

АКТУАЛЬНІ СУЧАСНІ ТЕНДЕНЦІЇ РОЗВИТКУ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ ТА ПІДХОДИ ДО ЇХ КІБЕРЗАХИСТУ

Вінницький національний технічний університет

Анотація.

Розглянуто основні тенденції розвитку технологій Інтернету речей в сучасному світі та проблематику їх кібербезпеки. Описані підходи до універсальної моделі забезпечення їх кібербезпеки та захисту інформації в технологіях Інтернету речей. Описані вимоги до моделі кіберзахисту та необхідні функціонал і властивості, які повинна мати модель. Сформовано підходи та способи підвищення захисту інформації в каналах систем і пристроїв Інтернету речей (IoT). Розглянуті окремі технології підвищення захищеності інформації, розглянуто особливості і проблематику захисту даних в екосистемі IoT. Визначено можливі способи підвищення кіберзахисту в моделі кіберзахисту IoT.

Ключові слова: IoT, Internet of Things, MITM, канали, мережі, кібератаки, кіберзахист шифрування, інформаційний захист, мультиконтроллер, канали передачі, вразливості, кіберзахист.

Abstract.

The main trends in the development of Internet of Things technologies in the modern world and the issues of their cybersecurity are considered. Approaches to a universal model for ensuring their cybersecurity and protecting information in Internet of Things technologies are described. Requirements for a cyber protection model and the necessary functionality and properties that the model should have are described. Approaches and methods for increasing cyber protection of information in the channels of Internet of Things (IoT) systems and devices are formed. Individual technologies for increasing information security are considered, the features and issues of data protection in transmission channels in the IoT are considered. Possible ways to increase cyber protection in the IoT protection model are identified.

Keywords: IoT, Internet of Things, MITM channels, networks, cyberattacks, cyber security encryption, information security, multicontroller, transmission channels, vulnerabilities, cyber security.

Вступ

У зв'язку із значним збільшенням інформатизації та діджиталізації основних сфер людського життя і розвитку інформаційних технологій значно розвиваються технології Інтернету речей (Internet of Things, IoT) [1, 2].

Концепція розвитку Інтернету речей (IoT) передбачає використання кінцевих пристроїв із смарт-функціями та можливістю комунікацій із іншими ІТ-застосунками та пристроями із використанням мережі Інтернет. Також, поряд із розвитком Інтернету речей розвивається і сфера кібератак і інформаційних впливів на у IoT [2] та на суміжні і пов'язані комп'ютерні системи.

Розвиток систем і пристроїв Інтернету речей, в умовах і часи значних інформаційних протистоянь, дещо сповільнюється проблемою їх кібербезпеки, але ніколи не зупиняється і має чітку зростаючу тенденцію, яка зростає поряд із загальним розвитком Інформаційних технологій та інноваціями в світі. Звісно, поряд із кібербезпекою у технологіях IoT постає гостра необхідність забезпечення надійності роботи самих пристроїв IoT, їх захищеності, функціональності, сумісності із іншими ІТ-сервісами та ПЗ, гнучкості та комфортності у використанні і взаємодії із користувачами.

Аналіз тенденцій розвитку технологій Інтернету речей

Значне збільшення інтенсивності розвитку інформаційних технологій і сфери інновацій та розробок, у т.ч. в сфері кібербезпеки та ІТ-сервісів IoT сприяє появі на ринку нових продуктів та технологій Інтернету речей, розвитку програмних продуктів і додатків для IoT, спеціального ПЗ і хмарних технологій для IoT. Також це сприяє їх адаптивності і максимальній ергономічності і комфортності для кінцевого користувача. Більшість пристроїв Інтернет речей орієнтовані на роботу і вирішення конкретних

функціональних задач, що робить їх затребуваними і актуальними продуктами для кінцевого користувача як у широких, так і у вузько-орієнтованих колах.

