УДК 004.738.5:004.77

Висоцький С.В., Висоцька І.П., Куницька С.Ю.
Черкаський державний технологічний університет

Методи захисту даних при розробці охоронних систем

В даному матеріалі розглядається охоронна система, яка розроблена на базі мікроконтролера Arduino. Охоронна сигналізація складається з 4-х основних частин: модуль сигналізації, де буде виконуватися охорона; серверна частина системи, яка буде виконувати роль управляючого даної сигналізації; мобільний додаток, за допомогою якого користувачі будуть отримувати інформацію про змін стану охоронної сигналізації; WEB-додаток, для відображенні звітів по роботі системи. Всі розроблені частини системи є взаємо-незалежними. Тобто сигналізація може працювати без серверу,але при цьому вона втрачає ряд важливих функцій.

Розглянемо основну частину розробленої системи – це модуль охоронної сигналізації. Даний модуль розроблений таким чином, що він не містить в собі функцій зміни його налаштувань. Тобто змінити принцип його роботи віддалено не можливо. Також даний модуль неможливо налаштувати без використання пристроїв для його програмування. Тобто, якщо дана система охорони працює, ніхто, крім інженера, який виконує підтримку даного пристрою, не може змінити навмисно стан роботи системи. Для уникнення проблем із живленням та проблем із інтернет-з'єднанням було використано батарею на 10000 мА-г та модуль для роботи з 3G інтернетом.

Так як охоронна сигналізація працює з сервером за допомогою його API, потрібно також розглянути методи захисту доступу до серверу. Після запуску охоронної системи виконується ідентифікація пристрою на стороні серверу. Кожна охоронна система має в собі GPS-датчик, який знаходиться в модулі для роботи з 3G інтернетом, має унікальний ідентифікатор плати Arduino. При спробі активувати роботу API, система передає всі ці дані на сервер, та у разі, якщо сервер дозволяє роботу даній частині системи, виконується створення робочого токену, який представляє собою «візу» для роботи з API. Сервер також перевіряє дозволений діапазон IP-адрес, з яких може виконуватися активація пристрою. Усі наступні дії, які буде виконувати охоронна система (відправка інформації про стан системи, про зміну стану системи та інше), буде виконуватися тільки з використанням токену доступу. В іншому разі доступ до API буде заблокований для даного пристрою.

На мережевому рівні використовується базові методи захисту інформації: використовується захищене з'єднання HTTPS з використанням SSL сертифікату.

Мобільні додатки, в даній системі, використовуються тільки для інформування користувача про зміни стану системи та не потребують захисту інформації, так як для відправлення PUSH-інформування для користувачів, використовується унікальний ідентифікатор мобільного пристрою. Таким чином ми можемо бути впевнені, що дане повідомлення буде доставлено потрібному користувачеві.

Список використаних джерел

1. *Петін, В. А. Arduino и Raspberry Pi в проектах Internet of Things / В.А. Петін. – К.: БХВ-Петербург, 2016. – 320с.*
2. *Иго Т., Arduino, датчики і мережі для зв'язку пристроїв / Т. Иго – К.: БХВ-Петербург, 2015. – 544с.*
3. *Кантелон М., Node.js в дії / М. Кантелон – К.: БХВ-Петербург, 2014. – 548с.*