CZU: 004.7

SECURITATEA ŞI CONFIDENȚIALITATEA „RFID" CA PARTE IMPORTANTĂ A TEHNOLOGIILOR „IOT"

Rodica BULAI,
asistent universitar,
Catedra „Procedură penală, criminalistică și Securitate informațională"
a Academiei „Ștefan cel Mare" a MAI
ORCID: 0000-0002-7878-2431

Iurie BULAI,
doctor în drept, conferențiar universitar,
Catedra „Procedură penală, criminalistică și Securitate informațională"
a Academiei „Ștefan cel Mare" a MAI
ORCID: 0000-0001-5914-340X

Rezumat

În cadrul acestui articol a fost abordată o tehnologie ce este omniprezentă și ia amploare – tehnologia Internet lucrurilor/of Things. Tehnologie ce facilitează gestionarea și efectuarea diferitelor activități atât cu caracter profesional cât și personal/domiciliar. Dar pe lângă oportunitățile ce le oferă sunt și unele dificultăți ce solicit soluționarea, acestea fiind vulnerabilitățile tehnologiilor respective. Abordarea vulnerabilităților specifice și tehnologiei RFID, parte componentă a tehnologiei Internet lucrurilor/of Things, identificarea vulnerabilităților tehnologiilor va permite conștientizarea dilemelor, precum și lansarea unor direcții, măsuri de soluționare, minimalizare și contracarare a acestora. Acest fapt va permite sporirea gradului de securizare a tehnologiilor RFID și implicit a tehnologiei Internet lucrurilor/of Things. De asemenea, se va realiza identificarea vulnerabilităților, precum și lansarea unor măsuri de minimalizare și contracarare a consecințelor acestora.

Cuvinte-cheie: Internetul Obiectelor/lucrurilor (IoT), tehnologie RFID, criptare, autentificare, etichetă, cititor.

Summary

In this article, a technology that is ubiquitous and growing - the Internet of Things technology was addressed. Technology that facilitates the management and performance of various activities, both professional and personal/domiciliary. But in addition to the opportunities they offer, there are also some difficulties that require solving, these being the vulnerabilities of the respective technologies. Addressing the specific vulnerabilities and RFID technology, a

component of the Internet of Things technology, the identification of technology vulnerabilities will allow the identification and awareness of dilemmas as well as the launch of directions, measures to solve, minimize and counteract them. This fact will allow increasing the degree of security of RFID technologies AND IMPLIEDLY the Internet of Things technology. identifying vulnerabilities as well as launching measures to minimize and counteract their consequences

Keywords: Internet of Things/Things (IoT), RFID technology, encryption, authentication, tag, reader.

Introducere. Internetul Obiectelor/lucrurilor (IoT) este o infrastructură globală de rețea, care leagă obiectele fizice și virtuale, prin exploatarea capabilităților de captare și comunicare a datelor, infrastructură, care include evoluții existente și în curs de dezvoltare în rețea. Internetul Obiectelor va oferi capabilități specifice de identificare a obiectelor, senzori și conexiuni ca bază pentru dezvoltarea de servicii și aplicații de cooperare independente, care vor fi caracterizate printr-un grad ridicat de captare autonomă a datelor, transfer de evenimente, conectivitate în rețea și interoperabilitate [3, p. 13].

Internetul lucrurilor (IoT) este cel mai recent concept în care Internetul evoluează de la conectarea/conexiunea computerelor și a oamenilor la conectarea/conexiunea obiectelor/lucrurilor (inteligente) [8].

Termenul „Internet of Things" a fost inventat de Kevin Ashton, care este co-fondatorul Auto-ID Center, în acest mod el a numit raportul său pentru Procter & Gamble în 1999 [8]. A fost o încercare de a introduce o idee nouă, de utilizare a tehnologiei de identificare a frecvenței prin unde radio (RFID) în lanțul de logistică/aprovizionare cu mărfuri industriale și, ca urmare, a atras atenția asupra ideii de a conecta la rețea noi tipuri de dispozitive.

