DOI: https://doi.org/10.36910/6775-2524-0560-2020-41-31
УДК: 004.056:681.5.042
Самойленко Максим Юрійович, аспірант
https://orcid.org/0000-0002-2237-7138
Київський національний університет імені Тараса Шевченка

ПРОБЛЕМИ БЕЗПЕКИ У ПРАКТИЦІ РЕАЛІЗАЦІЇ ТЕХНОЛОГІЇ ІНТЕРНЕТ РЕЧЕЙ

Самойленко М.Ю. Проблеми безпеки у практиці реалізації технології інтернет речей. Розкрито проблеми безпеки у практиці реалізації технології Інтернету речей. Здійснено аналіз проблем Інтернету речей, головною з яких обрано проблему забезпечення інформаційної безпеки. Зазначається, що численні програми Інтернету речей можна об'єднати в три групи – індустріальну або промислову, навколишнього середовища, громадську. Описано всі технології, що входять до безперервних обчислювальних процесів Інтернету речей, такі як: радіочастотна ідентифікація; обробка великих масивів інформації, Big Data; між машинна взаємодія (Machineto Machine, M2M); кібер-фізичні системи (біологічних, фізичних і ін., операції яких інтегруються, контролюються і управляються комп'ютерним ядром); визначення місця розташування за допомогою ГЛОНАСС і GPS; надання широкосмугового зв'язку, в тому числі глобального стандарту цифрового мобільного стільникового зв'язку з розділенням каналів за часом (TDMA) і частотою (FDMA); бездротових сенсорних мереж та інших сучасних технологій. Підкреслено, що враховуючи всі характеристики Інтернету речей, він має три рівні: рівень сприйнятті, мережевий рівень і прикладний рівень, кожен з яких здійснює завдання та виконує покладені на нього функції. Запропоновано окремо до кожного зазначеного рівня низку проблем інформаційної безпеки. Описано причини програмної вразливості Інтернету речей та визначено складність програмного забезпечення в Інтернеті речей із зазначенням заходів здатних знизити рівень вразливості. Наголошено, що для проектування програмного забезпечення необхідно емулювати поведінку приладів Інтернету речей, тобто створити імітатор зовнішнього середовища для серверів. Унаслідок обмежень в приладах (енергозабезпечення, продуктивність процесора, пам'ять) в Інтернеті речей стоїть складне завдання уникнути сильної розбіжності між емулятором і приладом. Наведено поняття бекдор та описано принципи застосування бекдору.
Ключові слова: Інтернет речей, інформаційна безпека, програмне забезпечення, зв'язок, інформаційна технологія, ідентифікація.

Самойленко М. Ю. Проблемы безопасности в практике реализации технологии интернет вещей. Раскрыты проблемы безопасности в практике реализации технологии Интернета вещей. Осуществлен анализ проблем Интернета вещей, главной из которых выбрана проблема обеспечения информационной безопасности. Отмечается, что многие программы Интернета вещей можно объединить в три группы - индустриальную или промышленную, окружающей среды, общественную. Описаны все технологии, входящие в непрерывных вычислительных процессов Интернета вещей, такие как: радиочастотная идентификация; обработка больших массивов информации, Big Data; между машинная взаимодействие (Мачинето Machine, M2M) кибер-физические системы (биологических, физических и др., операции которых интегрируются, контролируются и управляются компьютерным ядром) определение местоположения с помощью ГЛОНАСС и GPS; предоставление широкополосного доступа в том числе глобального стандарта цифрового мобильной сотовой связи с разделением каналов по времени (TDMA) и частотой (FDMA) беспроводных сенсорных сетей и других современных технологий. Подчеркнуто, что учитывая все характеристики Интернета вещей, он имеет три уровня: уровень восприятии, сетевой уровень и прикладной уровень, каждый из которых осуществляет задачи и выполняет возложенные на него функции. Предложено отдельно к каждому указанного уровня ряд проблем информационной безопасности. Описаны причины программной уязвимости Интернета вещей и определено сложность программного обеспечения в Интернете вещей с указанием мер способных снизить уровень уязвимости. Отмечено, что для проектирования программного обеспечения необходимо эмулировать поведение приборов Интернета вещей, то есть создать имитатор внешней среды для серверов. Вследствие ограничений в приборах (энергообеспечение, производительность процессора, память) в Интернете вещей стоит сложная задача избежать сильной разногласия между эмулятором и прибором. Приведены понятия бэкдор и описаны принципы применения бэкдора.
Ключевые слова: Интернет вещей, информационная безопасность, программное обеспечение, связь, информационные технологии, идентификация.

