ВИСНОВКИ

Кіберфізичні системи, що є рушійною силою інновацій, охоплюють безліч різних дисциплін. Співпраця різних галузей може зробити їх важливою виробничою силою. Кіберфізичні системи мають величезний потенціал для зміни і вдосконалення кожного аспекту життя людей, допомагаючи вирішувати критично важливі для нашого суспільства проблеми і перевершуючи сучасні розподілені системи в плані безпеки, продуктивності, ефективності, надійності, зручності використання і за багатьма іншими показниками.

ЛІТЕРАТУРА

1. Городецький В.І. Сучасний стан та перспективи індустріальних застосувань багатоагентних систем / Городецький В.І., Бухвалов О.Л., Скобелєв П.О. // Управління великими системами: збірник праць. - 2017. - №66. - С. 97-157.
2. Загитова А. І. Система підтримки життєвого циклу складного технічного об'єкта на основі агентних технологій / Загитова А. І., Кондратьєва Н. В., Валєєв С. С. // Вісник УГАТУ. - 2018. - Т. 22. - №. 2 (80). - С. 113-121

Кобас А. І.
Криворізький національний університет
Рябчина Л. С.
асистент, Криворізький національний університет

СИСТЕМА БЕЗПЕКИ ПРОТОКОЛІВ ОБМІНУ ДАНИМИ У МЕРЕЖАХ IOT

Розглянуто актуальність використання систем безпеки протоколів обміну даних у мережах Інтернету речей. Проведено огляд існуючих технологій безпеки Інтернету речей. Наведено класифікацію систем зв'язку та основні принципи кібербезпеки.

З розвитком інформаційно-комунікаційних технологій, автоматизації та роботизації промислових процесів людина перейшла у час цифрової революції.

Інтернет речей (Internet of Things, IoT) – це мережа фізичних об'єктів та пристроїв, які мають вбудовані технології та програмне забезпечення, що дозволяють здійснювати взаємодію з зовнішнім

середовищем, передавати відомості про свій стан і приймати дані ззовні, за допомогою використання стандартних протоколів зв'язку [1]. Така комплексна мережа взаємопов'язаних пристроїв дозволяє виконувати зчитування та приведення цих пристроїв у дію. За рахунок використання інтелектуальних інтерфейсів, стало можливе виключення необхідності участі людини в програмуванні та ідентифікації.

Швидке поширення IoT сприяло звертанню уваги на більш детальний розгляд проблеми конфіденційності інформації, що послужило появі поняттю безпека інтернету речей.

В даній роботі перед проектуванням власної системи безпеки передачі даних (СБПД), треба спочатку провести аналіз існуючих технологій, протоколів зв'язку та систем тощо.

Велику увагу при розробці IoT та його розвитку звертається на завдання встановлення з'єднання, зв'язку та налаштування роботи мережі. Передача даних і встановлення мережевого з'єднання будуються за принципом систем зв'язку ближньої дії – персональних мереж (PAN), які будуються без встановлення правил IP-протоколу. Дані мережі можуть бути дротовими та бездротовими. До бездротових IoT-мереж/протоколів можна віднести протоколи Zigbee, Z-Wave, mesh-мережі, Bluetooth. Для IIoT (Industrial IoT) відносять Wireless Hart та ISA100. Список дротових мереж більший, ніж бездротових, оскільки до даного переліку відносять всі існуючі промислові мережі/протоколи.

Крім персональних мереж використовуються бездротові локальні мережі та системи зв'язку на основі IP-протоколу, включаючи до даного переліку широкий діапазон Wi-Fi-мереж на базі стандартів IEEE 802.11, 6LoWPAN і технології Thread [2].

Для передачі даних датчиків до Інтернет-простору для даної СБПД необхідні дві технології: маршрутизатор-шлюз та опорні інтернет-протоколи, які забезпечують ефективність обміну даними. Маршрутизатор виконує важливі функції у сферах безпеки, управління та напряму самих даних. Граничні маршрутизатори (Edge routers) керують і стежать за станом відповідних mesh-мереж, а також вирівнюють і підтримують якість даних. Також велике значення належить конфіденційності та безпеки даних. Маршрутизатор відіграє важливу роль в створенні віртуальних приватних ме-

реж, віртуальних локальних мереж і програмно-визначених глобальних мереж. Дані мережі можуть містити тисячі вузлів, що обслуговуються єдиним граничним маршрутизатором, і в якійсь мірі маршрутизатор служить розширенням для хмари (edge device) [2].