În ultimul deceniu, Internetul lucrurilor a intrat lejer în viața noastră odată cu apariția sistemelor de comunicații fără fir: RFID, Wi-Fi, 4G, IEEE 802.15.x, care sunt cel mai des folosite în softurile de monitorizare și control. Astăzi, sistemele Internet of Things sunt folosite nu numai pentru rețele private, ci și în fabrici, întreprinderi și spitale, biblioteci etc., chiar agenții guvernamentale.

În ciuda popularității sale, răspândirea tehnologiei Internet of Things este împiedicată de numeroasele probleme de securitate în acest domeniu. Astfel, printre cele peste 50% dintre companiile chestionate în 2022 de Kaspersky Lab, dificultățile în implementarea dispozitivelor Internet of Things su fost direct legate de preocupările de securitate a acestor tehnologii [2].

Ca și orișicare tehnologie, pe lângă facilități și beneficii posedă unele vulnerabilități ce necesită a fi identificate, analizate în vederea stabilirii calității și posibilelor consecințe în caz de valorificare a acestora de persoane rău intenționate.

Principalele tipuri de amenințări și vulnerabilități ale tehnologie IoT, vectorii potențialelor atacuri asupra dispozitivelor IoT pot fi împărțiți în trei grupe, în funcție de ținta atacului: hardware, software și date transmise [6].

Nivelul de codificare: identifică obiectul de interes (este baza/temelia IoT). Acest aspect atribuie fiecărui obiect un identificator unic (ID), ce permite obiectul să fie ușor de găsit. Nivelul de percepție ține de nivelul dispozitivelor IoT care conferă fiecărui obiect o semnificație fizică. El este format din diverse tipuri de senzori de date, cum ar fi etichete RFID, senzori IR sau alte rețele de senzori care pot citi temperatura, umiditatea, viteza, locația etc.

La dezvoltarea IoT pe scară largă pot contribui mai multe tehnologii, una dintre acestea fiind identificarea prin radiofrecvență tehnologiile (RFID). RFID este o tehnologie cheie concepută pentru a identifica în mod unic obiectele. Dimensiunea mică a etichetei și costul redus fac posibilă integrarea tehnologiei în orice obiect. O etichetă este un transceiver în formă de microcip, asemănător unui autocolant, care poate fi activ sau pasiv, în funcție de tipul de aplicație. Etichetele au o baterie încorporată, deoarece sunt active în mod constant, în timp ce etichetele pasive sunt activate doar atunci când sunt pornite. Etichetele active sunt mai scumpe decât cele pasive. Un sistem RFID constă din cititoare și etichete care generează date de identificare, topografice și altele.

Semnalele de date ale obiectului/dispozitivului emitent sunt transmise cititorilor prin unde radio și apoi procesate pentru a analiza datele în funcție de tipul de aplicație. Frecvențele RFID sunt împărțite în 4 game de frecvență: 1. Frecvență joasă (135 kHz sau mai puțin); 2. Frecvență înaltă (13,56 MHz); 3. Frecvență ultra-înaltă (862 MHz – 928 MHz); 4. Frecvența cuptorului cu microunde. De asemenea există și o altă tehnologie: identificarea - cod de bare, care are aceeași funcție ca RFID, deși tehnologia RFID este considerată mai eficientă. Fiind o tehnologie radio, RFID nu necesită contact vizual direct cu cititorul, în timp ce codul de bare este o tehnologie optică care nu funcționează decât dacă cititorul se află direct în fața acestuia. Mai mult, RFID poate acționa ca un mobil/actuator, ce impulsionează diverse acțiuni, posedând capacitatea de a fi modificat.

Sarcinile de securitate și confidențialitate IoT fac posibilă identificarea/depistarea oricărei persoane, totodată oferind posibilitatea de simplificare a vieții; cu toate acestea, fără o încredere adecvată în securitatea și confidențialitatea datelor utilizatorilor, acest sistem nu va fi acceptat de multe persoane. Prin urmare, pentru implementarea pe scară largă, IoT trebuie să aibă o infrastructură de securitate puternică/viabilă [9]. Vă prezentăm aici doar câteva posibile probleme specifice legate de securitatea IoT și utilizarea tehnologiilor.