Samoilenko Maksym. Security problems in the practice of implementation of the internet of things technology. The article reveals security issues in the practice of the Internet of Things technology. The author provides an analysis of the problems of the Internet of Things, where the problem of information security is chosen as the major one. It is noted that numerous Internet of Things programs can be combined into three groups — industrial, environmental, public. All technologies included in the continuous computational processes of the Internet of Things are described, such as: radio frequency identification; processing of large arrays of information, Big Data; machine-to-machine interaction (MachinetoMachine, M2M); cyber-physical systems (biological, physical, etc. operations of which are integrated and controlled by a computer core); location identification through GLONASS and GPS; providing broadband communication, including the global standard for digital mobile cellular communication with time division multiple access (TDMA) and frequency division multiple access (FDMA); wireless sensor networks, and other modern technologies. It is emphasized that taking into account all the characteristics of the Internet of Things, it has three levels: the level of perception, network level and applied level, each fulfilling the tasks and performing its functions. The author proposed a number of information security issues for each level. The causes of software vulnerabilities of the Internet of Things are described, and the complexity of software on the Internet of Things is determined, indicating measures that can reduce the level of vulnerability. It is emphasized that for software design it is necessary to emulate the behaviour of IoT devices, i.e. to create a simulator of the environment for servers. Due to limitations in devices (power supply, processor performance, memory), the Internet of Things faces a difficult task to avoid a

strong discrepancy between the emulator and the device. The concept of backdoor is provided, and the principles of backdoor application are described.

Keywords: Internet of Things, information security, software, communication, information technology, identification.

Вступ та постановка проблеми дослідження. У широкому сенсі Інтернет речей (Internet of Things, IoT) розглядається як можливість об'єктів і людей дистанційно взаємодіяти через Інтернет в будь-якому місці і в будь-який час завдяки конвергенції різних технологій; в той же час розвиток IoT як концепції еволюції людства може мати технологічні та соціальні наслідки [1]. Розгортання протоколу IPv6 стало одним з вирішальних умов втілення IoT в життя.

В даний час існує можливість ідентифікувати обладнання, предмети побуту та віртуальні об'єкти (такі, як цифрові фотографії) таким же чином, як і окремих користувачів в Інтернеті людей. Таким чином, речі можуть бути інтегровані в широку мережу взаємозв'язків, в якій вони в будь-який час виявляться здатними взаємодіяти один з одним або з людьми. По суті, речі в світі Інтернету речей знаходяться тепер на одному рівні з людьми [2].

Багато технологій, що розвиваються в останні роки, мають на увазі найтісніший зв'язок з технологіями безпеки. Завдяки використанню сучасних можливостей ідентифікації, збору, обробки і передачі даних, в IoT забезпечується найбільш ефективне використання речей для надання послуг для всіх типів додатків при одночасному виконанні вимог безпеки. В тому числі, в IoT мається на увазі і недоторканність приватного життя [1]. Розглянемо Інтернет речей з точки зору інформаційної безпеки.

Аналіз останні досліджень та публікацій. На сьогодні питання інформаційної безпеки у сфері Інтернету речей досліджувало чимало як зарубіжних так і вітчизняних вчених. Так І. М. Сотник та К. Ю. Завражний [3] розкрили підходи до забезпечення інформаційної безпеки промислового Інтернету речей на підприємстві. Авторами обґрунтовані перспективи розвитку Інтернету речей та промислового Інтернету речей, акцентована увага на економічних ефектах впровадження масштабних інформаційних систем управління виробництвом сучасних підприємств шляхом використання системних рішень класу ERP. У статті, доведено, що погіршення інформаційної безпеки діяльності підприємств та організацій є однією з важливих проблем, що супроводжують розбудову промислового Інтернету речей. Проаналізовано підходи до забезпечення інформаційної безпеки промислового Інтернету речей у суб'єктів господарювання з урахуванням сучасних досягнень у сфері інформаційних технологій.

