https://doi.org/10.31649/1997-9266-2024-175-4-104-114

УДК 004.056:683. 281

В. І. Маліновський[1]
Л. М. Куперштейн[1]
В. В. Лукічов[1]
А. В. Дудатьєв[1]

ПРОБЛЕМАТИКА І ПІДХОДИ ПІДВИЩЕННЯ РІВНЯ ЗАХИСТУ В КАНАЛАХ ПЕРЕДАЧІ ДАНИХ СИСТЕМ І ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ

[1]Вінницький національний технічний університет

Розглянуто сучасні технології кіберзахисту пристроїв і систем Інтернету речей (IoT, Internet of Things), особливості забезпечення їхньої кібербезпеки. Також розглянуто сучасні ризики, новітні та дієві підходи до забезпечення високого рівня кіберзахисту в архітектурі Інтернету речей.

Проблематика кіберзагроз у сучасних пристроях Інтернету речей є різноманітною і формує значну проблему на шляху подальшого просування технологій IoT. Це пов'язано з різноманітними і комплексними інформаційними ризиками кібербезпеки для процесів оброблення та передавання інформації у структурах і пристроях IoT, які використовують різні технології втручання в основний функціонал. Оскільки пристрої і системи IoT використовують здебільшого канали та інтерфейси мережі Інтернет, а також бездротові радіо інтерфейси у поєднанні з мобільними операційними системами на базі високопродуктивних ARM архітектур процесорів, то ризики кібербезпеки IoT значно зростають і ставлять під сумнів тривале стабільне функціонування IoT систем. Інколи ці ризики кібербезпеки створюють досить значну проблему для інформаційних даних в системах IoT, і значно гальмують їхнє просування в низці галузей промисловості. Тому ця проблема повинна бути вирішена. В роботі оцінено та проаналізовано проблематику кібербезпеки в IoT, розглянуто наявні та запропоновано нові окремі дієві практичні положення і підходи для забезпечення високого кіберзахисту систем та пристроїв Інтернету речей. Розглянуто аспекти і проведено аналіз проблем кібербезпеки Інтернету речей з використанням підходів і методів поліпшеного захисту передачі даних в системах і каналах Інтернету речей, підключених до сучасної інформаційної мережі Інтернет.

Запропоновано підходи до захищенішої передачі даних в IoT, які базуються на комплексному поєднанні відомих технологій з комбінацією їхнього сукупного використання і симбіозом з іншими технологіями. Це дозволяє підвищити рівень кібербезпеки і зменшити ризики кіберзагроз в системах IoT, що мають місце і також виникають у інших сучасних інформаційних системах, які часто підключаються і керуються через мережу Інтернет. Ці підходи і принципи дозволяють підвищити надійність і загальну захищеність передачі даних у IoT, оцінити основні чинники впливу інформаційних загроз та зменшити наслідки їхнього впровадження. Розглянуто перспективи розвитку цих підходів і методів у комплексних системах обміну даними IoT. Описано переваги методу і підходів кіберзахисту під час передачі даних у IoT і захищеної криптографічної обробки і передачі інформації у приладах і інформаційних системах Інтернету речей.

Ключові слова: кіберзахист, кіберзагроза, математична модель, ймовірність кіберзагрози, Інтернет речей, Internet of things (IoT), канали зв'язку, процесорні тракти, ПЗ, ШПЗ.

Вступ

Сучасні технології і прилади Інтернету речей (IoT, Internet of Things) широко охоплюють всі сфери сучасного життя від побутового і персонального використання до промислових індустріальних систем Інтернету речей (IIoT — Industrial Internet of Things) і спеціалізованих систем IoT. Останні тенденції впровадження технологій IoT для телемоніторингу та телеуправління свідчать про високі переваги цих систем, їхній широкий і ефективний функціонал [1], [2].

Разом з тим, існують значні ризики і проблематика кіберзагроз у сучасних системах і пристроях

IoT [1], [2]. Це різноманітні і комплексні інформаційні ризики кібербезпеки для інформаційних процесів і структур IoT, які використовують канали та інтерфейси мережі Інтернет та мобільні операційні системи на базі архітектур процесорів ARM. Ризики кібербезпеки IoT інколи утворюють значні проблеми для інформаційних даних в системах IoT, і часто є одним із головних стримуючих факторів з впровадження цих систем в технологічних сферах, особливо в сфері промисловості і критичної інфраструктури.

Проблематика галузі та стан сучасних технологій IoT

Наразі цифрові інформаційні технології IoT набули широкого розвитку, але, разом з тим, набула й нового поштовху хвиля нових інформаційних протистоянь та кібератак на Інтернет речей [1]. Фактично у кожного користувача персонального мобільного пристрою чи іншого пристрою IoT постає проблема кібербезпеки: конфіденційності, цілісності, стабільності і приватності персональних інформаційних даних користувача [1]—[3]. Це характерно у разі використання каналів мережі Інтернет з її численними інформаційними ризиками і кіберзагрозами. В сучасній мережі Інтернет та інформаційній еко-системі фактично для кожного персонального мобільного пристрою і пристрою IoT існують значні ризики і ймовірності кіберзагроз, які викликають необхідність безпечної їхньої експлуатації, дотримання кібергігієни та правил кібербезпеки у разі передавання, оброблення та зберігання даних в IoT, а також необхідність дотримання безпеки і кібербезпеки суміжних до IoT пристроїв і суміжних сервісів і даних.

Метою статті є визначення проблем кібербезпеки в IoT пристроях та формування узагальнювальних перспективних підходів підвищення рівня кіберзахисту в каналах систем і пристроїв Інтернету речей.

Основні кіберзагрози в сучасних пристроях Інтернету речей

На основі результатів аналізу кіберзагроз в IoT [1]—[5] можна зазначити основні з них :

– перехоплення і спотворення даних в каналах та інтерфейсах IoT;

– влаштовування «ін'єкція» шкідливого коду або перехоплення трафіка в каналах IoT;

– інформаційні втручання в інформаційні потоки і програмні модулі (в т. ч. окремі програмні компоненти) і функціонал керування пристроїв IoT;

– перехоплення керування IoT;

– кіберзагрози ядра і контролера операційних систем і контролерів управління IoT;

– інформаційні загрози для пограничних пристроїв IoT (IoT EDGE-Devices: комутатори, маршрутизатори, модеми, шлюзи і інтерфейси зв'язку);

– таргетовані/цілеспрямовані кібератаки атаки і підключення до програмних модулів систем і пристроїв IoT і виведення їх з ладу — DoS (Denial of Service в т. ч. розподілений DDoS -Distributed Denial of Service);

