Аналіз кіберзагроз для IoT-систем.

1.0.

Хоча Інтернет речей може здатися новим явищем, його походження сягає XIX століття. У 1832 році барон Шиллінг створив перший електромагнітний телеграф, що дозволяв здійснювати пряму комунікацію між двома машинами за допомогою передачі електричних сигналів. Ця міжмашинна взаємодія (M2M) лягла в основу подальшого розвитку Інтернету речей.

Він має широкі можливості, від спрощення повсякденного життя користувачів до перетворення різних галузей, у тому числі виробництва. Можна припустити, що розвиток промислового Інтернету речей (IIoT) почався у 1992 році, коли програмовані логічні контролери (ПЛК) отримали здатність до підключення. З того часу вони відіграють важливу роль у розробці та використанні автоматизованих ліній зборки та промислових роботів на заводах.

Сучасний світ вже важко уявити без Інтернету речей, повсякденне життя охоплено низкою технологічних процесів. За допомогою IoT пристроїв ми можемо здійснювати моніторинг, управління та взаємодію з навколишнім середовищем, збільшуючи ефективність, зручність та безпеку нашого життя та бізнесу. Проте разом з неймовірними можливостями IoT виникають і нові виклики, пов'язані з безпекою, конфіденційністю та захистом даних.

Всі знають наскільки важливо зберігати конфіденційну інформацію, але чи точно знають як це роботи? Багато речей залежить безпосередньо від користувача, його відповідальності, розуміння та готовності забезпечити захист для себе. Багато залежить і від виробників, зокрема фізична захищеність пристрою та можливість його цифрового захисту, але якщо не користуватися певними правилами та можливостями захисту, то нараженя на небезпеку стає надто вірогідною подією. В нашому часі хакери можуть скористатися будь якими пристроями з вашої системи, для досягнення своєї мети, тому дуже важливо знати можливі ризики та вміти їх запобігати.

1.1. Загальна характеристика IoT-мереж та систем.

Інтернет речей (IoT) описує мережу фізичних об'єктів - "речей", оснащених датчиками, програмним забезпеченням та іншими технологіями для підключення та обміну даними з іншими пристроями та системами через Інтернет. Ці пристрої можуть бути як звичайними предметами побуту, так і складними промисловими інструментами. Експерти очікують, що кількість активних пристроїв буде налічувати близько 22 мільярдів до 2025 року.

Протягом останніх років IoT став однією з ключових технологій XXI століття. Тепер, коли ми можемо підключати предмети побуту - кухонне обладнання, автомобілі, термостати, радіоняні - до Інтернету за допомогою вбудованих пристроїв, відбувається безперешкодна комунікація між людьми, процесами та об'єктами.

Завдяки доступним обчислюваним ресурсам, хмарним технологіям, великим даним, аналітиці та мобільним технологіям фізичні об'єкти можуть обмінюватися даними та збирати їх, при цьому втручання людини мінімальне. У цьому гіперпов'язаному світі цифрові системи можуть реєструвати, відстежувати та регулювати кожну взаємодію між підключеними об’єктами. Фізичний світ зустрічається з цифровим - і вони співпрацюють.

Хоча ідея IoT існує вже давно, останні досягнення в різних технологіях зробили її практичною:

1. Доступність недорогих сенсорних технологій. Доступні та надійні датчики роблять IoT доступним для більшої кількості виробників.

2. Зв'язок. Багато мережевих протоколів спростили підключення датчиків до хмари та інших "речей" для більш ефективної передачі даних.

3. Платформи хмарних обчислень. Збільшення доступності хмарних платформ дозволяє як підприємствам, так і споживачам отримувати доступ до інфраструктури, необхідної для масштабування, без необхідності фактичного управління цим.

4. Машинне навчання та аналітика. Завдяки досягненням у сфері машинного навчання та аналітики, а також доступу до різноманітних та

великих обсягів даних, що зберігаються в хмарі, компанії можуть збирати інформацію швидше та простіше. Поява цих супутніх технологій продовжує розширювати межі, і дані, що виробляються Інтернетом речей, також живлять ці технології.

