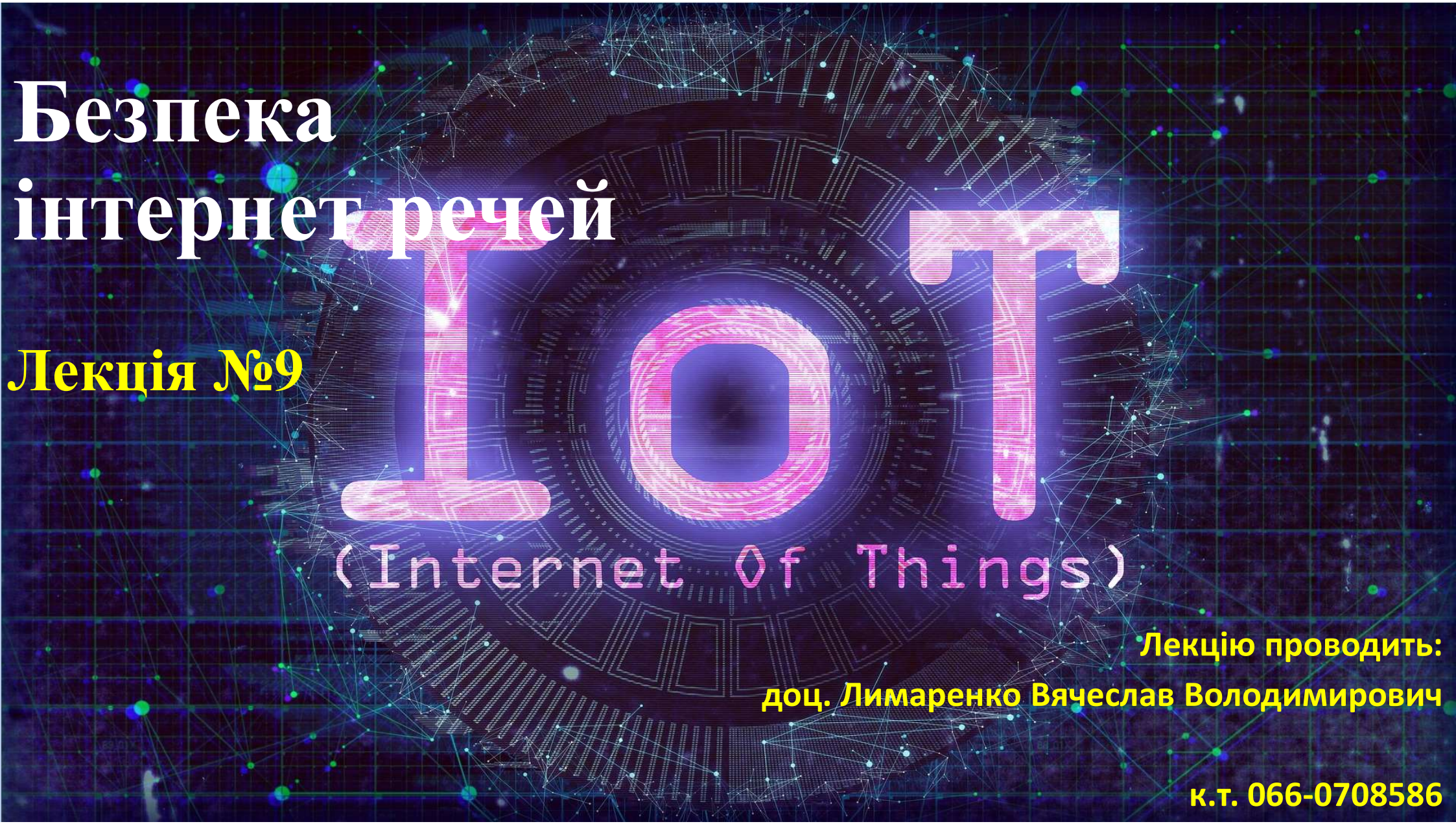
Безпека інтернет речей

Лекція №9



Лекцію проводить:
доц. Лимаренко Вячеслав Володимирович
к.т. 066-0708586

Програмне забезпечення IoT

Програмне забезпечення IoT:

- IoT платформа (спеціалізоване);
- засоби розробки (спеціалізовані/загального використання);
- ПЗ забезпечення безпеки (спеціалізовані/загального використання).

IoT платформа – програмне забезпечення, призначене для підключення інтернет речей (давачів, контролерів та інших пристроїв) до хмари та віддаленого доступу до них.

