхідність забезпечення гнучкості та надійності систем захисту, а також їх багатоваріантності та постійного удосконалення.

Дуже важливою характеристикою комп'ютерної мережі є надійність - здатність працювати протягом усього часу і має такі складові: власна надійність, зручність і готовність обслуговування мережі.

Щоб підвищити надійність в запобіганні технічних несправностей та вимірювати інтенсивність відмов, треба забезпечити оптичну зв'язність вузлів між собою та знизити час простою системи, яка включає в себе велику кількість різноманітних елементів.

Основним засобом підвищення готовності є надмірність. Чим вище готовність системи, тим вище відмовостійкість. На основі надмірності реалізуються різноманітні варіанти відмовостійких архітектур. Для забезпечення відмовостійкості необхідна надмірність по ключовим елементам мережі (сервера баз даних, Web-сервера, інші сервера), які повинні бути зарезервовані. Якщо мережа виступає як транспортна система, то для всіх маршрутів треба створити надмірність.

Переключення з основного пристрою на резервний може відбуватися вручну та в автоматичному режимі (в ньому коефіцієнт готовності системи вище).

Основні види комп'ютерних систем з відмовостійкістю [2]:

- high availability – системи, що побудовані по комп'ютерній технології з застосуванням апаратних і програмних засобів. Готовність поліпшується шляхом введення надмірності в структуру системи. Високонадійна мережа має високу готовність та підтримує узгодженість даних (забезпечується збереження і захист даних від спотворень);
- fault tolerance – системи, які мають в резерві апаратуру для всіх блоків з процесорами, блоками живлення, пристроїв вводу/виводу та пам'яттю. Мають здатність приховати від користувача відмову окремих їх елементів, тобто відмова одного з їх елементів призведе до зниження якості роботи, але системи залишаються працювати в межах своїх функцій;
- security – здатність системи захистити свої дані від несанкціонованого доступу.

Відсутність деградації є додатковою вимогою до комп'ютерних систем з відмовостійкістю. Тому система повинна підтримувати постійний рівень функціональних можливостей і продуктивності незалежно від існуючих відмов.

Рівень надійності визначається багатьма факторами: структура мереж зв'язку, їх призначення, вартість, умови експлуатації, алгоритми управління та рівень їх надійності.

Для досягнення надійності використовують різноманітні методи та засоби. У кожної системи свій рівень доступної надійності, так як наслідки відмов різних систем можуть значно відрізнятися. Надійність елементів задається часом на відмову або ймовірністю відмови за визначений проміжок часу [3].

Задачі забезпечення надійності вирішуються при синтезі та в ході управління існуючих мереж зв'язку. При синтезі мереж зв'язку забезпечення надійності зводиться до визначення призначення типів елементів, що забезпечує необхідний рівень надійності при мінімальній вартості. Дана задача являє собою велику розмірність, тому до всієї мережі зв'язку дане рішення неможливе. А також розраховувати точні значення показників надійності складної системи, як і підтвердити їх випробуваннями, практично неможливо через неадекватності математичних моделей фізичним і складності розрахунків через велику розмірність рівнянь. Тоді є сенс обчислити показники надійності системи оціночними методами в процесі моделювання, а на фізичному рівні спочатку розглянути дві підмережі, що зв'язують пару абонентів з вищим пріоритетом. Потім перейти до наступної пари і так доти, поки не буде опрацьована вся мережа. При цьому, вимоги по надійності зв'язку повинні задовольняти всі задані пари. На етапі управління існуючих мереж зв'язку задача забезпечення надійності вирішується з використанням внутрішніх ресурсів мереж та зводиться до формування маршрутів для кожної пари і розрахунку ймовірності успішної реалізації сеансу на кожному кроці. Процес є завершеним, якщо ймовірність стає менше заданої. Це забезпечує необхідний рівень надійності. Крім цього вирішення поставленої завдачі ускладнюється тим, що період експлуатації складних об'єктів залежить від технічних, економічних і моральних чинників, причому останній для комп'ютерних систем являється визначальним.

