Полотай Орест Іванович, кандидат технічних наук, доцент

Зюзін Анатолій Володимирович, здобувач вищої освіти

Львівський державний університет безпеки життєдіяльності, м.Львів

**ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ WI-FI ТА WIMAX МЕРЕЖ**

Wi-Fi – це мережева технологія, яка використовує радіохвилі для забезпечення високошвидкісної передачі даних на короткі відстані. Він зазвичай використовується для забезпечення бездротового широкосмугового доступу в Інтернет для різноманітних пристроїв.

WiMAX (World Interoperability for Microwave Access), є стандартом, заснованим на технології широкосмугового бездротового доступу IEEE 802.16 для міської зони, і це стандарт повітряного інтерфейсу для мікрохвильового та міліметрового діапазону.

Основні вразливості Wi-Fi ТА WIMAX мереж наступні:

Використання SSID - (назва бездротової мережі) і паролів за замовчуванням. Точки доступу Wi-Fi постачаються зі стандартним SSID і паролем, які потрібно змінити, але дуже часто ці паролі за замовчуванням залишаються на місці. Це дозволяє зловмиснику легко ввійти в систему та взяти під контроль маршрутизатор, змінити налаштування, завантажити шкідливі сценарії або навіть змінити DNS-сервер, щоб увесь трафік спрямовуватися на IP-адресу, що належить зловмиснику.

Перехоплення пакетів. Перехоплення незашифрованого трафіку, коли точки доступу Wi-Fi взагалі не шифрують трафік. Хакери можуть використовувати сніфери пакетів для перехоплення трафіку в незашифрованих мережах Wi-Fi. Перехоплення пакетів є однією з найпоширеніших бездротових атак.

Атака глушіння. Глушіння як атака, що “досягається шляхом введення джерела шуму, достатньо сильного, щоб значно зменшити пропускну здатність каналу”, таку атаку глушіння зробити неважко. Можна запобігти атаці глушіння, збільшуючи потужність сигналів або збільшуючи смугу пропускання сигналів. Крім того, оскільки за допомогою обладнання для моніторингу радіочастоти, легко виявити перешкоди, а джерела перешкод легко виявити за допомогою засобів радіопеленгації.

Скремблююча атака. Скремблювання є різновидом заглушення, але лише на короткі проміжки часу та націлено на конкретні кадри WiMAX або частини кадрів на рівні PHY. Зловмисники можуть вибірково шифрувати контрольну інформацію, щоб вплинути на нормальну роботу мережі.

Атака водних тортур. Загальна загроза для WiMAX виникає внаслідок атаки водних тортур, під час якої зловмисник надсилає серію кадрів, щоб розрядити акумулятор приймача. Крім того, зловмисник із правильно розміщеним радіочастотним приймачем може переривати повідомлення, надіслані через бездротовий зв’язок, і тому потрібен механізм безпеки в конструкції.

Аналізуючи безпровідні мережі, виявлено ряд недоліків, серед яких: є нехтування безпекою в публічних місцях, коли у точках доступу, які є загальнодоступними, відстутні протоколи захисту бездротової мережі або застарілі протоколи захисту WEP та WPA, які підлягають зміні на більш новіші та безпечніші WPA2 та WPA3.

**Література**

1. Belej O., Nestor N., Panchak S., Polotai O. Developing a Model of Cloud Computing Protection System for the Internet of Things. International Conference on the Perspective Technologies and Methods in MEMS Design, MEMSTECH 2020. 2020. Article ID 9109456. P. 53–58.
2. Belej O., Nestor N., Sadeckii J., Polotai O.I. Features of Application of Data Transmission Protocols in Wireless Networks of Sensors. 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT 2019. Proceedings. 2019. Article ID 8847878. P. 317–322.
3. Базилевич В. М. Аналіз методів захисту від кіберзагроз в бездротових мережах стандарту IEEE 802.11 // Захист інформації. - 2017. - Т. 19.
4. Джон Росс. Wi-Fi. Бездротові мережі. Конфігурування. Використання – 2007. -320c.
5. Булашенко А. В., Гордієнко Т.В. Порівняльний аналіз безпровідних технологій 4G// ІІ Всеукраїнська науково-методична конференція, м. Шостка, 20 квітня 2017 року. – Суми: Сумський державний Університет. – С. 177 – 181.