Accesul neautorizat la RFID.

Accesul neautorizat la etichete, care pot conține informații de identificare, este o problemă majoră de securitate IoT (posibila dezvăluire a oricărei informații sensibile despre utilizator). Eticheta poate fi nu doar descifrată de dispozitivul de citire al unui atacator, ci chiar și modificată sau deteriorată. Există mai multe amenințări reale la adresa RFID, care includ virusul RFID, atacul pe telefonul mobil și hackul SpeedPass.

Riscurile asociate securității informaționale a Internetului obiectelor sunt atestate de mai multe tipuri: - risc de interceptare: interceptarea pasivă a canalului de comunicație, metodele de implementare presupun interceptarea conexiunilor wireless la noduri, interceptarea datelor între nodurile rețelei; - risc de furt de informații înregistrate: furt din medii de informare înregistrate, precum memoria etichetelor RFID, nodurile rețelei; - riscuri de compromitere a datelor: încălcarea securității, faptul că un atacator a obținut informații confidențiale, astfel de riscuri pot fi împărțite în aplicații pentru persoane fizice și pentru afaceri: primele aplicații includ aplicații RFID, controlul accesului, colectarea plăților electronice, etichetarea produselor. Pentru utilizator, amenințarea este o invazie în viața privată, afectarea confidențialității sale, posibile pierderi financiare, supraveghere a deplasărilor utilizatorului; aplicațiile de gestionare a afacerilor includ aplicații implementate pentru nevoile unei afaceri sau o combinație a acestora. Obținerea accesului la astfel de aplicații poate perturba funcționarea și execuția atât a întregului proces cât și a proceselor individuale ale întreprinderilor/companiilor, compromițând informațiile cu caracter confidențial. De exemplu, aplicații care se ocupă de procesul de management al lanțului de aprovizionare;

Unul dintre elemente frecvent utilizate în tehnologiile IoT sunt tehnologiile RFID, care atestă o serie de riscuri și vulnerabilități. Să aruncăm o privire mai atentă asupra eficienței protecției informațiilor folosind exemplul: vulnerabilitățile obiectelor RFID utilizate în tehnologiei Internet of Things [12].

Opțiunile pentru amenințările de securitate sunt următoarele tipuri: - interceptarea pasivă; înlocuire (elementului de identificare) ID; - refuzul de efectuare a serviciului; - interferență/bruiajul intenționată; - „retransmitere și substituție"; - „ man in the middle" sau „om la mijloc"; - atac prin canale terțe [4].

Elementele de protecție a acestor tehnologii este necesar atât la nivel individual cât și un complex de măsuri la nivel general. Următoarele opțiuni pentru asigurarea protecției informațiilor pot fi considerate ca o opțiune de protecție individuală sau ca un complex care combină mai multe opțiuni selectate pentru a crește eficacitatea protecției. Securitatea sediului – dacă toate etichetele sunt cu siguranță; a fi într-o singură locație/cameră; este necesar să se asigure securitatea acestei încăperi, aceasta eliminând vulne-

rabilităţile asociate cu accesul direct la etichete. Dar cel mai frecvent, aplicaţiile RFID solicită deplasarea obiectelor, această situaţie impunând organizarea securităţii la nivel fizic. Utilizarea etichetelor RFID numai pentru citire protejează datele de a fi şterse sau modificate prin citirea/interceptarea semnalului de un dispozitiv neautorizat. Limitarea distanţei de conexiune „cititor-tag (etichetelor RFID transmitere-recepţionare)" se efectuează prin limitarea parametrilor fizici ai etichetei, citirea/interceptarea antenei.