Методом підвищення надійності в роботі систем зв'язку є також отримання об'єктивної інформації щодо апробації обладнання в екстремальних умовах для прийняття якісного рішення у його виборі для застосування на власних технологічних об'єктах.

Комп'ютеризована система забезпечує збір даних у реальному часі та відслідковує реакцію системи на цю інформацію. Сигнали датчиків надходять на пристрій збору даних, зв'язок з яким здійснюється за допомогою відповідного програмного забезпечення та телефонної мережі GSM.

Режим реального часу передачі інформації дає можливість ефективно спостерігати за створеною системою в межах заданих параметрів. Але в цей час система уразлива, тому розглядають шляхи створення довірчого мікропрограмного середовища.

Через комп'ютерну мережу комп'ютерна система має можливість розширювати й створювати єдине середовище для керування і уніфікації комп'ютерного устаткування [4].

У процесах розробки і дослідження комп'ютерних систем важливу роль відіграють моделі безпеки, які вирішують такі завдання:

- вибір і обґрунтування базових принципів архітектури комп'ютерних систем, які визначають механізми реалізації засобів і методів захисту інформації;
- складання формальної специфікації політики безпеки, як найважливішої складової частини організаційного та документаційного забезпечення розроблюваних комп'ютерних систем;
- підтвердження властивостей систем шляхом формального дотримання політики безпеки.

Системи захисту, що використовуються в комп'ютерних системах, орієнтовані на забезпечення конфіденційності або на забезпечення цілісності інформації. Але для повного захисту дана система повинна поєднувати обидва механізми. При побудові та аналізу системи спільно використовують декілька формальних моделей безпеки. Ці моделі можуть переслідувати різні завдання, але обов'язково треба оцінювати стійкість архітектури реальних систем для їх забезпечення.

Рівень захисту комп'ютерної мережі залежить від її розміру та інформації, яку потрібно безпечно передавати. При чому використовують фізичний та/або логічний захист інформації.

Існує декілька моделей безпеки захисту роботи комп'ютерних систем та мереж, кожна з яких має свої індивідуальні можливості [5]. Дві моделі можуть бути реалізовані в системі незалежно одна від одної зі своїми рівнями секретності та цілісності. За рахунок виділення загальних компонентів можливо логічне об'єднання моделей, наприклад, порядок розмежування доступу на одному рівні секретності, або використання однієї і тієї ж решітки рівнів для цілісності і секретності. При цьому суб'єкти та об'єкти моделей з високим рівнем цілісності будуть розташовуватися на низьких рівнях секретності, а з низьким рівнем цілісності - на високих рівнях секретності.

З оглядом на вищевикладене, захист інформації завжди є завданням, "прив'язаним" до конкретної комп'ютерної системи. Для дослідження проблеми захисту інформації треба визначити її через об'єкт захисту. Якщо захисту підлягає мовна інформація, то об'єктом захисту є засоби відтворення звуку і середовище його поширення. Коли захищається інформація в каналах

електрозв'язку, об'єктом захисту є лінії зв'язку та апаратура перетворення. Коли захищається інформація в комп'ютерних системах і мережах, то об'єктом захисту є машинні носії інформації, засоби обчислювальної техніки та канали зв'язку між комп'ютерними системами.

Якщо інформаційний процес є послідовністю збору, накопичення, обробки, передачі, видачі та споживання інформації, то процес захисту інформації можна умовно поділити на два етапи:

- захист інформації під час її збирання, накопичення, обробки та видачі;
- захист інформації під час споживання.

Отже, об'єкт захисту інформації має складну структуру, що відображає технологію обробки і споживання інформації, та її властивості як об'єкта права, характеристики процесів обробки і споживання, які зумовлюють існування загроз. Визначення та оцінка загроз інформації, передумов їх виникнення та шляхів протидії їм є предметом захисту інформації. Така структура об'єкта і предмета захисту інформації являє собою різноманітність методів, які застосовуються для організації її захисту.

