КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (11), 2021
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2021.11.3142
УДК 004.49

Опірський Іван Романович
д.т.н., доц., професор кафедри захисту інформації
Національний Університет "Львівська Політехніка", Львів, Україна
ORCID ID: 0000-0002-8461-8996
ivan.r.opirskyi@lpnu.ua

Головчак Романа Василівна
студентка спеціальності “Кібербезпека”
Національний Університет “Львівська Політехніка”, Львів, Україна
ORCID ID: 0000-0002-2932-3466
romana.holovchak.kb.2018@lpnu.ua

Мойсійчук Ірина Русланівна
студентка спеціальності “Кібербезпека”
Національний Університет “Львівська Політехніка”, Львів, Україна
ORCID ID: 0000-0002-7531-5811
iryna.moisiichuk.kb.2018@lpnu.ua

Балянда Тетяна Степанівна
студентка спеціальності “Кібербезпека”
Національний Університет “Львівська Політехніка”, Львів, Україна
ORCID ID: 0000-0002-0066-6131
tetiana.balianda.knm.2018@lpnu.ua

Гаранюк Софія Петрівна
студентка спеціальності “Кібербезпека”
Національний Університет “Львівська Політехніка”, Львів, Україна
ORCID ID: 0000-0002-0626-2859
sophiegaranyk96@gmail.com

ПРОБЛЕМИ ТА ЗАГРОЗИ БЕЗПЕЦІ IoT ПРИСТРОЇВ

Анотація. Інтернет речей або IoT - це мільярди фізичних пристроїв підключених до Інтернету. Його основна передумова - це просто розширений тип підключення, який потім може бути використаний як основа для виконання всіх видів функцій. IoT описує мережу фізичних об'єктів - "речей", які вбудовані в датчики, програмне забезпечення та інші технології з метою підключення та обміну даними з іншими пристроями та системами через Інтернет. Проблеми захисту систем які, включають використання IoT пристроїв досліджуються багатьма науковцями та спеціалістами цієї галузі, проте в сучасному світі далеко не кожна компанія-виробник готова заявити про вразливості і загалом незахищеність своїх продуктів (пристроїв). У всьому середовищі IoT, від виробників до користувачів, все ще існує багато проблем безпеки IoT, таких як: норми виготовлення, управління оновленнями, фізичне загартовування, знання та обізнаність користувачів. У цій статті проведено дослідження вразливостей систем інтернету речей. Проведено аналіз технологій передачі інформації IoT пристроїв (зокрема ZigBee, Signfox та Bluetooth). Визначено та проаналізовано найпоширеніші загрози, з якими може зустрітися користувач. Встановлено також, що зазвичай не лише виробник створює загрози безпеці IoT пристроїв. Також наведено ряд порад для користувачів, котрі хочуть знизити ризик витоку даних, пов’язаний із вразливостями систем інтернету речей. Нажаль, неодиничними випадками є некоректне налаштування, використання та зберігання таких приладів. Надзвичайно поширеним явищем є відмова користувача від оновлення програмного забезпечення, що в свою чергу залишає відкритими ті

вразливості, які виробник намагається усунути. Основною метою статті є визначення причин виникнення загроз безпеці пристроїв інтернету речей, шляхом аналізу технологій передачі даних, аналіз самих загроз, визначення найкритичніших із них та шляхів зменшення ризиків викрадення даних

Ключові слова: IoT пристрої; безпека; інформація; загрози: технології; мережеві технології; безпровідний зв'язок; ризики використання.

ВСТУП

Інтернет речей або IoT - це мільярди фізичних пристроїв підключених до Інтернету. Його основна передумова - це просто розширений тип підключення, який потім може бути використаний як основа для виконання всіх видів функцій. IoT описує мережу фізичних об'єктів - "речей", які вбудовані в датчики, програмне забезпечення та інші технології з метою підключення та обміну даними з іншими пристроями та системами через Інтернет. Ці пристрої можуть бути як звичайні побутові предмети, так і складні промислові інструменти. Маючи сьогодні понад 7 мільярдів підключених пристроїв IoT, експерти очікують, що ця кількість зросте до 22 мільярдів до 2025 року. Підключення всіх цих різних об'єктів та додавання до них датчиків, дає рівень цифрового інтелекту пристроям, які в іншому випадку були б німими, дозволяючи їм передавати дані в режимі реального часу без участі людини.

