Дивлячись на вищенаведені алгоритми роботи сканера, можемо побачити що зі сторони його програмування були збережені певні норми кібербезпеки. При скануванні пальця, якщо його схожість менша за 60 одиниць, при максимальному рівні в 100 одиниць, користувачу буде відказано в доступі. Кожному відбитку присвоюється унікальний ID. При занесенні нового відбитку в базу сканера, притуляти палець потрібно 2 рази, щоб сканер мав змогу чітко провести дактилоскопічна ідентифікацію. Тільки програміст має змогу редагувати або видаляти безпосередньо відсканованні відбитки.

Таким чином, за допомогою аналізу ринку відповідних пристроїв, пошук необхідних компонентів відповідно поставлених цілей було створено робочу модель контролю доступу за допомогою сканера відбитку пальців з цифровим дисплеєм та багатофункціональним меню. Шляхом вдосконалення проекту є забезпечення автономного живлення пристрою за допомогою акумуляторів та написання програми для керування приладом з ПК.

Список використаних джерел

1. IARDUINO [Электронный ресурс] // Урок 28. Контроль доступу по відбитку пальця. URL: https://lesson.iarduino.ru/page/urok-28-kontrol-dostupa-po-otpechatku-palca/

2. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах - НД ТЗІ 2.5-008-2002

3. Ленков, С.В. Методы и средства защиты информации. В 2-х томах / Ленков С.В., Перегудов - Д.А., Хорошко В.А., Под ред. В.А. Хорошко. - К. : Арий, 2008

УДК 004.056.53

ОСНОВНІ ЗАХОДИ ЗАПОБІГАННЯ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО ПЕРСОНАЛЬНИХ ДАНИХ THE INTERNET OF THINGS

Мальцева М. В., студ. гр. КБ-161
Науковий керівник**: Базилевич В. М.,** к.е.н., доцент
Національний університет «Чернігівська політехніка»

На даний момент ми є свідками посилення тенденції автоматизації різноманітних сфер життєдіяльності. Інформаційні та телекомунікаційні технології стали не тільки невід'ємною частиною повсякденного життя сучасної людини, але і необхідною технологічною платформою для організації сучасних бізнес-процесів. Активний розвиток смартфонів, створення мобільних додатків для гаджетів дозволяють оперативно відслідковувати, фіксувати, зберігати різну інформацію, пов'язану з життєдіяльністю людини: від списку контактів, здійснення банківських транзакцій, покупок в Інтернеті до відстеження фізичного та емоційного самочуття людини [1] Однією з технологій, яка стає все більш популярною за останні роки стала концепція Інтернет речей (The Internet of Things, IoT). Інтернет Речей або Internet of Things (IoT) - це мережа речей, які підключені до мережі Інтернет. Ці речі включають IoT-пристрої і фізичні об'єкти, оснащені IoT [2].

Інтернет Речей (IoT) це новий крок в еволюції сучасного Інтернету, де будь-який фізичний об'єкт (в термінах Інтернету Речей Thing), оснащений обчислювальними і комунікаційними можливостями, може бути ефективно інтегрований на різних рівнях в Інтернет. Метою роботи є визначення сфер застосування, основних принципів та методів захисту концепції Інтернет речей.

Інтернет речей дає можливість нових способів управління і моніторингу віддалено виконуваних операцій в будь-яких сферах. Він дозволяє повністю контролювати віддалено розташовані об'єкти і постійно передавати інформацію в сховище даних. Інтернет речей - це не тільки виконавчий холодильник, який сам замовляє улюблену їжу господаря, або послужливий чайник, який кип'ятить воду на першу вимогу зі смартфону. Це розумні датчики

на полях, дрони з камерами, завдяки яким можна віддалено моніторити стан ґрунтів, це датчики в громадському транспорті і єдині системи для моніторингу життя міста. Іншими словами, вже через кілька років Інтернетом речей стане світ навколо нас. Нижче можна бачити таблицю сфер застосування та прикладів девайсів IoT. [3, 4]

Таблиця 1 – Використання IoT в різних сферах життя

The Internet of Things		
Сфера застосування		Приклади девайсів
1.	Транспорт	Електромобілі, безпілотний транспорт, «розумний транспорт» (використання RFID, GPS, трекерів відстеження транспорту і т.д.)
2.	Медицина	2.1 IoT для пацієнтів – профілактичні пристрої (фітнес трекери) 2.2 IoT для медичних установ – пристрої діагностики (узд-апарат, тонометр, пристрій ЕКГ, МРТ ітд.).
3.	Безпека	Розумні вікна, замки, камери відоспостереження, датчики руху, домофони.
4.	«Розумний дім»	Смарт-холодильник, робот-пилосос, інтелектуальний чайник, «розумна» праска, телевізор, ваги, лампочка та ін.
5.	Сільське господарство	Комплексні системи управління фермами (моніторингові панелі, датчики з аналітичними можливостями), автоматизовані теплиці (контроль вологості, температури) та ін.
6.	Навколишнє середовище	Аналізатори складу повітря, води, електромагнітного поля, рівня радіації та звукових перешкод. Регулятори вологості повітря. «Розумні» мусорні контейнери
7.	Промисловість	Спеціальні датчики, що дозволяють отримати актуальні дані про стан обладнання.
8.	Енергетика	Датчики обліку енергоресурсів: води, електрики, газу, тепла; датчики оповіщення: датчики протікання води, чадного газу, пожежні датчики і т. д