М. В. Грайворонський [4] дослідив безпеку пристроїв Інтернету речей. Науковець описав зв'язок та взаємодію пристроїв Інтернету речей, який відбувається за допомогою стандартних протоколів передачі даних бездротовими та дротовими мережами на різних рівнях, а саме: HHTP/HTTPS, TCP, UDP, IP, XMPP, Ethernet, ICMP, Telnet та інші. Автором виділено ряд проблем безпеки Інтернету речей.

Питання криптології в Інтернеті речей розглянув А. І. Петренко [5]. У роботі зазначено, що простого універсального рішення не існує, і для забезпечення безпеки недостатньо замкнути двері, залишивши вікна відкритими. Безпека повинна бути комплексною, інакше хакери просто скористаються найслабшою ланкою.

Зарубіжні фахівці приділяють велику увагу науковим і експериментальним дослідженням в забезпеченні інформаційної безпеки IoT. Наприклад, в роботі [6] показано, що найбільший ризик безпеки можливий на нижньому рівні архітектури – на рівні сприйняття. При цьому відзначається, що деяким загрозам безпеки на інших рівнях архітектури IoT так само характерний високий рівень ризику. В роботі [7] наводяться результати досліджень забезпечення безпеки приватних даних на прикладі «Розумного будинку» в IoT.

Однак, незважаючи на масштабність наукових досліджень, питання забезпечення інформаційної безпеки у практиці реалізації технології Інтернет речей залишаються відкритими та потребують детального опрацювання.

Формулювання мети статті, постановка завдання. У рамках даної статті метою є дослідження проблем безпеки у практиці реалізації технології Інтернет речей. Для досягнення поставленої мети необхідно виконання наступних завдань:

- розкрити технології Інтернету речей;
- дослідити рівні Інтернету речей та визначити проблеми інформаційної безпеки кожного окремого рівня;
- описати сутність та уразливості програмного забезпечення Інтернету речей.

Виклад основного матеріалу дослідження. XXI століття відзначилося стрімким проривом у сфері інформаційних технологій. На ринок вийшли новітні роботизовані системи, розвивалося поняття «Інтернету речей», життя сучасної людини з кожним наступним роком стає все більш автоматизованим. На першу ланку виходять системи бездротового зв'язку, які все частіше використовуються в якості рушійної сили для розвитку технології інтелектуального контролю та управління додатками [8].

Сьогодні Інтернет речей також набирає популярність в логістиці, різних галузях промисловості, роздрібній торгівлі та фармацевтиці. У зв'язку з розвитком бездротового зв'язку, смартфонів і датчиків мережевих технологій все більше і більше мережевих «речей», або «розумних» об'єктів, беруть участь в IoT. В результаті всі ці IoT-технології роблять значний вплив на нові інформаційні та комунікаційні технології (ІКТ) і технології корпоративних систем (рис. 1).