– перехоплення керування та/або спотворення потоків даних моніторингу;

– шкідливе програмне забезпечення (ШПЗ) та підмінене (модифіковане) ПЗ (МПЗ);

– шкідливі посилання і фішинг;

– несанкціоноване перехоплення, втручання на фізичному рівні і спотворення даних;

– генерація та впровадження підмінених сертифікатів захисту шифрування;

– «ін'єкція» шкідливого коду та сертифікату;

– перехоплення (на фізичному) рівні трафіка із супутніх вузлів і дешифрування інформаційних потоків і функціоналу керування системами передачі даних;

– таргетовані кібератаки атаки на системи керування каналів зв'язку і 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;

– атаки на канали передачі Wi-Fi та Bluetooth та кабельні комунікації;

– атаки на ядро і компоненти введення-виведення на суміжних мобільних операційних системах пристроїв керування та моніторингу;

– втручання в захищені механізми формування VPN/Proxy та механізми генерації ключів шифрування;

– використання мережевих експлойтів і «модулів пробиття зв'язку» спрямованих на компоненти управління передачі з шифруванням в складі систем та/або каналів IoT з порушенням штатного

функціоналу ПЗ ядра операційних систем IoT та/або їхніх прошивок, що призводить до порушення та/або модифікування системних програмних функцій ПЗ модулів;

– некоректні системні налаштування та/або помилки операційного персоналу;

– порушення безпеки пограничних пристроїв та модулів зв'язку у IoT (маршрутизатори, комутатори, обладнання оптичного, радіозв'язку тощо), у сукупності з вразливостями проміжних протоколів зв'язку і передачі даних;

– порушення механізму встановлення захищеного з'єднання та атаки MITM;

– недосконаліть і кіберзагрози опорної архітектури і суміжних пристроїв;

– таргетовані віруси і троянські коні, які адаптовані і спеціально спрямовані на конкретний програмний чи апаратний системний компонент інфраструктури системи передачі даних (СПД);

– недосконаліть апаратної структури і мережевих особливостей і хмарних сервісів;

– недосконаліть системних налаштування і мережевих протоколів передачі даних;

– відсутність інформаційного захисту IPS/IDS та захисту каналів IoT з належним рівнем шифрування (IP Sec + IKE RSA) та відсутність мережевого екрану;

– порушення механізму захисту пам'яті ECC на рівні ядра пристроїв IoT (виконання методів несанкціонованого доступу до захищених областей пам'яті: переповнення буфера, вичитування з буфера, доступ до пам'яті в захищених областях);

– недосконаліть мережевих і хмарних сервісів, програмних інтерфейсів API і недосконаліть налаштування безпеки мобільних пристроїв. Використання відомих вразливостей CVE XXn;

– використання і експлуатація інформаційних загроз і вразливостей «0-го» для (Zero day Threats, Zero day Exploution).

Сучасні технології і прилади передачі даних високої швидкості і функціональності базуються на швидкісних і захищених підходах передачі інформації з надійним шифруванням (AES, DES , RSA тощо) і передбачають впровадження достатньо високоінтелектуальних розгалужених алгоритмів оброблення даних в інтерфейсах і каналах та у ядрі з метою їхнього захисту. Трафік даних в каналах та інтерфейсах IoT агрегується (обробляється) і шифрується певним видом кодування за одним спеціалізованим алгоритмом. Але часто тільки цих підходів не достатньо, і повинні використовуватись інші додаткові комплексні підходи захисту даних в IoT: підходи з потоковим захистом даних, ідентифікацією та авторизацією самих пристроїв IoT в інформаційній мережі IoT та інші.

Використання сучасних протоколів IoT може забезпечити достатньо захищений і надійний зв'язок і обмін даними у мережах передачі даних з пристроями Інтернету речей в їхньому складі, і зокрема промислових систем. Часто одного рівня захисту в пристроях IoT не достатньо для організації надійного захисту даних і самої мережі IoT пристроїв. Існують ризики витоків і зламу захисту каналів в IoT інфраструктурі. Також можуть існувати додаткові ризики кіберзагроз і приватності, які можуть стати причиною успішно-проведеної кібератаки і шкідливого інформаційного впливу в IoT.

Інколи для захищеної передачі інформації в інфраструктурі IoT можуть використовуватись сучасні оптичні технології, які базуються на перших 3-х рівнях L1—L3 рівні моделі взаємодії відкритих систем OSI. Це дозволяє організовувати підвищений захист самого процесу передачі інформації на фізичному рівні з використанням ефектів самого світлового випромінювання.

Останні тенденції показують, що використання оптичних та інших перспективних захищених комунікацій у поєднанні з протоколами IoT та налаштованим і увімкненим (на рівні системного ПЗ IoT-пристроїв) надійним шифруванням, дозволяє забезпечити якісний і захищений зв'язок в IoT для передачі даних телемоніторингу і телекерування [2], [3], [5], [8].

Ризики росту чинників загроз, і зокрема несанкціонованого підключення і зчитування і модифікації даних існує в інфраструктурі IoT. Потенційні ризики порушення функціоналу і кібербезпеки сучасних інформаційних систем IoT зростають зі зростанням рівня технологій і розвитком нових методів і засобів втручання.

Ризики перехоплення і модифікації інформації в каналів зв'язку сучасних IoT і промислових мереж залежать від рівня налаштувань безпеки в протоколах IoT, рівня технологій і захищеності самих каналів IoT. До прикладу промислові оптичні мережі з включеним і налаштованим протоколом IoT поверх основного протоколу передачі інформації є більше захищеним, ніж традиційний канал з також включеним і налаштованим протоколом передачі IoT. Це досягається завдяки специфіці використання оптичного випромінювання як носія інформаційного сигналу, що порівняно складніше зчитати, ніж електричний чи радіосигнал.

За своєю природою і структурною організацією канали і алгоритми спеціалізованих протоколів передачі IoT (таких як, Lora(LoraWAN/LoraPAN); ZigBee; AMQP; MQTT, HTTP/HTTPS; CoAP;

DDS; LwM2M; LpWAN; WiFi/WiMax; Z-Wave; RFID; BlueTooth; LTE/BLE ; NFC) подібні до інших традиційних і поширених каналів і протоколів зв'язку (наприклад, TCP/IP- IPSec) з генерацією пар ключів захищеного каналу RSA для шифрування, а також алгоритмів захищеного з'єднання в складі протоколів. На системному рівні часто в більшості протоколів IoT шифрування і захисту виключені за замовчуванням і потребують примусового включення і контролю, в процесі роботи.

