

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

ЯКУБІВ ПЕТРО СТЕПАНОВИЧ

УДК 004.62; 621.326

**РОЗРОБКА КОМПЛЕКСНОГО ПІДХОДУ ДО РЕАЛІЗАЦІЯ
ЗАХИЩЕНОГО МЕТОДУ АУТЕНТИФІКАЦІЇ НА БАЗІ WI-FI ПРИСТРОЇВ
ФІРМИ CISCO”.**

8.05010101 «Інформаційні управляючі системи та технології»

Автореферат

дипломної роботи на здобуття освітнього ступеня «магістр»

Тернопіль
2017

Роботу виконано на кафедрі комп'ютерних наук Тернопільського національного технічного університету імені Івана Пулюя Міністерства освіти і науки України

Керівник роботи: кандидат фізико-математичних наук, професор кафедри комп'ютерних наук
Михайлишин Михайло Стахович,
Тернопільський національний технічний університет імені Івана Пулюя

Рецензент: кандидат фізико-математичних наук, доцент кафедри фізики
Скоренький Юрій Любомирович,
Тернопільський національний технічний університет імені Івана Пулюя

Захист відбудеться 21 лютого 2017 р. о 10⁰⁰ годині на засіданні екзаменаційної комісії №31 у Тернопільському національному технічному університеті імені Івана Пулюя за адресою: 46001, м. Тернопіль, вул. Руська, 56, навчальний корпус №1, ауд.701.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми роботи. Дана робота присвячена розробці комплексного підходу до реалізації захищеного методу аутентифікації на базі Wi-Fi пристроїв фірми Cisco.

Бездротові мережі здобувають ринок інтернет послуг у більшості розвинених країн світу завдяки простоті використання та широким функціональним можливостям присутнім в пристроях Wi-Fi. Доступ до сервісів мобільної оплати послуг і проведення операцій за допомогою банківських карт там, де встановлені хоти-стопи, може бути здійснений за допомогою кишенькового комп'ютера, ноутбука, смартфона.

Враховуючи особливості технології, ефективна система забезпечення безпеки повинна містити в собі кілька компонентів, і головними з них вважаються механізми, які гарантують, що дані дійсно надходять із передбачуваного джерела, а їхній несанкціонований перегляд і зміна неможливі.

Адміністратори мереж шукають такі рішення, які забезпечили б гнучку політику авторизації, прив'язану до конкретних ідентифікованих користувачів, а також до видів мережного доступу та до систем безпеки пристроїв, використовуваних для доступу в мережу.

Здатність до централізованого відстеження та моніторингу підключень мережних користувачів відіграє основну роль у нейтралізації небажаного надмірного завантаження мережних ресурсів.

Мета роботи: реалізація підходу для забезпечення надійного механізму аутентифікації, авторизації та аудиту в корпоративній мережі на базі Wi-Fi пристроїв фірми Cisco.

Об'єкт дослідження. процес аутентифікації на пристроях Wi-Fi (фірми Cisco).

Методи дослідження: теоретичний аналіз протоколів автентифікації, вивчення роботи технології Wi-Fi. можливість захисту, огляд програмних продуктів, що дозволяють організувати автентифікацію на віддаленому сервері.

Наукова новизна отриманих результатів:

- визначено технології стандартів, що підходять для реалізації поставлених задач;
- проведено аналіз та порівняння технологій захисту Wi-Fi мереж;
- проведено аналіз та порівняння серверів аутентифікації;
- забезпечено можливості аудиту: введених команд, часу роботи користувачів, спроб перебору імені/паролів;
- здійснено збільшення захищеності мережі Wi-Fi додатковими методами.

Практичне значення отриманих результатів.

Розроблено реальні рішення, які може бути впроваджені в практичну діяльність.

Проведена робота виявила елементи бездротової мережі які найбільше вразливі до атак, тобто маршрутизатори та точки доступу, та описаних методів захисту є достатньо для забезпечення високого рівня безпеки бездротових мереж, та

можливість організації безпечного віддаленого доступу для адміністраторів інших компаній.

Апробація. Окремі результати роботи доповідались на ІХ Всеукраїнській студентській науково-технічній конференції «Природничі та гуманітарні науки. Актуальні питання», Тернопіль, ТНТУ, 20 – 21 квітня 2016 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 – ___ арк. формату А4.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі проведено огляд сучасного стану методики побудови гібридної інтелектуальної системи для вирішення основного класу задач Data Mining.

В першому розділі проведено детальний аналіз стандарту 802.11. Проведено огляд технології WLAN, технології CSMA/CA, технології стрибкоподібної перестройки частоти, технології широкосмугової модуляції.