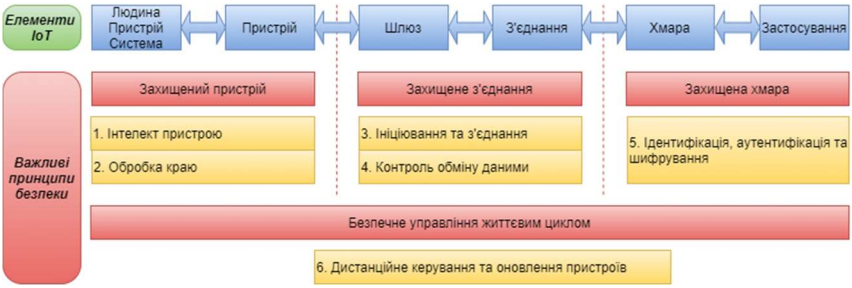

Рис. 1 – Схема основних принципів кібербезпеки в IoT

За типом реалізації даної системи доречно обрати систему загального призначення, так як вона не буде заглиблюватись у специфіку однієї галузі, але дасть загальне представлення основних принципів кібербезпеки обміну даних в IoT (рис. 1), що є більш важливим при бажанні працювати в цій галузі у майбутньому.

ВИСНОВОК

На основі проведеного аналізу можна зробити висновок, що питання безпеки протоколів обміну даними в мережах IoT має велике значення, адже втрата конфіденційності інформації може завдати великих витрат. Захист передачі даних та встановлення безпечного з'єднання мережі повинен здійснюватися комплексно за основними принципами кібербезпеки та в різних напрямках. Чим повніше та досконаліше буде виконано аналіз призначення типу мережі та встановлено її з'єднання, тим стійкіше та безпечніше матиме захист сама система.

ЛІТЕРАТУРА

1. Industrial Internet of Things – IIoT Промышленный интернет вещей [Електронний ресурс] – Режим доступу до ресурсу: http://www.tadviser.ru/index.php/Статья:IIoT_-Industrial_Internet_of_Things.

2. Understanding IoT Security – Part 2 of 3: IoT Cyber Security [Електронний ресурс] – Режим доступу до ресурсу: https://iot-analytics.com/understanding-iot-cyber-security-part-

Голіков В.В.
Криворізький економічний інститут Київського національного університету ім. Вадима Гетьмана
Вдовиченко І.Н.
К.т.н.,доцент, Криворізький національний університет

ВИКОРИСТАННЯ БЕЗСЕРВЕРНИХ ОБЧИСЛЕНЬ У WEB-ДОДАТКАХ

Проаналізовано перспективи безсерверних обчислень та serverless архітектури додатку. Огляд сильних та слабких сторін використання безсерверних технологій при розробці web-додатків.

Останнім часом хмарні технології набирають все більшої популярності. Це відбувається з простої причини - легкої доступності, відносної дешевизни і відсутності початкового капіталу - як знань для підтримки і розгортання інфраструктури, так і фінансового характеру. Serverless - безсерверна архітектура додатків. Насправді, не така вже вона й безсерверна. Основу архітектури складають мікросервіси, або функції (lambda), що виконують певне завдання і запускаються на логічних контейнерах, захованих від сторонніх очей. Тобто кінцевому користувачеві дано тільки інтерфейс завантаження коду функції (сервісу) і можливість підключення до цієї функції джерел подій (events). Іноді безсерверні обчислення також іменують «Функція як послуга», тому що одиницею коду є функція, яка виконується платформою. По суті для виконання одного запиту створюється окремий контейнер, який знищується після виконання.

Основними платформами, що надають послуги безсерверного середовища виконання є такі як AWS Lambda від Amazon, Google Cloud Functions від Google, OpenWhisk від IBM, Azure Functions від Microsoft Azure та інші [1].

Ідея безсерверних обчислень полягає в чотирьох рисах: абстракція, еластичність, ефективна вартість та обмежений життєвий цикл. За допомогою абстракції користувач не керуєте сервером, на