Але такий підхід не завжди дозволяє організувати високонадійний та захищений зв'язок в промислових і захищених мережах і каналах передачі даних і системах IoT, особливо у випадках, якщо десь відбувається збій налаштувань безпеки в протоколах IoT чи такі налаштування відсутні та/або відключені тощо.

Можливості сучасних апаратно-програмних засобів зчитування та/або прихованого втручання також значно зросли, як зросли і інтелектуальні функції таких систем. У подальшому прогнозується збільшення кількості атак на комунікаційну інфраструктуру захищених мереж і систем IoT, охоплюючи при цьому і системи типу «розумний будинок», і «розумний офіс» з окремими компонентами автоматизації і кінцевим функціоналом.

Зі зростанням популярності пристроїв IoT і їхніх сервісів зростає інтенсивність кіберзагроз і інформаційних втручань. Способи і інструменти для атак постійно еволюціонують. Велика частина кібератак та інформаційних загроз спрямовані на персональні і IoT пристрої.

У 2021—2024 рр. зросли атаки на комунікації та комунікаційні канали і інтерфейси зв'язку мобільних і функціональних пристроїв IoT: Wi-Fi, 3/4/5G, Bluetooth та провідні комунікаційні інтерфейси, які активно інтегровані у функціонал сучасних розумних пристроїв, що створюють фактори кіберзагроз для мереж IoT і мереж захищеної передачі інформації.

Серед основних причин кібератак і порушення кібербезпеки можна виділити основні:

– відсутність захищених каналів IoT з шифруванням, IPS та VPN/ Proxy , а також відсутність мережевого екрану та неправильні налаштування [1]—[3];

– використання атак з експлуатацією вразливостей систем IoT для порушення штатного функціоналу ПЗ/ядра операційний систем IoT пристрою (системи). Це призводить до порушення/додавання/модифікування/зрізання системних програмних функцій ПЗ [3], [4];

– порушення безпеки пограничних і суміжних пристроїв та модулів зв'язку у суміжних пристроях і в опорній архітектурі (маршрутизатори, комутатори, обладнання радіозв'язку та інше) [3]—[6];

– порушення механізму встановлення захищеного з'єднання та атаки типу MITM [3]—[5];

– недосконаліть і кіберзагрози операційних систем IoT та суміжних системних модулів і ПЗ [5], [6];

– ШПЗ IoT (віруси, троянські коні і бекдори, інші шкідливі модулі і скрипти) [1]—[4];

– недосконаліть мережевих і хмарних сервісів, програмних інтерфейсів API [6].

Враховуючи це, необхідною є розробка нових підходів до захисту передачі даних в IoT, які можуть використовуватись у критичній інфраструктурі IoT. Такий засіб повинен забезпечували повну безпеку функціоналу і захищену передачу даних та їхню обробку для забезпечення сталості і надійності процесу передачі інформації по оптичних каналах зв'язку. Ці підходи повинні базуватись на поєднані комплексному захисту функціоналу на різних рівнях: апаратному та програмному. Тому постає завдання використати поєднання стандартних принципів захисту в протоколах IoT з новими принципами і їхнім симбіозом для підвищення рівня захисту і IoT.

Високий рівень інформаційної захищеності IoT дозволить організовувати високоефективне, комфортне і автоматизоване керування та моніторинг інформаційних процесів і захищену передачу інформації у них. Разом з тим, це дозволить зменшити ризики від впровадження інформаційних технологій IoT, і пов'язаних з ними суміжних технологій у промислові та/або інші критичні системи.

Підвищення безпеки каналів передачі мобільних платформ і пристроїв та пристроїв IoT

Основну частину атак в каналах передачі інформації і комунікаціях IoT складають атаки типу Man in The Midle (MITM). Принцип таких атак показаний на рис. 1 [1]—[6].

Враховуючи значну кількість наявних потенційно можливих кіберзагроз та інформаційних ризиків для IoT [1], [2]—[5], окрім MITM-атак (рис. 1), також це стосується і мобільних персональних пристроїв користувачів, необхідним є використання комплексних підходів і механізмів захисту пристроїв і інфраструктури IoT на всіх рівнях з метою зменшення ймовірностей ризиків кіберзагроз. Актуальною є розробка як нових прогресивних підходів та методів захисту, так і використання їх у поєднанні з відомими але ефективними передовими світовими практиками захисту

— такими як: сегментація мережі IoT; використання сегментів та областей LAN/VLAN зі змінною та нульовими областями довіри (Zero Trust Architeckture Concept), використання прогресивних механізмів та алгоритмів пограничного захисту і контролю трафіка [8].

Рис. 1. Основна схема реалізації атак в каналах і комунікаціях IoT типу MITM (Man in The Midle: «Людина посередині»)

Також актуальними є використання комплексного методу перевірки і нейтралізації кіберзагроз в IoT: з використанням декількох одночасно працюючих інформаційних систем захисту IDS/IPS (Intruder Preventition System / Intruder Defense System) у комплексі з моделями захисту даних для критичної інфраструктури IoT .

В загальному випадку структурний механізм захисту IoT і його компоненти повинен включати комплексне використання механізмів інформаційного захисту, який можна подати у вигляді абстрактної формули захисту:

$$\begin{aligned} &Max\ IoT\ Data\ Security \rightarrow f_i(x_i, y_i, c_i, t_i, k_i, t_i) \cup F\,\mathrm{sec}_i[End\ Point\ IDS / IPS\ + \\ &+ End\ Point\ Component\ Firewall + VPN / VPS\left(L2TP / S2TP / IPSec\right)\ + \\ &+ RSA\ Sessions + \ Zero\ Trust\ Zone\ Policies\ + System\_SIEM + \\ &+ System\_XDM\ /\ XDR + System\_ManagmentRules]; \end{aligned} \quad (1)$$

$$Max\ IoT\ Data\ Security = \sum_{k=1}^{n} F\,\mathrm{sec}_i[x_i] \cup f_i(x_i, y_i, c_i, t_i, k_i, t_i, j_i);$$

$$Max\ IoT\ Data\ Security \rightarrow F(Functiona\_Component\_\mathrm{Sec}urity);$$

$$F\left(x, y, c, t, k, t, j\right) = \overline{k}_i \sum_{i=1}^{n} \overline{f}_i\left(x_i, y_i, c_i, t_i, k_i, j_i\right) + \sum_{i=1}^{n} \overline{S}_{iAdd}\left(t_i\right),\ t \geq t_i,\ t_i > 0, \quad (2)$$