5. Голосовий штучний інтелект (AI). Досягнення у сфері нейронних мереж внесли обробку природної мови (NLP) до пристроїв IoT (таких як цифрові особисті помічники Alexa, Cortana та Siri) і зробили їх привабливими, доступними та придатними для домашнього використання.

Промисловий Інтернет речей (IIoT) використовується для застосування технології Інтернету речей в промисловому середовищі, особливо щодо контролю і вимірювань, а також управління датчиками та пристроями, які використовують хмарні технології. Останнім часом галузі використовують міжмашинну комунікацію (M2M), щоб забезпечити бездротову автоматизацію та контроль. Проте з появою хмарних і супутніх технологій (таких як аналітика та машинне навчання) галузі можуть досягти нового рівня автоматизації та створити нові джерела доходів і бізнес-моделі. IIoT іноді називають четвертою промисловою революцією або Індустрією 4.0. Нижче наведено деякі загальні області використання IIoT:

1.Розумне виробництво;

2.Підключені активи та передбачуване обслуговування;

3.Розумні електромережі;

5.Розумні міста;

5.Підключена логістика;

6.Розумні цифрові ланцюги постачання.

Організації, які найбільше виграють від IoT, це ті, які можуть інтегрувати датчикові пристрої у свої бізнес-процеси.

Виробництво:

Виробники можуть здобути конкурентну перевагу, використовуючи моніторинг виробничих ліній для передбачуваного технічного обслуговування обладнання за умови виявлення датчиками майбутньої несправності. Це

дозволяє знижувати витрати на експлуатацію, забезпечувати кращу доступність обладнання та покращувати управління активами.

Автомобільна промисловість:

Використання IoT в автомобільній галузі може значно підвищити безпеку водіїв та забезпечити прогнозоване технічне обслуговування для автомобілів на дорозі за допомогою реальних часових сповіщень про можливі відмови обладнання.

Транспорт та логістика:

Застосування в транспорті та логістиці дозволяє ефективне управління транспортними засобами та вантажами з використанням даних від датчиків. Це дозволяє оптимізувати маршрутизацію та знижувати затримки.

Інші галузі, такі як роздрібна торгівля, охорона здоров'я та загальна безпека праці у всіх галузях промисловості, також можуть виграти від використання технологій для вдосконалення своїх процесів та забезпечення безпеки.

До основних характеристик мереж та систем Інтернету речей відносяться наступні:

Можливість підключення: слідкує за можливістю підключення пристроїв до Інтернету, що забезпечує обмін даними між пристроями, користувачами та хмарними сервісами.

Датчики та виконавчі механізми: зазвичай прилади оснащені різними типами датчиків (температури, вологості, руху тощо), які збирають дані з навколишнього середовища, а також виконавчими механізмами, які можуть виконувати певні дії на основі зібраних даних.

Зв'язок: IoT можуть використовувати різні технології зв'язку, такі як Wi-Fi, Bluetooth, Zigbee, LoRaWAN і т.д., для передачі даних.

Хмарне зберігання та обробка даних: зібрані данні можуть бути збережені та оброблені у хмарних сервісах для аналізу, використання та подальшого управління.

Масштабованість: Системи IoT повинні мати здатність масштабуватися, щоб враховувати зростання кількості підключених пристроїв і обсягу оброблюваних даних.

Безпека: спираючись на попередній фактор, безпека є критичною характеристикою мереж та систем Інтернету речей. Забезпечення конфіденційності, цілісності та доступності даних стає важливою задачею.

Отже, основною характеристикою мереж та систем є їхня здатність до підключення, збору, передачі, аналізу та управління даними з різних пристроїв для досягнення певних цілей у різних сферах.

1.2. Типи загроз, які впливають на безпеку IoT

З розвитком технологій зростає онлайн-вразливість пристроїв та мереж Інтернету. Безпека IoT передбачає захист пристроїв та мереж, до яких вони підключені, від онлайн-загроз і вторгнень.

Взагалі безпека Інтернету речей - це широкий термін, що охоплює стратегії, інструменти, процедури, системи та методи, які використовуються для захисту всіх складових. Для забезпечення доступності, цілісності та конфіденційності екосистеми необхідно захищати фізичні компоненти, додатки, дані та мережеві з'єднання.

