CZU:005:22:004.056.53.

METODE TEHNICE ŞI MANAGERIALE ALE SECURITĂŢII INFORMAŢIEI

Dr. Mihail GUZUN, ing. Lilian FRIPTULEAC

Institutul de Dezvoltare a Societăţii Informaţionale (IDSI), R. Moldova, idsi@asm.md

Rezumat. *Lucrarea descrie cele mai frecvente ameninţări de securitate, provenite atât din interiorul cât şi din exteriorul organizaţiei, precum şi metodele tehnice, organizatorice, de altă natură, utilizate pentru prevenirea consecinţelor negative ale incidentelor de securitate. Ca bază metodologică pentru elaborarea şi implementarea metodelor de securitate menite să asigure confidenţialitatea, disponibilitatea şi integritatea informaţiei sunt recomandate standardele internaţionale ale familiei ISO/IEC 27000 care prevăd aplicarea unor practici recunoscute la nivel internaţional orientate spre instituirea şi îmbunătăţirea continuă a unui sistem de management al securităţii informaţiei (SMSI). Sunt descrise, de asemenea, procesul de implementare a SMSI bazat pe cerinţele standardului ISO/IEC 27001:2013 la Institutul de Dezvoltare a Societăţii Informaţionale (IDSI) şi beneficiile pe care le asigură respectarea cerinţelor standardului.*

Cuvinte cheie. *Standardele familiei ISO/IEC 27000, sistem de management, incident de securitate, audit al SMSI, analiză a SMSI, tehnologii informaţionale.*

Abstract. *The paper describes the most common security threats from both inside and outside the organization and technical, organizational and other methods used to prevent negative consequences of security incidents. As a methodological base for the development and implementation of security measures to ensure the confidentiality, availability and integrity of information are recommended international standards of the family ISO/IEC 27000, which provides internationally recognized practices oriented to establishing and continuous improving the information security management system (ISMS). The implementation of ISMS based on the requirements of ISO/IEC 27001:2013 in the Information Society Development Institute (ISDI) and benefits that ensure compliance with the standard are described.*

Keywords. *ISO/IEC 27000 standards, management system, security incident, ISMS audit, ISMS analysis, information technologies.*

1. Introducere

În ultimii ani, dezvoltarea tehnologiilor informaţionale în Republica Moldova a luat o deosebită amploare, înregistrându-se progrese importante în toate ramurile, începând cu dezvoltarea şi implementarea celor mai noi sisteme de comunicare până la implementarea de noi tehnologii, unele din ele fiind în premieră pentru ţara noastră. Una dintre ramurile tehnologiilor informaţionale, Internetul, s-a bucurat de un mare succes în rândul populaţiei Moldovei, ajungând în mai puţin de 10 ani la o cifră de 518.385 de abonaţi la Internet prin linie fixă şi la peste 1.691.575 de abonaţi la Internet mobil, ceea ce înseamnă că mai mult de jumătate din populaţia ţării este abonată la serviciul Internet în bandă largă, fiind înregistrate venituri de peste 400 milioane de lei per trimestru. La fel, putem observa că avem de trei ori mai mulţi abonaţi ai Internetului mobil (3G, 4G), ceea ce denotă faptul că cetăţenii R. Moldova preferă să acceseze Internetul prin intermediul telefonului mobil (odată cu procurarea telefoanelor noi, majoritatea fiind smartphone) sau al tabletelor [1]. Cetăţenii au devinit membri ai unei formaţiuni sociale noi – societatea cunoştinţelor online, care presupune integrarea informaţiei într-un sistem digital, facilitând astfel accesul populaţiei la informaţie şi, totodată, asigurând durabilitatea şi prezervarea acesteia.

Odată cu dezvoltarea multitudinii de tehnologii digitale, riscurile au luat amploare, îndeosebi când este vorba de utilizarea acestor tehnologii în mediul corporativ. Atacurile cibernetice s-au intensificat în ultima perioadă, atât în R. Moldova cât şi la nivel mondial. Doar din atacurile care implică malware, care este şi unul dintre cele mai periculoase tipuri de atacuri, se câştigă anual peste un miliard de dolari, această sumă fiind în creştere de la o zi la alta. Până în anul 2021 piaţa neagră a atacurilor cibernetice este estimată la o cifră de 6 trilioane de dolari [2]. Circa 85 % din incidentele cibernetice se produc din vina angajaţilor (laptop-uri în afara controlului, acces al ex-angajaţilor la sistemele informaţionale, abuzul de e-mailuri, pierderea sau scurgerea informaţiilor confidenţiale etc.) [3].