де *Max IoT Data Security* — умовне позначення максимального інформаційного захисту для забезпечення мінімальної кількості потенційних загроз в системах IoT; *End Point IDS/IPS* — сучасні інструменти кіберзахисту і аналізу даних в IoT; *End Point Component Firewall* — сучасні мережевий екран з аналізатором трафіка даних в трактах мережі IoT; *VPN/VPS(with IPSec)* — використання компонент мережевого тунелю з шифруванням на основі протоколу IPSec; *RSA Sessions* — використання механізмів і алгоритмів криптографічного захисту під час обміну даних з ключами шифрування; *Zero Trust Zone Policies* — використання політик розмежування прав доступу та інформаційних політик безпеки заснованих на концепції нульової довіри в зонах для IoT(рис.); *System_SIEM* — умовне позначення інформаційного моніторингу процесів в системі IoT; *SystemXDM/XDR* — інформаційний мережевий захист в системі IoT (Extended Network Monitoring/Extended Network Detection and Responce)*; System Managment Rules* — система управління та організаційних заходів по забезпеченню інформаційної безпеки в системі у менеджменту моніторингу; $F\,\mathrm{sec}_i[x_i]$ — функція (окрема компонентна складова) захисту системи; x_i, y_i, t_i, c_i, j_i, k_i — параметри *i*-го блока інформаційної системи; $f_i(x_i, y_i, c_i, t_i, k_i, t_i)$ — функція станів інформаційної системи (функція, що описує стани *i*-го блока інформаційної системи).

Використання підходів безпеки в критичних зонах архітектурі IoT показане на рис. 2 і рис. 3.

На рис. 3 показані окремі технології з новітніми підходами, які поєднуються з відомими підходами захисту в IoT [8] та разом формують відносно стійкий захист систем IoT.

Взагалі досягти максимального рівня захисту в IoT можливо тільки з використанням комплексного підходу використання окремих вищезазначених компонент у вищенаведеній абстрактній моделі захисту — формули (1) та (2).

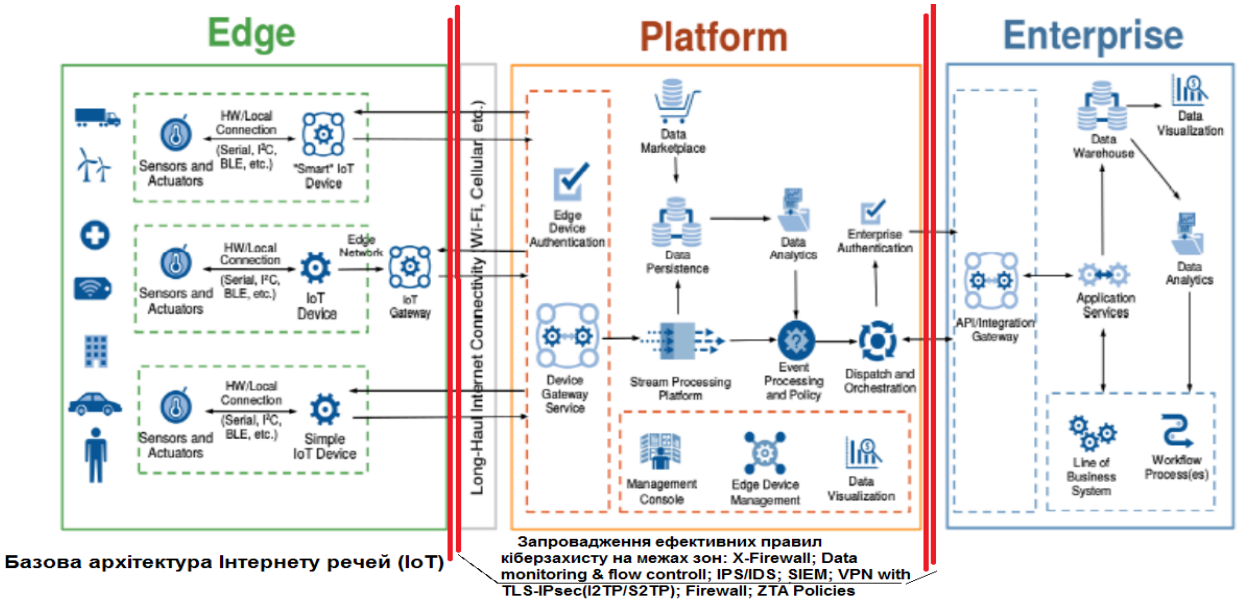

Рис. 2. Вказані зони впровадження мережевих екранів (X-Firewall) між областями у відомій архітектурі систем Інтернету речей [7]

На рис. 3 показано узагальнений принцип комплексної реалізації технологій захисту з досягненням максимуму функції захисту *IoT Data Security → Max IoT Data Security* в каналах передачі даних в IoT.

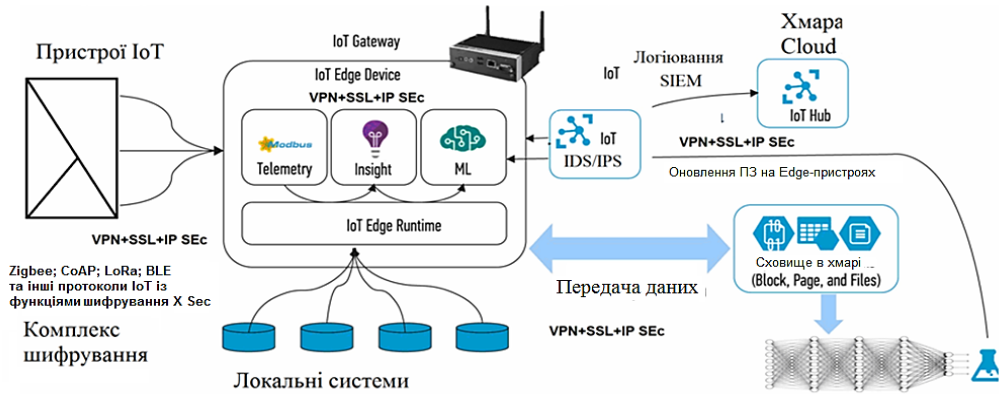

Рис. 3. Підходи і технології підвищення комплексного захисту з досягненням максимуму функції захисту (1) в каналах передачі даних в IoT

Принципи комплексної реалізації технологій захисту IoT показані на рис. 4 та на рис. 5.