Постановка проблеми. Гучні кібератаки, орієнтовані на IoT, змушують галузі визнавати та управляти ризиками, пов'язаними з розгортанням пристроїв IoT для захисту своїх основних бізнес-операцій. Проводячи це дослідження ми виявили, що 98% всього трафіку пристроїв IoT є незашифрованим, що призводить до викриття особистих та конфіденційних даних в мережі та дозволяє зловмисникам слухати незашифрований мережевий трафік, збирати особисту або конфіденційну інформацію, а потім використовувати ці дані для отримання прибутку чи інших особистих цілей.

Загрози продовжують розвиватися для цільових пристроїв IoT, використовуючи нові складні та методи втручання, такі як однорангове керування та управління, черв'якові функції для самопоширення. У поєднанні зі слабким пристроєм та позицією безпеки мережі зловмисники мають широкі можливості компрометувати системи IoT. 57% пристроїв IoT вразливі до атак середньої або високої ступеня тяжкості, що робить IoT плодом для зловмисників. 41% атак використовують вразливості пристроїв, оскільки атакери проводять сканування через підключені до мережі пристрої, намагаючись знайти найслабкіші для взлому місця.

Аналіз останніх досліджень і публікацій. Проблеми захисту систем які, включають використання IoT пристроїв досліджуються багатьма науковцями та спеціалістами цієї галузі, проте в сучасному світі далеко не кожна компанія-виробник готова заявити про вразливості і загалом незахищеність своїх продуктів (пристроїв). Одні з останніх досліджень та публікацій по виявленню загроз безпеці пристоям інтернету речей серед світових компаній було опубліковано у статтях Ammar, M., Russello, G.,Crispo, B., "Internet of Things: A survey on the security of IoT frameworks"[1] та Toptal, "Are We Creating An Insecure Internet of Things (IoT)? Security Challenges and Concerns"[2].

Світовий ринок Інтернету речей (IoT) вперше досяг 2017 мільярдів доларів у 2017 році, і, за прогнозами, до 2025 року ця цифра зросте до приблизно 1,6 трильйонів доларів. При такому прогнозі технологія передбачає крок далеко вперед. Але з ростом популярності пристроїв IoT буде розвиватися розвиток додатків IoT, а разом з ними зростатимуть і проблеми безпеки.

ISSN 2663 - 4023

Мета статті. Метою статті є визначення причин виникнення загроз безпеці пристроїв інтернету речей, шляхом аналізу технологій передачі даних, аналіз самих загроз, визначення найкритичніших із них та шляхів зменшення ризиків викрадення даних.

РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ

За останні кілька років Інтернет Речей став однією з найважливіших технологій 21 століття, він допомагає людям отримати повний контроль над своїм життям. Тепер, коли ми можемо підключити повсякденні предмети - кухонні прилади, машини, термостати, няні - до Інтернету через вбудовані пристрої, стало можливим безперервне спілкування між людьми, процесами та речами. За допомогою недорогих обчислень, хмари, великих даних, аналітики та мобільних технологій, фізичні речі можуть обмінюватися даними та збирати їх з мінімальним втручанням людини.

IoT чудовий у багатьох відношеннях. Але, на жаль, технологія ще не дозріла, і це не зовсім безпечно. У всьому середовищі IoT, від виробників до користувачів, все ще існує багато проблем безпеки IoT, таких як: норми виготовлення, управління оновленнями, фізичне загартовування, знання та обізнаність користувачів.

IoT дозволяє компаніям автоматизувати процеси та зменшити витрати на робочу силу. Це також скорочує витрати відходів та покращує надання послуг, роблячи виробництво та доставку товарів дешевшим, а також забезпечуючи прозорість транзакцій клієнтів У цьому гіперпов'язаному світі цифрові системи можуть записувати, контролювати та регулювати кожну взаємодію між пов'язаними речами. Фізичний світ відповідає цифровому - і вони співпрацюють.

Екосистема IoT складається з розумних пристроїв з підтримкою Інтернету, які використовують вбудовані системи, такі як процесори, датчики та комунікаційне обладнання, для збору, надсилання та дії на дані, які вони отримують із свого середовища. Пристрої IoT обмінюються даними датчиків, які вони збирають, підключаючись до шлюзу IoT або іншого крайового пристрою, де дані або надсилаються в хмару для їх або локального аналізу. Іноді ці пристрої спілкуються з іншими суміжними пристроями та діють на основі інформації, яку вони отримують один від одного. Пристрої виконують більшу частину роботи без втручання людини, хоча люди можуть взаємодіяти з пристроями - наприклад, для їх налаштування, надання їм інструкцій або доступу до даних.

IoT також може використовувати штучний інтелект (ШІ) та машинне навчання, щоб полегшити та зробити динамічнішими процеси збору даних.