Numărul atacurilor cibernetice a crescut în ultimii ani şi în R. Moldova. Conform datelor Centrului de Telecomunicaţii Speciale, numărul atacurilor cibernetice asupra serverelor web a crescut în anul 2014 cu circa 26% faţă de anul 2013, iar vulnerabilităţile porturilor deschise au sporit cu circa 385%. Posibilităţile de infectare a calculatoarelor cu viruşi informatici au crescut cu circa 27% [4]. Doar în primele 6 luni ale anului 2016 au fost pornite 60 de cauze penale privind infracţiunile cibernetice, faţă de 58 de cauze penale iniţiate în perioada similară a anului 2015 [5]. În anul 2015 au avut loc 27 de tentative de penetrare sau perturbare a funcţionalităţii sistemelor informatice de stat, fiind afectate peste 12 instituţii de stat din R. Moldova. Au fost identificate şase servere localizate peste hotare, de la care erau infectate calculatoarele [6]. Un atac recent a fost cel din ziua alegerilor prezidenţiale de la Chişinău din data de 30 octombrie 2016, când serverele Comisiei Electorale Centrale au fost atacate de peste 41.000 de ori [7]. Faptul că atacurile cibernetice capătă o frecvenţă, o complexitate şi o amploare din ce în ce mai mare, aducând pagube enorme sectorului guvernamental, al celui privat şi persoanelor particulare, dictează implementarea unor măsuri complexe de securitate atât la nivel naţional, cât şi la nivel de organizaţie. Experienţa acumulată în domeniul securităţii informaţiei confirmă necesitatea abordării sistemice în acest domeniu, care include aplicarea concomitentă a metodelor juridice, tehnice şi manageriale prin aplicarea cadrului legislativ şi instituţional, a cadrului normativ şi tehnico-normativ.

2. Cadrul legal în domeniul securităţii informaţiei în R. Moldova

Cadrul legal în domeniul securităţii informaţiei din R. Moldova are ca punct de referinţă Convenţia de la Budapesta împotriva criminalităţii informatice, adoptată la 23 noiembrie 2001 de Consiliul Europei [8] și ratificată de Parlament prin Legea nr. 6 din 02.02.2009 [9]. În vederea realizării prevederilor documentelor susnumite, au fost adoptate Legea nr.20-XVI din 3 februarie 2009 privind prevenirea şi combaterea criminalităţii informatice [10], Programul naţional de securitate cibernetică a Republicii Moldova pentru anii 2016-2020 (Hotărârea Guvernului nr. 811 din 29.10.2015 [4]) şi alte documente menite să contribuie la sporirea eficacităţii şi eficienţei activităţilor de securizare a informaţiei atât la nivel naţional cât şi la nivel de organizaţii, fără deosebire de forma de proprietate, domeniul de activitate, mărime, etc.

În R. Moldova funcţionează un centru special, CERT-GOV-MD din cadrul Centrului de Telecomunicaţii Speciale, al cărui sarcină este să răspundă la incidente ce ţin de securitatea sistemelor informaţionale. Acesta asigură serviciile necesare pentru gestionarea incidentelor şi sprijinirea procesului de recuperare a datelor în urma încălcărilor sau incidentelor de securitate. CERT-GOV-MD a fost creat pentru a asista procesul de utilizare a sistemelor informaţionale şi de telecomunicaţii ale autorităţilor administraţiei publice, implementarea măsurilor proactive şi reactive în vederea reducerii efectelor negative ale incidentelor de securitate IT şi acordarea asistenţei în cazul incidentelor. Centrul, de asemenea, examinează incidentele apărute în reţelele din R. Moldova şi care sunt raportate de către cetăţeni şi instituţii din ţară şi din străinătate [11].

Având la bază cadrul naţional legal, organizaţiile urmează să-şi proiecteze şi să implementeze propriul sistem de securitate a informaţiei, care include măsuri tehnice, organizatorice şi de altă natură, orientate spre diminuarea şi chiar excluderea efectelor negative ale potenţialelor incidente care pot afecta disponibilitatea, integritatea sau confidenţialitatea informaţiei, independent de sursele din care provin aceste incidente.