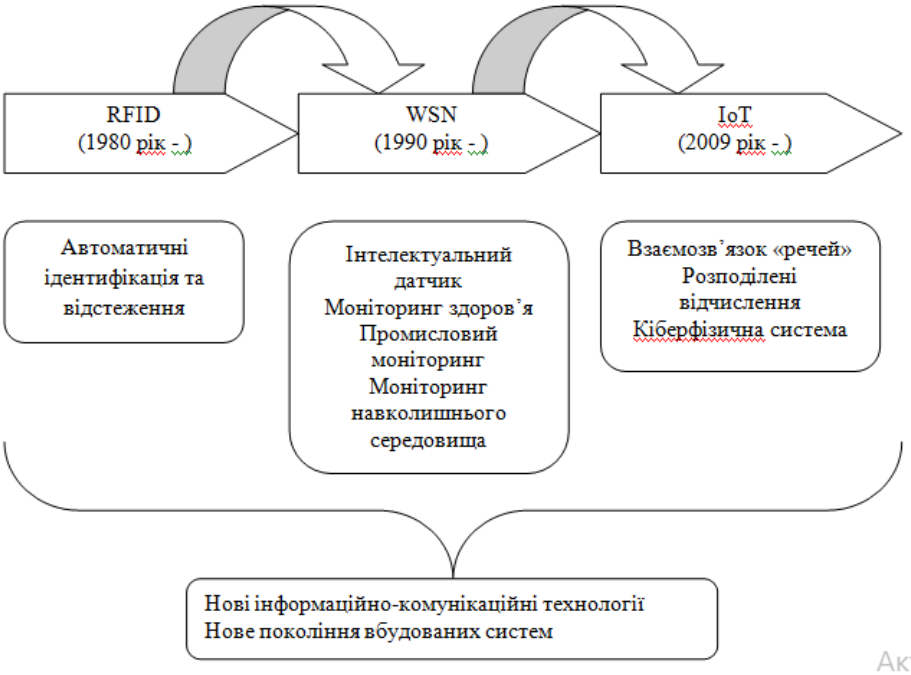

Рис. 1. Пов'язані з Інтернетом речей технології та їх вплив на нові інформаційно-комунікаційні технології і на корпоративні системи

Концепція IoT включає в себе безліч різних технологій, послуг, стандартів і сприймається як наріжний камінь на ринку інформаційно-комунікаційних технологій (ІКТ) принаймні на найближчі десять років. Однією з головних проблем IoT є забезпечення інформаційної безпеки (ІБ). Всі численні програми IoT можна об'єднати в три групи – індустріальний або промисловий (industry), навколишнього середовища (environment), громадський (society).

Інтернет речей включає в себе безперервні обчислювальні процеси з використанням технологій:

- радіочастотної ідентифікації (Radio Frequency Identification, RFID);
- обробки великих масивів інформації, Big Data;
- між машинної взаємодії (MachinetoMachine, M2M);
- кібер-фізичних систем (біологічних, фізичних і ін., операції яких інтегруються, контролюються і управляються комп'ютерним ядром);
- визначення місця розташування за допомогою ГЛОНАСС і GPS;
- надання широкосмугового зв'язку, в тому числі стандарту GSM;
- бездротових сенсорних мереж та інших сучасних технологій.

Для Інтернету речей визначені три основні характеристики – комплексні знання, надійна передача, інтелектуальна обробка. Враховуючи три описані характеристики структура IoT може бути розділена на певні рівні – рівень сприйнятті (perception), мережевий рівень і прикладний рівень [9]. Кожен з трьох рівнів здійснює завдання та виконує покладені на нього функції.

Рівень сприйняття – отримує постійне зчитування з датчиків, RFID-міток. Мережевий рівень – виконує завдання по передачі інформації, її обробці та забезпеченню доступу до інформації. Прикладний рівень – аналізує і обробляє прийняту інформацію для прийняття правильного рішення і контролю за управлінням, додатками і послугами. У рамках рівня прикладного фундаментальною основою є виконання функцій зі збору та зберігання даних, з метою забезпечення ефективності енергозабезпечення, логістики та ін.

Як ключова технологія інтеграції гетерогенних систем або пристроїв, сервіс-орієнтована архітектура (SOA) може бути застосована для підтримки «Інтернету речей». SOA успішно використовується в таких науково-дослідних областях, як хмарні обчислення, бездротові сенсорні мережі (WSN) і транспортні мережі [2]. Чимало ідей було запропоновано для створення багаторівневих архітектур SOA для «Інтернету речей» відповідно до обраної технології, потребами бізнесу і технічними вимогами.

