ХЕРСОНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
(повне найменування вищого навчального закладу)
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ДИЗАЙНУ
(повне найменування інституту, назва факультету (відділення))
КАФЕДРА ПРОГРАМНИХ ЗАСОБІВ І ТЕХНОЛОГІЙ
(повна назва кафедри (предметної, циклової комісії))

Пояснювальна записка

до кваліфікаційної роботи
магістра
(освітньо-кваліфікаційний рівень)

на тему:

Розробка інформаційної системи захисту програмно-конфігурованої мережі від атак

Виконав: студент 6 курсу, групи 6ПР
спеціальності
121 «Інженерія програмного забезпечення»
(шифр і назва напряму підготовки, спеціальності)

Мищенко Є.О._____
(прізвище та ініціали)
Керівник д.т.н.,професор Жарікова М.В.
(прізвище та ініціали)
Рецензент _____
(прізвище та ініціали)

Хмельницький - 2023

ФАКУЛЬТЕТ ІНФОРМАЦІНИХ ТЕХНОЛОГІЙ ТА ДИЗАЙНУ
КАФЕДРА **Програмних засобів і технологій**
Освітньо-кваліфікаційний рівень магістр
Галузі знань 12 «Інформаційні технології»
Спеціальність 121 «Інженерія програмного забезпечення»
Освітньо-професійної програми «Програмна інженерія»/«Програмне забезпечення систем»

ЗАТВЕРДЖУЮ
в.о.завідувача кафедри

доцент Огнєва О.Є.

“____” _____ 2023 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Мищенко Євген Олександрович
(прізвище, ім’я, по батькові)

1. Тема роботи: «Розробка інформаційної системи захисту програмно-конфігурованої мережі від атак»

керівник роботи Жарікова Марина Віталіївна д.т.н., професор
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від “ ”_____2023 року №

2. Строк подання студентом проекту (роботи)_____

3. Вихідні дані до проекту (роботи) Аналіз предметної області, Огляд існуючих рішень,

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити): ТЕОРЕТИЧНІ АСПЕКТИ КОНФІДЕНЦІЙНОСТІ ДАНИХ В ПРОГРАМНО-КОНІФГУРОВАНИХ МЕРЕЖА, АНАЛІЗ АЛГОРИТМІВ ШИФРУВАННЯ, АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ЗАХИСТУ ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖ ВІД АТАК

5. Перелік графічного матеріалу (з точним зазначенням обов’язкових креслень) Комп'ютерна презентація

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Відбір та вивчення літературних джерел	16.10.2023 року	
2	Постановка задачі	22.10.2023 року	
3	Вибір методу для рішення задачі	29.10.2023 року	
4	Розробка моделі	07.11.2023року	
5	Опис програмного продукту	19.11.2023 року	
6	Оформлення пояснювальної записки	29.11.2023 року	
7	Захист кваліфікаційної роботи бакалавра	19.12.2023 року	

Студент_____**Мищенко Є.О.**
(підпис) (прізвище та ініціали)

Керівник проекту (роботи)_____ **Жарікова М.В.**
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота магістра містить: 116 сторінок тексту, 15 рисунків, 15 таблиць, 29 літературних джерел, 1 додаток.

В даній роботі розгядаються основні поняття конфіденційності данних, загрози конфіденційності данних та технічні засоби забезпечення конфіденційності даних в програмно-коніфгурованих мережах. Також розглядаються криптографічні методи забезпечення конфіденційності даних. В рамках цієї роботи досліджуються алгоритми симетричного та асиметричного шифрування та проводиться їх порівняння. У даній роботі звертається увага на віртуальні приватні мережі (VPN) та протоколи забезпечення конфіденційності даних (наприклад SSL). Також в роботі надані рекомендації щодо практичного застосування нових методів забезпечення конфіденційності даних. Ключові слова: поняття конфіденційності даних, алгоритми симетричного шифрування, алгоритми асиметричного шифрування, віртуальні приватні мережі (vpn), протоколи забезпечення конфіденційності даних .

КЛЮЧОВІ СЛОВА: ПРОГРАМНО-КОНФІГУРОВАНА МЕРЕЖА, АТАКА, КОНФІДЕНЦІЙНІСТЬ ДАНИХ, АЛГОРИТМ ШИФРУВАННЯ

ЗМІСТ

ВСТУП

Актуальність. Конфіденційність даних в програмно-коніфгурованих мережах є надзвичайно актуальною темою в сучасному цифровому світі. З розвитком програмно-конфігурованій та глобальної інформаційної інфраструктури, обсяги інформації, що передається та обробляється, набули непередбачуваного масштабу. У цьому контексті забезпечення конфіденційності даних стає життєво важливим завданням. Зростаюча кількість кіберзагроз, включаючи хакерські атаки, фішинг, крадіжки даних та порушення приватності, створює небезпеку для безпеки та конфіденційності інформації, що передається через мережі. Відомі випадки витоку конфіденційних даних, такі як особисті інформація, комерційні та державні секрети, медичні записи, демонструють потребу в ефективних засобах та методах захисту. Окрім того, суспільне усвідомлення щодо приватності та конфіденційності даних росте. Користувачі стають більш обізнаними та свідомими щодо ризиків, пов'язаних зі збереженням та передачею їхніх особистих даних в мережі. Це стимулює вимоги до організацій і компаній забезпечувати надійний захист конфіденційності даних своїх клієнтів.

