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

ХАРІН ДМИТРО ВЛАДИСЛАВОВИЧ

УДК 004.056

ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНІЙ МЕРЕЖІ НА БАЗІ WI-FI ПРИСТРОЇВ (НА ОСНОВІ СТАНДАРТУ IEEE 802.11)

123 «Комп'ютерна інженерія»

Автореферат
дипломної роботи на здобуття освітнього ступеня «магістр»

Тернопіль, 2018

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

Керівник роботи: **Баран Ігор Олегович**
кандидат технічних наук, доцент
декан факультету комп'ютерно-інформаційних систем та програмної інженерії
Тернопільський національний технічний університет імені Івана Пулюя

Рецензент: **Савків Володимир Богданович,**
доцент, кандидат технічних наук, доцент кафедри автоматизації технологічних процесів і виробництв
Тернопільський національний технічний університет імені Івана Пулюя

Захист відбудеться _29_ грудня 2018 р. о $9^{.00}$ годині на засіданні екзаменаційної комісії № 34 у Тернопільському національному технічному університеті імені Івана Пулюя за адресою: 46001, м. Тернопіль, вул. Руська, 56, навчальний корпус №1, ауд. 603.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми роботи. Завдяки зручності, простоті використання та широким функціональним можливостям присутнім в пристроях Wi-Fi бездротові мережі (побудовані на основі стандарту 802.11) здобувають більшу популярність у більшості розвинених країн світу. 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 або ноутбука, які використовуються персоналом різних закладів. Якщо для проникнення у звичайну мережу зловмисникові необхідно фізично до неї підключитися, то у випадку з Wi-Fi всі набагато простіше - потрібно всього лише перебувати в зоні прийому мережі. І тоді окрім доступу до конфіденційних файлів, зловмисник може розсилати спам, викрадати інтернет-трафік, прослуховувати незахищені розмови, змінювати та підтасовувати дані і т.д.

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. Але при безлічі плюсів бездротових технологій передачі даних, є один суттєвий мінус: відкрите середовище передачі інформації, яка веде до можливості безперешкодного перехоплення кодованих потоків, що передаються по мережі. Збільшення частки інформації, що передається по бездротових каналах, тягне за собою і збільшення частки атак на бездротові мережі. Саме з цієї причини настільки важливе питання захисту інформації при її передачі по радіоканалах у Wi-Fi мережах.

Мета роботи: реалізація комплексного підходу для забезпечення надійного механізму захисту інформації в корпоративній Wi-Fi-мережі на основі стандарту IEEE 802.11.

Об’єкт та методи дослідження. Основним об’єктом дослідження є процес забезпечення захисту інформації в комп'ютерній мережі на базі Wi-Fi пристроїв. Методика проведення аудиту захищеності безпровідної мережі розробляється з використанням теорії надійності, методів автентифікації, авторизації та аудиту. Методика дослідження базується на теоретичних і прикладних результатах, досягнутих у комп’ютерній інженерії.

Предмет дослідження: процедури, протоколи алгоритми і засоби для забезпечення захисту інформації комп'ютерній мережі на базі Wi-Fi пристроїв.

Наукова новизна отриманих результатів:

- сформульовано систему критеріїв оцінки захищеності безпровідної мережі на основі реалізованих в ній механізмів;
- розроблено систему рівня довіри до безпровідної мережі;
- проведено аналіз та порівняння серверів аутентифікації;;
- розроблено метод побудови профілів захисту для безпровідної мережі;
- запропоновано методику проведення аудиту захищеності безпровідної мережі.

Практичне значення отриманих результатів. Можливість використання результатів роботи при проектуванні та аудиті безпровідних мереж, а також використання окремих розроблених методів і алгоритмів при розробці та дослідженні широкого кола безпровідних комп'ютерних мереж.

Апробація. Окремі результати дослідження доповідалися на VI Міжнародній науково-технічній конференції молодих учених та студентів «Актуальні задачі сучасних технологій» Тернопільського національного технічного університету імені Івана Пулюя (м. Тернопіль, 16-17 листопада 2017 р.)