Варто зазначити, що в деяких роботах розглядається більш, ніж трирівнева архітектурі IoT. В роботі [10] прийнята п'ятирівнева архітектура IoT, яка включає, наприклад, проміжний рівень (Middleware) між мережним і прикладним рівнем. Цей рівень виконує функцію обробки повідомлень інформації взаємодіючих однотипних сенсорних датчиків. Рекомендована Міжнародним телекомунікаційним союзом архітектура IoT також складається з п'яти різних рівнів (або шарів): виявлення, доступ, підключення до мережі, проміжне програмне забезпечення, шар додатків. Функціональні можливості чотиришарової SOA для IoT наведені в таблиці 1. Таблиця 2 ілюструє проектування архітектури додатків промислового «Інтернету речей».

Таблиця 1

Чотирирівнева архітектура для «Інтернету речей»

Рівень	Опис
Рівень зондування	Рівень інтегрований з існуючими апаратними засобами (RFID, датчиками, виконавчими механізмами і т.д.), для того щоб розпізнавати / контролювати фізичний світ і збирати відповідні дані
Мережевий рівень	Рівень забезпечує базову мережеву підтримку і передачу даних по бездротовій або провідній мережі
Сервісний рівень	На цьому рівні створюються сервіси і здійснюється управління ними
Інтерфейсний рівень	Рівень забезпечує взаємодію між користувачами і зі сторонніми додатками

Таблиця 2

Проектування додатків «Інтернету речей»

Мета розробки	Опис
Енергія	Як довго можуть IoT-пристрої працювати з обмеженим електроживленням?
Час очікування	Скільки часу потрібно для передачі та обробки повідомлення?
Продуктивність	Який максимум даних, які можна передати через мережу?
Масштабованість	Скільки пристроїв підтримується?
Топологія	Хто і з ким повинен взаємодіяти?
Надійність і безпека	Наскільки надійний і безпечний додаток?

Архітектура «Інтернету речей» охоплює мережі і комунікації, «розумні» об'єкти, веб-сервіси і додатки, бізнес-моделі і відповідні процеси, спільну обробку даних, безпеку і т. д. З точки зору технології при розробці архітектури «Інтернету речей» потрібно продумати її розширюваність, масштабованість, модульність і можливість взаємодії гетерогенних пристроїв. Оскільки «речі» можуть пересуватися або потребувати у взаємодії з навколишнім середовищем в режимі реального часу, необхідна адаптивна архітектура. Також децентралізована і гетерогенна природа «Інтернету речей» вимагає, щоб його архітектура надавала різні ефективні подієві можливості. Таким чином, сервіс-орієнтована архітектура є хорошим методом для досягнення взаємодії різнорідних пристроїв безліччю різних шляхів [3].

У даній роботі обмежимося аналізом проблем інформаційної IoT на кожному з трьох рівнів – рівні сприйняття, мережевому і прикладному рівнях. На рис. 2 показана IoT на три рівні.