В другому розділі досліджено технології захисту автентифікації, авторизації та аудиту та технології захисту передачі даних та доступу до мережі Wi-Fi. Здійснено детально опис роботи технології WEP, WPA / WPA2 та 802.1x та їх порівняння.

В третьому розділі описано реалізацію засобів захищеної аутентифікації, авторизації та аудиту, на прикладі Wi-Fi пристроїв фірми Cisco. Конфігурування точки доступу Wi-Fi для автентифікації через FreeRADIUS. Налаштування точки доступу для роботи з технологіями WEP та WPA.

В спеціальній частині було описано і проведено порівняльний аналіз MathCAD 14, MathCAD 15, Mathcad Prime.

В розділі «Обґрунтування економічної ефективності» розглянуто питання категорії продуктивність праці та категорії гроші і їх функції і проведено розрахунки техніко-економічної ефективності проектних рішень.

В розділі «Охорона праці та безпека в надзвичайних ситуаціях» розглянуто питання аналізу впливу моніторів на зорову систему людини. Розглянуто заходи, щодо зменшення негативного впливу електромагнітних випромінювань. Лписано негативний вплив шумів та вібрацій обладнання на людину.

В розділі «Екологія» проаналізовано застосування екологічних знань у різних галузях соціально-політичного життя. Описано кореляційний аналіз зв'язків в екології.

У загальних висновках щодо дипломної роботи описано прийняті в проекті технічні рішення і організаційно-технічні заходи, які забезпечують виконання завдання; оригінальні технічні рішення, прийняті автором в процесі роботи; технічні рішення роботи, які можуть бути впроваджені; техніко-економічні показники та їх порівняння з базовими.

ВИСНОВКИ

З зростанням масштабів використання бездротових мереж питання безпеки мереж відіграє досить велике значення. Перед мережевими адміністраторами постає

задача у забезпеченні користувачам мобільності, при цьому не надаючи зловмисникам можливості доступу до мережі та до інформації, що передається в бездротовій мережі.

Виходячи з мети дипломної роботи, необхідно було забезпечити надійний механізм автентифікації на пристроях Wi-Fi для їх конфігурування та захищеність даних що передаються.

Для реалізації поставленої задачі було виконано наступне: вивчено роботу бездротових мереж на фізичному рівні; проаналізовано можливості протоколів автентифікації та їх характеристики; розглянуто сучасні можливості технологій шифрування даних в бездротових мережах; було протестовано можливість серверів автентифікації на забезпечення захищеності Wi-Fi мереж; налаштоване відповідне програмне забезпечення та Wi-Fi пристрої; перевірено можливість автентифікації на Wi-Fi пристроях з аудитом подій на сервері ACS.

Здійснена робота виявила найбільше вразливі елементи бездротової мережі до атак.

СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

1. Якубів П. EMBER.JS концепції для Ruby on Rails розробника / П. Якубів – Тези доповіді на IX Всеукраїнській студентській науково-технічній конференції «Природничі та гуманітарні науки. Актуальні питання». – Тернопіль, ТНТУ, 2016. – с. 128.

АНОТАЦІЯ

В дипломній роботі проведений аналіз існуючих систем, розглянуто їх класифікацію та архітектуру. Детально вивчено роботу бездротових мереж на фізичному рівні та проаналізовано можливості протоколів аутентифікації та їх характеристики.

Розглянуто сучасні можливості технологій шифрування даних в бездротових мережах, а також протестовано можливість серверів аутентифікації на забезпечення захищеності Wi-Fi мереж, налаштоване відповідне програмне забезпечення та Wi-Fi пристрої.

Перевірено можливість аутентифікації на Wi-Fi пристроях з аудитом подій на сервері ACS.

Ключові слова: БЕЗДРОТОВА МЕРЕЖА WI-FI, CISCO, IEEE, WEP, WPA, АУТЕНТИФІКАЦІЯ, АВТОРИЗАЦІЯ, АУДИТ, СЕРВЕРИ TACASC+ I RADIUS, CISCO SECURE ACCESS CONTROL SERVER.

ANNOTATION

In the thesis work is the analysis of existing systems, considered classification and architecture. Studied in detail the wireless networks at the physical level and analyzes the possibility of authentication protocols and their characteristics.

The modern technology of data encryption capabilities in wireless networks, and authentication servers tested the possibility to ensure security of Wi-Fi networks configured software and Wi-Fi devices.

Checked opportunity authentication for Wi-Fi devices on the server audit events ACS.

Key words: Wireless Network WI-FI, AUTHORIZATION, CISCO, IEEE, WEP, WPA, AUTHENTICATION, AUDIT, SERVERS TACASC+ I RADIUS, CISCO SECURE ACCESS CONTROL SERVER.