16. **Андреева Л. И**. Оценка факторов, влияющих на эксплуатационные показатели карьерного автотранспорта /Л. И. Андреева, Ю.Ю. Ушаков// Мир дорог. Спецвыпуск. –2016.–С. 62-64.

17. **Фролова Л.В.** Формирование бизнес-модели предприятия [Электронный ресурс]: учебник / Л.В. Фролова, Е.С. Кравченко. Электронные текстовые данные. – Киев: ЦУЛ, 2012. – 384 с. – Режим доступа: http://www.studfiles.ru/preview/5429943/

18. **Озорнин С.П.** Технический сервис мобильных машин: Стратегия ситуационно-комбинированного обслуживания: монография / С.П. Озорнин. – Чита: ЧитГУ, 2004. – 250 с.

19. **Озорнин С.П.** Совершенствование организации мониторинга изменений технического состояния машин в эксплуатации: сб. научн. тр. / С.П. Озорнин, И.Е. Бердников // Вестник ЗабГУ – Чита, 2014. – Вып. 111. – С. 64-69

20**. Макарова А.Н.** Методика оперативного корректирования нормативов периодичности технического обслуживания с учетом фактических условий эксплуатации автомобилей: дис. канд. техн. наук / А.Н. Макарова. – Тюмень, 2015. – 208 с.

21**. Ушаков Ю.Ю.**Повышение эффективности системы технической эксплуатации карьерных автосамосвалов на горнодобывающих предприятиях // Технологическое оборудование для горной и нефтегазовой промышленности: сборник трудов XIII междунар. науч.-техн. конф. «Чтения памяти В.Р. Кубачека»/УГГУ.–Екатеринбург, 2015. – С. 380-383.

Рукопись поступила в редакцию 21.08.2019

УДК 004.67

Д.І. КУЗНЄЦОВ*, канд. техн. наук, доц., Л.С. РЯБЧИНА, асист.
Криворізький національний університет

ІНФОРМАЦІЙНА БЕЗПЕКА СИСТЕМ ІНТЕРНЕТУ РЕЧЕЙ

Мета. Метою роботи є аналіз існуючих методів та засобів передачі інформації у системах Інтернету речей та їх подальше удосконалення та стандартизація з точки зору безпеки. Зокрема використання гетерогенних пристроїв не дає можливості коректно протистояти кіберзагрозам, так як це пов'язано із тим, що архітектура Інтернету речей має складну будову, не є універсальною та потребує вивчення і удосконалення. Аналіз безпеки в IoT є важливим, так як кінцеві суб'єкти мають довіряти технології. Унікальність полягає в тому, що повинні відбуватися автентифікація, авторизація кінцевого обладнання, зберігання та обробка інформації, в тому числі і конфіденційної та критично важливою.

Методи досліджень. Під час вирішення наукової задачі було використано методи теоретичного дослідження, аналізу та синтезу.

Наукова новизна. Науковою новизною роботи є систематизація існуючих моделей та алгоритмів взаємодії вузлів мережі Інтернету речей та розробка концепції централізованого доступу до мережі Інтернет з підвищеними вимогами безпеки, що дозволяє вдосконалити процес автентифікації, авторизації та аудиту вузлів IoT.

Практична значимість. Використання отриманих результатів дає більш точну оцінку щодо існуючих методів та засобів у мережах типу Інтернет речей та дозволяє підвищити криптостійкість процесу обміну даними у вищезазначених системах. Досліджено основні ризики, яким може піддаватися мережа і спланово засоби забезпечення безпеки, починаючи з проектування та закінчуючи інтеграцією всієї системи.

Результати. У статті розглянуто основні проблеми безпеки систем Інтернет речей та запропоновано рекомендації для зниження ризиків втрати і компрометування інформації, що обробляються вищезазначеними системами. Додатково було розглянуто основні поняття технології Інтернету речей, досліджено архітектуру та основні компоненти IoT. Приведено характеристики складових елементів. Також наведено рекомендації щодо управління цілісністю системи та шифрування конфіденційних даних з метою протидії їх компрометування.

Ключові слова: інтернет речей, інформаційна безпека, кібербезпека, автентифікація, авторизація, криптостійкість.

doi: 10.31721/2306-5451-2019-1-49-80-84

Проблема та її зв'язок з науковими та практичними завданнями. На сьогоднішній день системи інтелектуального керування отримали достатньо широке розповсюдження у всіх сферах людського життя, від побуту до промисловості. Зважаючи на це збільшується й об'єм інформації у мережах передачі даних. Поряд із цим такі системи керування розвиваються доволі хаотично й не мають загальної стандартизації та їх розробники ще не приділяють багато уваги методам та способам захисту. Інформаційні системи типу IoT все ще мають

велику кількість недоліків, незважаючи на високу популярність і використання сучасних технологій при розробці.