Являє собою проміжний рівень між апаратним рівнем (рівнем сенсорів) та прикладним.

Програмне забезпечення IoT. IoT платформа. Історія створення та розвитку

З моменту появи терміна «Інтернет речей» мережі, що складаються з великої кількості пристроїв, що спілкуються між собою, швидко розвиваються. Внаслідок цього, IoT (Internet of Things) стає однією з основних технологій у суспільстві. З погляду технологічних та технічних аспектів розвитку IoT в даний час існує чіткий поділ між апаратними та програмними платформами для підключення пристроїв, причому більшість постачальників пропонують саме програмні IoT платформи.

Платформи IoT забезпечують безшовну інтеграцію різних апаратних засобів, використовуючи протоколи зв'язку, застосовуючи різні типи топології (пряме підключення або шлюз) та використовуючи SDK у разі потреби, тощо.

Використовуючи інтерфейси інтеграції з північним кордоном, що надаються платформою, можна передавати зібрані дані IoT в певні системи аналізу та зберігання даних, а також передавати дані на підключені пристрої (конфігурація, повідомлення) або між ними (елементи управління, події), використовуючи різні види користувацьких застосунків.

Найпопулярнішими програмними IoT платформами є: Microsoft Azure IoT, Amazon Web Services (AWS) IoT, Google Cloud, ThingWorx IoT, IBM Watson, Artik від Samsung Electronics, Cisco IoT Cloud Connect, Salesforce IoT Cloud та багато інших.

IoT платформа. Технічні характеристики

Критеріями відмінності програмних IoT платформ одна від одної є:

- масштабованість – кількість кінцевих пристроїв, які можуть підключатися до платформи, включаючи ефективне балансування навантаження серверів;
- простота використання – гнучкість API інтеграції та простота управління вихідним кодом;
- варіанти розгортання – публічна або приватна хмара;
- безпека – захист даних шляхом шифрування, контролю доступу користувачів тощо;
- база даних – варіант зберігання даних, одержуваних із пристроїв, наявність гібридних хмарних баз даних тощо.

Серед протоколів, що використовуються платформами IoT, найпопулярнішими є Constrained Application Protocol (CoAP), Message Queue Telemetry Transport (MQTT), DirectDraw Surface (DDS), eXtensible Messaging and Presence Protocol (XMPP) и HyperText Transfer Protocol Secure (HTTP/HTTPS).

Більшість сучасних програмних плат IoT підтримують аналітику в реальному часі – агрегування потоків, фільтрацію та ін. (наприклад, Storm, Samza), пакетну – операції з накопиченим набором даних (наприклад, Hadoop, Spark) та інтерактивну аналітику даних – багаторазовий дослідницький аналіз як потокових, так і пакетних даних (Spark MLLIB). Також існує прогностичний метод аналітики, що базується на різних способах статистичного та машинного навчання.

IoT платформа. Кейси застосування

IoT платформи використовуються постачальниками та виробниками розумних пристроїв для оснащення своїх продуктів функціями дистанційного керування, моніторингу в режимі реального часу, настроювання попереджень та повідомлень, інтеграції зі смартфонами та іншими пристроями.

Також широкою сферою застосування IoT платформ є оптимізація роботи компаній у промисловому секторі (так званий IIoT) за допомогою інтелектуального обслуговування обладнання, збору даних із сенсорів та їх аналізу у реальному часі. Крім того, IoT платформи використовуються при створенні систем розумного міста для надання різних послуг приватним і державним компаніям, кінцевим клієнтам.

Серед таких послуг можна відзначити забезпечення безпеки на вулицях міста та в будинках, моніторинг екологічної ситуації, інтелектуальний моніторинг мереж та ін.

IoT платформа. Завдання

- Збір інформації
- Інтеграція пристроїв
- Аналітика реального часу
- Розширення застосунків та процесів.

Збір інформації – це програмне забезпечення керує зондуванням, вимірами, фільтрацією даних, безпекою даних та агрегацією даних. Воно використовує певні протоколи, щоб допомогти сенсорам підключатися до мереж у реальному часі. Потім воно збирає дані з декількох пристроїв і розповсюджує їх відповідно до налаштувань. ПЗ також працює у зворотному порядку, розподіляючи дані по пристроях. Зрештою, система передає всі зібрані дані на центральний сервер.

