Якщо узагальнити, то структура моделі що розробляється має такий вид:

- Естетика:
  - зображення;
  - роздільна здатність сторінки;
  - колір;
  - акцент.
- Зручність використання:
  - послідовність;
  - навігація;
  - анотація.
- Мультимедіа:
  - підтримка плагіна;
  - мультимедійні компоненти;
  - один медіа на одній сторінці;
  - використання ескізів.
- Вміст:
  - дошка оголошень;
  - інформаційний довідник;
  - пошукова система;
  - уникнення автоматичного оновлення.
- Репутація:
  - відгук клієнтів;
  - веб-трафік;
  - домене ім’я;
  - публічна інформація.

Тут естетика, зручність використання, мультимедіа, вміст та репутація це атрибути якості, а те що вони вміщують це характеристики. До того ж характеристики складаються з метрик.

Під час роботи булу проаналізовано сучасні підходи до оцінок якості веб-сайтів, структуровано та описано метрики якості веб-сайту, виконано налаштування методики оцінки якості веб-сайту закладу вищої освіти, проведена оцінка якості веб-сайту ДонНУ імені Василя Стуса та були виявлені його недоліки та переваги.

Однак, оцінка проводилась людиною на основі суб’єктивного сприйняття метрик якості. Тому подальша робота над цією темою полягає в тому щоб розробите автоматичну систему оцінки якості сайтів, з можливістю адаптувати її під різні види веб-сайтів.

УДК 544.421.43:544.421.032.76:544.431.122.2:547.541:547.636.3

ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА СТУПЕНІ ЗАХИЩЕНОСТІ МЕРЕЖ WI-FI ТА LI-FI

С. П. Сергієнко, В. В. Васянович

Бездротові мережі вже використовуються практично у всіх сферах діяльності. Актуальність забезпечення безпеки бездротової мережі обумовлена тим, що якщо в провідних мережах зловмисник повинен спочатку отримати фізичний доступ до кабельної системі або кінцевим пристроям, то в бездротових мережах для отримання доступу достатньо звичайного приймача, встановленого в радіусі дії мережі.

Незважаючи на відмінності в реалізації зв'язку, підхід до безпеки бездротових мереж і їх дротових аналогів ідентичний. Але при реалізації методів захисту інформації в

бездротових мережах більше уваги приділяється вимогам до забезпечення конфіденційності і цілісності переданих даних, до перевірки автентичності бездротових клієнтів і точок доступу.

Об'єктом дослідження є бездротові мережі wi-fi і li-fi.

Wi-Fi-технологія бездротового локальної мережі з пристроями на основі стандартів IEEE 802.11. Логотип Wi-Fi є товарним знаком Wi-Fi Alliance. Під абревіатурою Wi-Fi (від англійського словосполучення Wireless Fidelity, яке можна дослівно перекласти як «бездротова точність») в даний час розвивається ціле сімейство стандартів передачі цифрових потоків даних по радіоканалах.

Li-Fi (Light Fidelity) досить молода технологія. Її родоначальником вважається німецький фізик Гаральд Хаас, який в 2011 році в якості роутера використовував світлодіодну лампу. У лабораторних умовах він досяг швидкості передачі в 224 Гб/с.

Технології Li-Fi і Wi-Fi засновані на схожих протоколах IEEE 802.11. Однак Li-Fi використовує електромагнітні хвилі видимого світла, в той час як Wi-Fi – радіохвилі. Завдяки цьому, перша технологія отримує перевагу з точки зору більш широкої смуги пропускання.

Стандарт IEEE 802.15.7 визначає для Li-Fi фізичний рівень мережевої моделі OSI PHY (Physical layer), а також рівень управління доступом до середовища MAC-адреси (Media Access Control).

Таким чином, технологія Li-Fi в порівнянні з Wi-Fi:

1. Використовує хвилі видимого світла замість радіохвиль.
2. Має більш широку смугу пропускання.
3. Має велику швидкість передачі даних.
4. Більш інформаційно безпечна
5. Має меншу зону покриття.
6. Сприяє оптимізації енерговитрат, об'єднуючи систему освітлення та хот-споти.
7. Li-Fi-пристрої не створюють один одному перешкоди в мережі.

Виявлено, що безпечність бездротової мережі wi-fi залежить від виконаного налаштування, так як можуть бути відкриті мережі, які можуть небезпечними в плані захисту даних користувачів, так і налаштовані мережі.

Виявлено, що безпечність мережі li-fi залежить від області застосування, так як ця мережа може бути сконцентрована на конкретні пристрої, в той час коли wi-fi працює в певній області і зловмисник може потрапити в мережу навіть за межами офісу, але мережа li-fi також може бути небезпечною в громадських місцях з відкритим доступом.

Література

1. Светодиодная точка доступа к Интернету – Li-Fi технология. URL : https://artillum.ru/lighting-devices/123-light-fidelity-li-fi.html.
2. Преспективы развития LI-FI. URL : https://moluch.ru/conf/tech/archive/165/9905/.
3. Технология Li-Fi: характеристика технологии, сравнение с Wi-Fi и перспективы развития. URL : http://1234g.ru/novosti/li-fi.
4. Технология li-fi. Устройство и работа. URL : https://electrosam.ru/glavnaja/slabotochnye-seti/tekhnologiia-li-fi/.
5. Информационная безопасность в сетях Wi-Fi. URL : https://www.bibliofond.ru/view.aspx?id=16209.
6. Уязвимости WI-FI [Електронний ресурс] – Режим доступу до ресурсу: https://allbest.ru/k-3c0a65625a2ad69b4c43b89521216c27.html.
7. Защита беспроводных сетей. URL : http://cinref.ru/razdel/04650raznoe/20/408681.htm.
8. Безопасность в сетях WiFi. WEP, WPA, WPA2 шифрование. URL : https://www.getwifi.ru/psecurity.html.
9. Технологии защиты информации в Wi-Fi сетях. URL : https://www.bibliofond.ru/detail.aspx?id=725189