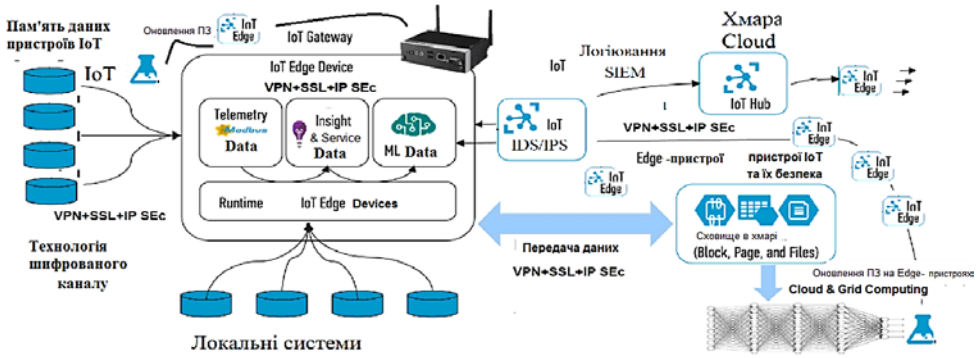

Рис. 4. Принцип реалізації технологій комплексного захисту з досягненням максимальних значень функції захисту (1) в структурі IoT

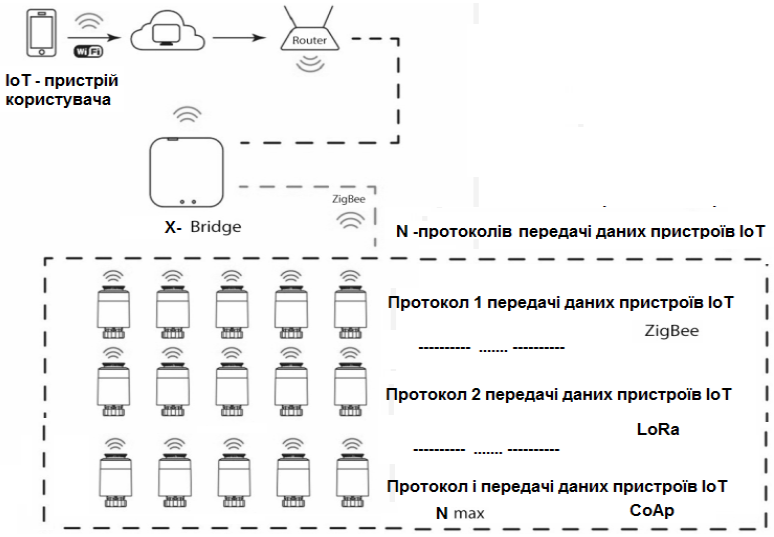

Рис. 5. Принцип підвищення безпеки на базі схеми розділених комунікацій пристроїв IoT на основі підходу використання комутації різних протоколів IoT у поєднанні з ZTA-підходом в архітектурі IoT

Зображення принципів безпеки комунікацій в IoT-пристроях (рис. 5) на базі використання різних протоколів передачі IoT в одній структурі Інтернету речей дозволяє підвищити безпеку, оскільки інформаційна складність ($g(N_{xi})$) умовної безпеки розширюється кожним додатковим протоколом IoT ($g\left(N_{xi}\right)=F\left(SUM\left[N_i\right]\right)$, де N_i — кількість використаних протоколів IoT) з використанням принципів підвищення безпеки на базі розділених комунікацій IoT-пристроїв на базі різних протоколів у їхньому поєднанні.

Забезпечити повну безпеку функціоналу і захищену передачу даних та їхню обробку для IoT персонального спрямування з мобільними персональними пристроями користувачів в його складі вкрай складно, враховуючи різне функціональне спрямування і використання окремих компонент такої IoT, а також використання каналів Інтернет — як одного з джерел проникнення інформаційних загроз. Забезпечення сталості і надійності функціоналу, концепції цілісності, доступності та конфіденційності даних (CIA) в таких IoT — є одними з головних завдань. Нові моделі і методи повинні базуватись на комплексному поєднані функціоналу віртуалізації даних, перевірка їхніх компонентів *IDS/IPS* в окремих ізольованих програмних контейнерах для окремих потоків і процесів інформації зі змішаним додатковим функціоналом. Також для підвищення рівня безпеки повинні створюватися додаткові умови перевірки і контролю сторонніх інформаційних потоків з надійним вдосконаленим шифруванням зі зміщенням та у поєднанні з розпаралелюванням обчислювального процесу з розмежуванням прав доступу на різних рівнях обчислень і віртуальних обчислювальних середовищах(оболонок) для різних процесів.

Проблема використання кіберзахисту в універсальних архітектурах IoT полягає у ефективній взаємодії різних пристроїв та технологій IoT між собою, з організацією безпечного обміну інформацією в них. В окремих випадках виникає потреба використання принципів поєднання — «конвергенції» різних комунікацій виду дата-трафіка в одному каналі в IoT.

Використання принципів конвергентних комунікацій на базі різних протоколів у разі комплексної реалізації технологій захисту IoT — на прикладі використання різних протоколів IoT в одній мережі також дозволяє підвищити загальний рівень безпеки.

Основні і найвпливовіші ризики кібербезпеки в системах і пристроях Інтернету речей на пограничному рівні (Edge) та рівні представлення (*Enterprise*)

– вразливості проміжних каналів і радіоканалів та використання MiTM- та X-spoofing атак;

– ризики для вузлів пограничних пристроїв (шлюзи, маршрутизатори, комутатори, тощо);

– вразливості функціоналу в ПЗ та апаратної частині кінцевих пристроїв;

– шкідливий програмний функціонал, експлойти і ШПЗ для пристроїв Інтернету речей [5], [7], [12];

– отримання несанкціонованого адміністративного доступу нижнього рівня та рівня адміністратора системи (на нижньому рівні ОС або прошивки IoT пристрою) [5], [7]—[10], [12]—[19].

Дослідження і експериментальний досвід показують, що є декілька варіантів практичних ефективних підходів захисту проти вищезазначених видів кібератак в радіоканалах IoT. Наприклад, ізоляція і зменшення радіосигналу в каналах Wi-Fi/x-IoT протоколів по периметру будинку або

обмеження потужності, паралельно з використанням надійного шифрування та захисту в каналах [5], [7], [10], [14]. Цей спосіб в більшості випадків практично можливо легко реалізувати включенням відповідних системних налаштувань в IoT. Ще додатковий перспективний напрямок захисту — додавання контрольованого «шуму» до каналів радіосигналів IoT і створення обфускації каналів (до прикладу, додаванням фейкових каналів або додаткових шумів).

Сучасні виклики кібербезпеки, сучасні програмні та апаратні інструменти криптоаналізу ставлять під сумнів повну 100 % надійність схеми з використанням 128-бітних (AES 128 +) ключів шифрування, у разі використання її у IoT-пристроях. Тому надійні механізми захисту повинні передбачати:

– використання ключів підвищеної довжини > AES128 (в ідеалі на практиці AES 256–512);

– використання вдосконалених механізмів обміну: IKE ver. 2 і вище (IKE, Inter Key Exchange);

– використання додаткового функціонального захисту і практик захисту у поєднанні з наявними традиційними механізмами захисту і шифрування.