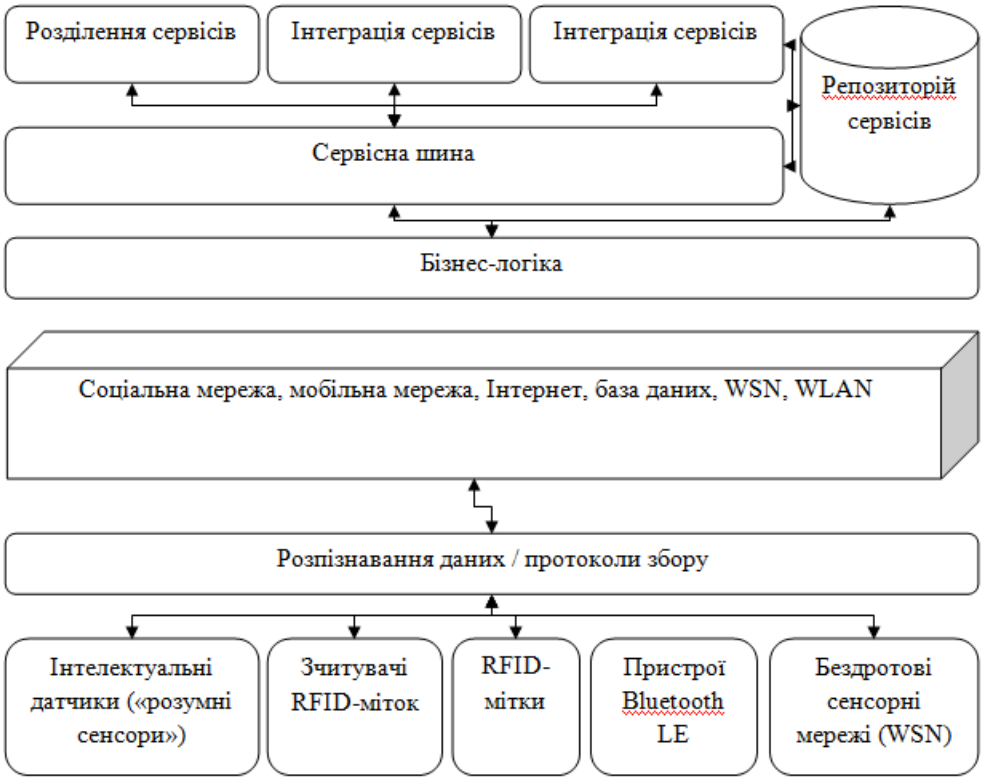

Рис. 2. Архітектура Інтернету речей на три рівня

Проблеми інформаційної безпеки на рівні сприйняття. Головною проблемою інформаційної безпеки на рівні сприйняття є проблема забезпечення повної фізичної безпеки приладів сприйняття та збору інформації. Більшість вузлів сприйняття, для яких характерне розгортання в не обслуговуваному людьми середовищі при відсутності стандартів, різноманітність, простота, обмеження енергозабезпечення та слабка здатність до захисту безпеки. Тому IoT не може забезпечити уніфіковану систему захисту безпеки і є вразливою до загроз, що надходять від зловмисника. Так як бездротова сенсорна мережа на рівні сприйняття є джерелом інформації, то ІБ на цьому рівні важлива.

Проблеми безпеки на цьому рівні включають:

- фізичне захоплення сенсорних вузлів;
- захоплення вузла шлюзу;
- витік інформації з сенсора;
- загрози цілісності даних;
- низький рівень енергозабезпечення;
- загроза перевантаження;
- атаки типу DoS (відмова в обслуговуванні);
- загроза маршрутизації встановленням в мережу нелегітимних сенсорів;
- загроза копіювання вузла.

Проблеми інформаційної безпеки на мережевому рівні. Загрози ІБ існуючих мереж зв'язку поширюються і на IoT, який побудований на них. До таких загроз варто віднести:

- несанкціонований доступ;
- перехоплення даних;
- конфіденційність;
- цілісність;
- атаки типу «людина посередині»;
- Dos-атаки (відмова в обслуговуванні);
- віруси, експлойти, мережеві черв'яки, руткити і ін.

Крім того, існують міжмережеві проблеми аутентифікації, які можуть бути причиною атак DoS.

У IoT стоять більш складні проблеми забезпечення безпеки в порівнянні з тими, з якими стикалися раніше [8]. Це викликано двома причинами – гетерогенний характер структури (різноманіття речей, різні технології мереж в з'єднанні) і великим числом об'єктів.

IoT приймає інформацію від великої кількості пристроїв, збирає великий масив даних різних форматів від безлічі джерел з неоднорідними характеристиками. В результаті цього на мережевому рівні мають місце більш складні проблеми безпеки. До них відносяться можливі проблеми масштабованості мережі, викликані малопередбачуваним обсягом передачі даних від великого числа вузлів, і що призводять до можливості здійснення атак DoS, DDoS.

Окрема увага приділяється уразливості програмного забезпечення (software vulnerabilities), що призводить до порушення інформаційної безпеки після впровадження. Причинами програмної вразливості, перш за все, є:

- неминучі помилки розробників складного багатошарового програмного забезпечення (ПЗ);
- помилки основи програми (недосконалість коду);
- часткова обробка винятків;
- застосування незахищеного коду;
- використання необроблених масивів;
- помилки в обробці Big Data;
- помилки у базі даних;
- відсутність належної індексації або закріплення запитів бази даних;
- web-уразливість;
- неповна продуктивність або масштабованість програмного забезпечення;
- помилки розподіленої роботи додатків, а також віртуальних платформ і хмар.