Оскільки Інтернет речей включає в себе такі пристрої, що постійно збирають і обробляють інформацію про оточуюче середовище, то вони є потенційно небезпечними для кінцевого користувача. Зважаючи на зростання рівня кіберзлочинності особливу увагу слід приділяти саме таким пристроям, адже не тільки втрата даних є основною проблемою. Можливе також використання обчислювальних ресурсів систем у проектуванні різноманітних кібератак.

Недоліками даних систем є потреба у сучасних датчиках, контролерах, методах та способах передачі інформації тощо. Тому впровадження пристроїв IoT та вирішення найбільш поширених задач і проблем пов'язаних із ними є досить актуальним напрямом досліджень.

Аналіз досліджень і публікацій. Інтернет речей або (IoT) - це система взаємопов'язаних обчислювальних пристроїв, механічних і цифрових машин, предметів, тварин або людей, яким надаються унікальні ідентифікатори та можливість передавати дані по мережі, не вимагаючи від людини взаємодії з людиною або людини з комп'ютером. Складовою частиною Інтернету речей є Індустріальний інтернет речей (IIoT). Також можна зазначити відносно новий термін: «Інтернет всього» (IoE), який потенційно може прийти на зміну Інтернету речей [1].

Через розширення областей застосування таких приладів як у повсякденному житті, так і у промисловості збільшується кількість загроз, що стосуються галузі кібербезпеки, та, відповідно з'являється все більше прецедентів несанкціонованого доступу. Такі проблеми існують в галузі через те, що ідея мережевих приладів та інших об'єктів є відносно новою, безпека не завжди вважалася першочерговим завданням на етапі проектування продукту.

Спираючись на дослідження «Uncovering IoT Threats in the Cybercrime Underground» від компанії Trend Micro можна сказати, що основною проблематикою безпеки приладів, що є підключеними до мережі Інтернет, є відсутність базового забезпечення безпеки [2]. Із вільним розповсюдженням розумних пристроїв збільшується кількість користувачів, що є звичайними користувачами і не мають досвіду роботи з безпекою Інтернет-пристроїв. Таким чином більшість паролів не змінюються власниками, а залишаються стандартними, що дає можливість отримати несанкціонований доступ та використовувати пристроїв у власних цілях, наприклад, для створення ботнетів чи здирництва.

Постановка завдання. Науковою задачею даних досліджень є забезпечення безпечного обміну інформацією між пристроями систем Інтернету речей та мережею Інтернет.

Задача є актуальною, оскільки процеси, за допомогою яких на сьогоднішній день передаються дані, у тому числі і критично важливі, є недостатньо захищеними. Таким чином, дослідження має за мету вивчення способів передачі, обробки і зберігання інформації, що використовується для керування системами управління й їх удосконалення з точки зору підвищених вимог безпеки.

Викладення матеріалу та результати. Важливими характеристиками для IoT є наступні:

споживання енергії - багато пристроїв IoT не підключені до постійного джерела живлення. чим більше енергії використовується, тим вище ймовірність того, що пристрій перейде в режим офлайн;

швидкість - це обсяг даних, який можна передавати протягом певного періоду часу. збільшена пропускна здатність зменшує суперечки та дозволяє мережі додавати більше пристроїв;

затримка - це кількість часу, яке потрібно для надсилання та отримання повідомлень. для додатків у режимі реального часу це більше фактор;

безпека - якщо є чутливі з'єднання або передача чутливих даних - вони повинні бути захищені [3].

Загалом, число атак на пристрої IoT з кожним роком збільшується для використання у кіберзлочинних цілях. На рис.1 можна побачити динаміку змін числа атак на такі пристрої [4]. Згідно з розрахунками фахівців, в 2018 році кількість хакерських атак на інтернет речей потроїлася і досягла 32,7 млн. Очікується, що до 2020 року в світі буде налічуватися більш 31 млрд IoT-пристроїв, тому проблема їх безпеки стане ще більш важливою [5].