Маючи на місці апаратне та програмне забезпечення пристрою, повинен існувати ще один рівень, який забезпечить розумним об'єктам способи та засоби обміну інформацією з рештою світу IoT. Хоча це правда, що механізми зв'язку тісно пов'язані з апаратним та програмним забезпеченням пристроїв, життєво важливо розглядати їх як окремий рівень. Рівень зв'язку включає як рішення для фізичного підключення (стільниковий, супутниковий, локальна мережа), так і конкретні протоколи, що використовуються в різних середовищах IoT (ZigBee, Thread, Z-Wave, MQTT, LwM2M). Вибір відповідного комунікаційного рішення є однією з найважливіших частин побудови кожного стеку технологій IoT. Вибрана технологія визначатиме не тільки способи надсилання / отримання даних із хмари, але й спосіб керування пристроями та спосіб їх взаємодії зі сторонніми пристроями.

ISSN 2663 - 4023

Отже, розглянемо кілька найпопулярніших рішень для рівня зв'язку. ZigBee популярний бездротовий мережевий стандарт знаходить своє найчастіше застосування в системах управління дорожнім рухом, побутовій електроніці та машинобудуванні (рис.1). Побудований поверх стандарту IEEE 802.15.4, Zigbee підтримує низькі швидкості обміну даними, низьку потужність, безпеку та надійність.

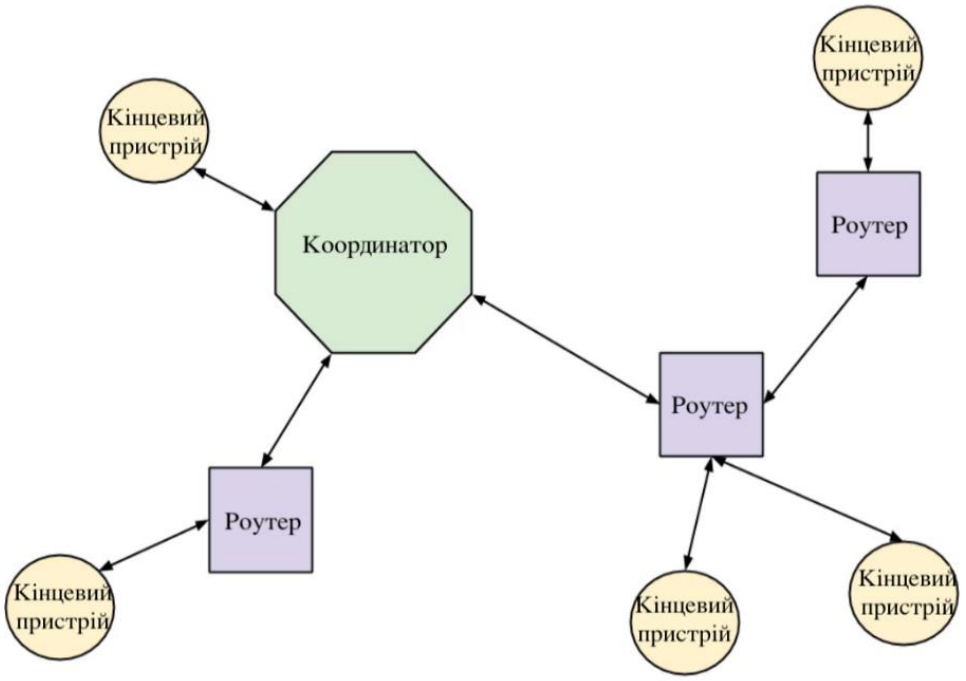

Рис.1. Архітектура мережі ZigBee.

Як добре налагоджена технологія підключення на короткий діапазон, Bluetooth вважається ключовим рішенням, особливо для майбутнього ринку носіїв електроніки, таких як бездротові навушники або датчики геолокації, особливо з огляду на його широку інтеграцію зі смартфонами (рис.2). Розроблений з урахуванням економічної ефективності та зменшеного споживання енергії, протокол Bluetooth Low-Energy (BLE) вимагає дуже мало енергії від пристрою. Однак це має компроміс: при передачі часто більших обсягів даних BLE може бути не найефективнішим рішенням. Проте ця технологія наділена і вразливостями. Наприклад уразливість, що отримала назву CVE-2018-5383 виявили вчені з Ізраїльського технологічного інституту Ліор Нейман і Елі Біхам. Проблема поширюється на стандарти Bluetooth і Bluetooth LE. Дана уразливість надає можливість зловмиснику віддалено отримати доступ до ключа шифрування і перехопити та розшифрувати дані, якими обмінюються гаджети, або впровадити шкідливі повідомлення. Щоб атака була успішною, хакерському пристрою. потрібно перебувати в бездротовому діапазоні з двох уразливих пристроїв Bluetooth, які проходили процедуру сполучення.