Implementarea unui protocol de comunicare de tip închis implică crearea unui protocol de comunicare şi a unei scheme de criptare a datelor care nu sunt disponibile publicului. În funcţie de metoda de criptare şi de complexitatea protocolului, metoda poate oferi un nivel sporit de securitate, dar protocoalele de tip închis fac mai dificilă utilizarea etichetelor şi aplicaţiilor RFID. Crearea unui paravan/ecranarea sau aşa numita cuşcă Faraday – scopul abordării de acest tip este de a exclude accesul undelor electromagnetice prin plasarea obiectului într-un mediu/material care poate oferi această posibilitate. Se poate de asigurat un nivel ridicat de securitate, acesta fiind posibil prin garantarea inaccesibilităţii etichetei pentru cititor. Prin folosirea opţiunii Kill vom bloca radio-etichetele. În acest caz, eticheta RFID nu mai poate recepţiona sau trimite informaţii sau încetează să mai funcţioneze. Avantajul unei asemenea modalităţi de abordare este garanţia protecţiei datelor cu caracter personal ale utilizatorului sau cumpărătorului. Eliminarea/distrugerea fizică este realizată printr-un câmp magnetic puternic.

Contramăsurile pot include utilizarea siguranţelor cu resetare automată (un dispozitiv folosit pentru a proteja echipamentele electronice) sau a diodelor Zener (o diodă care funcţionează sub polarizare inversă în modul de defecţiune). Criptare şi autentificare – Furnizarea accesului numai utilizatorilor autorizaţi folosind diverse scheme de criptare şi/sau autentificare. Autentificarea este verificarea autenticităţii unui identificator prezentat de utilizator. Un exemplu de schemă de autentificare ar fi ca un dispozitiv autorizat să introducă o parolă şi, în caz contrar, să blocheze datele de pe etichetă. Procesul de introducere a unei parole pentru deblocare poate fi implementat cu uşurinţă. Blocare selectivă – schema foloseşte blocarea etichetelor RFID care simulează prezenţa multor etichete tradiţionale, cu alte cuvinte, abordarea împiedică citirea.

Cititorul de semnal de etichetă neautorizat.

Blocantul trebuie să fie în raza de acţiune a cititorului, funcţionând ca o etichetă pasivă şi protejând doar un număr mic de dispozitive. Algoritmul de acces multiplu aleatoriu este blocat de la trecerea prin arbore, fiind protejat de cititorii externi rău intenţionaţi atunci când solicită etichete de utilizator UID. Ideea blocantului este de a folosi două antene pentru a emite

simultan „1" și „0" în timpul accesului multiplu aleatoriu, provocând o coliziune și împiedicând cititorul să treacă prin toate punctele de ramificare ale algoritmului de acces multiplu aleatoriu. Ca urmare, informațiile despre utilizarea etichetelor UID protejate rămân private, iar utilizatorul este protejat de scanarea nedorită. Nu poate fi implementat în sistemele care utilizează etichete doar pentru citire sau dispozitive fără cip, deoarece tehnologia necesită etichete care pot fi scrise.

Opțiuni pentru efectuarea unei blocării selective: crearea de etichete RFID ce blochează. Are loc blocarea completă a canalului, în care eticheta suprimă toate dispozitivele de citire a semnalului din raza sa și, o variantă opțională, implementează un atac de tip „denial of service" pentru a perturba funcționarea întregului sistem RFID. Se pot configura dispozitivele într-un mod încât să detecteze astfel de situații și să informeze un specialist. Protector RFID este un dispozitiv activ cu capacitatea de a fi integrat într-un PDA (asistent/computer digital personal) sau telefon mobil. Avantajul este că poate împiedica citirea informațiilor prin emiterea unui semnal de bruiaj în banda de frecvență a etichetelor RFID. Funcțiile dispozitivului sunt de mai multe tipuri: schimbul de informații cu cititorul pentru a gestiona cheile secrete, autentificarea și controlul accesului, monitorizarea mediului și avertizarea asupra posibilelor atacuri, crearea coliziunilor pentru a preveni citirea rău intenționată a informațiilor.