Також можуть бути додатні такі практики, як:

– додавання шуму та використання скремблювання в каналах;

– обфускації інформації в каналах (періодичні зміни ID/IP каналу в часі за прихованим алгоритмом);

– додавання додаткових інформаційних «шумових» послідовностей в канали передачі IoT;

– використання другорядних шифрів та інструментів захисту в каналі.

Практика та експерименти показують, що швидкий перехід на технології підвищеного захисту не можливий одразу без зміни обладнання і ПЗ. Оновлення відбуваються не одразу, а протягом якогось періоду часу (1—3 роки), що вимагає прийняття супутніх ризиків недостатнього шифрування і захисту в каналах IoT.

Безпека комунікацій IoT на базі спеціалізованих протоколів залежить від надійності шифрування в інтерфейсах IoT. Наприклад, протокол IoT LoRa передбачає обмін 2-ма ключами шифрування: AppSKey an NwkSKey за захищеним вдосконаленим механізмом IKE (Inter Key Exchange).

Як описано в роботах [7], [8], незалежно від використовуваної процедури активації канал IoT захищається двома сеансовими ключами AES128: AppSKey і NwkSKey. Ці ключі використовуються не для шифрування в блоковому режимі, а в режимі потоку (поточне шифрування) — режимі CTR [8], методом CTR : його різновидом під назвою CCM (режим лічильника). Сам метод CTR — добре відомий метод перетворення блочного шифру (наприклад, AES128) у потоковий шифр.

Отже, безпека в каналі IoT зводиться до належного керування криптографічним матеріалом та інформацією, необхідною для створення потоку ключів. Метод CCM використовує режим CTR для шифрування вмісту корисного навантаження за допомогою AppSKey і аутентифікує повідомлення за допомогою коду CMAC на основі ключа NwkSKey. Блоки генератора потоку ключів (A_i) шифруються певним ключем (AppSKey або NwkSKey) залежно від типів пакетів даних, і результат застосовується до 128-бітових блоків, які складають корисне навантаження повідомлення [8]

$$\begin{aligned} &A_i = [1]_8[O]_{32}[D]_8[DevAddr]_{32}[Cnt]_{32}[O]_8[i]_8; \\ &S_i = AES-128\left(K, A_i\right); \\ &EncFRMPayload = \left[S_0\right]\left[S_1\right]\left[S_2\right]...\left[S_m\right] \otimes FRMPayload. \end{aligned} \tag{3}$$

Індекси вказують на розмір кожного об’єднаного поля даних в бітах. Байти полів розміром понад 8 біт сортуються в порядку байтів. Поле D (адреса) має значення 0 для висхідної лінії зв’язку та 1 для низхідної лінії зв’язку. Лічильник Cnt — це лічильник повідомлень, який використовується залежно від напрямку повідомлення, і має значення 0 на початку сеансу. Лічильник блоків (i) показує блок AES, до якого застосовується результат шифрування.

Ключ K — це NwkSKey або AppSKey залежно від типу MAC-пакета (контрольний або пакет даних відповідно). Отримане повідомлення аутентифікується за допомогою AES-128-CMAC для генерації коду цілісності і автентичності повідомлення (MIC) за допомогою NwkSKey, незалежно від типу пакета даних. Цей код цілісності обчислюється на основі заголовка пакета, корисного навантаження та певного блоку B0, які вже зашифровано і об’єднано на початку. Це традиційна класична схема шифрування в IoT.

При цьому в більшості протоколів обміну повідомленнями в IoT-пристроях використовується зазвичай 128-бітні ключі шифрування. Що було цілком достатньо до тепер для забезпечення надійного захисту. Але сучасні ризики для каналів IoT вже не завжди дозволяють безпечно використ-

товувати 128-бітну схему.

Можна показати, що для того, щоб додатково функціонально захистити, потрібно додати обфускацію і контрольоване підмішування додаткових блоків даних в канал (скремблювання на передавальній стороні А за прихованим алгоритмом) разом з використанням традиційного шифрування і механізму перетворення даних в канал додаткової послідовності (функціонал FDRload[i]) і обчисленням потоку на основі комплексного поєднання скремблювання. Складність і стійкість потокового шифрування разом зі скремблюванням буде дещо вищою, що ускладнить декодування:

$$EncFRMPayload[a] = [S_0][S_1][S_2]...[S_n] \otimes FRMPayload \otimes FDRLoad[i]; \quad (4)$$

$$A_i = [1]_8[O]_{32}[D]_8[DevAddr]_{32}[Cnt]_{32}[O]_8[i]_8[n]_8;$$

$$EncFRMPayload[b] = [S_0][S_1][S_2]...[S_n] \otimes FRMPayload \otimes \left[\overline{-FDRLoad[i]}\right]; \quad (5)$$

$$S_i = AES-128\left(K, A_i, D_i\right).$$

На приймальній стороні ці блоки даних будуть відкидатись з синхронізацією алгоритму (на стороні передавача і приймача А–В). Таким чином (4) матимемо додаткову агрегацію потокових даних з використанням обфускаційного функціоналу скремблювання *FDRload*[*i*], що дозволить внести додаткові дані в канал (так звані контрольовані завади). Якщо функціонал скремблювання *FDRload*[*i*] детермінований і синхронізований в часі t_i (сторона А і В), то це може бути враховано і описано як на стороні А, так і на стороні В каналу IoT. Це врахування дозволить швидко і ефективно компенсувати складову *FDRload*[*i*] на стороні В, шляхом її відфільтровування.

Сама питома складність в каналі IoT та його криптонадійність буде вищою, але не значно, оскільки містить додаткові дані для обфускації.

На додаток до відсутності наскрізного шифрування, згаданого в роботах [7], [8], [10], [25], [19], відсутність надійної аутентифікації самих пристроїв IoT призводить до серйозних ризиків кібербезпеки каналів IoT.

Повторне використання лічильників повідомлень і кадрів в LoRaWAN 1.0 дозволяє більш-менш надійне шифрування в режимі CTR та CTM [**7**], [8], [14**]**. Останній метод за своєю суттю є безпечнішим, проте слабка політика оновлення ключів та замала їхня довжина може зробити його неефективним. Під час використання CTR пристрій IoT зазвичай зв'язується з мережею та сусідами зі скиданням початкового значення лічильника повідомлень. Це призводить до виникнення можливостей для атаки типу «атаки відкритого тексту», яку ще називають «атакою перетягуванням шпаргалки», яка фактично зводиться до зламу шифрів та дескремблювання за відомими алгоритмами криптоаналізу. Принцип її полягає в тому що, залежно від знань про загальну структуру повідомлення, її основу, періодичність та окремі регулярні ознаки в повідомленнях каналів IoT в режимах CTR та CTM, можна скомпрометувати комунікацію всіх повідомлень в каналі чи інтерфейсі IoT. Чим більше кадрів буде захоплено за такої атаки, тим більша ймовірність виконання цієї атаки в каналах IoT. Це відносно нові типи кіберзагроз і відносно небезпечні. Для протистояння ним потрібно використовувати вищезазначені комплексні підходи захисту.