Безпека Інтернету речей зосереджена на захисті пристроїв з підтримкою Інтернету, які підключаються один до одного в бездротових мережах. IoT-безпека - це компонент безпеки, пов'язані з Інтернетом речей, які прагнуть захистити пристрої та мережі IoT від кіберзлочинності. Підключені пристрої є збирачами даних. Особиста інформація збирається та зберігається за допомогою цих пристроїв - наприклад, ім’я, вік, дані про стан здоров’я, місцезнаходження та багато іншого - може допомогти злочинцям у крадіжці персональних даних. Одна з проблем: коли йде підключення до всіх пристроїв, є більше способів отримати доступ до вашої інформації. Кожен підключений пристрій може додати ще одну проблему конфіденційності, тим більше, що більшість з них підключається до смартфона. Незалежно від того, чи потрібно перевірити камери у вашому будинку, заблокувати чи розблокувати двері, відрегулювати температуру чи освітлення, попередньо нагріти духовку або вимкнути телевізор - все це можна зробити віддалено, лише за допомогою декількох дотиків на смартфоні. Але чим більше додавати функціональних можливостей до свого смартфона, тим більше інформації зберігається в пристрої. Це може зробити смартфони та все, що пов’язане з ними, уразливим для безлічі атак різних типів.

IoT технології становлять потенційну небезпеку для персональної безпеки в Інтернеті. Кожен день хакери атакують більше тисячі пристроїв. Ось чому корисно захистити своє цифрове життя, захистивши свої підключені до IoT пристрої. Існує багато заходів безпеки, які

можна вжити, щоб захистити свої пристрої, проте можна виділити вісім заходів, використовучі які, можна забезпечити надійних захист до IoT.

1. Встановлення на комп'ютери, планшети та смартфони надійне програмне забезпечення безпеки Інтернету. Наприклад, Norton Security Deluxe може забезпечити захист у режимі реального часу від існуючих та нових шкідливих програм, включаючи програмне забезпечення та віруси.

2. Використання надійних та унікальних паролів для облікових записів пристроїв, Wi-Fi мереж та підключених пристроїв. Не слід використовувати поширені слова або паролі, які легко здогадатися, наприклад "пароль" або "123456."

3. Необхідно бути в курсі, коли мова йде про додатки. Завжди слід переконатися, що читаєте політику конфіденційності застосованих програм, щоб побачити, як вони планують використовувати вашу інформацію та інше.

4. Проведення своїх досліджень перед покупкою. Пристрої стають розумними, оскільки вони збирають багато особистих даних. Хоча збір даних - це не обов'язково погано, але важливо знати про те, які типи даних збирають ці пристрої, як вони зберігаються та захищаються, якщо вони обмінюються з третіми сторонами, а також про політику чи захист щодо порушення даних.

4. Необхідно чітко знати, до яких даних пристрій чи програма хоче отримати доступ до телефону. Якщо функціональність додатка здається непотрібною або занадто ризикованою, відмовляйте у дозволі.

5. Використання VPN, як-от Norton Secure VPN, який допомагає захистити дані, передані у будинку чи загальнодоступному Wi-Fi.

6. Регулярна перевірка веб-сайт виробника пристрою на наявність оновлень мікропрограмного забезпечення.

7. Слід бути обережним, використовуючи функції соціального обміну з цими додатками. Функції спільного використання в соціальних мережах можуть розкривати інформацію, як місцезнаходження, і повідомляти хакерам, коли людини немає вдома. Кіберзлочинці можуть використовувати це для відстеження рухів.

8. Не слід залишати свій смартфон без нагляду, якщо він використовується у громадському просторі. У переповнених просторах можна вимкнути доступ Wi-Fi або Bluetooth, якщо вони не потрібні. Деякі марки смартфонів дозволяють автоматично обмінюватися з іншими користувачами в безпосередній близькості [5].

Список використаних джерел

1. IoT from cyber security perspective [Електронний ресурс] – Режим доступу до ресурсу: https://webcache.googleusercontent.com/search?q=cache:HM8IqbiIilAJ:https://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/%2524FILE/EY-cybersecurity-and-the-internet-of-things.pdf+&cd=2&hl=ru&ct=clnk&gl=ua.

2. Internet of things from research and innovation to market deployment [Електронний ресурс] – Режим доступу до ресурсу: research.eu/pdf/IERC_Cluster_Book_2014_Ch.3_SRIA_WEB.pdf.

3. Где применяется интернет вещей? [Електронний ресурс] – Режим доступу до ресурсу: https://rb.ru/story/iot-irl/.

4. Real World IoT Applications in Different Domains [Електронний ресурс] – Режим доступу до ресурсу: https://www.edureka.co/blog/iot-applications/.

5. Internet of Things (IoT) security: 9 ways you can help protect yourself [Електронний ресурс] – Режим доступу до ресурсу: https://us.norton.com/internetsecurity-iot-securing-the-internet-of-things.html