Впровадження IoT пристроїв ставить перед користувачем та IT-командою завдання забезпечення безпеки. Комплексний підхід може допомогти ефективно вирішувати проблеми.

В середньому, щотижня 54% організацій стикаються з спробами кібератак, спрямованими на пристрої Інтернету речей. Найбільш піддаються атакам пристрої в європейських організаціях, за якими слідують організації з Азіатсько-Тихоокеанського регіону та Латинської Америки. Сучасні технології стали неодмінною частиною нашого повсякденного життя. Одним з факторів, які сприяли зростанню кібератак, є швидка цифрова трансформація.

Атаковані пристрої різноманітні: маршрутизатори, IP-камери, DVR (цифрові відеореєстратори), NVR (мережеві відеореєстратори), принтери та

багато іншого. Динаміки та IP-камери, стають все більш поширеними в середовищах віддаленої роботи та навчання, що надає кіберзлочинцям безліч потенційних точок входу.

Надійна стратегія безпеки охоплює всі аспекти захисту, такі як підсилення компонентів, оновлення вбудованого програмного забезпечення, відстеження, контроль доступу, виявлення загроз та усунення вразливостей.

Проблеми безпеки часто виникають через те, що пристрої Інтернету речей не розробляються з урахуванням безпеки як головного пріоритету, більшість розробників систем більше зосереджуються на функціональності пристроїв. Це може мати серйозні наслідки для користувачів і призвести до потенційних витоків даних. Нижче наведений список проблем безпеки, пов'язаних із згаданими вище пристроями, які можуть піддатися ризику .

Відсутність фізичної безпеки.

Недостатня фізична безпека на пристроях є легкою мішенню для зловмисників. Протягом тривалого часу пристрої IoT, розміщені у віддалених районах, стають доступними за допомогою фізичних змін. Хакери можуть легко скористатися проблемами безпеки на пристроях з недостатньою або взагалі відсутньою фізичною безпекою.

Наприклад, пристрої Інтернету речей можуть бути інфіковані шкідливим ПЗ через USB-накопичувачі. Основна відповідальність виробників полягає в наданні пріоритету фізичній безпеці. Проте створення безпечних і захищених передавачів та датчиків за доступною ціною може виявитися складною задачею для розробників.

Відсутність видимості.

Для IT-команди є складним завданням забезпечити видимість всіх пристроїв в мережі, оскільки багато з них не зареєстровані в інвентарних записах IT. Наприклад, кавоварки, системи вентиляції та кондиціювання повітря, не мають значення для відстеження IT-командами.

Служби безпеки не зможуть запобігти взломам, якщо вони не зможуть бачити, що підключено до мережі. Відсутність видимості пристроїв ускладнює можливість точного обліку того, що потрібно захищати та контролювати.

Конфіденційність даних.

В Інтернеті речей серйозною проблемою є конфіденційність даних. Інформація користувачів передається через багато пристроїв, наприклад, дані пацієнтів з медичного обладнання та особиста інформація з розумних іграшок та носимих пристроїв.

Наприклад, хакер або кіберзловмисник може зібрати корпоративні дані та розголосити, продати або використовувати їх для вимагання викупу у власника.

Ботнет та DDoS-атаки.

Ботнети та DDoS-атаки є одними з найбільш поширених загроз для пристроїв IoT. Ботнети представляють собою мережі взламаних пристроїв, які керуються кіберзлочинцями. Ці ботнети можуть бути використані для запуску розподілених атак типу «відмова у обслуговуванні» (DDoS), які перевантажують цільовий сервер або веб-сайт великими обсягами трафіку, що призводить до його недоступності.

Програми-вимагачі.

У цій проблемі безпеки Інтернету речей атаки програм-вимагачів шифрують та блокують доступ до конфіденційних файлів. Хакер вимагає викуп за ключ розшифрування для розблокування файлів.

Пристрої Інтернету речей зі слабкою безпекою також можуть стати об'єктами, але випадки атак програм-вимагачів на IoT наразі не спостерігаються.

Шпигунство та прослуховування.

Пристрої з вбудованими мікрофонами та камерами можуть бути взламані для слідкування за окремими людьми чи організаціями. Це може призвести до порушення конфіденційності та розголошення приватних розмов чи інтелектуальної власності.