Розглядаючи сферу технологій Інтернету речей слід визначити основні тенденції розвитку IoT пристроїв та систем:

- технології IoT в сфері мобільних і персональних пристроїв користувачів (наприклад, смартфони, фітнес-браслети, фітнес-трекери, розумні годинники, екшн-відеокамери та інші портативні пристрої [2]);
- технології IoT в промисловій сфері (IIoT, Industrial Internet of Things), пристрої IoT в промисловості (наприклад, різні контролери, трекери та RFID-модулі, блоки IoT та датчики, смарт-датчики та сенсорні мережі на базі IoT);
- технології IoT в побутовій та користувацькій сферах (наприклад, розумні будинки, смарт-розетки та смарт-крани для води із керуванням по WiFi/Bluetooth, розумні GPS-трекери та побутова техніка із керуванням/моніторингом по WiFi/Bluetooth);
- технології IoT в транспортній сфері (як у персональних транспортних засобах (авто/мото/вело транспортні засоби) так і у міжміському громадському транспорті [2]);
- технології IoT в медичній сфері (наприклад, медичні пристрої моніторингу біо-показників, інсулінові помпи, кардіомонітори, інші мед. засоби);
- пристрої і технології IoT в сфері альтернативної енергії та енергетики (розумні електролічильники, електророзетки, смарт-контролери і смарт-вимикачі із керуванням по IoT-протоколам та Інтернет, інвертори та енергетичні комутатори IoT, пристрої IoT smart-grid тощо);
- технології IoT в регіональній і муніципальній інфраструктурі (контролери, сенсори та освітлення із дистанційним керуванням, відеокамери та смарт-контролери СКД на базі IoT пристроїв, концепція “Smart-city” розумного міста із його IoT-пристроями);
- технології IoT в агросекторі та агрогосподарстві (наприклад, розумний полив, розумні трекери та сенсори вологості ґрунтів, технології керування агрогосподарством із IoT інтерфейсом на базі планшета; інтеграція і бортовою електронікою сучасних агро комбайнів, GPS трекінг, використання дронів в агрогосподарстві із інтеграцією із IoT пристроями);
- хмарні (cloud-based) IoT технології у різних секторах IoT (Industrial IoT);
- технології сенсорних мереж і розумних IoT сенсорів у різних сферах;
- розвиток концепції IoE (Internet of Things Everywhere) “Інтернет речей всюди” - всеосяжного розповсюдження технологій і пристроїв IoT в сучасному інформаційному просторі та геосфері;
- розвиток інших типів технологій IoT в різних технологічних сферах.

Розширення комунікації пристроїв Інтернету речей (IoT Communication, використання 5G/6G технологій) та ріст кіберзагроз для IoT – теж відноситься до основних трендів останніх років. Глобальне розповсюдження IoT - один із трендів сучасних технологій в світі (Global IoT Devices & Network) в розподілених мережах.

Глобальне розповсюдження IoT та розвиток різних інформаційних сервісів XaaS для IoT - один із трендів сучасних технологій в світі (Global IoT Devices & Network) в сучасних ІТ технологіях і мережах.

Необхідність забезпечення кібербезпеки критичних систем із IoT є також актуальним напрямом розвитку технологій Інтернету речей. Зменшення ризиків кібератак і опанування навичок кіберзахисту IoT є ключовими задачами при цьому.

Зменшення кіберзагроз в IoT є ключовим фактором стабільності бізнес-процесів із IoT-обладнанням в складі. Розвиток технологій штучного інтелекту та глобальна діджиталізація в секторі IoT є другим трендом майбутнього.

Розвиток інноваційних технологій штучного інтелекту (AI) в секторі IoT та ПЗ для них - стабільний тренд розвитку технологій майбутнього.

Опанування нових сфер IoT-пристроями і використання їх в нових сферах - є також стабільним трендом. А також розробка новітніх інноваційних технологій IoT (наприклад, IoT, в складі дронів, побудови новітньої реклами на базі дронів і побудова доставки дронами із використанням та інтеграцією із IoT) - теж серед майбутніх і актуальних трендів.