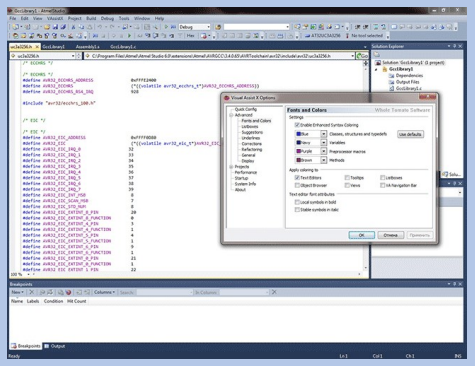
Інтеграція пристроїв – програмне забезпечення, що підтримує інтеграцію, пов'язує (залежні відносини) всі системні пристрої створення тіла системи IoT. Це забезпечує необхідну співпрацю та стабільну мережу між пристроями. Ці програми є визначальною програмною технологією мережі IoT, оскільки це не система IoT. Вони керують різними програмами, протоколами та обмеженнями кожного пристрою для забезпечення зв'язку.

IoT платформа. Завдання

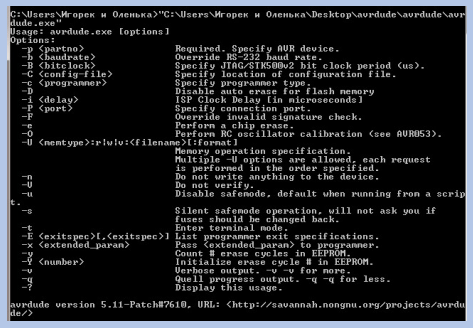
Аналітика у реальному часі – ці програми беруть дані з різних пристроїв і перетворять їх на життєздатні дії або чіткі шаблони для людського аналізу. Вони аналізують інформацію на основі різних налаштувань та конструкцій, щоб виконувати завдання, пов'язані з автоматизацією, або надавати потрібні дані.

Розширення застосунків та процесів – ці програми розширюють сферу застосування існуючих систем та програмного забезпечення, забезпечуючи ширшу та ефективнішу систему. Вони інтегрують попередньо визначені пристрої для певних цілей, таких як надання доступу до певних мобільних пристроїв або інструментів розробки. Вони підтримують підвищення продуктивності та більш точний збір даних.

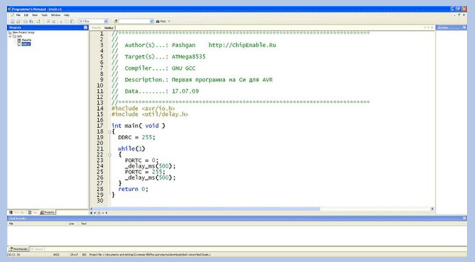
Програмне забезпечення IoT. Засоби розробки. Програми для мікроконтролерів



Atmel Studio – інтегроване середовище розробки (IDE) від компанії Atmel для розробки програм під мікроконтролери ARM Cortex-M та AVR. Freeware

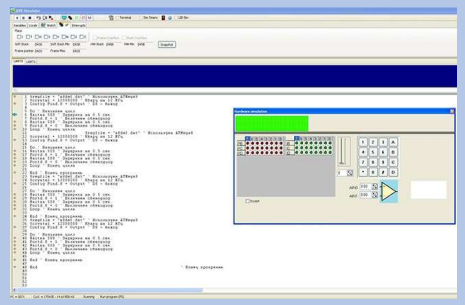


AVRDUDE – консольна програма для зчитування, зміни та запису вмісту пам'яті мікроконтролерів архітектури AVR, що застосовує технологію внутрішньосхемного програмування. Freeware

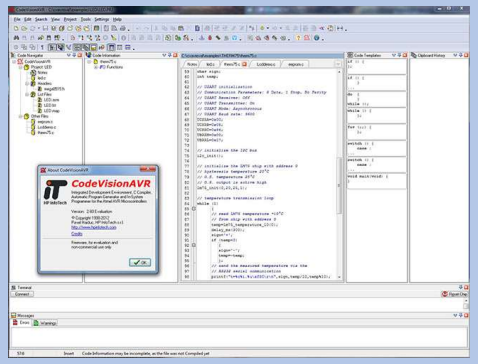


WinAVR – могутнє середовище розробки з відкритим вихідним кодом, створене з метою написання програм для мікроконтролерів серії AVR від компанії Atmel. Freeware