Оцінка інформаційної безпеки комп'ютеризованої системи повинна проводитися з метою перевірки відповідності досягнутого рівня інформаційної безпеки заданому рівню при проектуванні комп'ютеризованої системи. Ця оцінка також є важливим засобом забезпечення гарантованості реалізації вибраних механізмів, методів і засобів інформаційної безпеки.

Вибір методів залежить від наявності носіях, на яких існує інформація, від технічних засобів для обробки даних, в якому вигляді вона подається споживачеві. Для захисту інформації можуть використовуватись ті ж самі методи, що й при створенні інформаційних технологій, комп'ютерних систем тощо.

Окремо слід відзначити забезпечення безпеки в гетерогенних віртуальних обчислювальних середовищах, куди різні компанії переводять обчислювальні і інформаційні ресурси. У таких віртуальних інфраструктур виникають нові загрози. Перш за все це атаки на засоби управління віртуальними машинами, хмарні контролери, сховища даних, неавторизований доступ до вузлів віртуалізації, використання віртуального середовища для несанкціонованої передачі даних [6].

Управління ризиками інформаційної безпеки пов'язане із вжиттям заходів забезпечення інформаційної безпеки, спрямованих на зниження частоти реалізації загроз і розміру збитку у разі їх реалізації. Для того, щоб повною мірою використати послуги безпеки необхідна відповідна документація з детальним описом послуг, планом вказівок щодо їх використання. План відображає середовище випробувань, будь-які особливі умови для проведення випробувань, і засоби випробувань. Методика випробувань визначає процедури тестування кожного елемента комп'ютеризованої системи, а також для кожного окремого тесту описує використання засобів випробувань, необхідне оточення і особливі умови.

Тому пропонується для вирішення питання розширеного захисту мережі та підвищення ефективності роботи комп'ютеризованої системи комбінувати найпоширеніші і доволі специфічні способи захисту локальних комп'ютерних мереж із застосуванням сучасних технологій за умови використання вже існуючого обладнання та детальної документації, в якій визначені всі стадії життєвого циклу роботи комп'ютеризованої системи та їх граничні вимоги.

СПИСОК ЛІТЕРАТУРИ

1. Е. Вілсон, *Моніторинг і аналіз мереж*. Москва, Росія: Лорі, 2013.
2. А.Ф. Попов, *Комп'ютерні системи і мережі*. Чернівці, Україна: 2010.
3. А.М. Половко, С.В. Гуров, *Основы теории надежности*. Петербург, Росія: БХВ, 2006.
4. Д. Янішевський, «Актуальні питання захисту інформації в комп'ютерних системах і мережах», *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, вип. 8, с.81-85, 2004.
5. О. С. Кульчицький, О. А. Ладигіна, «Аналіз роботи захисту інформації в комп'ютерних системах та мережах», *матеріали Міжнародної науково-практичної конференції "Інформаційна безпека та інформаційні технології": тези доповідей, 24 – 25 квітня 2019 р*. Х.: ХНЕУ імені Семена Кузнеця, 2019. с. 14.
6. О. А. Ладигіна, «Дослідження загроз для віртуальної інфраструктури хмари та методи її захисту», *Інформаційна безпека держави, суспільства та особистості: Збірник тез доповідей Всеукраїнської науково-практичної конференції, 16 квітня 2015 року*, м. Кіровоград: КНТУ, 2015. с.45-47.

XII МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ І АВТОМАТИЗАЦІЯ – 2019

INFORMATION TECHNOLOGIES AND AUTOMATION– 2019

ОДЕСА
17– 18 ЖОВТНЯ, 2019

Збірник включає доповіді учасників XII Міжнародної науково-практичної конференції «Інформаційні технології і автоматизація – 2019»

Редакційна колегія: Котлик С.В., Хобін В.А., Плотніков В.М.

Комп'ютерний набір і верстка: Соколова О.П.

Відповідальний за випуск: Котлик С.В.