ISSN 2663 - 4023

Рис.2. Архітектура мережі Bluetooth.

Sigfox - це технологія LPWAN, яка використовує технології модуляції надвузької смуги (UNB). Методика модуляції дозволяє приймачу слухати лише крихітний фрагмент спектра, щоб мінімізувати перешкоди. Вони здатні досягти дальності від 10 до 50 км при мінімальних перешкодах. Стандарт розгортає диференціальну двійкову фазову маніпуляцію (DBPSK) та гауссову маніпуляцію з частотним зсувом, що забезпечує можливість зв’язку в діапазоні частот ISM. Sigfox працює на частотах 902 МГц та 868 МГц у США та Європі відповідно. Початковий випуск Sigfox був лише однією системою спрямованого зв'язку; однак останній випуск підтримує двонаправлений зв'язок. Стандарти зв'язку Sigfox підтримують до 140 повідомлень висхідної лінії зв'язку щодня, кожне з яких може нести корисне навантаження в 12 октетів зі швидкістю передачі даних до 100 біт в секунду. На рис.3. зображена архітектура типового стандарту Sigfox. Подібно до LoRaWAN, Sigfox також застосовує принцип ALOHA для доступу до каналу, а архітектурна структура типової мережі Sigfox також складається з різних кінцевих вузлів, шлюзів Sigfox, хмари Sigfox та сервера додатків. Мережа базується на топології зірок одного стрибка. Кінцеві вузли можуть бути підключені до шлюзу за допомогою топології зірки для передачі повідомлень на шлюзи. Індивідуальний шлюз пересилає отримані дані в хмару Sigfox, використовуючи захищені IP-з'єднання. Хмара відповідає за управління даними та обробку даних перед тим, як відправити їх на сервер додатків для подальшої обробки.

ISSN 2663 - 4023

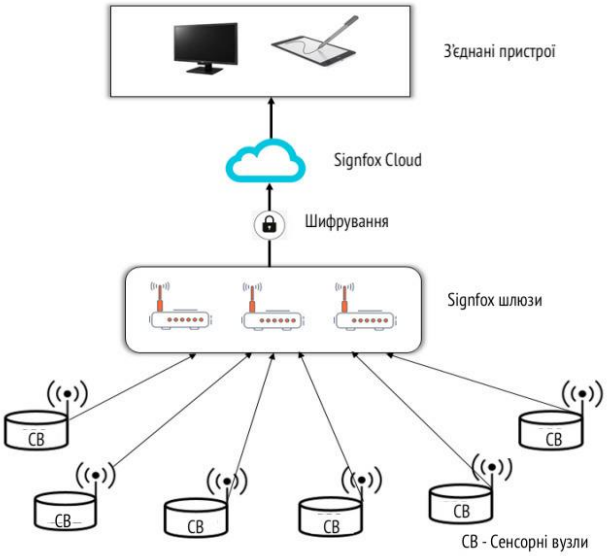

Рис.3. Архітектура стандарту Sigfox

Проаналізуємо основні проблеми та загрози безпеки IoT пристроїв:

1) Відсутність вимог з боку виробників IoT (нові пристрої IoT виходять майже щодня, всі з невиявленими вразливими місцями. Основним джерелом більшості питань безпеки IoT є те, що виробники не витрачають достатньо часу та ресурсів на безпеку. Наприклад, більшість фітнес-трекерів з Bluetooth залишаються видимими після першого сполучення, розумний холодильник може виставити облікові дані для входу в Gmail, а розумний замок із відбитками пальців можна отримати за допомогою ключа Bluetooth, який має ту саму MAC-адресу, що і пристрій замка.Це якраз одна з найбільших проблем безпеки IoT. Поки бракує універсальних стандартів безпеки IoT, виробники продовжуватимуть створювати пристрої з поганою безпекою. Виробники, які почали додавати з'єднання з Інтернетом на свої пристрої, не завжди мають концепцію "безпеки" як найважливіший елемент у процесі проектування своєї продукції. Як підсумок: слабкі, вгадувані або жорстко закодовані паролі; проблеми з обладнанням; відсутність захищеного механізму оновлення; старі та незмінні вбудовані операційні системи та програмне забезпечення; небезпечна передача та зберігання даних)

2) Відсутність знань та обізнаності користувачів(За ці роки користувачі Інтернету навчилися уникати спаму чи фішингу, виконувати сканування вірусів на своїх ПК та захищати свої мережі WiFi надійними паролями. Але IoT - це нова технологія, і люди все ще не дуже багато про це знають. Хоча більшість ризиків проблем безпеки IoT все ще залишаються на виробничій стороні, користувачі та бізнес-процеси можуть створювати більші загрози. Одним із найбільших ризиків та викликів безпеки IoT є незнання та недостатня обізнаність користувача про функціональність IoT. Як результат, усі піддаються ризику.