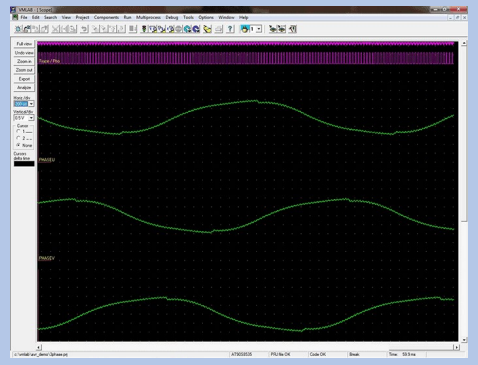
BASCOM-AVR – середовище розробки програмного коду для мікроконтролерів серії AVR компанії Atmel мовою, подібною до стандартного Бейсика. Freeware



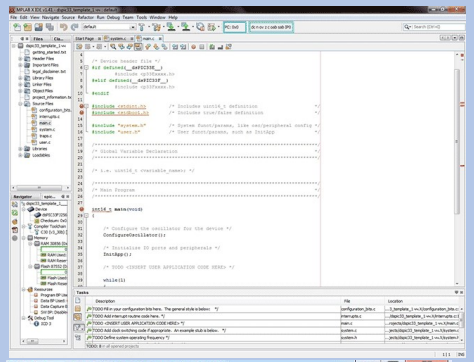
CodeVisionAVR – IDE для МК AVR. З основних переваг CodeVisionAVR можна відзначити те, що він не дуже складний для самостійного освоєння, підтримує все численне сімейство мікроконтролерів AVR, формує ємний та результативний програмний код. Платна



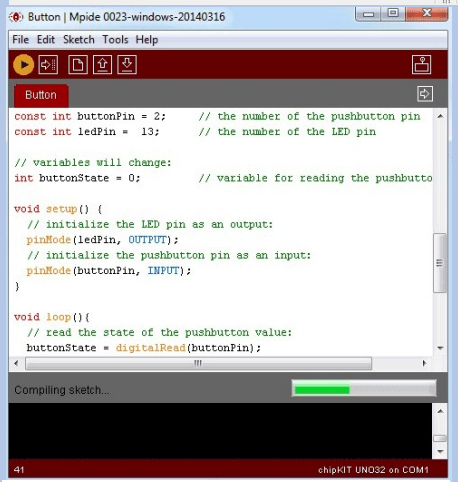
VMLAB – інструмент для розробки та налагодження програмного коду, а також моделювання роботи радіотехнічних пристроїв на базі мікроконтроллерів AVR. Freeware



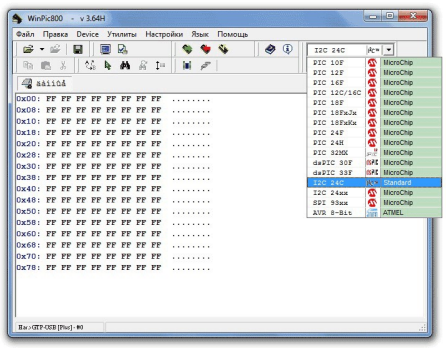
Програмне забезпечення IoT. Засоби розробки. Програми для мікроконтролерів



MPLAB – єдине безкоштовне інтегроване середовище розробки для контролерів виробництва Microchip. Freeware

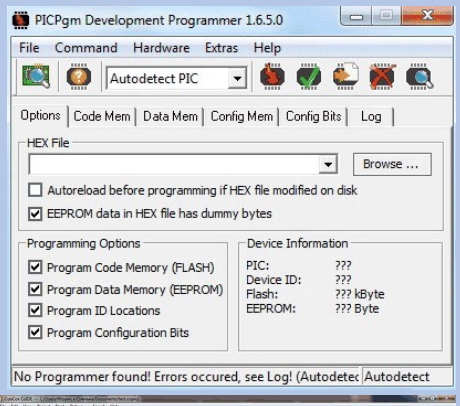


MPIDE – середовище розробки, виконане на базі відкритої системи Arduino IDE та призначене спеціально для контролерів PIC32 від компанії Microchip Technology.

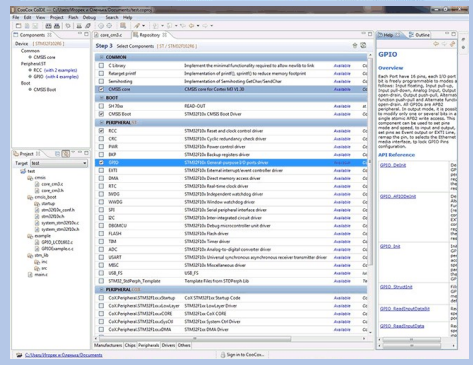


WinPic800 – невеликий, але ефективний безкоштовний програмний пакет для прошивки PIC-мікроконтролерів різних серій.