3. Metodele manageriale de asigurare a securităţii informaţiei în R. Moldova

Metodele manageriale de asigurare a securităţii informaţiei includ reglementări interne referitoare la relaţiile dintre angajaţi, care ar exclude sau limita divulgarea, scurgerea sau accesul nesancţionat la informaţii. Aceste metode includ selectarea şi instruirea personalului, formularea obligaţiunilor referitoare la securitatea informaţiei în contractele individuale de muncă şi fişele postului, organizarea accesului controlat la locurile unde se procesează informaţii sensibile, elaborarea şi păstrarea copiilor de rezervă, lichidarea controlată a informaţiei confidenţiale şi alte măsuri.

În ajutorul managementului care intenţionează să-şi asigure disponibilitatea continuă şi să-şi protejeze integritatea şi confidenţialitatea informaţiei vine Organizaţia Internaţională de Standardizare (ISO) cu familia de standarde ISO/IEC 27000, care oferă îndrumări bazate pe bunele practici acumulate în domeniu privind implementarea, menţinerea, îmbunătăţirea, evaluarea (auditul) şi certificarea unui sistem de management al securităţii informaţiei. Această familie de standarde include:

ISO/IEC 27000:2016 reprezintă o caracteristică generală a standardelor familiei ISO/IEC 27000 şi termenii utilizaţi în aceste standarde. Tot aici sunt formulate şi principiile, a căror respectare asigură beneficii organizaţiilor care recurg la implementarea unui SMSI bazat pe cerinţele standardelor internaţionale:

- conştientizarea de către întreaga organizaţie a necesităţii unei abordări sistemice în domeniul securităţii informaţiei;
- atribuirea responsabilităţii şi autorităţii pentru securitatea informaţiei;
- incorporarea necesităţilor şi aşteptărilor părţilor interesate referitoare la securitatea informaţiei în strategiile manageriale ale organizaţiei;
- accentul pe valorile socio-umane;
- evaluarea riscurilor pentru a determina controalele necesare ce ar conduce la atingerea unor niveluri acceptabile de risc;
- perceperea securităţii ca fiind un element esenţial al reţelelor şi sistemelor informaţionale;
- abordarea proactivă pentru detectarea şi prevenirea incidentelor de securitate a informaţiei;
- abordarea complexă în domeniul securităţii informaţiei;
- reevaluarea continuă şi revizuirea sistemului de management al securităţii informaţiei atunci când este necesar.

ISO/IEC 27001:2013 este standardul în baza căruia are loc evaluarea şi certificarea sistemelor de management al securităţii informaţiei. Acesta este unul din primele standarde manageriale adaptate la cerinţele Directivelor ISO/IEC, Anexa XL (a.2012) în ceea ce priveşte instituirea structurii de nivel avansat (”High level structure”), care prevede:

- titluri identice de subcapitole;
- text identic;
- termeni şi definiţii de bază comune

ISO/IEC 27002:2013 este un cod de bune practici în domeniul securităţii informaţiei, care include obiectivele de control în domeniul SMSI şi măsurile de securitate utilizate pentru atingerea acestor obiective.
ISO/IEC 27003:2010 este un ghid pentru implementarea standardului ISO/IEC 27001.
ISO/IEC 27004:2016 reprezintă îndrumări pentru aplicarea metricilor de securitate a informaţiei.
ISO/IEC 27005:2011 stabileşte abordările privind evaluarea, analiza şi tratarea riscurilor de securitate a informaţiei.
ISO/IEC 27006:2015 stabileşte cerinţe pentru organismele de certificare a sistemelor de securitate a informaţiei.
ISO/IEC 27007:2011 stabileşte regulile pentru auditul SMSI.

Standardele enumerate constituie un suport pentru proiectarea, implementarea, menţinerea şi îmbunătăţirea continuă a unui sistem de management al securităţii informaţiei în cadrul organizaţiei.

4. Politică de securitate într-o companie

În baza standardelor internaţionale, organizaţiile îşi stabilesc propriul sistem de management al securităţii informaţiei, care este îmbunătăţit continuu prin aplicarea instrumentelor manageriale de colectare şi analiză a datelor, evaluare a riscurilor de securitate şi stabilire a metodelor de tratare a acestora, organizare a auditurilor interne şi externe, întreprinderea de acţiuni corective pentru eliminarea cauzelor incidentelor de securitate şi a altor neconformităţi ale sistemului, efectuarea analizei periodice a sistemului de management etc. Abordările manageriale în domeniul securităţii informaţiei pot fi eficace dacă sunt completate cu metode de securitate de ordin tehnic ce reprezintă o componentă importantă în procesul de prevenire sau stopare a unui atac cibernetic şi anume: utilizarea unui antivirus, firewall, unor sisteme de detectare a intruziunilor, ”patch management systems” etc. [12].