3) Промислове шпигунство та прослуховування (Якщо хакери беруть на себе нагляд за місцем, заражаючи пристрої IoT, шпигунство може бути не єдиним варіантом. Вони також можуть виконувати такі атаки, вимагаючи грошей на викуп. Таким чином, вторгнення в конфіденційність є ще однією важливою проблемою безпеки IoT. Шпигунство та вторгнення через пристрої IoT є справжньою проблемою, оскільки багато різних конфіденційних даних можуть бути скомпрометовані та використані проти власника. На базовому рівні хакер може захотіти захопити камеру та

використовувати її для шпигунства. Тим не менш, не слід забувати, що багато пристроїв IoT записують інформацію користувачів, будь то медичне обладнання, розумні іграшки, носимі пристрої тощо. На промисловому рівні великі дані компанії, які хакери можуть зібрати для викриття конфіденційної ділової інформації. Деякі країни починають забороняти певні пристрої IoT із проблемами безпеки. Наприклад, інтерактивна лялька IoT зі шпилькою Bluetooth, яка давала доступ до мікрофона та динаміка іграшки будь-кому в радіусі 25-30 метрів. Лялька була позначена як шпигунське пристосування і була заборонена в Німеччині.)

4) Ботнет-атаки (Один пристрій IoT, заражений шкідливим програмним забезпеченням, не представляє реальної загрози; це їх колекція, яка може збити все, що завгодно. Для здійснення ботнет-атаки хакер створює армію ботів, заражаючи їх шкідливим програмним забезпеченням і направляючи відправляти тисячі запитів на секунду, щоб збити ціль. Багато галасу про безпеку IoT почалося після атаки на бота Mirai у 2016 році. Кілька атак DDoS (Рис.4) (розподілена відмова в обслуговуванні) із використанням сотень тисяч IP-камер, NAS та домашніх маршрутизаторів були заражені та спрямовані на збій DNS, який надавав послуги на такі платформи, як GitHub, Twitter, Reddit, Netflix та Airbnb. Проблема в тому, що пристрої IoT дуже вразливі до атак шкідливого програмного забезпечення. Вони не мають регулярних оновлень програмного забезпечення, які має комп'ютер. Тому їх швидко перетворюють на заражених зомбі і використовують як зброю для відправлення неймовірно величезного обсягу трафіку. Більше того, ботнет може загрожувати безпеці електричних мереж, виробничих підприємств, транспортних систем та очисних споруд, що може загрожувати великим групам людей. Наприклад, хакер може одночасно спрацьовувати систему охолодження та опалення, створюючи стрибки на електромережі; у разі масштабної атаки хакери можуть створити загальнонаціональне відключення електроенергії).

5) Проблеми безпеки IoT в управлінні оновленнями пристроїв (Іншим джерелом ризиків безпеки IoT є небезпечне програмне забезпечення чи мікропрограма. Хоча виробник може продати пристрій з останнім оновленням програмного забезпечення, майже неминуче з'являться нові уразливості. Оновлення є критично важливими для забезпечення безпеки пристроїв IoT. Їх слід оновити відразу після виявлення нових уразливостей. Однак, у порівнянні зі смартфонами або комп'ютерами, які отримують автоматичне оновлення, деякі пристрої IoT продовжують використовуватись без необхідних оновлень. Інший ризик полягає в тому, що під час оновлення пристрій надсилатиме свою резервну копію в хмару і матиме короткий час простою. Якщо з'єднання не зашифровано, а файли оновлення незахищені, хакер може викрасти конфіденційну інформацію.)

