МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ
ФАКУЛЬТЕТ КОМП'ЮТЕРНО-ІНФОРМАЦІЙНИХ СИСТЕМ І ПРОГРАМНОЇ ІНЖЕНЕРІЇ

ЛАЗОРКО АНДРІЙ ІВАНОВИЧ

УДК 004.056.53

АНАЛІЗ ВІДОМИХ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА ДОСТОВІРНОСТІ ДАНИХ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

125 «Кібербезпека»

Автореферат
дипломної роботи на здобуття
освітнього рівня «магістр»

Тернопіль
2019

Роботу виконано на кафедрі кібербезпеки Тернопільського національного технічного університету імені Івана Пулюя Міністерства освіти і науки України

Керівник роботи: кандитат юридичних наук, доцент кафедри кібербезпеки
Муж Валерій Вікторович,
Тернопільський національний технічний університет імені Івана Пулюя,

Рецензент: доктор наук із соціальних комунікацій, професор кафедри комп'ютерних наук
Кунанець Наталія Едуардівна,
Тернопільський національний технічний університет імені Івана Пулюя

Захист відбудеться 24 грудня 2019 р. о $9^{.00}$ годині на засіданні екзаменаційної комісії №32 у Тернопільському національному технічному університеті імені Івана Пулюя за адресою: 46001, м. Тернопіль, вул. Руська, 56, навчальний корпус №1, ауд. 806

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми роботи. В наш час обчислювальні можливості дозволяють користувачам локальних і глобальних систем обчислень збільшити на два, або три порядки обсяги даних, що надходять, а також нові послуги, що надаються користувачам комп'ютерних мереж. І тому збільшення обсягів даних в критичних системах локальної обчислювальної мережі (ЛОМ), глобальної обчислювальної мережі (ГОМ) висуває нові вимоги до забезпечення надійності і продуктивності комп'ютерних систем, безпеки та достовірності переданих і оброблюваних даних. Останнім часом не всі сучасні криптографічні засоби захисту інформації забезпечують своєчасну обробку величезних обсягів даних (десятки-сотні Мбіт/с) і задовольняють жорстким вимогам по достовірності та безпеки інформації.

Мета роботи: аналіз відомих методів забезпечення безпеки та достовірності інформації в комп`ютерних системах та мережах на основі каналів з пам`яттю та без пам`яті. Виявлення найліпшого протоколу, який забезпечує максимальну оцінку ефективності обміну даними в комп`ютерній мережі при різних засобах управління обміном.

Об’єкт, методи та джерела дослідження. Об’єкт дослідження – процес аналізу відомих протоколів забезпечення безпеки та достовірності обміну даними.
Предмет дослідження – способи управління обміном, які дозволяють оцінити значення показника ефективності обміну даними в комп'ютерній мережі.

Наукова новизна отриманих результатів: В роботі запропоновано метод оцінки ефективності функціонування комп’ютерної мережі та метод прийняття рішень для вибору оптимальної стратегії функціонування комп'ютерної мережі.

Практичне значення : Показник функціональної ефективності мережі досліджено в каналах з пам'яттю та без пам'яті. Для проведення дослідження були використані програмний пакет Mathcad 15 та редактор Microsoft Office Visio 2007. Проведення даного аналізу допоможе виявити найліпший протокол, який забезпечує безпеку та достовірність переданої та оброблюваної інформації в комп`ютерних системах та мережах на основі каналів з пам`яттю та без пам`яті.

Апробація. Окремі результати роботи доповідались на VII науково-технічній конференції «Інформаційні моделі, системи та технології», Тернопіль, ТНТУ, 11 – 12 грудня 2019 р.

Структура роботи. Робота складається з розрахунково-пояснювальної записки та графічної частини. Розрахунково-пояснювальна записка складається з вступу, 7 частин, висновків, переліку посилань та додатків.
Обсяг роботи: розрахунково-пояснювальна записка – 111 арк. формату А4, ілюстративна частина– 18 слайдів.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі сформульовано актуальність проблеми аналізу відомих методів забезпечення безпеки та достовірності даних в інформаційних системах та сформульовано мету і основні завдання роботи.

У першому розділі проведено аналіз умов функціонування та обґрунтування вимог, що пред'являються до сучасних комп'ютерних систем та мереж

У другому розділі проведено аналіз відомих методів забезпечення безпеки та достовірності інформації в комп`ютерних системах та мережах.

У третьому розділі проведено оцінку показника функціональної ефективності комп'ютерної мережі на основі протоколу Frame Relay

В спеціальній частині описано базові речі про симетричну та асиметричну криптографію.

В розділі "Обґрунтування економічної ефективності" обчислено основні показники економічної ефективності від розробки і реалізації запропонованого алгоритму.

У підрозділі "Охорона праці" розглянуто забезпечення безпечних і не шкідливих умов праці. У підрозділі "Безпека життєдіяльності" описано вплив факторів виробничого середовища та електромагнітного випромінювання на життєдіяльність людини.

В розділі "Екологія" висвітлено статистичні показники екологічних явищ та описано моніторинг довкілля.

У загальних висновках щодо дипломної роботи наведено короткий опис основної частини; сформульовано основні результати, отримані в роботі та сформульовано рекомендації для організацій, що працюють в корпоративній мережі.