Pe lângă toate acestea, sunt necesare crearea şi implementarea strategiilor de protecţie a datelor care să includă procedee de conştientizare a pericolelor unui atac cibernetic, dar şi acţiunile ce ar urma să fie realizate în urma unui atac cibernetic. Este deosebit de importantă focusarea asupra punctului de risc, în special, atunci când în joc sunt puse datele confidenţiale sau cele care au o circulaţie activă. Vizibilitatea datelor este şi ea o procedură actuală şi intens discutată, mai ales în cadrul instituţiilor publice, dar mai întâi trebuie să fie stabilit gradul de sensibilitate a acelor date şi riscurile la care sunt supuse atunci când ele sunt difuzate cu acces deschis. Este necesară o monitorizare permanentă a datelor, pentru a înţelege unde sunt stocate, prin ce metode sunt accesate, cât de frecvent sunt accesate, de unde sunt accesate şi care sunt grupurile de interes care accesează aceste date. Protecţia datelor trebuie să se extindă mai departe de hotarele organizaţiei. Niciodată nu trebuie să fie ignoraţi angajaţii care, după cum am menţionat mai sus, sunt responsabili în mare parte de numărul mare de atacuri cibernetice, partenerii, unele sisteme globale pe care le utilizăm, cum ar fi cloud-ul, etc.

O politică de securitate într-o companie trebuie neapărat să includă un regulament clar pentru angajaţi. Unul din motivele principale pentru implementarea unei politici de securitate constă în necesitatea de a informa toţi angajaţii despre metodele corecte de utilizare a calculatoarelor, Internetului, sistemelor informaţionale, utilizarea e-mailurilor şi a comunicărilor virtuale, importanţa utilizării serviciului de e-mail corporativ, păstrarea şi transportarea datelor, criptarea datelor sensibile, utilizarea parolelor. De asemenea, sunt necesare şi cunoştinţe privind modul de a reacţiona în cazurile unor incidente informatice, unde trebuie să se adreseze sau cum să stopeze un atac în faza incipientă. O politică de securitate trebuie să includă în mod obligatoriu:

- utilizarea de către angajaţi a serviciului de mail corporativ, reglementat la rândul său de un regulament strict. Blocarea anumitelor pagini web (în funcţie de tipul datelor puse la dispoziţia angajatului şi de pericolul acelor pagini web);
- stabilirea clară a grupurilor de lucru care trebuie să proceseze şi să stocheze date sensibile;
- securizarea şi gestionarea echipamentului informatic;
- gestionarea sistemelor instalate pentru a urmări cine şi în ce scopuri utilizează echipamentul IT din cadrul organizaţiei;
- implementarea unui sistem care să semnalizeze pătrunderea în organizaţie a unui dispozitiv străin.

Unele studii arată că utilizarea unui antivirus poate să diminueze cu aproape 98 % riscul unei infectări a calculatorului. Din acest motiv asigurarea condiţiilor minime de securitate este foarte importantă. Trebuie de stabilit ce sisteme antivirus, antispyware pot fi utilizate şi dacă ele au tehnici avansate de prevenire a atacurilor de tip RANSOMWARE. Dacă angajatul lucrează la distanţă este necesar să fie asigurată securitatea în timpul lucrului. Trebuie să fie utilizate întotdeauna tehnici de protecţie, cum ar fi VPN şi tehnici avansate de criptare care ne-ar asigura că informaţia nu este sustrasă, indiferent de locaţia angajaţilor. În cazul utilizării unui calculator personal, trebuie neapărat să se verifice ce sisteme antivirus sunt utilizate şi dacă sistemul de operare este unul licenţiat şi actualizat, ce browsere Web sunt folosite şi dacă alte software-uri sunt licenţiate şi actualizate. Este necesară implementarea unor metode confidenţiale de raportare a încălcărilor, incidentelor de securitate, etc. De multe ori angajaţilor le este dificil să raporteze unele probleme de securitate observate în companie. Dacă sunt oferite mecanisme confidenţiale de raportare, este foarte mare probabilitatea că ei vor raporta despre un incident înainte ca el să ia o amploare mai mare, asigurând astfel timpul necesar pentru acţiuni de remediere a lacunelor. Toate regulile expuse mai sus pot fi realizate în mod sistematic şi consecvent aplicând tehnicile oferite de standardele manageriale ale securităţii informaţiei elaborate de ISO.