Слід зазначити складність програмного забезпечення в Інтернеті речей, викликану масштабною різноманітністю використовуваних апаратних платформ і операційних систем. Для проектування ПЗ необхідно емулювати поведінку приладів Інтернету речей.

Також для відвантаження налагодженого робочого релізу IoT додатку, необхідно провести повноцінне тестування, включаючи навантажувальне випробування, випробування продуктивності, комплексне дослідження взаємодії модулів. Бекдори також виступають проблемним місцем. Бекдори – це ділянки програмного коду, які вставлено програмістом-розробником, з метою подальшого використання для перегляду даних, або віддаленого управління комп'ютером.

Проблеми інформаційної безпеки на прикладному рівні. Повсюдне застосування IoT є наслідком масштабної програмної інтелектуалізації всіх областей дії сучасної людини, це промисловість, освіта, комп'ютеризація, зв'язок та інше. Крім порушення інформаційної безпеки традиційних мереж зв'язку додатки Інтернету речей стикаються з вторинними проблемами безпеки на прикладному рівні – при використанні хмарних обчислень, обробці інформації, забезпеченні прав на інтелектуальну власність, захисті приватності та ін.

Висновки та перспективи подальших досліджень. Інтернет речей пропонує великий потенціал для організацій і товариств. Якщо вдасться успішно розвинути Інтернет речей, це відкриє багато цінностей, і переваги Інтернету речей будуть величезні для організацій і товариств. Тим не менш, є ще деякі серйозні проблеми.

Величезна кількість речей, процесів, великих даних і складних процесів вимагає комплексної стратегії тестування, яка буде контролювати «велику картину». Важливим кроком для успішної інтеграції в цифровому світі є скорочення часу циклу тестування за рахунок прийняття швидких методів і платформи для динамічного тестування. Це означає легке, швидке рішення для забезпечення якості та тестування, інтегроване з гнучкою розробкою.

Виявлення кращих практик тестування гарантує, що продукти і додатки будуть готові до встановлених термінів і будуть відповідати очікуванням клієнтів, а також забезпечать компанії поставками бездефектних продуктів і послуг для кількісного повернення інвестицій.

Список бібліографічного опису

1. Міхненко Я. О., Курдеча, В. В. (2019). Порівняння видів хмарних сервісів в IoT. *Перспективи телекомунікацій* : матеріали XIII міжнар. наук.-техн. конф. (м. Київ, 15-19 квіт. 2019 р.,). Київ, 2019. URL: https://cutt.ly/gpqg4id (дата звернення: 12.10.2020 р.)

2. Пороло Є. О., Курдеча В. В. (2020). Удосконалена архітектура мережі для хмарного Інтернету речей / Пороло Є. О., // Перспективи телекомунікацій : зб. матеріалів XIV міжнар. наук.-техн. конф. (м. Київ, 13-17 квіт. 2020 р.) / Ін-т телекомунікац. систем та НДІ телекомунікацій КПІ ім. Ігоря Сікорського. Київ. URL: https://cutt.ly/wpqjh4U (дата звернення: 12.10.2020 р.)
3. Сотник, І.М., Завражний, К.Ю. (2017). Підходи до забезпечення інформаційної безпеки промислового інтернету речей на підприємстві. *Маркетинг і менеджмент інновацій*, 3, 177-186. doi: 10.21272/mmi.2017.3-17.
4. Грайворонський, М.В. (2017). Безпека пристроїв Інтернету речей. *Інтернет речей: проблеми правового регулювання та впровадження*: матеріали науково-практичної конференції (м. Київ. 24 жовтня 2017 р.). / упоряд. : В. М. Фурашев, С. Ю. Петряєв. Київ : Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» Вид-во «Політехніка», 29-35.
5. Петренко, А. І. (2019). Криптологія в Інтернеті речей. *Моделювання та інформ. системи в економіці*, 97, 155-163. URL: https://cutt.ly/IorknVi (дата звернення: 12.10.2020 р.)
6. Zhang, B., Zou, Z., & Liu, M. (2011, May). Evaluation on security system of internet of things based on fuzzy-AHP method. In *2011 International Conference on E-Business and E-Government (ICEE)* (pp. 1-5). IEEE. doi:10.1109/ICEBEG.2011.5881939
7. Schurgot, M. R., Shinberg, D. A., & Greenwald, L. G. (2015, June). Experiments with security and privacy in IoT networks. In *2015 IEEE 16th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)* (pp. 1-6). IEEE.
8. Сорокін, Д. В., Бондарчук, А. П., & Сторчак, К. П. (2019). Інфраструктура промислових мереж IoT та кіберзагрози в доступі при використанні IoT рішень. *Телекомунікаційні та інформ. технології,* 4, 120-127.
9. Алексіна Л. Т., Шевченко О. О.Дослідження технологій інтернету речей. *Зв'язок*, 4, 24-26.
10. Базилевич В., Мальцева М., Петренко Т., Черниш Л. (2020). Захищена система розумного будинку з використанням Internet of Things. *Технічні науки та технології*, № 2 (20), 218-228.