В останні роки спостерігається значне збільшення кількості цифрових даних, які зберігаються та передаються через програмно-коніфгуровані мережі, завдяки таким новим технологіям як Інтернет речей, хмарні обчислення, соціальні мережі, електронна комерція та інші цифрові технології, що стали невід'ємною частиною нашого повсякденного життя. Це створює потребу в надійному захисті цих великих обсягів даних від несанкціонованого доступу та зловмисних дій. Кількість кіберзагроз постійно зростає. Зловмисники постійно розвивають нові методи атак та кіберзлочинності, що ставить під загрозу конфіденційність даних. Від атак хакерів, фішингу, шкідливих програм до крадіжок особистих даних та розкриття комерційної інформації - цифрові 8 загрози стають все більш складними та небезпечними. Забезпечення конфіденційності даних стає

критичною необхідністю для уникнення фінансових втрат, порушення приватності та інших негативних наслідків. Захист конфіденційності даних став предметом суворого законодавства та регулювання.

Багато країн та регіонів встановлюють нові правила, такі як загальний регламент про захист даних (GDPR) в ЄС, щоб регулювати збір, зберігання, обробку та передачу особистих даних. Компанії повинні відповідати цим вимогам, оскільки порушення конфіденційності даних може мати серйозні наслідки, такі як штрафи та втрати репутації. Інфокомунікації представляють собою сучасну концепцію, що об'єднує телекомунікаційні технології з інформаційними та комп'ютерними системами. Це нерозривний зв'язок між різними елементами, що забезпечують передачу та обмін інформацією. Інфокомунікації розвиваються шляхом конвергенції різних технологій, таких як передавання сигналів, маршрутизація, перетворення сигналів та програмування, забезпечуючи оптимальну обробку інформації. програмно-коніфгуровані мережі є складним комплексом технічних засобів, що включають елементи програмно-коніфгурова, споруди та системи маршрутизації. Вони призначені для передавання, приймання та обміну різних видів сигналів, повідомлень, тексту, зображень та звуку через різні види комунікаційних систем, таких як радіо, провідні та оптичні.

Глобальна інформаційна інфраструктура включає в себе мережі та системи програмно-коніфгурова, які сполучають вузли зв'язку, комп'ютери та пристрої електроніки, щоб забезпечити передавання різноманітної інформації. Вона створює базову інфраструктуру для організації різних програмно-коніфгурованих послуг та забезпечує зв'язок між користувачами по всьому світу. Враховуючи швидкий технологічний розвиток і зростаючу залежність від інформаційних систем, конфіденційність даних в програмно-коніфгурованих мережах стає дедалі важливішою. Потреба у захисті особистої інформації, 9 комерційних даних та інших конфіденційних даних вимагає розробки ефективних методів та засобів забезпечення безпеки в цих мережах. У сучасному світі інформаційних технологій і інтернету

зростає значущість питань, пов'язаних з конфіденційністю даних. Забезпечення конфіденційності даних стає надзвичайно важливим завданням для забезпечення приватності користувачів, бізнесу та держави в цифровому середовищі. Вчені та спеціалісти у галузі інформаційної безпеки та криптографії активно досліджують та розробляють нові методи та алгоритми для забезпечення конфіденційності даних в програмно-коніфгурованих мережах. Постійні зусилля спрямовані на поліпшення систем шифрування, аутентифікації та контролю доступу, щоб забезпечити захист інформації від несанкціонованого доступу та зловмисницьких дій.

Метою роботи є дослідження конфіденційності даних в програмно-коніфгурованих мережах та аналіз засобів її забезпечення. Об’єктом дослідження є конфіденційність даних в програмно-коніфгурованих мережах.

Предмет дослідження - засоби забезпечення конфіденційності даних в програмно-коніфгурованих мережах. Включаючи методи шифрування, аутентифікації, контролю доступу, аналіз загроз та ризиків.

Для досягнення мети було сформовано наступні завдання: - дослідити теоретичні аспекти конфіденційності даних в програмно-коніфгурованих мережах, включаючи розгляд основних принципів інформаційної безпеки, аналіз загроз конфіденційності даних та вивчення засобів забезпечення конфіденційності;

- проаналізувати основні алгоритми шифрування і зробити їх порівняльний аналіз;

- визначити основні методи та засоби забезпечення конфіденційності даних в програмно-коніфгурованих мережах, включаючи криптографічні методи, протоколи та засоби контролю доступу;

- провести оцінку існуючих методів забезпечення конфіденційності даних, визначити їх переваги та недоліки;

- сформулювати висновки і рекомендації щодо забезпечення конфіденційності даних в програмно-коніфгурованих мережах.