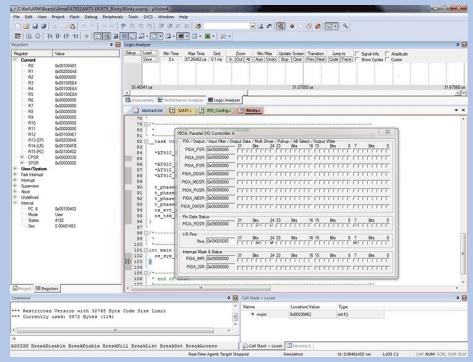
PICPgm – просте програмне забезпечення для прошивки PIC-мікроконтролерів, що відрізняється стабільністю, якістю та швидкістю програмування. Freeware



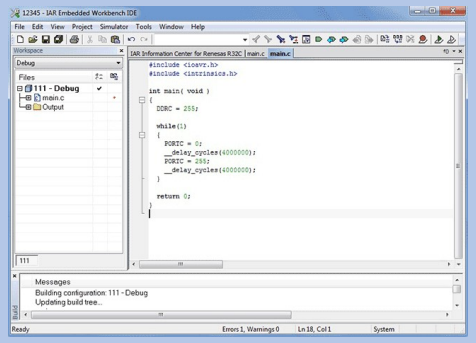
CooCox CoIDE – безкоштовне високоінтегроване програмне середовище, призначене для розробки коду мікроконтролерів архітектури ARM та ін.



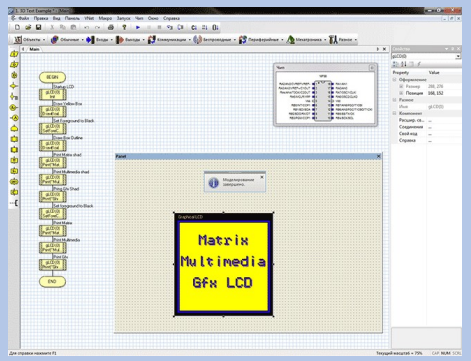
Keil uVision – середовище розробки, що є набором утиліт для виконання повного комплексу заходів щодо написання ПЗ для МК різних сімейств. Платна



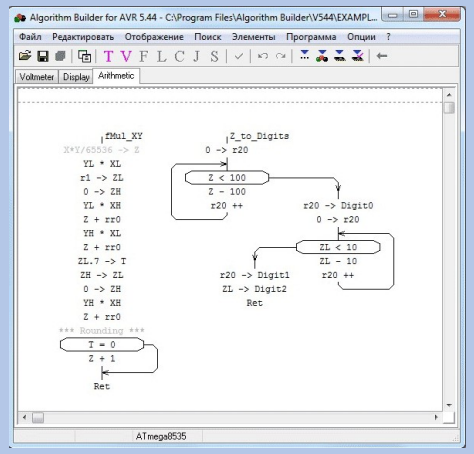
Програмне забезпечення IoT. Засоби розробки. Програми для мікроконтролерів



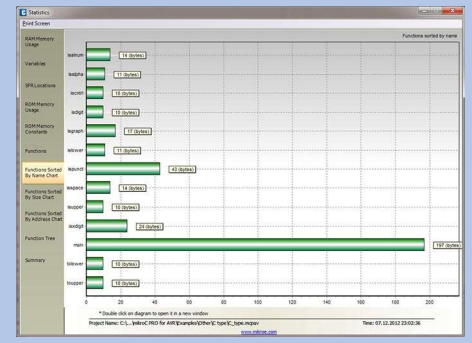
IAR Embedded Workbench – багатофункціональне середовище розробки застосунків мовами C, C++ та асемблер для цілого ряду МК від різних виробників. Платне



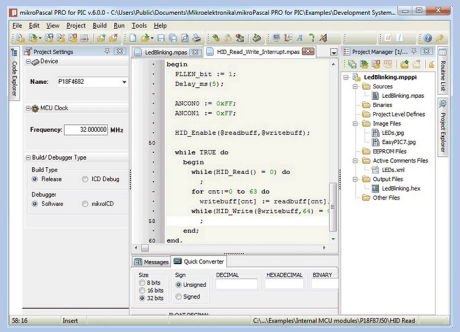
Flowcode – одна з передових графічних мов програмування для МК. Платне