ISSN 2663 - 4023

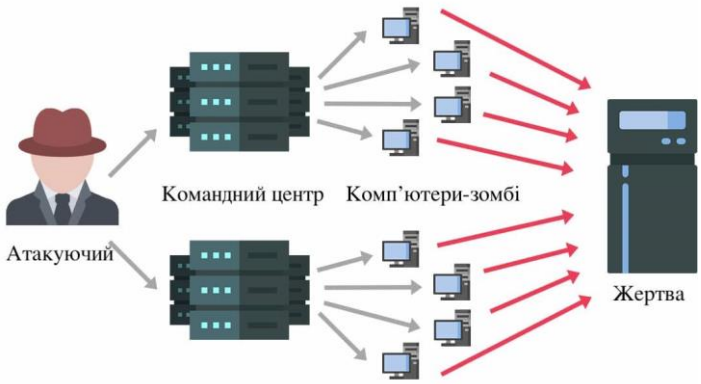

Рис. 4. Архітектура DDOS атаки

6) Бурхлива конкуренція у видобутку, в поєднанні з нещодавнім зростанням оцінок криптовалют, виявляється занадто привабливою для хакерів, які намагаються заробити на криптовалюті.(Хоча більшість вважає блокчейн стійким до злому, кількість атак у секторах блокчейну збільшується. Основна вразливість полягає не в самому блокчейні, а в додатках на основі блокчейну. Соціальна інженерія вже використовується для вилучення імен користувачів, паролів та приватних ключів, і ми побачимо, що в майбутньому це буде частіше використовуватися для злому таких програм. Криптовалюта з відкритим кодом Monero є однією з багатьох цифрових валют, які в даний час видобуваються на пристроях IoT. Деякі з хакерів навіть переробили IP та відеокамери для видобутку криптовалют.Порушення блокчейну, майнери бот-мереж IoT та маніпуляції цілісністю даних представляють величезний ризик для затоплення відкритого криптовалютного ринку та порушення і без того нестабільної вартості та структури криптовалют.)

7) Складність екосистеми.(Оскільки він не повинен виглядати як збірка окремих пристроїв, IoT заплутується у своїй складності. IoT слід розуміти як багату, широку та різноманітну екосистему, яка об'єднує людей, комунікації та інтерфейси. Хоча це спрощує життя та промислове виробництво, застосування концепції не є простим, оскільки в її екосистемі є багато складових. Вони варіюються від датчиків (пристроїв), мереж (мостів, маршрутизаторів, технології WiFi, LiFi тощо) та технологічних стандартів (протоколи: мережа, зв'язок та дані) та нормативних документів (конфіденційність та безпека).)

8) Брак ясності розподілу відповідальностію(Що стосується безпеки пристроїв IoT, є три ключові гравці: виробник, постачальник послуг та користувач. У разі кібератаки розподіл відповідальності не зовсім зрозумілий і може призвести до конфліктів.)

9) Невідповідність рівня захисщеності пристроїв до їх ефективності.(Швидкість виготовлення пристроїв IoT обмежує захисні міркування, і бюджет, ймовірно, матиме вплив, а це означає, що компанія наголошує на зручності використання, а не на безпеці. У деяких випадках не існує рівноваги для оптимізації обладнання та вимог комп'ютера, що використовується з Інтернетом речей.).

10) Обмежені можливості пристроїв. (Це трапляється з більшістю пристроїв, оскільки вони мають обмеження в потужності, обробці та пам'яті. Як наслідок, ними не керують, як мали б за розширеними схемами безпеки, саме тому вони мають більший ризик атак або піддавання дефектам.)

Рекомендації щодо безпеки IoT, які слід врахувати:

- Усі дані, що збираються та інформація, яка зберігається, повинні бути враховані. Кожен фрагмент даних та інформації, що циркулює в системі IoT, повинен бути відповідно відображений. Це стосується не лише того, що збирають датчики та пристрої, розгорнуті в навколишньому середовищі, але також стосується будь-яких можливих облікових даних на серверах автоматизації або інших додатках IoT.
- Кожен пристрій, що підключається до мережі, повинен бути налаштований з урахуванням безпеки. Перед підключенням пристрою до мережі слід забезпечити безпечні налаштування. Це включає використання надійних комбінацій імені користувача та пароля, багатофакторну автентифікацію та шифрування.
- Стратегія безпеки організації повинна будуватися з урахуванням компромісу. Хоча уникати порушень і компромісів важливо, визнання того, що немає ідеального захисту від нових загроз, може допомогти у створенні протоколів пом'якшення наслідків, які можуть значно містити та зменшувати наслідки успішної атаки.
- Кожен пристрій повинен бути фізично захищений. Важливо також враховувати фізичну доступність пристроїв IoT. Якщо сам пристрій IoT не має фізичних засобів захисту від фальсифікацій, його слід тримати в обмеженому місці або закріпити відповідними замками або іншими інструментами. Наприклад, IP-камери можна підробляти безпосередньо, якщо до них дістанеться кіберзлочинець. Їм можна імплантувати шкідливе обладнання або програмне забезпечення, яке може спричинити збої в системі або поширити зловмисне програмне забезпечення.
- Додатки, структури та платформи IoT, які покладаються на технологію блокчейн, повинні регулюватися, постійно відстежуватися та оновлюватися, щоб запобігти будь-яким майбутнім використанням криптовалюти.
- Одним з найкращих способів захисту від викрадення даних є використання транспортного шифрування та стандартів, таких як TLS. Інший спосіб - використовувати різні мережі, які ізолюють різні пристрої.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Отже, в даній статті проведено аналіз роботи найпопулярніших існуючих технологій, які використовуються в IoT системах. Також, розглянуто найбільші та найпоширеніші проблеми, з якими можуть зустрітися користувачі таких систем, та наведено перелік рекомендацій щодо безпеки використання IoT пристроїв. Захищеність IoT систем на разі дуже далека від ідеалу, проте не всі ризики використання пов’язані з виробником. Користувач повинен розуміти яким саме пристроєм він користується, як правильно його застосовувати, налаштовувати та зберігати. Необхідно не забувати про комплексний підхід до підбору пристроїв та побудови як масштабних, так і дрібних розумних систем, оскільки в кінцевому результаті вони утворюють єдину мережу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Internet of Things: A survey on the security of IoT frameworks. (2018). https://www.scopus.com/record/display.uri?eid=2-s2.0-85034956984&origin=inward&txGid=37c46c8a89ed3b875d1535151abfcd20.