В додатках до пояснювальної записки приведено тези.

В ілюстративній частині приведено Вимоги, які висуваються до обчислювальних мереж та систем; Основна вимога обчислювальної мережі, Класифікація протоколів канального рівня, Ймовірносно-часові характеристики технології ГОМ, Ефективність функціонування комп’ютерної мережі, Стратегії функціонування комп'ютерної мережі, Протоколи управління обміном даними, Показник ефективності при різних довжинах кадрів, Показник ефективності при різних довжинах, Дослідження часу доставки кадру, Показник функціональної ефективності в каналах без пам'яті, Показник функціональної ефективності в каналах з пам'яттю, Порівняння коефіцієнта ефективності обміну даними в комп'ютерній мережі, Висновки

ВИСНОВКИ

У даній роботі були проаналізовані відомі методи забезпечення безпеки та достовірності інформації в комп`ютерних системах та мережах на основі каналів з пам`яттю та без пам`ятті. В процесі проведення дослідження були враховані всі можливі дії та виконанні основні задачі: аналіз умов функціонування та обґрунтування вимог, що пред'являються до сучасних комп'ютерних систем та мереж; аналіз протоколів канального рівня глобальної обчислювальної мережі та оцінка ефективності обміну даними в комп'ютерній мережі при різних засобах управління обміном даних.

Під час дослідження був проведений аналіз локальних та глобальних обчислювальних мереж, канального рівня мережевої моделі OSI для ЛОМ та ГОМ, був наведений закон Мура. Були розглянуті протоколи канального рівня глобальної обчислювальної мережі – X.25, Frame Relay та протокол ATM, наведені відповідні структурні схеми.

У результаті даного дослідження був визначений найліпший протокол забезпечення безпеки та достовірності переданої та оброблюваної інформації в комп'ютерних системах та мережах – Frame Relay. Була розрахована оцінка показника ефективності в комп'ютерних системах та мережах на основі даного протоколу. У результаті даний протокол забезпечує найбільш точну оцінку показника ефективності комп`ютерної мережі. Оцінка розраховувалася при різних стратегіях управління обміном даних: без зворотного зв'язку з виправленням t-кратних помилок, без зворотного зв'язку з виявленням r-кратних помилок, з вирішальним зворотним зв'язком і безперервною передачею кадрів (ВЗЗбп) "Повернення-на-N" та з вирішальним зворотним зв'язком і позитивною квитанцією (ВЗЗпк).

Згідно з проведеним дослідженням було виявлено, що узагальнений показник ефективності комп'ютерної мережі на основі протоколу Frame Relay дозволяє всебічно оцінити протоколи обміну даними. Технологія Frame Relay в порівнянні з протоколом X.25 більш точно оцінює ефективність протоколів обміну даними в комп'ютерних мережах.

СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

1. Ситник О. Метод реплікації даних з використанням NFC-технології [Текст] / Ситник О., Лазорко А**.** Збірник тез VII науково-технічної конференції Тернопільського національного технічного університету імені Івана Пулюя «Інформаційні моделі, системи та технології» – Тернопіль (11 – 12 грудня 2019 р.), ТНТУ, 2019. – с.97.

АНОТАЦІЯ

Дана магістерська кваліфікаційна робота присвячена дослідженню відомих методів забезпечення безпеки та достовірності даних в інформаційних системах. Для проведення дослідження було введено узагальнений показник ефективності комп'ютерної мережі (Wi). При цьому були досліджені залежності коефіцієнта готовності від довжини кадру, часу доставки кадру при різних можливостях помилки в каналі передачі з використанням асимметричних і симетричних

алгоритмов шифрування. Для дослідження були використані різні стратегії управління обміном даних.

В результаті дослідження було виявлено, що на коефіцієнт готовності істотно впливає довжина кадру (оперативність), час шифрування і розшифрування (безпека), ймовірність помилки (надійність). Розроблено стратегії функціонування комп'ютерної мережі для каналів з пам'яттю та без пам’яті.

Ключові слова: БЕЗПЕКА, ДОСТОВІРНІСТЬ, НАДІЙНІСТЬ, КАНАЛИ З ПАМ`ЯТТЮ, КАНАЛИ БЕЗ ПАМ`ЯТІ, КАНАЛЬНИЙ ПРОТОКОЛ, FRAME RELAY, X.25, ЗВОРОТНІЙ ЗВ'ЯЗОК

ANNOTATION

This master's qualification thesis is devoted to the study of known methods of data security and reliability in information systems. For the study, a generalized measure of the performance of a computer network (Wi) was introduced. The dependencies of the readiness factor on the frame length, the frame delivery time at different error possibilities in the transmission channel were investigated using asymmetric and symmetric encryption algorithms. Different data sharing management strategies were used for the study.As a result of the study, it was found that the readiness factor is significantly affected by the frame length (operability), encryption and decryption time (security), error probability (reliability). Computer network strategies for memory and non-memory channels have been developed.

Key words: SAFETY, ACCURACY, RELIABILITY, MEMORY CHANNELS, MEMORYLESS CHANNELS, CHANNEL PROTOCOL, FRAME RELAY, X.25, FEEDBACK.