Dispozitivul își folosește bateriile interne și generează un semnal la o distanță de 0,5 m, în timp ce generează două benzi laterale la un nivel de putere aproximativ egal cu semnalul purtător al cititorului. Poate fi folosit și pentru un atac DoS. În continuare, va fi necesar să se determine eficiența utilizării echipamentului de protecție descris mai sus pentru obiectul RFID. Este necesar să se ia în considerare scopul obiectului RFID: acesta trebuie să transmită date în timp real, fără întârzieri, iar datele trebuie să fie de încredere. Eficiența este probabilitatea de a finaliza o sarcină de sistem, în acest caz un obiect cu etichetă RFID, și constă în conceptul de adecvare (îndeplinirea obiectivelor, cerințelor) și de optimizare (nevoia de a introduce una sau alta măsură de protecție fără a afecta funcționarea) a sistemului. În conformitate cu opțiunea pentru utilizarea ecranului, criptare și blocaj, sistemul funcționează fără defecțiuni, cu o eficiență de protecție ridicată.

Problemele de securitate sunt asociate cu caracteristicile tehnologiei RFID: • transmisia wireless între identificator și cititor provoacă atacuri bazate pe utilizarea interfeței de radiofrecvență; • implementarea hardware a algoritmilor de criptare permite metodelor de reinginerire să aibă acces la informații cheie; • resursele hardware limitate ale identificatorului fac imposibilă implementarea unei game largi de măsuri de securitate; • dimensi-

unea redusă a etichetelor de frecvență radio le face aproape invizibile, care pot fi folosite pentru monitorizarea neautorizată a obiectelor folosind tehnologia RFID.

Direcțiile posibile de atac asupra sistemelor care utilizează tehnologia RFID sunt împărțite în funcție de scop: • atacuri asupra identificatorului, atacuri asupra cititorului; • atacuri asupra canalului de comunicare. Cea mai mare amenințare de securitate este utilizarea complexă a atacurilor pe canalul de comunicare. Interceptarea este un tip pasiv de atac în care datele dintr-o sesiune între un identificator și un cititor sunt interceptate fără a le modifica sau suprima. Principala măsură împotriva interceptării este criptarea datelor. Retransmiterea este un tip activ de atac în care schimbul de date între etichetă și cititor are loc printr-un dispozitiv de interceptare. Modificarea datelor este posibilă.

Un alt tip de atac este reluarea prin înregistrarea și retransmiterea unui semnal. Dispozitivul „atacator" accesează eticheta, imitând cititorul, înregistrează semnalul de răspuns, apoi îl transmite cititorului ca pe o etichetă. Această vulnerabilitate este tipică pentru protocoalele de autentificare slabe fără utilizarea marcajelor de timp. Refuzarea serviciului este un atac asupra unui sistem RFID cu scopul de a-l duce la eșec, adică de a crea condiții în care serviciul pentru utilizatorii legitimi este întrerupt sau blocat complet. Contracararea în așa cazuri este posibilă de realizat prin detectarea și eliminarea din sistem fizic sau folosind software-ul dispozitivelor atacatoare. Bruiajul electronic activ este generarea de interferențe radio active care interferează cu funcționarea sistemului RFID. Ca și în cazul atacului anterior, contracararea este de a detecta și elimina sursa interferenței. Imitarea identității conexiunii – atacul se realizează prin clonarea identificatorului și uzurparea identității unei conexiuni cu un cititor. Ca protecție sunt utilizați algoritmi criptografici.

Atacul asupra dispozitivului de citire.

De obicei cititorul se află într-o zonă controlată (pază/securitate, supraveghere video), ceea ce limitează foarte mult posibilitatea unui atac. Cea mai productivă abordare este de a recrea aspectul sistemului RFID al obiectului atacat în laborator pentru a dezvolta și eficientiza mecanismul de atac. Astfel, pot fi dezvoltate: • etichete false percepute de sistem pentru a accesa informații protejate; • diverse software malițioase care distrug sau modifică modul de operare a sistemului. Ca o contramăsură, se recomandă eliminarea sau ascunderea tuturor semnelor vizibile prin care cititorul poate fi determinat că aparține unui anumit sistem RFID, precum și modificarea setărilor standard, cum ar fi parola administratorului.