References

1. Mikhnenko Ya.O., Kurdecha, V.V. (2019). Comparison of Types of Cloud Services in IoT. *Modern Challenges in Telecommunications*: Materials of the XIII International Scientific Conference (Kyiv, April 15-19, 2019). Kyiv, 2019. URL: https://cutt.ly/gpqg4id (retrieved: 12.10.2020)
2. Porolo, Ye.A., Kurdecha, V.V. (2020). Improved Network Architecture for the Cloud Internet of Things. *Modern Challenges in Telecommunications*: Materials of the XIV International Scientific Conference (Kyiv, April 13-17, 2020) / Inst. of Telecommunication Systems and Research Institute of Telecommunications of NTU Igor Sikorsky KPI. Kyiv. URL: https://cutt.ly/wpqjh4U (retrieved: 12.10.2020)
3. Sotnik, I.M., Zavrazhnyi, K.Yu. (2017). Approaches to Information Security of the Industrial Internet of Things at the Enterprise. *Marketing and Management of Innovations*, 3, 177-186. doi: 10.21272/mmi.2017.3-17.
4. Hraivoronskyi, M.V. (2017). Internet of Things Security. *Internet of Things: Problems of Legal Regulation and Implementation*: Materials of the Research and Training Conference (Kyiv, October 24, 2017). / Ed. by: V.M. Furashev, S.Yu. Petriaev. Kyiv: National Technical University of Ukraine, Igor Sikorsky Kyiv Polytechnic Institute, Polytechnika Publishing House, 29-35.
5. Petrenko, A.I. (2019). Cryptology in the Internet of Things. *Modelling and Information Systems in Economics*, 97, 155-163. URL: https://cutt.ly/IorknVi
6. Zhang, B., Zou, Z., & Liu, M. (2011, May). Evaluation on security system of internet of things based on fuzzy-AHP method. In *2011 International Conference on E-Business and E-Government (ICEE)* (pp. 1-5). IEEE. doi:10.1109/ICEBEG.2011.5881939
7. Schurgot, M. R., Shinberg, D. A., & Greenwald, L. G. (2015, June). Experiments with security and privacy in IoT networks. In *2015 IEEE 16th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)* (pp. 1-6). IEEE.
8. Sorokin, D.V., Bondarchuk, A.P., Storchak, K.P. (2019). Infrastructure of Industrial IoT Networks and Cyber Threats in Access when Using IoT Solutions. *Telecommunication and Information Technology*. No. 4. Pp. 120-127. URL: https://cutt.ly/6orjhfo
9. Aleksina, L.T. Shevchenko, O.O. (2019). Research of the Internet of Things Technologies. *Connectivity*, 4, 24-26.
10. Bazylevych, V., Maltseva, M., Petrenko, T., Chernysh, L. (2020). Secure Smart Home System Using the Internet of Things. *Technical Sciences and Technologies*, 2(20), 218-228.