Без наскрізного захисту або з його слабким налаштуванням, а також без додаткових підходів захисту, комунікації в каналах IoT викликають значні ризики кіберзахищеності передачі повідомлень через них.

Вирішення цієї проблеми можливе за використання комплексних підходів кібербезпеки в IoT на різних рівнях. Це викличе подальший розширений розвиток галузі IoT з безпечнішим впровадженням у інші сфери життєдіяльності, зокрема використання в критичних системах.

Висновки

Розглянуто проблематику кібербезпеки у разі комунікації через канали IoT. Також розглянуто основні види атак і підходи підвищення кібербезпеки в комунікаційних каналах IoT на базі комплексних підходів. Розглянуто основні ризики, вразливості та атаки у комунікаційних інтерфейсах IoT, також підходи підвищення рівня їхньої захищеності у разі передачі інформації у комунікаційних інтерфейсах пристроїв Інтернету речей (IoT). Зокрема, визначено основні проблеми та втрати інформації у цих місцях. Розглянуто матеріали окремих досліджень, які ґрунтуються на практичному досвіді і роботах з дослідження кіберзагроз в інтерфейсах IoT.

Подані матеріали показують підходи, які можуть бути використані для реалізації ефективнішо-

го захисту у разі комунікації в інтерфейсах і каналах пристроїв і систем Інтернету речей (IoT), зокрема, дозволять підвищити рівень захисту від атак типу MITM (людина посередині), які проводяться в інтерфейсах передачі IoT. Проведена робота може дати змогу оцінювати та організовувати захист від основних кіберзагроз і зменшувати ризики їхньої появи в IoT або мінімізувати їхній сумарних вплив на стабільність функціонування систем і мереж IoT. Також проведений аналіз і запропоновані підходи можуть бути використані для розробки методу ефективнішого захисту та управління ризиками з метою підвищення захищеності в IoT та для їхнього стабільного і безпечного функціонування.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Vadym Malinovskyi, Leonid Kupershtein, and Vitaliy Lukichov, “Cybersecurity and Data Stability Analysis of IoT Devices,” *Materials of 2022 IEEE 9th International Conference on Problems of Infocommunications. Science and Technology (PIC S&T`2022). IEEE Ukraine Section.* Kharkiv National University of Radio Electronics.

[2] Vadym Malinovskyi, Leonid Kupershtein, and Vitaliy Lukichov, “Risks Assessment and Approaches to Creative of the Reliable Software Modules for IoT Devices,” *Materials of International Conference on Innovative Solutions in Software Engineering*. November 29-30, 2022. Ivano-Frankivsk, Ukraine.

[3] Yuan Xiao, Yinqian Zhang, and Radu Teodorescu, *Speechminer: a Framework for investigating and measuring speculative execution vulnerabilities*. [Electronic resource]. Available: https://arxiv.org/pdf/1912.00329.pdf . Accesed: 18.01.2024.

[4] В. І. Маліновський, «Мінімізація факторів кіберзагроз і спеціалізовані підходи до інформаційного захисту мікропроцесорних систем індустріального Internety речей,» *Матеріали LI-ї науково-технічної конференції факультету інформаційних технологій та комп’ютерної інженерії.* Факультет інформаційних технологій та комп’ютерної інженерії (ФІТКІ). 2022. 31.05.2022. ВНТУ: [Електронний ресурс]. Режим доступу: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2022/paper/view/15000 . Дата звернення 19.01.2024.

[5] В. І. Маліновський, «Сучасні кіберзагрози і захист даних в системах і пристроях Internety речей,» *Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення*, матеріали міжнародної наукової Internet-конференції, вип. 6, 4-5 липня 2022. [Електронний ресурс]. Режим доступу: http://www.konferenciaonline.org.ua/ua/article/id-595/ . Дата звернення 19.01.2024.

[6] Alper Kerman, Oliver Borchert, Scott Rose, and Eileen Division Allen Tan, “Implementing a Zero Trust Architecture: [Nist project Description],” *The National Cybersecurity Center of Excellence (NCCoE) Project Descriptions*, 2020, 17 p. [Electronic resource]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.ZTA.pdf . Accessed: 19.01.2024.

[7] S. Rose, et al., “Zero Trust Architecture,” *National Institute of Standards and Technology (NIST) Special Publication 800-207*, Gaithersburg, Md., August 2020. [Electronic resource]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf . Accesed:19.01.202.

[8] T. Dönmez, and C. Nigussie, “Security of LoRaWAN” vol. 1.1 in *Backward Compatibility Scenarios. Procedia Computer science*, no. 134, pp. 51-58, 2018. [Electronic resource]. Available: https://www.sciencedirect.com/science/article/pii/S1877050918311062 . Accessed: 19.01.2024.

[9] Л. М. Куперштейн, і С. П. Бондарчук, «Загрози та вразливості бездротових мереж,» [Електронний ресурс]. Режим доступу: http://dspace.kntu.kr.ua/jspui/bitstream/123456789/5022/1/AUConferenceCyberSecurity_November2016_p146.pdf . Дата звернення 19.01.2024.

[10] Joshua Franklin, et al., “*Mobile Device Security Cloud and Hybrid Builds*,” *NIST SPECIAL PUBLICATION 1800-4A / The MITRE Corporation McLean*, VA, February 2019. [Electronic resource]. Available: https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/cloud-hybrid .

[11] E. Perelman, G. Hamerly, M. Van Biesbrouck, T. Sherwood, and B. Calder, “Using Simpoint for accurate and efficient simulation in ACM sigmetrics performance evaluation review,” *IEEE Access*, vol. 31, no. 1, pp. 318-319, 2003.

[12] Miloud Bagaa, Tarik Taleb, Jorge Bernal Bernabe, and Antonio Skarmeta, “A machine learning security framework for lot systems,” *IEEE Access*, may 21, 2020. IEEE Press. Digital Object Identifier 10.1109/ACCESS, 2996214, 2020.