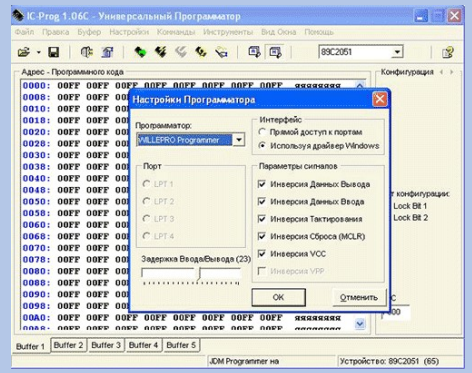
Algorithm Builder – графічне середовище програмування для розробки програм під МК з архітектурою AVR. Freeware



MikroC – найпотужніше середовище розробки програм для МК, що включає редактор коду, компілятор, відладчик, програмні та апаратні бібліотеки, що використовують готові функції. Платне

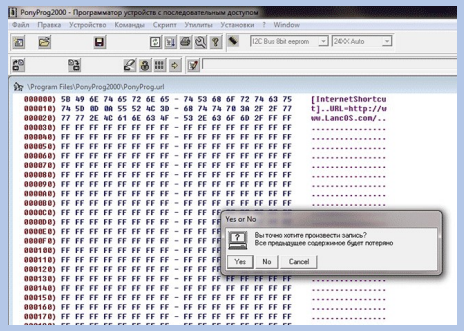


MicroCode Studio Plus – програма для створення та налагодження коду, написаного мовою програмування BASIC, під PIC. Платне

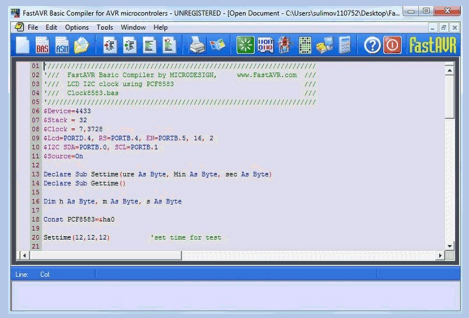


IC Prog – одна з найпопулярніших оболонок для програмування, що підтримує безліч МК, ППЗУ та адаптерів різної конструкції. Freeware

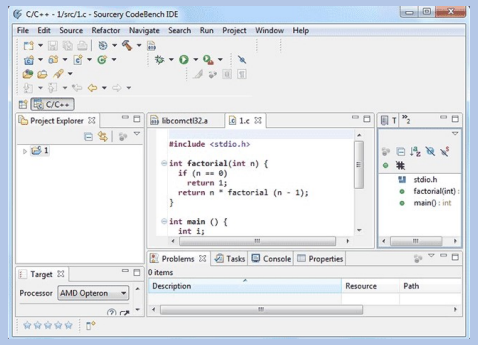
Програмне забезпечення IoT. Засоби розробки. Програми для мікроконтролерів



Pony Prog 2000 – невимоглива і багатофункціональна програма, призначена для роботи з МК і ПЗП, з послідовним доступом різних виробників. Freeware.

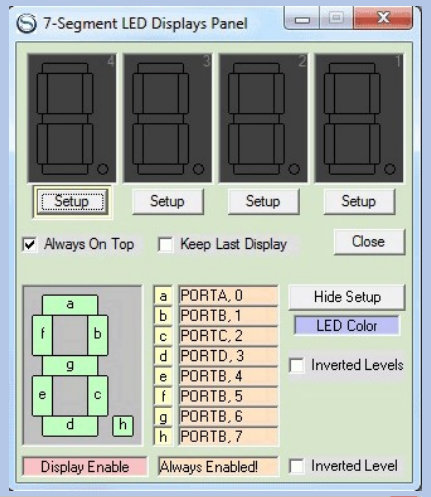


FastAVR – один з найкращих компіляторів Basic-подібної мови для серії восьмибітних мікроконтролерів AVR.