Структура роботи. Робота складається з розрахунково-пояснювальної записки та графічної частини. Розрахунково-пояснювальна записка складається з вступу, 7 частин, висновків, переліку посилань, додатків. Обсяг роботи: розрахунково-пояснювальна записка – ____ арк. формату А4, графічна частина – 9 аркушів формату А1.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі проведено аналіз актуальності та мети роботи, поставлено задачі дослідження, сформульовано об'єкт та предмет дослідження, наведена наукова новизна та практичне значення одержаних результатів.

В першому розділі «АНАЛІТИЧНИЙ ОГЛЯД АРХІТЕКТУРИ КОМПЮТЕРНОЇ МЕРЕЖІ НА БАЗІ WI-FI ПРИСТРОЇВ» проведено огляд архітектури комп'ютерної мережі стандарту EEE 802.11 та топології WLAN за зонами обслуговування, описані основні характеристики стандартів групи IEEE 802.11 та механізм доступу до середовища стандарту.

В другому розділі «ДОСЛІДЖЕННЯ ПРОЦЕДУР ТА МЕХАНІЗМІВ ЗАХИСТУ ІНФОРМАЦІЇ У WI-FI МЕРЕЖІ» проведено огляд алгоритмів аутентифікації в безпровідних мережах, сформульовано основні цілі та завдання аудиту комп'ютерної мережі, описано методика та засоби проведення аудиту комп'ютерної мережі, досліджено технології захисту доступу до Wi-Fi-пристроїв за допомогою засобів автентифікації, авторизації, аудиту (сервери TACACS+, RADIUS, служба Kerberos).

В третьому розділі «ДОСЛІДЖЕННЯ ТА ПРАКТИЧНА РЕАЛІЗАЦІЯ МОДЕЛІ ПРОВЕДЕННЯ АУДИТУ ЗАХИЩЕННОСТІ БЕЗПРОВІДНИХ МЕРЕЖ» описано механізм проведення аудиту захищеності безпровідних мереж, розроблено профіль захисту для мереж стандарту 802.11, досліджено логічні зв'язки в структурі механізмів захисту, наведено використання технологій захисту передачі даних та доступу до мережі Wi-Fi.

В четвертому розділі «Спеціальна частина» описано процеси встановлення та налаштовування програмного продукту Cisco Secure Access Control Server, а також конфігурування точки доступу Wi-Fi для аутентифікації через CS ACS.

В п'ятому розділі «Обґрунтування економічної ефективності» розглянуто питання розрахунку економічної ефективності і терміну окупності капітальних вкладень.

В шостому розділі «Охорона праці та безпека в надзвичайних ситуаціях» розглянуто питання охорони праці, санітарних норм і вимог до ПК, освітленості

виробничих приміщень для роботи з відеодисплейними терміналами та забезпечення безперебійного електроспоживання об’єкту при надзвичайних ситуаціях техногенного характеру.

В сьомому розділі «Екологія» описано кореляційний аналіз зв’язків в екології, а також класифікація показників екологічності виробництва.

У загальних висновках щодо дипломної роботи описано прийняті в проекті технічні рішення і організаційно-технічні заходи, які забезпечують виконання завдання на проектування; оригінальні технічні рішення, прийняті автором в процесі роботи, технічні рішення роботи, які можуть бути впроваджені; наведено рекомендації по розробці схожих систем.

В **графічній частині** представлені основні алгоритми аутентифікації, процеси аутентифікації; авторизації та аудиту на серверах RADIUS і TACACS+; порівняння основних можливостей протоколів аутентифікації; загальна структура та формування профілів захисту; схема аутентифікації користувача стандарту 802.11x; конфігурація серверу Cisco.

ВИСНОВКИ

Бездротові локальні мережі, побудовані відповідно до стандарту IEEE 802.11, уже достаньо довго використовуються як в корпоративній, так і в приватній сферах. Проте, існує серйозна проблема – забезпечення надійного захисту передачі даних в мережі.

За результатами проведеного дослідження, враховуючи особливості технології безпровідної передачі даних по радіоканалах, можна стверджувати, що ефективна система захисту інформації у WI-FI мережі повинна складатися із комплексу апаратних та програмних компонентів. Головними з них вважаються механізми, які гарантують, що дані дійсно надходять із передбачуваного джерела, а їхній несанкціонований перегляд і зміна неможливі.