2 *Are We Creating An Insecure Internet of Things (IoT)?* (б. д.). Security Challenges and Concerns. https://www.toptal.com/it/are-we-creating-an-insecure-internet-of-things.

3 *2020 Unit 42 IoT Threat Report 2020 Unit 42 IoT Threat Report*. (б. д.). Unit42. https://unit42.paloaltonetworks.com/iot-threat-report-2020/

4 *8 types of security threats to IoT | IoT security threats* |. (б. д.). Application development | Big data| IoT | Digital Business | Cloud. https://www.allerin.com/blog/8-types-of-security-threats-to-iot

5 *IoT News - Common Threats to IoT Devices & How to Protect Yourself - IoT Business News*. (б. д.). IoT Business News. https://iotbusinessnews.com/2020/01/29/06026-common-threats-to-iot-devices-how-to-protect-yourself/

6 *Counting Down the Top Ten IoT Security Threats*. (б. д.). IoT Evolution World. https://www.iotevolutionworld.com/iot/articles/445972-counting-down-top-ten-iot-security-threats.htm

7 Smith, A. (2020, 2 лютого). *The Five Biggest Security Threats and Challenges for IoT - DZone IoT*. dzone.com. https://dzone.com/articles/the-biggest-security-threats-and-challenges-for-io

8 *The IoT Attack Surface: Threats and Security Solutions - Noticias de seguridad*. (б. д.). Trend Micro (DE) | Cybersicherheitslösungen für Unternehmen. https://www.trendmicro.com/vinfo/mx/security/news/internet-of-things/the-iot-attack-surface-threats-and-security-solutions

9 *The Top 10 IoT Security Threats and Vulnerabilities – Particle Blog*. (б. д.). Particle Blog. https://blog.particle.io/the-top-10-iot-security-threats/

10 *Top 10 IoT Security Issues: Ransom, Botnet Attacks, Spying*. (б. д.). Intellectsoft Blog. https://www.intellectsoft.net/blog/biggest-iot-security-issues/

11 Безпека IoT починається з ідентифікації. https://iot-ssl.com.ua/iot.html.

12 У Bluetooth знайшли масштабну вразливість. https://nv.ua/ukr/techno/it-industry/u-bluetooth-znajshli-masshtabnu-vrazlivist-2484381.html.

13 *A Survey on the Security of Low Power Wide Area Networks: Threats, Challenges, and Potential Solutions*. (б. д.). PubMed Central (PMC). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7602051/

14 AVSystem. (2020, 5 травня). *What technologies are used in IoT – technology behind Internet of Things*. AVSystem – Shaping The World of Connected Devices. https://www.avsystem.com/blog/iot-technology/

15 *Інтернет речей - IoT пристрої та їх безпека, рекомендації ESET*. (б. д.). ESET - офіційний сайт. Антивірусні програми Ісет в Україні. | ESET. https://eset.ua/ua/news/view/669/Internet-veshchey-v-biznes-srede-vyzovy-dlya-kiberbezopasnosti.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (11), 2021
ISSN 2663 - 4023

Ivan R. Opirskyy
Dc.S., Associate Professor, Professor of Information Security Department
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0002-8461-8996
ivan.r.opirskyi@lpnu.ua

Holovchak V. Romana
Cybersecurity student
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID:0000-0002-2932-3466
romana.holovchak.kb.2018@lpnu.ua

Moisiichuk R. Iryna
Cybersecurity student
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID:0000-0002-7531-5811
iryna.moisiichuk.kb.2018@lpnu.ua

Balianda S. Tetyana
Cybersecurity student
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID:0000-0002-0066-6131
tetiana.balianda.knm.2018@lpnu.ua