Atacul asupra identificatorului. Distrugere fizică – distrugere mecani-

că, chimică, iradiere cu influenţă electromagnetică puternică, tăierea microcipului de la antenă. Ecranarea - folosind folie de aluminiu în jurul antenei, reglarea greşită a transponderului - dezacordarea dielectrică a antenelor UHF (reducerea diapazonului de citire). Distrugerea fizică şi ecranarea sunt probleme deosebite în cazurile în care etichetele RFID sunt folosite nu numai pentru identificare, ci şi, de exemplu, pentru a număra/evalua cantitatea de medicament rămasă într-un depozit. Manipularea datelor stocate pe un identificator - schimbarea, copierea, modificarea - modificarea deliberată a conţinutului unei etichete, denaturarea atributelor elementelor de descriere. Se face posibilă introducerea de software maliţios. De exemplu, datele de pe identificator pot fi modificate astfel încât să fie interpretate de sistem ca comenzi. Folosind echipamente speciale, cum ar fi o staţie FIB, cu un fascicul de ioni focalizat, se poate modifica conţinutul memoriei (EEPROM sau ROM) în etichete nereinscriptibile [7].

În cazul distrugerii fizice este necesară, în opinia noastră, lansarea şi sporirea măsurilor de Securitate fizică şi restricţionarea accesului.

Cercetătorii Lucinin V.V. şi Sadovaia I.M. afirmă că această tehnică poate fi folosită pentru a seta o cheie „secretă" la o valoare cunoscută. Pentru aceasta, trebuie de determinat locaţia cheii în memorie. Utilizarea unor astfel de metode complexe necesită utilizarea unor echipamente scumpe şi un nivel ridicat de cunoştinţe. Contramăsurile corespund metodelor de contracarare a ingineriei inverse (straturi de protecţie, senzori de influenţe externe neautorizate) şi criptarea datelor de memorie [11]. Tehnologiile RFID se folosesc în diferite domenii inclusive, după cum am specificat anterior; în domeniul medicinei.

Unele particularităţi de asigurare a securităţii tehnologiilor RFID în domeniul medical.

Datorită prezenţei unui canal radio în sistemele medicale şi biologice de identificare prin radiofrecvenţă, trebuie luate măsuri suplimentare pentru protejarea acestora, deoarece sesiunile de schimb de informaţii pot fi interceptate destul de uşor: 1. Transferul de date trebuie organizat astfel încât atacatorul, chiar dacă este posibil să interfereze cu sesiunea de informare pentru a asculta sau a introduce blocuri de date străine, să nu poată atinge scopul dorit. Cu toate acestea, puterea scăzută de calcul şi viteza schimbului de informaţii în astfel de sisteme nu permite utilizarea unui număr de mecanisme şi proceduri fiabile pentru protejarea mesajelor utilizate în tehnologia de transmisie a datelor.

2. Analiza posibilelor aspecte de interceptare a canalului de comunicaţie dintre identificator şi cititor, în combinaţie cu posibilitatea efectuării ingineriei inverse a cristalului circuitului integrat (IC), creşte semnificativ vul-

nerabilitatea sistemului în cauză. Implementarea hardware și a algoritmilor de criptare permite prin metode de inginerie inversă să se obțină informații despre criptocheile secrete și funcționarea criptosistemului. Pe cip, blocurile care implementează criptoalgoritmul sunt ușor de identificat datorită prezenței elementelor caracteristice în blocul corespunzător: • LE „SAU exclusiv"; • un număr de declanșatori - registre de deplasare cu feedback liniar, permițând obținerea unei secvențe pseudo-aleatoare de vectori; • viperă. 3. Resurse limitate a etichetei (RFID) și, în consecință, incapacitatea de a implementa multe măsuri de protecție pentru a preveni accesul neautorizat, în special un set de metode active pentru a preveni pătrunderea cipului.