Атаки «людина посередині».

Під час цих атак кіберзлочинці перехоплюють і змінюють зв'язок між пристроями Інтернету речей та пов'язаними з ними серверами або мережами. Це може призвести до маніпулювання даними, несанкціонованого доступу або прослуховування повідомлень.

Медичні гаджети, розумний дім та інші інтелектуальні пристрої можуть бути у небезпеці у майбутньому через їх зростаючу цінність для власників та залежність від цих пристроїв як від критично важливих систем.

Звісно теоретично легко обговорювати можливі загрози, тому розглянемо чотири реальні приклади взлому Інтернету речей.

1. Незахищена мережа університету: У звіті Verizon Data Breach Digest за 2017 рік описується приклад університету, чиє мережа була завалена запитами DNS для ресторанів морепродуктів. Зловмисники використовували 5000 пристроїв Інтернету речей, таких як торгові автомати та системи освітлення, для атаки на університетську мережу через слабкі паролі.

2. Взлом IoT-камер: Деякі камери безпеки IoT, зокрема NeoCoolCam, виявились з важливими проблемами безпеки, що дозволяє їх взламувати. Використовуючи ці камери, зловмисники можуть незаконно спостерігати або навіть проникнути в мережу.

3. Ботнет Mirai: Це зловмисна програма, яка заражає мережеві пристрої, які працюють на Linux, шукаючи вразливі пристрої IoT в Інтернеті. Вона використовує фабричні імена користувачів та паролі, що встановлені за замовчуванням, для доступу до пристроїв.

4. Взлом автомобіля Jeep: Дослідники Чарлі Міллер і Кріс Валасек змогли використати вразливості в системі розваг автомобіля Jeep Cherokee, щоб віддалено керувати автомобілем. Це включало можливість впливати на рульове керування та гальма, що створювало серйозну загрозу безпеці.

1.3. Інструменти, технології, методи для підвищення рівня безпеки IoT мереж.

Найкращі практики забезпечення безпеки Інтернету речей включають в себе наступне:

Використання надійних протоколів аутентифікації та шифрування: Застосування надійних методів аутентифікації користувачів та шифрування даних є важливими для запобігання несанкціонованому доступу та збереження конфіденційності інформації. Адміністраторам важливо розуміти широкий спектр протоколів, які використовуються в їх системах Інтернету речей, оскільки це дозволить їм ефективно зменшити ризики та запобігти загрозам безпеки. Ці протоколи можуть варіюватися від стандартних і широко відомих, таких як Bluetooth та Near Field Communication (NFC), до менш відомих, таких як nRF24, nRFxx, 443МГц, LoRA та LoRaWAN, а також оптичних та інфрачервоний зв'язок. Це допоможе забезпечувати сумісність та інтеграцію різних протоколів в межах системи IoT.

1. Протоколи аутентифікації розуміють під собою використання надійних протоколів, таких як двофакторна аутентифікація (2FA) або багатофакторна аутентифікація (MFA), дозволяє впевнитися у легальності доступу до системи. Прикладом може бути введення пароля та отримання коду підтвердження на мобільний телефон.

2. Шифрування є процесом кодування даних, який робить їх доступними лише авторизованим користувачам, є ключовим для забезпечення безпеки в IoT. Широко використовується стандарт шифрування AES, який забезпечує надійний рівень захисту. Використовуйте надійні та унікальні паролі для всіх облікових записів. Надійні паролі допомагають у запобіганні багатьох кібератак. Менеджери паролів можуть допомогти користувачам створювати унікальні та надійні паролі, які користувачі можуть зберігати в самому додатку або програмному забезпеченні.

Контроль доступу: Встановлення правильного контролю доступу до пристроїв і мережі зберігає дані в безпеці та допомагає уникнути їх несанкціонованого використання . Загалом, це визначення того, хто або що має право доступу до конкретних ресурсів. Це може бути реалізовано через

управління обліковими записами користувачів та наділення їх відповідними правами доступу. Програмні рішення, такі як AWS IoT Core від Amazon, забезпечують ці функції.