5. Sistemul de Management al Securităţii Informaţiei

Institutul de Dezvoltare a Societăţii Informaţionale (IDSI) a elaborat, a certificat şi menţine un Sistem de Management al Securităţii Informaţiei, bazat pe cerinţele standardului internaţional ISO/IEC 27001:2013 (certificat Nr. 268/14, emis de organismul de certificare româno-italian RINA SIMTEX).

Etapele principale ale implementării cerinţelor standardului au inclus:

- decizia echipei manageriale de nivel superior de a implementa şi certifica sistemul standardizat de management al securităţii informaţiei (SMSI);
- stabilirea structurii organizatorice de implementare a SMSI;
- evaluarea SMSI existent în organizaţie în raport cu cerinţele standardului ISO/IEC 27001;
- elaborarea politicilor şi a obiectivelor de securitate;
- inventarierea resurselor informaţionale şi clasificarea lor în dependenţă de consecinţele pierderii confidenţialităţii, disponibilităţii şi a integrităţii;
- analiza riscurilor care pot afecta securitatea resurselor;
- definirea şi documentarea domeniului de aplicare a sistemului;
- elaborarea şi implementarea planului de tratare a riscurilor;
- auditul intern, analiza sistemului efectuată de echipa managerială.

Sistemul de management al securităţii informaţiei al IDSI s-a constituit în baza unui set de documente interne (proceduri, instrucţiuni, regulamente), prin intermediul cărora au fost adaptate cerinţele generale ale standardului ISO/IEC 27001:2013 la specificul activităţilor IDSI – servicii de cercetare-dezvoltare în domeniul tehnologiilor informaţionale si al comunicaţiilor. În cadrul realizării SMSI a fost documentată metodologia de evaluare a riscurilor şi au fost stabilite metode de tratare a riscurilor de securitate a informaţiei prin aplicarea măsurilor de control, enumerate în Anexa A (normativă) a standardului ISO/IEC 27001:2013 şi descrise în mod detaliat în standardul ISO/IEC 27002:2013, articolele 5-18.

Astfel, au fost stabilite şi documentate Politica şi obiectivele în domeniul securităţii informaţiei, cadrul organizatoric pentru iniţierea, controlul implementării şi administrării securităţii informaţiei, cerinţele privind securitatea resurselor umane, identificarea, clasificarea şi controlul resurselor informaţionale care urmează să fie protejate, controlul accesului la aceste resurse, implementarea cerinţelor de securitate fizică şi a mediului de lucru, asigurarea operării corecte şi în condiţii de securitate a sistemelor de comunicare şi de procesare a informaţiei.

Cerinţele de securitate sunt luate în consideraţie în relaţiile cu clienţii, furnizorii şi alte părţi interesate la proiectarea de noi servicii şi planificarea realizării acestora, la procurarea noilor sisteme de comunicare şi de procesare a informaţiei, la angajare, în timpul activităţii şi la concedierea personalului, etc. Politica de securitate a informaţiei, adoptată la cel mai înalt nivel, face apel către toţi angajaţii să raporteze orice incident de securitate în vederea unei intervenţii prompte şi eficace. Situaţiile de urgenţă care pot afecta securitatea informaţiei sunt gestionate prin aplicarea unei proceduri interne, care include activităţi de pregătire pentru asemenea situaţii şi asigurare a capacităţii de răspuns în cazul declanşării lor.

La toate etapele de implementare a SMSI au fost organizate seminare de instruire privind cerinţele standardului ISO/IEC 27001:2013, prevederile legislaţiei şi documentele interne referitoare la securitatea informaţiei. Paşii întreprinşi pentru implementarea SMSI în cadrul organizaţiei sunt descrişi mai detaliat în [13].