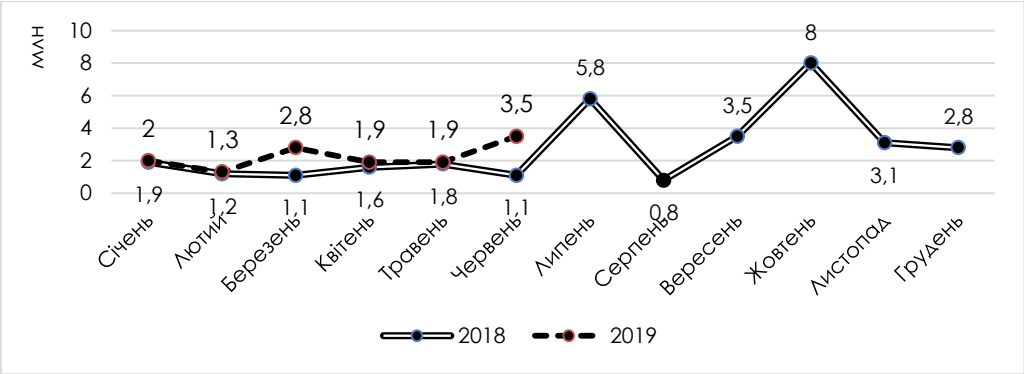

Рис.1. Динаміка числа атак на пристрої IoT

Якщо звернутися до рис. 2, то можна побачити, що зв'язок сенсорів/виконуючих пристроїв і керуючого центру відбувається за допомогою мережі Інтернет. Це дозволяє перенести обчислення і взаємодію складових до хмарних центрів Але саме на цьому рівні дані і можуть бути компрометовані і сторонні особи можуть отримати інформацію про кінцеві пристрої. Саме через такі «діри» у безпеці можливе використання пристроїв IoT для організації DDos-атак і у якості вузлів виходу VPN. Також цілями, у яких використовуються зламані пристрої IoT є побудова ботнетів і криптомайнерів на їх базі [2].

Варіантом обходу загроз такого виду є приведення систем до вигляду, представленого на рис. 3. Суміщення керуючого контролера із мережевим пристроєм, типу маршрутизатора, дозволяє не виводити кожен із пристроїв мережі за її межі. Також можливе використання програмного захисту від хакерських атак. Таким чином дані, що використовуються у системі можуть не передаватися у зовнішню мережу без необхідності, а при її наявності можуть бути зашифровані безпосередньо керуючим центром і передані ним же.

Рис.2. Стандартна модель взаємодії пристроїв IoT і мережі Інтернет

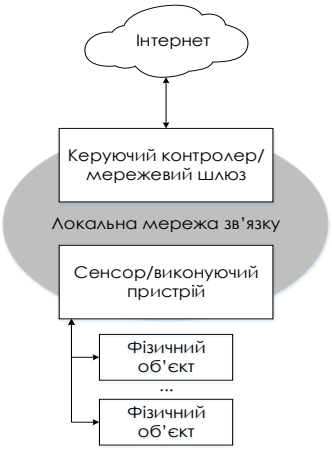

Рис.3. Суміщення керуючого центру і мережевого кордону

Такий спосіб має свої недоліки у тому, що дана архітектура може бути реалізована на базі одної локалізації системи. У випадку більшого географічного охоплення можна розширити запропоновану схему. Створення віртуальних приватних мереж допомагає вирішити такі питання. Таким чином географічно розкидані пристрої можна віртуально об'єднати в одну мережу і забезпечити виконання вищенаведеної схеми.

Слід звернути увагу на способи зберігання інформації. Дані, що збираються можуть бути конфіденційними, мати стратегічно важливий характер і їх втрата або компрометування нанесуть шкоду користувачам. Кожна складова системи IoT має збирати і використовувати лише ту інформацію, що є важливою саме для оброблюваного пристроєм аспекту.

Доцільним у системах Інтернету речей є наскрізне шифрування. При використанні такого методу ключі шифрування є відомими тільки пристроям-учасникам однієї системи [6]. У такому випадку, інформація може бути розшифрована тільки кінцевими пристроями і не буде доступна у відкритому вигляді третім сторонам (сторонні сервери, постачальник Інте-

рнет-послуг тощо). Є й недоліки такого методу захисту. Мережеві атаки із підміною чи перехопення даних можуть видати третіх осіб за учасників інформаційного обміну.