[13] J. Pacheco and S. Hariri, “IoT security framework for smart cyber infrastructures,” in *Proc. IEEE 1st Int. Workshops Found*. Appl. Self Syst. (FAS*W), Sep. 2016, pp. 242247.

[14] A. Souri, A. Hussien, M. Hoseyninezhad, and M. Norouzi, “A systematic review of IoT communication strategies for an efcient smart environment,” *Trans. Emerg. Telecommun. Technol.* Aug. 2019, Art. № e3736. [Electronic resource]. Available: https://onlinelibrary.wiley.com/action/showCitFormats?doi=10.1002%2Fett.3736 .

[15] Amjad Mehmood, Gregory Epiphaniou, Carsten Maple, Nikolaos Ersotelos, and Richard Wiseman, “A hybrid methodology to assess cyber resilience of IoT in energy management and connected sites,” *Sensors*, no 23, 8720, pp. 2-46, 2023. [Electronic resource]. Available: https://www.mdpi.com/journal/sensors. MDPI Sensors https://doi.org/10.3390/s23218720 .

[16] T. Taleb. “Toward carrier cloud: Potential, challenges, and solutions,” *IEEE Wireless Commun*, vol. 21, no. 3, pp. 80-91, Jun. 2014.

[17] S. Lal, T. Taleb, and A. Dutta, “NFV: Security threats and best practices,” *IEEE Commun*. Mag., vol. 55, no. 8, pp. 211-217, Aug. 2017.

[18] V. Varadharajan, and U. Tupakula, “Security as a service model for cloud environment,” *IEEE Trans. Netw. Service Manage*, vol. 11, no. 1, pp. 60-75, Mar. 2014.

[19] Y. Khettab, M. Bagaa, D. L. C. Dutra, T. Taleb, and N. Toumi, “Virtual security as a service for 5G verticals,” *IEEE Wireless Commun. Netw. Conf. (WCNC*), Apr. 2018, pp. 1-6.

[20] X. Wang, C. Wang, X. Li, V. C. M. Leung, and T. Taleb, “Federated deep reinforcement learning for Internet of Things with decentralized cooper-ative edge caching,” *IEEE Internet Things J.*, early access., Apr. 9, 2020, https://doi.org/10.1109/JIOT.2020.2986803 .

[21] *Zero-Touch Network and Service Management* (ZSM), Reference Architecture. Standard ETSI GS ZSM 002, V1.1.1.

Aug. 2019.

[22] K. S. Sahoo, B. Sahoo, and A. Panda, “Asecured SDN Framework for IoT,” in *Proc. Int. Conf. Man Mach. Interfacing (MAMI), Dec*. 2015, pp. 1-4.

[23] C. Gonzalez, S. M. Charfadine, O. Flauzac, and F. Nolot, “SDN-based security Framework for the IoT in distributed grid,” in *Proc. Int. Multidis-ciplinary Conf. Comput. Energy Sci. (SpliTech)*, Jul. 2016, pp. 15.

[24] T. Nowatzki, J. Menon, C. Ho, and K. Sankaralingam, “Architectural simulators considered harmful,” in *IEEE Micro*, vol. 35, no. 6, pp. 4-12, 2015.

Рекомендована кафедрою захисту інформації ВНТУ

Стаття надійшла до редакції 28.06.2024

Маліновский Вадим Ігоревич — канд. техн. наук, доцент кафедри захисту інформації, e-mail: vad.malinovsky@gmail.com ;

Куперштейн Леонід Михайлович — канд. техн. наук, доцент, доцент кафедри захисту інформації;

Лукічов Віталій Володимирович — канд. техн. наук, доцент, доцент кафедри захисту інформації;

Дудатьєв Андрій Веніаміновіч — канд. техн. наук, доцент, доцент кафедри захисту інформації.

Вінницький національний технічний університет, Вінниця

V. I. Malinovskyi [1]
L. M. Kupershtein[1]
V. V. Lukichov[1]
A. V. Dudat’ev[1]

Problems and Approaches to Increase the Cybersecurity Level in the Data Transmission Channels of the Internet of Things Systems and Devices

[1]Vinnytsia National Technical University

The article deals with modern technologies and devices of the Internet of Things, features of providing their cybersecurity, current risks and the latest and effective approaches to high-level cyber defense in the architecture of the Internet of things.

The problems of cyber threats in modern internet devices are diverse and generate a significant problem on the path of further promotion of IoT technologies. These are various and complex information risks of cybersecurity for processing and transmission processes in the IoT structures and devices that use different technologies of intervention in the main functionality. As the IoT devices and systems use the Internet and interfaces of the Internet, as well as wireless radio interfaces in combination with mobile operating systems based on high -yielding ARM processors, the risks of IoT cybersecurity are growing significantly and put in question the long - term stable functioning of IoT systems. Sometimes these risks of cybersecurity create a significant problem for information data in IoT systems, and significantly slow down their promotion in a number of industries. Therefore, this problem must be resolved. The work has evaluated and analyzed the problems of cybersecurity in the IoT, the existing approaches are considered and new effective practical provisions and approaches to ensure high cyber defense systems and Internet devices are suggested.

The aspects have been considered and the analysis of the problems of cybersecurity of the Internet of things using approaches and methods of the improved protection of data transmission in systems and channels of the Internet of things that are connected to modern Internet information network is carried out.

Approaches to more protected data transmission in IoTs, based on a comprehensive combination of known technologies with a combination of their aggregate use and symbiosis with other technologies, are proposed. This enables to enhance cybersecurity and reduce the risks of cyber threats in IoT systems that occur and also takes place in other modern information systems that are often connected and guided via the Internet. These approaches and principles allow to increase the reliability and overall protection of data transmission to IoT, evaluate the main factors of the impact of information threats and to reduce the consequences of their implementation. The prospects for the development of these approaches and methods in complex IoT data exchange systems are considered. The advantages of the method and approaches of cyber defense while the transmission of data to IoT and protected cryptographic processing and transmission of information in the devices and information systems of the Internet of things are described.

Keywords: cyber defense, cyber threats, mathematical model, probability of cyber threats, internet things, Internet of things (IoT), communication channels, processor tracts, software, malware.

Malinovskyi Vadym I. — Cand. Sc. (Eng.), Associate Professor with the Chair of the Data Security, e-mail: vad.malinovsky@gmail.com ;

Kupershtein Leonid M. — Cand. Sc. (Eng.), Associate Professor, Assistant Professor with the Chair of the Data Security;

Lukichov Vitalii V. — Cand. Sc. (Eng.), Associate Professor, Associate Professor with the Chair of the Data Security;

Dudat’ev Andrii V. — Cand. Sc. (Eng.), Associate Professor, Associate Professor with the Chair of the Data Security