РОЗРОБКА СИСТЕМИ УПРАВЛІННЯ КІБЕРІНЦИДЕНТАМИ В МЕРЕЖАХ LTE

Барсуков А. І., Гук А. С.
Харківський національний університет радіоелектроніки, Харків, Україна

Архітектура мережі LTE розроблена таким чином, щоб забезпечити підтримку пакетного трафіку з так званою «гладкою» («безшовною», seamless) мобільністю, мінімальними затримками доставки пакетів і високими показниками якості обслуговування. Тому мережі LTE стали однією із ключових технологій, що дозволяють абонентам отримувати, а бізнесу запроваджувати принципово нові сервіси для Інтернету речей (IoT), M2M, V2X тощо. В цих умовах (ріст абонентської бази, розгортання нових мереж, удосконалення технологічних рішень тощо), не зважаючи на всі існуючі переваги, в LTE є також ряд недоліків, серед яких предметом розгляду даної наукової праці є вразливості від кібератак.

Метою роботи було проведення досліджень кіберінцидентів, які можуть виникнути в стільникових мережах LTE, щоб їх класифікувати та вибрати найбільш відповідні механізми захисту. Оскільки технологія LTE збільшує швидкість шкідливого програмного забезпечення (оскільки цей стандарт сам по собі є високошвидкісним), необхідно запровадити систему управління кіберінцидентами. Тому було проведено дослідження традиційної архітектури комп'ютерної системи реагування на інциденти, щоб виявити слабкі місця та напрямки вдосконалення для впровадження в архітектуру мобільної мережі. Архітектура стільникових мереж була покращена за рахунок введення додаткових функцій безпеки та послідовного збору інформації про кіберінциденти в стільниковій мережі, визначення типів кібератак, об'єктів та масштабів впливу, реагування на кібератаки та зберігання інформації про кіберінциденти в спеціалізована база даних. Запропоноване рішення дозволяє здійснювати моніторинг кібербезпеки в режимі реального часу та підвищує її рівень.

Також в роботі був запропонований варіант реалізації системи управління кіберінциентами на базі обладнання netForensics. Як показали проведені дослідження, служба реагування на комп'ютерні інциденти (CERT) та система netForensics знижують рівень загроз інформаційній безпеці в мережах LTE. CERT здійснює збір, зберігання і обробку статистичних даних, пов'язаних з поширенням шкідливих програм і мережевих атак. До компетенції служби входить обробка комп'ютерних інцидентів з метою їх виявлення і нейтралізації.

Список літератури

1. І.А. Пількевич, В.І. Котков, Н.М. Лобанчикова, І.І. Сугоняк. «Модель підсистеми моніторингу інцидентів безпеки інформації в інформаційних системах організацій»

2. LTE.Специфіка мереж. URL: http://Rohdeschwarz.ru/tech.