Задля захисту від несанкціонованого втручання сторонніх осіб у IoT використовується така функція, як AAA(автентифікація, авторизація та аудит). AAA - це архітектурна база для налаштування набору з трьох незалежних функцій безпеки:

автентифікація - користувачі та адміністратори повинні довести, що вони є саме тими, якими вони повідомляють. Автентифікацію можна встановити, використовуючи комбінації імен користувача та пароля, питання виклику та відповіді, картки жетонів та інші методи. Автентифікація AAA забезпечує централізований спосіб контролю доступу до мережі;

авторизація – після автентифікації користувача служби авторизації визначають, до яких ресурсів користувач може отримати доступ та які операції користувачеві дозволено виконувати;

аудит – записує дії користувача, включаючи доступ до нього, кількість часу доступу до ресурсу та будь-які внесені зміни [7].

Такий метод використовується також у вищезазначених віртуальних приватних мережах, що модна застосовувати для «зближення» географічно віддалених пристроїв і централізованої обробки даних.

Висновки та напрямок подальших досліджень. Проведено аналіз та оцінку ризиків при використанні систем інтернету речей. Дані системи знаходяться на тісному стику системної інженерії та комп'ютерних мереж. Тому для подібних досліджень необхідним є як вивчення принципів роботи IoT-пристроїв, так і способів мережевого обміну даними.

Оскільки такі системи мають застосування у всіх сферах життя, безпека обміну даними має бути одним із найголовніших аспектів даної галузі. Використання IoT зумовлене розвитком автоматизації і є наступним кроком еволюції інформаційних технологій. Тому галузь все ще є недостатньо стандартизованою і потребує подальших досліджень.

Також можна зазначити, що централізовані пристрої, що суміщують у соті IoT-контролер та мережевий шлюз можуть мати широке застосування особливо у побутовому сегменті застосування Інтернету речей.

На основі отриманих результатів доцільно проводити дослідження в напрямку забезпечення інформаційної безпеки у мережах Інтернету речей, розвивати методи обміну інформацією та практично застосовувати такі способи.

Список літератури

1. **Rosencrance L.** Internet of things (IoT) [Електронний ресурс] / **L. Rosencrance, S. Sharon, I. Wigmore** – Режим доступу до ресурсу: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.
2. The Internet of Things in the Cybercrime Underground / [**H. Stephen, K. Vladimir, M. Fernando** та ін.].2019. – 47с.
3. IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things, 2017. – 576 с.
4. 2019 SonicWall Cyber Threat Report, 2019.
5. Интернет вещей стандартизуется. Блог Мачека Кранца (Maciej Kranz), вице-президента и генерального менеджера отдела корпоративных технологий компании Cisco [Електронний ресурс]. – 2015. – Режим доступу до ресурсу: https://www.cisco.com/c/ru_ru/about/press/press-releases/2015/07-30a.html.
6. **Васильев Г**. Интернет вещей и информационная безопасность / **Г. Васильев**. // Первая миля. – 2016. – №6. – С. 50–55.
7. CCNA Cybersecurity Operations Companion Guide, 2018. – 1010 с.
8. **Грингард С**. Интернет вещей: Будущее уже здесь / **Сэмюэл Грингард**. – Москва: Альпина Паблишер, 2016. – 188 с.
9. **Полегенько А. М.** "Особенности защиты информации в Интернете вещей" International Journal of Open Information Technologies, том. 6, номер. 10, 2018, С. 41-45.
10. **McEwen A**. Designing the Internet of Things / **A. McEwen, H. Cassimally**. – Chichester: Wiley, 2014. – 338 с.
11. **Кузнецов Д. И**. Информационная система интеллектуального регулирования микроклимата жилых помещений / **Д. И. Кузнецов, А. И. Купин**. // Проблемы физики, математики и техники. – 2016.– №2. – С. 84–89.
12. **Апостолюк В. О.** Інтелектуальні системи керування: конспект лекцій / **В. О. Апостолюк, О. С. Апостолюк**. – Київ: НТУУ «КПІ», 2008. – 88 с.
13. Структура мобільного робота для людей з обмеженими можливостями як частини системи «Розумний дім» / **Л. С.Рябчина, Д. І. Кузнєцов, Н. А. Моцун, О. В. Градовий**. // Гірничий вісник. – 2017. – №102. – С. 96–100.
14. **Evans D**. The Internet of things: How the next evolution of the Internet is changing everything / **D.Evans**. – San Jose: Cisco Press, 2011.
15. **Лоднева О. Н**. Анализ трафика устройств Интернета вещей / **О. Н. Лоднева, Е. П. Ромасевич**. // Современные информационные технологии и ИТ-образование. – 2018. – №1. – С. 149–169.
16. Архитектура безопасности "Интернета вещей" [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://docs.microsoft.com/ru-ru/azure/iot-suite/iot-security-architecture.

Рукопис подано до редакції 24.09.2019