Haraniuk P. Sofiia
Cybersecurity student
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID:0000-0002-0626-2859
sophiegaranyk96@gmail.com

PROBLEMS AND SECURITY THREATS TO IOT DEVICES

Abstract. The Internet of Things or IoT is billions of physical devices connected to the Internet. Its main premise is simply an extended type of connection, which can then be used as a basis for all kinds of functions. IoT describes a network of physical objects - "things" that are built into sensors, software and other technologies to connect and communicate with other devices and systems over the Internet. Problems of system protection, including the use of IoT devices are studied by many scientists and specialists in this field, but in today's world, not every manufacturer is ready to declare vulnerabilities and general insecurity of their products (devices). Throughout the IoT environment, from manufacturers to users, there are still many IoT security issues, such as manufacturing standards, update management, physical hardening, user knowledge and awareness. This article examines the vulnerabilities of the Internet of Things. The analysis of information transfer technologies of IoT devices (in particular ZigBee, Signfox and Bluetooth) is carried out. The most common threats that a user may encounter have been identified and analyzed. It is also established that usually not only the manufacturer poses a threat to the security of IoT devices. There are also a number of tips for users who want to reduce the risk of data leakage associated with vulnerabilities in the Internet of Things. Unfortunately, it is not uncommon for such devices to be incorrectly set up, used and stored. Extremely common is the user's refusal to update the software, which in turn leaves open those vulnerabilities that the manufacturer is trying to fix. The main purpose of the article is to determine the causes of security threats to the Internet of Things, by analyzing data transmission technologies, analysis of the threats themselves, identifying the most critical of them and ways to reduce the risk of data theft

Keywords: IoT devices; security; information; threats: technology; network technologies; wireless communication; risks of use.

REFERENCES

1 Internet of Things: A survey on the security of IoT frameworks. (2018). https://www.scopus.com/record/display.uri?eid=2-s2.0-85034956984&origin=inward&txGid=37c46c8a89ed3b875d1535151abfcd20.
2 Are We Creating An Insecure Internet of Things (IoT)? Security Challenges and Concerns. https://www.toptal.com/it/are-we-creating-an-insecure-internet-of-things.
3 2020 Unit 42 IoT Threat Report 2020 Unit 42 IoT Threat Report. Unit42. https://unit42.paloaltonetworks.com/iot-threat-report-2020/
4 8 types of security threats to IoT | IoT security threats. Application development | Big data | IoT | Digital Business Cloud. https://www.allerin.com/blog/8-types-of-security-threats-to-iot
5 IoT News - Common Threats to IoT Devices & How to Protect Yourself - IoT Business News. IoT Business News. https://iotbusinessnews.com/2020/01/29/06026-common-threats-to-iot-devices-how-to-protect-yourself/
6 Counting Down the Top Ten IoT Security Threats. IoT Evolution World. https://www.iotevolutionworld.com/iot/articles/445972-counting-down-top-ten-iot-security-threats.htm
7 Smith, A. (2020, February 2). The Five Biggest Security Threats and Challenges for IoT - DZone IoT. dzone.com. https://dzone.com/articles/the-biggest-security-threats-and-challenges-for-io
8 The IoT Attack Surface: Threats and Security Solutions - Security News. Trend Micro (DE) | Cybersecurity solutions for companies. https://www.trendmicro.com/vinfo/mx/security/news/internet-of-things/the-iot-attack-surface-threats-and-security-solutions
9 The Top 10 IoT Security Threats and Vulnerabilities - Particle Blog. Particle Blog. https://blog.particle.io/the-top-10-iot-security-threats/
10 Top 10 IoT Security Issues: Ransom, Botnet Attacks, Spying. Intellectsoft Blog. https://www.intellectsoft.net/blog/biggest-iot-security-issues/
11 IoT security begins with identification. https://iot-ssl.com.ua/iot.html.
12 A large-scale vulnerability has been found in Bluetooth. https://nv.ua/ukr/techno/it-industry/u-bluetooth-znajshli-masshtabnu-vrazlivist-2484381.html.
13 A Survey on the Security of Low Power Wide Area Networks: Threats, Challenges, and Potential Solutions. PubMed Central (PMC). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7602051/
14 AVSystem. (2020, May 5). What technologies are used in IoT - technology behind Internet of Things. AVSystem - Shaping The World of Connected Devices. https://www.avsystem.com/blog/iot-technology/
15 Internet of Things - IoT devices and their security, ESET recommendations. ESET is the official site. Iset antivirus programs in Ukraine. | ESET. https://eset.ua/ua/news/view/669/Internet-veshchey-v-biznes-srede-vyzovy-dlya-kiberbezopasnosti.