Опанування нових сфер IoT-пристроями і використання їх в нових сферах - є теж стабільною і актуальною тенденцією майбутнього та сьогодення.

Крім розвитку самих технологій Інтернет речей, також розвивається їх кібербезпека - не менш важлива проблема в сфері технологій Інтернету речей.

Проблематика кібербезпеки в системах і пристроїв Інтернету речей

Розглядаючи сучасні кіберзагрози в секторі IoT [2-3], більшість із яких спрямовані на канали і інтерфейси IoT пристроїв, завдяки відомим їх недолікам і вразливостям (наприклад, таких як багато направленість сигналу і широкий період охоплення, розкриття даних мережі шляхом надсилання ініціалізуючих пакетів, початкову сервісну інформацію (net ID, MAC, тощо). До кіберзагроз IoT також відноситься маніпуляція та спуфінг (підробка) параметрів мережі та інтерфейсів IoT, що спричиняє до значних ризиків втрат інформації, MITM-атак та кібератак обходу авторизації/автентифікації та сторонніх інформаційних втручань в систему IoT. Більші інформаційних атак і загроз в секторі пристроїв і систем IoT, які використовують радіо інтерфейси припадає саме на MITM-атаки та Spoofing-атаки із організацією MITM/Rogue-точок доступу. Таким чином інформація може витікати по стороннім комунікаціям в IoT піз використанням захищених протоколів, Це обумовлює використання нових методів підвищення рівня захисту шляхом наскрізного шифрування і додаткових методів захисту для збільшення інформаційної захищеності даних в каналах IoT. Інша область кібератак - маніпуляція параметрів та невірні та/або слабкі конфігурації чи налаштування обладнання IoT, що призводить до значних ризиків кібератак. Винні при цьому в основному самі користувачі або сервіс-спеціалісти, що відповідальні за експлуатацію параметрів IoT.

Тренди сучасних років говорять, що основними кіберзагрозами в каналах IoT є:

- несанкціоноване перехоплення, втручання на фізичному рівні і спотворення даних за допомогою MITM-атак із використанням Rogue/FakeAP (фейкових) точок доступу та інтерфейсів підключення;
- атаки на сертифікати захисту і шифрування, маніпуляція рівнями захисту;
- влаштування («ін'єкція») шкідливих пакетів та/або сертифікату в дата-потіки;
- перехопленого (на фізичному) рівні трафіку із супутніх вузлів і дешифрація інформаційних потоків із крипто аналізом ключів шифрування в каналах передачі даних IoT;
- цілеспрямовані сторонні підключення і кібератаки на системні інтерфейси і API керування каналів зв'язку у IoT, та/або виведення їх з ладу та/або порушення функціоналу;
- перехоплення керування та/або перехоплення потоків даних моніторингу окремих параметрів (або опосередкованих параметрів інформаційних величин) у каналах зв'язку;
- канали передачі на базі інтерфейсів і протоколів IoT та їх комунікацій;
- втручання в захищені механізми формування VPN/Proxy та механізми генерації ключів шифрування RSA при DES/AES шифруванні;
- використання мережевих експлойтів інтерфейсів і компрометація радіомодулів і протоколів IoT;
- компрометація компонент управління кодуванням та шифрування в складі системи протоколу та/або інтересу каналу передачі IoT для порушення штатного його функціоналу;
- некоректні системні налаштування та/або помилки операційного персоналу;
- порушення безпеки пограничних пристроїв та модулів зв'язку у мережах пристроїв IoT (маршрутизатори, комутатори, обладнання оптичного/радіозв'язку та інше), у сукупності із - вразливостями проміжних протоколів зв'язку і передачі даних;
- порушення механізму встановлення захищеного з'єднання за допомогою атак MITM;
- недосконалість і кіберзагрози опорної архітектури і суміжних пристроїв;
- впровадження вірусного шкідливого коду, троянської програми або шкідливих пакетів даних в системні області IoT із подальшою компрометацією функціоналу і дистанційним виконанням інструкцій та пониженням/відключенням рівня безпеки в каналі чи інтерфейсі IoT;

- недосконалість апаратної структури і особливостей будови мережевих інтерфейсів IoT;
- недосконалість та відсутність належних системних налаштувань і мережевих протоколів в IoT;
- загрози 0-го дня для інтерфейсів і каналів IoT.