Надайте перевагу безпеці Wi-Fi. Деякі способи, якими користувачі можуть це зробити, включають увімкнення брандмауера роутера, вимкнення WPS та ввімкнення протоколу безпеки WPA2, а також використання надійного пароля для доступу до Wi-Fi. Забезпечення безпеки налаштувань роутера також є важливою частиною цього кроку.

Забезпечте збіг IoT-хмар та використовуйте хмарні рішення. Інтернет речей та хмара стають все більш інтегрованими. Важливо враховувати вплив кожної технології на безпеку іншої. Хмарні рішення також можна розглядати як додаткові засоби безпеки та можливості обробки даних на периферійних пристроях Інтернету речей.

Регулярне оновлення програмного забезпечення: оновлення ПЗ є критично важливим для забезпечення безпеки пристроїв. Своєчасне оновлення дозволяє виправляти виявлені вразливості та запобігати потенційним атакам. Однією з ключових рекомендацій є постійне відстеження та впровадження оновлень для всіх пристроїв та програмного забезпечення.

Особливу увагу варто приділяти бібліотекам та пакетам, які використовуються в розробці програмного забезпечення. Оскільки більшість оновлень спрямовані на усунення відомих шляхів проникнення, що знаходять зловмисники, своєчасне застосування цих оновлень значно знижує ризик компрометації.

Загалом, регулярне оновлення ПЗ є фундаментальною практикою для підтримання безпеки IoT-систем, що допомагає мінімізувати ризики та захищати дані від потенційних загроз.

Існують інструменти автоматичного оновлення залежностей, такі як Dependabot або Renovate. Вони спрощують процес підтримки актуальності кодової бази. Ці інструменти автоматизують завдання перевірки та застосування оновлень до залежностей. Вони усувають необхідність ручних

перевірок з боку розробників. Ці інструменти гарантують, що кодова база буде оновлена до останніх безпечних версій.

Моніторинг уразливостей та аудити безпеки: Проведення регулярних моніторингів уразливостей системи та аудитів безпеки допомагає вчасно виявляти потенційні загрози та запобігати їхньому використанню зловмисниками. Аудит безпеки відіграє ключову роль у забезпеченні надійності та цілісності додатків Інтернету речей. Вони включають в себе:

1. Ретельне тестування, аналіз та оцінку заходів безпеки,

2. Виявлення потенційних вразливостей (наприклад, потенційних точок входу для шкідливих атак).

Вони також повідомлять вас про слабкі механізми аутентифікації чи недостатні протоколи шифрування. Проводячи аудит безпеки, організації можуть виявити та усунути слабкі місця безпеки.

Огляд коду - важка практика для забезпечення безпеки. В ньому бере участь людина, яка відрізняється від розробника, що написав код. Така особа переглядає код з іншої точки зору, що дозволяє їй виявити потенційні проблеми безпеки та кодування, які могли бути пропущені автором.

Завдяки перевірці коду розробники можуть скористатися новими поглядами та досвідом. Інтегруючи регулярну перевірку коду в процес розробки, організації можуть підвищити безпеку.

Юридичний аудит включає перевірку політики на відповідність певним законам та правилам. Оцінюючи вимоги, юристи виявляють прогалини в заходах безпеки. Вони можуть рекомендувати необхідні дії та забезпечувати відповідність правових рамок. Це дозволить знизити юридичні та нормативні ризики.

Політика конфіденційності також є важливою складовою, яка описує, як ви збираєте, зберігаєте та передаєте дані своїх користувачів. Юристи також допомагають у впровадженні механізмів захисту даних та механізмів згоди.

Створення культури безпеки: важливо розвивати усвідомленість про безпеку серед користувачів та персоналу, щоб уникнути простих помилок та захистити систему від внутрішніх загроз.

Забезпечення безпеки важкого використання GPS є важливим аспектом для деяких пристроїв та застосунків Інтернету речей, оскільки це може створювати потенційні проблеми з захищеностю. Особливу увагу слід приділяти випадкам, коли сигнали GPS можуть бути перешкоджені або навіть підроблені, особливо якщо вони використовуються для систем позиціонування у виробництві, моніторингу та інших функцій. Якщо ці системи є важливими для компанії, у ній також повинні існувати засоби моніторингу сигналів GPS. Ще одним варіантом може бути використання компанією інших систем позиціонування, таких як Real-Time Kinematic (RTK) або Differential GNSS (DGNSS або DGPS).