Concluzie. Asigurarea nivelului necesar de securitate al tehnologiilor RFID este asociată cu următoarele domenii: • consolidarea mecanismelor hardware și software pentru protecția criptografică a datelor de identificare și a protocolului de comutare, folosind algoritmi de criptare atât simetrici, cât și asimetrici, precum și prin protecția fizică a cristalului etichetei IC (folosirea diferitelor abordări ale implementării straturilor de protecție ale cristalului); • „ofucarea" topologiei cristalului („criptarea vizuală" a logicii) pentru a face imposibilă restaurarea criptosistemului de cristal, folosind metode de inginerie inversă și pentru a face dificilă identificarea magistralelor de semnal în timpul atacurilor sondelor. O soluție eficientă la problemele de organizare a unui mecanism de protecție a sistemelor de identificare prin radiofrecvență în contextul dispozitivelor utilizate în scopuri medicale și biologice se coraportează cu limitările determinate de incapacitatea și limitările hardware de a implementa algoritmi criptografici puternici și de a utiliza întreaga gamă de metode active pentru a contracara accesul neautorizat la cristalul IC. În setul general de sarcini de asigurare a protecției sistemelor care utilizează tehnologii RFID, una dintre cele mai actuale este contracararea utilizării instrumentelor și metodelor de reinginerie (inversă), care permit accesul fizic direct la unitatea de criptare și obținerea datelor în formă necriptată.

Referințe bibliografice

1. Claroty Team. BIANNUAL ICS RISK & VULNERABILITY REPORT: 2H 2021 // Claroty: Claroty Ltd., 2023. Дата публикации: 09.12.2022. – URL: https://claroty.com/2h21-biannualreport/.

2. Kaspersky. Pushing the limits: How to address specific cybersecurity demands and protect IoT // Kaspersky: [сайт]. – AO Kaspersky Lab, 2023. Дата публикации: 08.02.2022. URL: https://www.kaspersky.com/blog/iot-report-2022/,

3. Oancea C. Aspecte privind rolul securității cibernetice asupra in-

ternetului obiectelor (IoT). Teză de doctorat. Rezumat. Academia de Poliţie „Alexandru Ioan Cuza", Bucureşti, 2018, p. 13.

4. Schurgot M.R., Shinberg D.A., Greenwald L.G. *Experiments with security and privacy in IoT networks.* În: World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2015 IEEE 16th International Symposium on, 2015.

5. Vervier P.A., Shen Y. *Before Toasters Rise Up: A View Into the Emerging IoT Threat Landscape.* În: Research in Attacks, Intrusions, and Defenses – Cham: Springer, 2018, p. 556-576. DOI: http://dx.doi.org/10.1007/978-3-030-00470-5_26.

6. Williams P., Dutta I. K., Daoud H., Bayo M. *A survey on security in internet of things with a focus on the impact of emerging technologies / umi.* În: Internet of Things; Engineering Cyber Physical Human Systems. 2022. Vol. 19. Nr. 100564. DOI: https://doi.org/10.1016/j.iot.2022.100564.

7. Гасников А.О., Ершов М.И., Кондрашов К.К., Лучинин В.В. Информационная защита микроконтроллеров при использовании в системах медицинского назначения. În: Биотехносфера. 2016. № 1 (43). p. 56-58.

8. Довгаль В.А., Довгаль Д.В. Интернет Вещей: концепция, приложения и задачи. În: Вестник Адыгейского государственного университета. Сер. Естественно-математические и технические науки. 2018. Вып. 1 (221), p. 129-135. URL: http://vestnik.adygnet.ru.

9. Довгаль В.А., Довгаль Д.В. Проблемы и задачи безопасности интеллектуальных сетей, основанных на Интернете Вещей. În: Вестник Адыгейского государственного университета. Сер. Естественно-математические и технические науки. 2017. Вып. 4 (211), p. 140-147. URL: http://vestnik.adygnet.ru.

10. Довгаль В.А., Довгаль Д.В. Управление ресурсами в Интернете Вещей. În: Дистанционные образовательные технологии: материалы II Всерос. науч.- практ. конф., г. Ялта, 2017 г. Симферополь: АРИ-АЛ, 2017, p. 168-173.

11. Лучинин В.В., Садовая И.М. Информационная безопасность смарт-микросистем и технологий. СПб.: СПбГЭТУ «ЛЭТИ», 2015, 157 p.

12. Финкенцеллер К. *RFID-технологии:* справочное пособие. М.: ДМК Пресс, Додэка XXI, Hanser Publishers, 2016, p. 45-53.