АНАЛІЗ ЗАГРОЗ ОСНОВНИХ КОМПОНЕНТІВ IOT

Піхота К. В.
Науковий керівник: **Кононова І.В.**
Інститут телекомунікаційних систем,
КПІ ім. Ігоря Сікорського, Україна
E-mail: pihotka19.11@gmail.com

На сьогоднішній день прилади і системи IoT уже неодноразово зазнавали атак, тому забезпечення їх захисту є одним з ключових завдань.

Розглядаючи основні компоненти IoT можна виділити такі технології: RFID, NFC та WSNs. Най вразливішою з них є NFC (загроза прослуховування та атаки відмови в обслуговуванні(DoS)). В RFID-системі виникають загрози десинхронізації, витік інформації та повторення атак. WSNs є вразливими до різних видів атак майже на всіх рівнях стеку протоколів.

Для захисту від втручання в код програми та підміни показників датчиків слід використовувати технологію блокчейн. Блокчейн дозволить відстежувати вимірювання даних сенсора та запобігання дублюванню шкідливими даними, а також забезпечить автентифікацію та безпечну передачу даних.

ANALYSIS OF THREATS TO THE MAIN COMPONENTS OF THE IoT

Pikhota K.V.
Scientific adviser: **Kononova I.V.**
Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: pihotka19.11@gmail.com

Today, the devices and systems of the IoT have already been attacked many times, so ensuring their protection is one of the key tasks.

Considering the main components of the IoT, the following technologies can be distinguished: RFID, NFC and WSNs. The most vulnerable of these is NFC (listening threat and Denial of Service (DoS) attack). The RFID system has threats of desynchronization, information leakage, and repetition of attacks. WSNs are vulnerable to various types of attacks at almost all levels of the protocol stack.

Blockchain technology should be used to protect against program code interference and sensor offenses. Blockchain will allow to monitor sensor data measurement and avoid harmful data duplication, as well as provide authentication and secure data transmission.