– Bluetooth або Wi-Fi модуль для дистанційного управління мобільною платформою.

Звичайно, цей перелік можна покращувати, але тим самим піднімаючи вартість компонентів. Саме з такого набору компонентів можна зібрати мобільну платформу, зображену на рис.1.

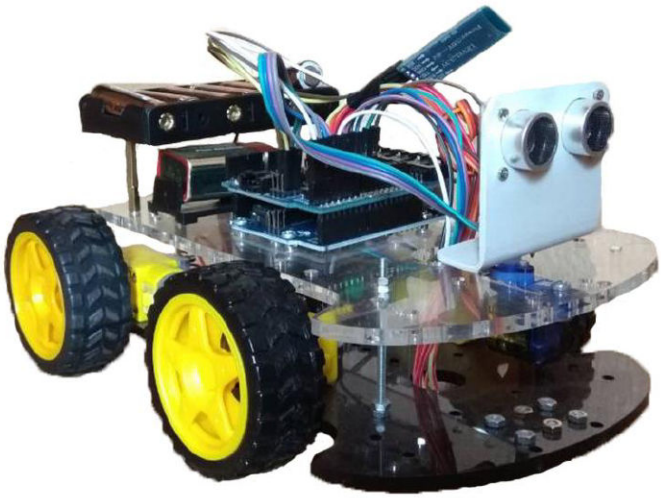

Рис.1 Мобільна платформа

Таким чином, результатами роботи є: створена мобільна платформа з програмним забезпеченням для мікроконтролера та розроблений додаток для дистанційного управління нею, що є легким для будь-якого користувача.

Розроблена модель може бути в майбутньому удосконалена новими елементами та виконувати нові, більш складні завдання.

УДК 004.056

МЕХАНІЗМ КОНТРОЛЮ ЦІЛІСНОСТІ ДАНИХ В ЛОКАЛЬНИХ МЕРЕЖАХ

к..т.н., доцент Дегтярьова Л.М., Сідокур О.О.

Полтавський національний технічний університет
імені Юрія Кондратюка, Полтава
E-mail: ladegt12@gmail.com

Сучасні обчислювальні системи стали набагато простіше в експлуатації, і тому велика кількість нових користувачів одержує доступ до інформаційного простору. Мережеві технології об'єднали окремі машини в локальні мережі, що спільно використовують загальні ресурси, а застосування технології «клієнт-сервер» перетворило такі мережі в розподілені обчислювальні середовища, тому безпека мережі і захист даних починають залежати від безпеки кожного її компонента, забезпечуючи вимоги конфіденційності, цілісності та доступності.

Контроль цілісності файлових об'єктів являє собою самостійну задачу захисту інформації. При цьому основу механізмів контролю цілісності файлових об'єктів представляє перевірка відповідності контрольованого об'єкта еталонному зразку. Для контролю можуть використовуватися контрольні суми і ряд інших ознак, наприклад, дата останньої модифікації об'єкта і т.д. При необхідності утримувати контрольований об'єкт в категорії «еталон», механізми контролю можуть здійснювати автоматичне або автоматизоване відновлення несанкціоновано зміненого файлового об'єкта з еталонної копії. Система захисту повинна перехоплювати функцію читання файлу, запускати процедуру контролю і потім (при необхідності, вже після відновлення файлу з еталонної копії) видавати цю функцію на обробку в ядро операційної системи. Але якщо контроль цілісності реалізується програмно, то виникає проблема контролю цілісності і коректності функціонування власне контролюючої програми, тому в загальному випадку здійснення контролю реалізується апаратною частиною.

Література

1. Нормативний документ "Системи технічного захисту інформації: Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу". — Київ. 1999. — 61 с.

2. Богуш В. М., Юдін О. К. «Інформаційна безпека держави». — К.: «МК-Прес», 2005. — 432с.

3. Богуш В. М., Кривуца В. Г., Кудін А. М., «Інформаційна безпека: Термінологічний навчальний довідник» За ред. Кривуци В. Г. — Київ. 2004. — 508 с.

4. Бирюков А.А. Информационная безопасность. Защита и нападение. — М.: ДМК Пресс, 2012. — 474 с.

5. Джеймс С. Фостер. Защита от взлома. Сокеты, shell-код, эксплойты. — М.: ДМК Пресс, 2006. — 783 с.

УДК 681.321

КІБЕРЗАХИСТ ЗАБЕЗПЕЧЕННЯ ДОСТУПУ ДО ДАНИХ ТА СИСТЕМ

Ромашко І.В., старший викладач кафедри

Полтавський національний технічний університет
імені Юрія Кондратюка, Полтава

Існують сфери, де від доступності систем і даних буквально залежить життя і смерть, тому в таких сферах застосовуються найвищі стандарти доступності.

У доповіді розглянуто різні способи досягнення цільових показників доступності в організаціях. Наприклад, резервне копіювання дозволяє зберегти доступність за рахунок резервних і додаткових компонентів комп'ютерних та мережевих систем. Резервування охоплює як апаратні (дискові накопичувачі,