Основні результати, отримані в роботі:

– проаналізовано та досліджено можливості протоколів та служб аутентифікації, авторизації та аудиту бездротових мереж;

– описано механізм проведення аудиту захищеності безпровідних мереж;

– запропоновано модель профілю захисту для мереж стандарту 802.11 з критеріями оцінки захищеності безпровідної мережі;

– протестовано можливість серверів автентифікації на забезпечення захищеності Wi-Fi мереж;

– перевірено можливість автентифікації на Wi-Fi пристроях з аудитом подій на сервері ACS.

Досягнути надійного рівня захисту інформації у Wi-Fi мережі можливо тільки при спільному використанні теоретичних та практичних результатів, отриманих в роботі.

СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

1. Харін Д.В. Технології захисту інформації в комп'ютерній мережі на базі Wi-Fi пристроїв (на основі стандарту IEEE 802.11) / Д.В. Харін.– Матеріали VI Міжнародної науково-технічної конференції молодих учених та студентів «Актуальні задачі сучасних технологій». Том 2. – Тернопіль, ТНТУ, 16-17 листопада 2017 – с. 176

АНОТАЦІЯ

Харін Д.В. Технології захисту інформації в комп'ютерній мережі на базі WI-FI пристроїв (на основі стандарту IEEE 802.11)

Дипломна робота на здобуття освітнього ступеня магістра, 123 «Комп'ютерна інженерія». – Тернопільський національний технічний університет імені Івана Пулюя, Тернопіль 2018

Дипломна робота присвячена реалізації комплексного підходу для забезпечення надійного механізму автентифікації, авторизації та аудиту в корпоративній мережі на базі Wi-Fi пристроїв фірми Cisco.

Проаналізовано архітектуру комп'ютерної мережі стандарту IEEE 802.11 та механізми доступу до середовища. Сформульовано основні етапи проведення аудиту інформаційної безпеки, проаналізовано можливості протоколів автентифікації та їх характеристики. Розглянуто сучасні можливості технологій шифрування даних в бездротових мережах; протестовано можливість серверів автентифікації на забезпечення захищеності Wi-Fi мереж. Побудовано модель сімейства профілів захисту для бездротових мереж Налаштовано програмне забезпечення для реалізації моделі захищеності, перевірено можливість автентифікації на Wi-Fi пристроях з аудитом подій на сервері ACS.

Описаних та досліджених в роботі технологій, механізмів, методів та засобів захисту є достатньо для забезпечення високого рівня безпеки бездротових мереж, та можливості організації безпечного віддаленого доступу для адміністраторів інших компаній.

Ключові слова: БЕЗДРОТОВА МЕРЕЖА, АВТЕНТИФІКАЦІЯ, АВТОРИЗАЦІЯ, АУДИТ, ШИФРУВАННЯ, KERBEROS, TACASC+, RADIUS, WPA, WEP

ANNOTATION

Kharin D.V. Technologies of information security in Wi-Fi based computer network (based on IEEE 802.11 standard)

The diploma paper for obtaining the Master's degree, 123 «Computer Engineering» – Ternopil Ivan Puluj National Technical University, Ternopil 2018

The thesis deals with the implementation of a comprehensive approach to provide a reliable mechanism for authentication, authorization and accounting in the corporate network based on Wi-Fi devices by Cisco.

The architecture of the IEEE 802.11 computer network and the mechanisms for access to the environment are analyzed. The main stages of the information security accounting are formulated, the possibilities of authentication protocols and their characteristics are analyzed. The modern possibilities of data encryption technologies in wireless networks are considered. The ability of authentication servers to secure Wi-Fi networks has been tested. The model of the family of security profiles for wireless networks was built. The software for implementation of the security model was configured; the possibility of authentication on Wi-Fi devices with the accounting of events on the ACS server was verified.

The described and studied technologies, mechanisms, methods and means of protection are sufficient to provide a high level of security of wireless networks, and the possibility of organizing secure remote access for administrators of other companies.

Keywords: AUTHENTICATION, AUTHORIZATION, ACCOUNTING, ENCRYPTION, KERBEROS, TACASC+, RADIUS, WIRELESS NETWORK, WPA, WEP