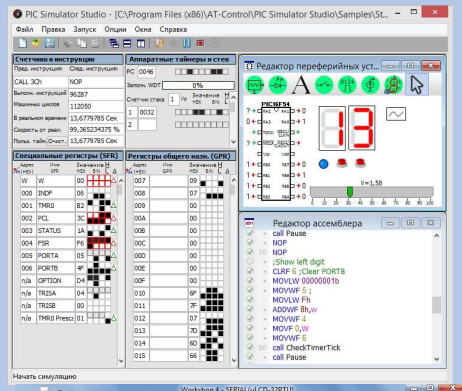


Sourcery CodeBench – самодостатнє інтегроване середовище розробки, призначене для створення застосунків на C/C++ для IA32, ColdFire, Power, MIPS, ARM та деяких інших архітектур МК. Платне

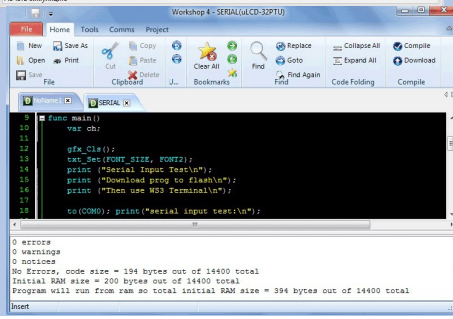
PIC Simulator IDE – програма призначена для налагодження коду МК PIC. Платне



PIC Simulator Studio – багатофункціональне та високопродуктивне ПЗ, призначене в першу чергу для симуляції в реальному часі цифрових та аналого-цифрових схем, ядром яких виступає МК PIC. Freeware



4D Workshop IDE – спеціалізоване ПЗ, призначене для роботи з МК у графічних контролерах та готових дисплейних модулях компанії 4D Systems. Freeware.



Програмне забезпечення IoT. Інформаційна безпека

Експерти вважають, що «нині безпечної екосистеми Інтернету речей не існує». Через те, що в багатьох пристроях, підключених до Інтернету, не шифрується бездротовий трафік, не передбачені паролі достатньої складності, а також через багато інших факторів хакери можуть, наприклад, включати та відключати чужі посудомийні та пральні машини, замикати господарів у їхньому власному будинку або навіть спостерігати за їхнім домашнім життям за допомогою, наприклад, відеокамери, встановленої на роботі-пилососі.

Для підвищення безпеки пропонується запровадження обов'язкової сертифікації пристроїв, розрахованих на підключення до Інтернету, встановлення на них спеціальних уніфікованих чіпів та інші заходи.

Інформаційна безпека IoT. Ключові вимоги щодо забезпечення безпеки IoT

Далі перераховані ключові вимоги до будь-якого рішення щодо безпеки IoT:

- безпека пристроїв та даних IoT, включаючи автентифікацію пристроїв, конфіденційність та цілісність даних;
- впровадження та виконання операцій із забезпечення безпеки у масштабі IoT;
- дотримання нормативно-правових вимог та запитів;
- відповідність вимогам до продуктивності залежно від варіанта використання.

Інформаційна безпека IoT. Ключові функціональні блоки безпеки IoT

У рішеннях із забезпечення безпеки IoT повинні бути реалізовані перераховані нижче функціональні блоки як взаємопов'язані, а не ізольовані модулі, щоб задовольняти вимоги щодо масштабу IoT, безпеки даних, довіри до пристроїв, а також нормативно-правових вимог:

- довіра до пристроїв IoT: встановлення та керування ідентифікацією та цілісністю пристроїв;
- довіра до даних IoT: наскрізний захист даних на основі політики;
- конфіденційність із моменту створення до моменту споживання;
- практична реалізація довіри: автоматизація та взаємодія з перевіреними технологіями та продуктами, що базуються на стандартах.

Інформаційна безпека IoT. Вимоги для безпечної участі пристроїв, що підключаються в IoT

Для безпечного з'єднання з IoT кожному пристрою, що підключається, потрібен унікальний ідентифікатор – ще до того, як у нього з'явиться IP-адреса. Таке цифрове посвідчення встановлює корінь довіри для всього життєвого циклу пристрою – від початкового проектування до розгортання та виведення з експлуатації.

Наприклад, можуть використовуватися апаратні модулі безпеки (HSM) nShield у поєднанні з підтримуючими програмами із забезпечення безпеки, щоб виробники могли привласнити кожному пристрою унікальний ідентифікатор, використовуючи найефективнішу криптографічну обробку, захист ключів та управління ключами. Кожний пристрій вводить цифровий сертифікат, щоб забезпечити дотримання зазначених нижче умов:

- аутентифікація кожного пристрою, що вводиться в архітектуру організації;
- перевірка цілісності операційної системи та програм на пристрої;
- захищені комунікації між пристроями, шлюзом та хмарою;
- санкціоновані оновлення програмного забезпечення та прошивок на основі затвердженого коду.

