ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

М.П. ТРЕМБОВЕЦЬКИЙ
М.В. ГЛАДКА,
І.І. БОРИСЕНКО
Г.М. ТЕРЕЩУК

ЗАХИСТ ІНФОРМАЦІЇ

В ІНТЕРНЕТІ РЕЧЕЙ

Навчальний посібник

Київ-2025

Рецензенти:

д.т.н., професор, професор кафедри кібербезпеки та захисту інформації Толюпа Сергій Васильович;

к.т.н., доц., професор кафедри інженерії програмного забезпечення ФКНТ, ДНП ДУ «Київський авіаційний інститут» Гізун Андрій Іванович

Рекомендовано до публікації кафедрою інформаційних систем та технологій, протокол №02_25/26 від «11» вересня 2025 р.

Рекомендовано до публікації Вченою радою факультету інформаційних технологій, протокол прот №2/25-26 від 22 жовтня 2025

М.П. Трембовецький, М.В. Гладка, І.І. Борисенко, Г.М. Терещук

Захист інформації в інтернеті речей [Електронний ресурс]: навчальний посібник для здобувачів освіти у вищих навчальних закладах / М.П. Трембовецький, М.В. Гладка, І.І. Борисенко, Г.М. Терещук – К.: Факультет інформаційних технологій КНУ імені Тараса Шевченка, 2025. – 153 с.

Викладено основні положення та понятійно-термінологічний апарат захисту інформації в інтернеті речей та його особливості, в тому числі для IoT в хмарному середовищі.

Посібник розраховано на здобувачів вищої освіти, які навчаються за напрямами: інформаційні технології, комп'ютерні науки, кібербезпека тощо та фахівців, які цікавляться подібними питаннями. Зокрема, для здобувачів ОС «Бакалавр» вищих навчальних закладів, що вивчають курс «Захист інформації в інтернеті речей».

Публікується в авторській редакції.

Електронна версія цього видання опублікована на сайті кафедри інформаційних систем та технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка за адресою: https://www.ist.fit.knu.ua/

ЗМІСТ

ВСТУП

Захист інформації в IoT на сьогодні є важливим і актуальним завданням як з точки зору наукових досліджень, так і реалізації їх на практиці. Важливість безпеки інформаційних систем та мереж напряму визначається залежністю більшості процесів менеджменту підприємствами, установами та організаціями від їх інформаційних ресурсів, зокрема IoT.

В даному посібнику розглядаються ключові аспекти захисту інформації в IoT-системах та мережах, в тому числі і таких, що побудовані на базі хмарного середовища, базові поняття організаційного та криптографічного захисту.

Основні аспекти захисту інформації включають політику безпеки, організаційну та технічну практику. Перша група заходів безпеки в основному відноситься до політик і процедур, які повинні бути прописані в організаціях, щоб допомогти забезпечити хороший рівень кібербезпеки, особливо там, де є рішення IoT.

Крім того, тут важливі і юридичні питання конфіденційності виробників, які повинні гарантувати, що їхні рішення не порушують правила конфіденційності та оператори, яким слід звертати увагу до конфіденційності пов’язаних із цим ризиків та інформувати про те, як використовувати пристрої IoT без розкриття особистої інформації користувачів.

Окрім запровадження політик та організаційних підходів, безпеку необхідно забезпечувати також за допомогою відповідних технічних можливостей рішень IoT та середовища їх розгортання.

– Технічні практики поділяються на десять основних категорій:

– Керування довірою та доброчесністю – включає заходи, спрямовані на забезпечення цілісності та надійності даних і пристроїв.

– Хмарна безпека – охоплює механізми захисту, що стосуються різних аспектів хмарних обчислень.

– Безперервність роботи та відновлення – передбачає створення, тестування та оновлення планів для забезпечення стійкості та безперервності бізнес-процесів у разі виникнення інцидентів.

– Безпека між машинами – включає зберігання ключів, використання шифрування, перевірку введених даних і захист у процесі міжмашинної комунікації.

– Захист даних – спрямований на охорону конфіденційної інформації на різних рівнях організації та контроль доступу до неї.

– Оновлення програмного забезпечення та прошивки – передбачають перевірку, тестування й впровадження виправлень безпеки.

– Контроль доступу – включає механізми управління віддаленим доступом, автентифікацією, правами користувачів, обліковими записами та фізичним доступом до пристроїв.

– Мережі, протоколи та шифрування – охоплюють заходи, що забезпечують захищеність комунікацій завдяки правильному впровадженню протоколів, використанню шифрування та сегментації мережі.

– Моніторинг і аудит – передбачають відстеження мережевого трафіку та доступності ресурсів, збирання журналів подій і здійснення перевірок.

– Керування конфігурацією – включає забезпечення безпечних налаштувань, контроль змін конфігурацій, підвищення захищеності пристроїв та перевірку резервних копій.

Вище наведені технічні заходи є завершальним елементом системи, що дозволяє компаніям, які працюють з IoT, підвищувати рівень захищеності.

Саме ці питання в тій чи іншій мірі розкриті в даному посібнику, а їх вивчення дозволить майбутнім фахівцям зрозуміти основні підходи до забезпечення безпеки в IoT та застосовувати їх на практиці.