Також самі технології комунікацій IoT і протоколів IoT мають низьку власних вразливостей та потенційних ризиків впровадження кіберзагроз, що обумовлює необхідність використання додаткових методів і моделі захисту інформації у IoT.

Окремі технології і підходи до розвитку моделі кіберзахисту IoT-пристроїв

Проблема реалізації росту чинників інформаційних та кіберзагроз в IoT ще не вирішена [3] через здійснення різних кібератак, в т.ч. із організацією MITM/Rogue AP (фейкових точок доступу) і з використанням шкідливих маршрутів (при атаках на маршрутизацію) із несанкціонованим зчитування і модифікацією даних в каналах. Це одна із основних проблем при поширенні та інтеграції технологій IoT.

Перехоплення інформації із цих каналів, може призвести до втручання та/або перехоплення конфіденційної інформації, якщо вона не захищена надійним шифруванням, або із втручання чи впровадження (ін'єкцію) шкідливого коду у інформаційну структуру пакетів даних в каналах передачі створює значні загрози безпеки для центральних вузлів всієї інформаційної мережі IoT. Це може значно вплинути на структуру і основний функціонал сучасних критичних інформаційних систем на базі чи із супутнім використанням IoT. Це створює додаткові проблеми кібербезпеки і потенційні ризики порушення функціоналу сучасних інформаційних систем Інтернету речей.

Як показує практика, локальний кіберзахист в IoT не вирішує завдання повного комплексного захисту усієї системи IoT. До того ж, неповнота, а й часто й взагалі відсутність оцінок впливу призводять до – прояву реальних кіберзагроз в IoT та до складних наслідків від цих атак. Тому завдання розробки моделі кіберзахисту для оцінки і врахування впливу в IoT повинно базуватись на:

- на аналізі самих кіберзагроз і їх індикаторів в IoT;
- на оцінці їх окремих впливів і наслідків [3];
- на оцінці комплексного впливу багатьох факторів кіберзагроз на структуру IoT;
- на точному визначенні основних і супутніх факторів впливу кіберзагрози на IoT-модуль;
- на оцінці вектору атаки і профілю захищеності IoT – системи;
- на аналізі самих типів і факторів кіберзагроз і їх впливів на інформаційний процес МК системи.

Тому задача оцінки ризиків і розробки моделі захисту і кіберзагроз в IoT зводиться до розроблення підходів на базі: оцінювання ризиків та інформаційних впливів із максимальним врахуванням факторів впливу в IoT (факторів кіберзагроз); аналізу параметрів та індикаторів вторгнень та порушення кібербезпеки IoT; оцінці та аналізу кіберзагроз "0"-го дня і перспективних загроз в IoT за допомогою штучного інтелекту та методів евристики AI; на індикації та визначення факту кіберзагрози із формуванням кіберінциденту; на інтерактивного блокування самої кіберзагрози; на ізоляції і використання активного захисту в IoT; на відновленні попередніх станів ІС IoT до нормальних значень параметрів до інциденту; на принципі визначення та організації фіксації параметрів ІС IoT до кіберзагрози; на гнучкості архітектури; на принципі гнучкості та толерантності до функціоналу МК.

Модель кіберзахисту IoT повинна бути максимально адекватною і в той же час простою і ефективною в оперуванні, повинна дозволяти проводити аналіз інформаційної складової та водночас рівня кіберзахищеності IoT системи, хоча б на базовому рівні по одному або декільком показникам.