Інформаційна безпека IoT. Рекомендації з безпеки в IoT

Ряд організацій розробили рекомендації щодо безпеки для IoT. До них відносяться наведені нижче:

- Best Practice Guidelines («Посібник з передової практики») фонду IoT Security Foundation;
- Security Guidance («Посібник з безпеки») проекту Open Web Application Security Project (OWASP);
- GSMA IoT Security Guidelines & Assessment («Правила та оцінка GSMA щодо безпеки Інтернету речей») асоціації Groupe Spéciale Mobile Association (GSMA);
- Спеціальна публікація Guidance 800-160 («Керівництво щодо забезпечення безпеки в пристроях Інтернету речей (IoT)») Національного інституту стандартів та технологій (NIST) Міністерства торгівлі США;
- Future Proofing the Connected World: 13 Step to Developing Secure IoT Products («Запас на майбутнє цифрового світу: 13 кроків до розробки безпечних продуктів Інтернету речей») організації Cloud Security Alliance (CSA).

Інформаційна безпека IoT. Чому потрібна автентифікація пристроїв для IoT?

Надійна автентифікація пристроїв IoT потрібна для того, щоб гарантувати, що підключені пристрої в Інтернеті є саме тим, чим вони вважаються.

Отже, кожен пристрій IoT потребує унікального ідентифікатора, який використовується для аутентифікації пристрою при спробі підключення до шлюзу або центрального сервера. Завдяки цьому унікальному ідентифікатору адміністратори IoT-систем можуть відслідковувати кожен пристрій протягом усього його життєвого циклу, безпечно здійснювати зв'язок з ним та запобігати виконанню шкідливих процесів пристроєм. Якщо пристрій демонструє несподівану поведінку, адміністратори можуть просто відкликати його привілеї.

Інформаційна безпека IoT. Чому для пристроїв IoT потрібне безпечне виробництво?

Пристрої IoT, виготовлені за допомогою незахищених виробничих процесів, дають злочинцям можливість втручатися у виробничі цикли, щоб запровадити несанкціонований код або зробити додаткові копії, які згодом продаються на чорному ринку.

Один із способів захистити виробничі процеси – використовувати апаратні модулі безпеки (HSM) та підтримуюче програмне забезпечення безпеки, щоб вводити криптографічні ключі та цифрові сертифікати, а також контролювати кількість створених копій та код, включений до кожної з них.

Інформаційна безпека IoT. Чому для пристроїв IoT необхідно підписувати код?

Щоб захистити підприємства, бренди, партнерів та користувачів від шкідливого програмного забезпечення, розробники програмного забезпечення застосовують підписання коду. В Інтернеті речей підписання коду в процесі випуску програмного забезпечення гарантує цілісність оновлень програмного забезпечення та прошивок для пристроїв IoT, а також захищає від ризиків, пов'язаних зі зломом програмного коду IoT або відхиленням коду від організаційних політик.

У криптографії відкритих ключів підписання коду є спеціальним використанням цифрових підписів на основі сертифікатів, яке дозволяє організації перевіряти особу видавця програмного забезпечення та відсутність змін у програмному забезпеченні з моменту його виходу.

Інформаційна безпека IoT. Що таке IoT PKI?

Сьогодні до Інтернету підключено більше речей, ніж людей на планеті. Пристрої є головними користувачами Інтернету, і для їхньої безпечної роботи потрібні цифрові ідентифікатори. У міру того, як підприємства прагнуть трансформувати свої бізнес-моделі для підтримки конкурентоспроможності, швидке впровадження технологій IoT створює зростаючий попит на інфраструктуру відкритих ключів Інтернету речей (IoT PKI). PKI забезпечують цифровими сертифікатами зростаючу кількість пристроїв, а також програмне забезпечення та прошивки, що використовуються у пристроях.

Для безпечного розгортання IoT потрібна не тільки впевненість у тому, що пристрої є справжніми і є тим, чим названі, але й у тому, що дані, які вони збирають, дійсні та не змінені. Якщо пристроям IoT та даним довіряти не можна, немає сенсу збирати дані, виконувати аналітику та реалізовувати рішення на основі зібраної інформації.

Для безпечного впровадження IoT потрібне дотримання зазначених умов:

- забезпечення взаємної автентифікації між підключеними пристроями та застосунками;
- підтримка цілісності та конфіденційності даних, що збираються пристроями;
- забезпечення правомірності та цілісності програмного забезпечення, що завантажується на пристрої;
- збереження секретності конфіденційних даних у світлі суворіших норм забезпечення безпеки.

Лекцію закінчено
Дякую за увагу