Також не слід забувати, що з моменту створення будь-який фізичний пристрій може підлягати несанкціонованому втручанню способом, не передбаченим виробником чи продавцем.

Пристрої Інтернету речей є особливою ціллю, оскільки вони мають багато функцій, які можуть бути цікавими для інших:

1.Можуть знаходитися в приватних, віддалених або необслуговуваних місцях, тому доступ не обмежений як фізично, так і за часом.

2.Деякі пристрої IoT можуть мати невеликий розмір, тому їх легко приховати в разі крадіжки.

3. З характеру та місцезнаходження пристрою часто стає зрозуміло, що якщо він буде скомпрометований, то його використають для атаки на конкретну ціль. Як тільки один пристрій опиниться в руках зловмисника, багато подібних пристроїв також будуть взламані, що в подальшому призведе до можливої розподіленої атаки типу "відмова в обслуговуванні" на бажаний об’єкт. Такий алгоритм дій, спрямований на пристрої IoT, може надати хакеру подальший доступ до мережі.

4. Деякі пристрої можуть використовуватися протягом багатьох років. Технології розвиваються, тож з часом може стати легше взламати пристрій, створений на базі застарілих технологій.

Щоб скомпрометувати пристрій, що знаходиться безпосередньо перед злодієм, він скоріш за все виконає наступні дії:

1.Фізичне відкриття пристрою для доступу до його складових частин. Це може включати розбірку корпусу або видалення захисних панелей для доступу до компонентів пристрою.

2.Підключення до фізичного порту пристрою. Це може бути використання різних кабелів або адаптерів для підключення до портів, які можуть надати доступ безпосередеьо до системи або даних пристрою.

3.Використання безконтактної технології для виявлення активності пристрою. Наприклад, це може включати використання приладів для виявлення електромагнітного випромінювання, високо- або низькочастотних звуків, коливань напруги живлення тощо.

Ключем до досягнення будь-якої з цих цілей є доступ до пристрою. Чим більше захисних заходів використовується для забезпечення безпеки пристрою, тим більше часу і зусиль потрібно для його компрометації.

Як вже раніше згадувалось, про майбутню безпеку мають піклуватися не лише безпосередні користувачі, але й виробники пристроїв, розглянемо способи забезпечення захищеності пристроїв з точки зору виробництва, та що варто зробити, якщо постачальники все ж таки знехтували цими заходами.

Першим кроком у захисті пристрою перед запуском у виробництво є видалення всіх фізичних, радіо- або оптичних портів, які використовувалися для розробки. Звичайно, для підключення виробничого пристрою до локальної мережі або знову до хмари потрібен принаймні один порт, але всі інші порти, які вже не потрібні, повинні бути видалені, включаючи будь-які відповідні доріжки на печатній платі, які з'єднують порт зі схемою.

Аналогічно, ідеально видалити всі тестові точки, включаючи контакти та доріжки, або, принаймні, ефективно заборонити доступ до тестування, наприклад, спалюючи вбудовані запобіжники для JTAG.

Якщо виробничому пристрою необхідно мати який-небудь порт адміністрування, це стане основною ціллю зловмисників. Тому логічний доступ до цього порту повинен бути дуже жорстко заблокований. Отже, на ньому повинен працювати єдиний сервіс, необхідний для адміністрування, всі інші сервіси повинні бути вимкнені і не відповідати на запити інструментів сканування тощо. Сервіс адміністрування повинен використовувати безпечний протокол, такий як SSH; використання небезпечного протоколу, такого як Telnet, на адміністративному порту фактично залишає пристрій широко відкритим. Управління обліковими даними для доступу до цього порту повинно бути безпечним та ефективно управленим, щоб гарантувати, що доступ не може бути несанкціонованим.

Чіпи, які керують критично важливими функціями, іноді можуть бути видалини зловмисниками з печатних плат, щоб вони могли підключити їх до випробувального обладнання для аналізу. Щоб запобігти цьому, чіпи ключів можна приклеїти епоксидною смолою до печатної плати або інших елементів, щоб чіп руйнувався під час його видалення. Крім того, вся схема може бути вбудована в блок смоли, що зробить її абсолютно недоступною для всіх, крім самих рішучих.