Для визначення і протидії інцидентам в моделі кіберзахисту IoT повинні застосовуватись першочергові принципи: індикації та визначення кіберзагрози; інтерактивного блокування джерела та відновлення значень параметрів ІС IoT до попереднього стану трафіку і джерела кіберзагрози; принцип ізоляції і використання захисного периметра оточення IoT.

Модель повинна організовувати високоефективне, комфортне і надійне і захищене передавання та оброблення даних в ІС IoT із використанням надійних принципів і протоколів зв'язку із належним рівнем шифрування та захисту даних в моделі.

Тому мінімізація складності процесу захисту і водночас максимально повне включення надійного і високого рівня шифрування ($L_{key} > 128-192\text{bit}$) і нейтралізація супутніх факторів кіберзагроз і витоків інформації із каналів IoT і обладнання сучасних інформаційних мереж є важливою задачею у галузі безпеки IoT і інтелектуальних систем і мереж, які мають у своєму складі захищений комунікаційний і «розумний» функціонал і входять у концепцію захищених мереж, а також і захищених IoT:

Можливості сучасних інструментів і апаратно-програмних засобів зчитування та/або прихованого втручання також значно зросли, як зросли і смартфункції таких систем. В подальшому прогнозується збільшення числа атак на комунікаційну інфраструктуру захищених мереж і систем, в т.ч. IoT-пристроїв та на сфері їх IT-інфраструктури передачі даних, охоплюючи при цьому і системи "розумний будинок" із окремими компонентами автоматизації і кінцевим функціоналом і окремі кінцеві пристрої IoT.

Аналітики і експерти говорять [1-3], що в найближчі роки з'явиться більше проблем для систем безпеки і захищеної передачі інформації в сфері IoT.

Модель безпеки IoT повинна забезпечувати повну безпеку функціоналу і захищену передачу даних в IoT, їх оброблення для забезпечення стійкості і надійності процесу передачі інформації по захищеним каналам зв'язку і інтерфейсах в пристроях IoT. Модель і метод повинні базуватись на поєднанні функціоналу на різних рівнях в IoT: апаратного та програмного.

Висновки

Технології і протоколи і IoT швидко і стрімко розвиваються залишаючи стабільний зростаючий тренд в різних секторах. Але проблема забезпечення кібербезпеки в сфері Інтернету речей залишається. Тому для забезпечення стабільності роботи пристроїв Інтернету речей необхідне вирішення проблеми кібербезпеки в IoT із погляду комплексного і багаторівневого захисту в IoT. Забезпечення кібербезпеки IoT вважається перспективним напрямком для подальших досліджень, оскільки проблема ще не вирішена. На основі технологій IoT потрібний розвиток технологій IoT і зокрема ефективної моделі кіберзахисту IoT із оцінкою кіберзагроз для пристроїв і кінцевих вузлів Інтернету речей.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Маліновський В.І. Аналіз загроз безпеки мікроконтролерів/В.І. Маліновський, Л.М. Куперштейн // «Інформаційні технології та комп'ютерна інженерія», Вінниця, ВНТУ. - №3(55). - С. 21-32.
2. Маліновський В.І. Мінімізація факторів кіберзагроз і спеціалізовані підходи до інформаційного захисту мікропроцесорних систем індустриального Інтернету речей : [Електронний ресурс] / Матеріали LI-ї Науково-технічної конференції факультету інформаційних технологій та комп'ютерної інженерії (ФІТКІ), Вінниця, Україна: ВНТУ. - 2022. - Режим доступу URL: <https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2022/paper/view/15000> . (Дата звернення 13.02.2024).
3. Шологон Ю. 3. Вразливості апаратного забезпечення кіберфізичних систем. Репозитарій Національного університету «Львівська політехніка» (Lviv Polytechnic National University Institutional Repository), 12.с., 2023. [Електронний ресурс]. - Режим доступу URL: <http://ena.lp.edu.ua>. (Дата звернення 24.02.2024).

Маліновський Вадім Ігорович — канд. техн. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, Україна.

Malinovskyi Vadym I. — PhD, associate professor, Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, Ukraine.