Звичайно, останньою лінією захисту є сам корпус пристрою. Це може забезпечити фізичний захист внутрішніх частин, стати частиною монтажного вузла та допомогти захиститися від виявлення випромінювання. Один з варіантів — зробити пристрій постійно відключеним, якщо корпус відкритий.

Завжди існує ризик того, що пристрій може бути підроблений десь у ланцюжку постачання, наприклад, на складі або під час транспортування. Для візуальної індекації будь-якої спроби втручання у продукт можна використовувати упаковку або пломби, що захищають від несанкціонованого доступу.

Не слід забувати що є спеціальні пристрої Інтернету Речей, такі як датчики або камери відеоспостереження, які допомагають у підвищенні безпеки, але їх також слід в свою чергу захищати та налаштовувати відповідно. Доцільно створювати своєрідні «обманки», які будуть відволікати зловмисника, концентруючи увагу на собі, поєднувати системи захисту та інше.

Ще одна корисна порада буде розглянути можливість отримання реально-часових повідомлень про небезпеку та виявляти здатність до передбачення в управлінні кібербезпекою майбутніх загроз, для забезпечення фізичної безпеки пристроїв Інтернету речей

1.4.

В наші часи, де технології постійно розвиваються та вдосконалюються, Інтернет речей грає важливу роль у перетворенні нашого оточення та взаємодії з ним. Від побутових пристроїв до великих промислових систем, IoT надає безліч можливостей для управління. Для максимального використання потенціалу мережі необхідно розробляти та впроваджувати найкращі практики забезпечення безпеки, бо це є дуже важливим аспектом. Оскільки все більше пристроїв стають підключеними до Інтернету, ризики стати жертвою кіберзлочинності зростають. Тож інтегрування заходів безпеки є ключовим правилом.

Це означає розробку та впровадження надійних механізмів аутентифікації та авторизації, використання шифрування для захисту конфіденційності даних, а також регулярне оновлення програмного забезпечення для усунення виявлених уразливостей. Крім того, важливо проводити аудит безпеки та моніторинг мережі для виявлення та запобігання потенційним загрозам.

Зокрема, слід приділяти увагу захисту від атак типу DDoS, використанню надійних паролів та безпеці Wi-Fi мереж. Також важливо бути готовим до можливих атак на системи з використанням GPS та вміти вчасно реагувати на них.

Однак зусилля забезпечення безпеки не повинні обмежуватися лише технічними заходами. Важливо також мати відповідні юридичні та організаційні політики, які регулюють збір, зберігання та обробку даних, а також реагування на можливі інциденти безпеки.

У висновках необхідно підкреслити важливість фізичного захисту в контексті Інтернету речей. Фізичний захист пристроїв є одним з головних елементів загальної стратегії безпеки, оскільки він забезпечує захист від прямого доступу до обладнання та його компонентів.

Приділяти увагу слід обмеженням доступу до пристроїв та їх з'єднань. Це може включати в себе видалення непотрібних портів та тестових точок з плат, а також застосування захисних кожухів або блокувань для запобігання фізичному втручанню.

Не слід забувати про фізичний захист у контексті розміщення пристроїв. Наприклад, для пристроїв, що встановлюються в публічних місцях або віддалених локаціях, важливо забезпечити їх захист від несанкціонованого доступу та втручання.

Фізичний захист також включає заходи для запобігання від крадіжок та втрати пристроїв. Це може включати в себе застосування систем відстеження, використання безпекових кріплень та неможливості відкриття корпусу без авторизованого доступу.

Загалом, фізичний захист є невід'ємною складовою стратегії безпеки Інтернету речей і варто надавати йому належну увагу при розробці та впровадженні IoT-систем.

Тільки комплексний підхід до забезпечення безпеки в умовах IoT дозволить максимально використати потенціал цієї технології та забезпечити надійність та конфіденційність інформації в цифровому світі. Це дозволить забезпечити безпеку та прозорість в світі, де IoT стає все більш важливим елементом нашого повсякденного життя.