Un sistem de management bazat pe bunele practici internaţionale, completat cu metode tehnice de protecţie a informaţiei, asigură avantaje esenţiale organizaţiei, şi anume:

- creează o metodă optimă de rezolvare a problemelor de securitate a informaţiei în baza unor reguli standardizate;
- sporeşte încrederea partenerilor în capacitatea organizaţiei de a proteja informaţia proprie şi informaţia partenerilor;
- reduce riscul pierderilor din cauza incidentelor de securitate;
- asigură conştientizarea importanţei problematicii de securitate a informaţiei in cadrul unei organizaţii.
- susţine dezvoltarea celor mai bune practici în cadrul unei organizaţii şi consolidează continuitatea afacerii.

Pentru grupul managerial al organizaţiei, abordarea sistemică în domeniul securităţii informaţiei este importantă datorită:

- informării asupra riscurilor rezultate din utilizarea informaţiei în procesele de furnizare a serviciilor pentru a putea să determine relevanţa şi nivelul critic al acesteia în conformitate cu cerinţele afacerii;
- posibilităţii de a decide în cunoştinţă de cauză cum trebuie să controleze riscurile prin planificarea, implementarea şi monitorizarea masurilor luate pentru a evita, reduce, transfera sau a-şi asuma riscurile şi pentru a fi capabil să administreze incidentele posibile.

6. Concluzii

Organizaţiile, îndeosebi cele cu activităţi de cercetare şi dezvoltare, sunt preocupate de protejarea propriei informaţii, a informaţiei pe care le-o încredinţează partenerii. Prin urmare, este necesară o abordare sistemică în domeniul securităţii informaţiei, care include metode tehnice şi organizatorice, cunoaşterea şi respectarea cerinţelor legale şi de reglementare în acest domeniu. Ţinând cont de faptul că Organizaţia Internaţională de Standardizare ISO, prin analiza, sistematizarea şi generalizarea bunelor practici acumulate în domeniul securităţii informaţiei, ne oferă tehnici care au fost testate pe parcursul anilor, este oportună adaptarea cerinţelor standardelor ISO la cele mai diverse domenii de activitate în care protecţia resurselor informaţionale este de importanţă critică. Argumentele expuse mai sus au stat la baza implementării şi certificării SMSI în cadrul Institutului de Dezvoltare a Societăţii Informaţionale.

Prin implementarea Sistemului de Management al Securităţii Informaţiei, IDSI a rezolvat concomitent două probleme:

- a instituit şi a certificat un Sistem de securitate a informaţiei, asigurându-şi anumite avantaje concurenţiale în domeniul de activitate şi un nivel mai înalt de încredere din partea partenerilor;
- a completat baza de date a cunoştinţelor tehnice şi organizatorice deţinute de orgaizaţie cu un nou domeniu – proiectarea, implementarea, auditul şi îmbunătăţirea continuă a unui SMSI.

Certificarea SMSI de către un organism acreditat la nivel internaţional, rezultatele auditurilor de supraveghere sunt o dovadă a implementării corecte şi a menţinerii acestui sistem.

Referinţe.

1. http://anrceti.md/files/filefield/Raport%20ev.pieteiCE%202Q_2016.pdf. Vizitat la 18.12.2016.
2.https://www.google.com/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=MALWARE+%E2%80%93A+BILLION+DOLLAR+BUSINESS%2C+Liviu+ARSENE.+Senior+e-Threat+Analyst+Bitdefender. Vizitat la 18.12.2016.
3. http://www.itsecurity.com/features/the-top-5-internal-security-threats-041207/ Vizitat la 18.12.2016.
4. Hotărârea nr. 811 din 29.10.2015 cu privire la Programul naţional de securitate cibernetică a Republicii Moldova pentru anii 2016-2020. Publicat:13.11.2015 în Monitorul Oficial, nr. 306-310 art nr: 905.
5. http://www.procuratura.md/md/com/1211/1/6717/. Vizitat la 18.12.2016.
6.http://www.realitatea.md/sis--12-institutii-de-stat-din-republica-moldova--tinta-unor-atacuri-cibernetice-din-exteriorul-tarii_34218.html. Vizitat la 18.12.2016.
7. http://www.cotidianul.ro/41000-de-tentative-de-atac-cibernetic-asupra-comisiei-electorale-centrale-de-la-chisinau-290604/. Vizitat la 18.12.2016.
8.https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561. Vizitat la 18.12.2016.
9.Legea nr. 6 din 02.02.2009 pentru ratificarea Convenţiei Consiliului Europei privind criminalitatea informatică. Publicat: 20.02.2009 în Monitorul Oficial, nr. 37-40, art nr: 104.
10.Lege nr.20-XVI din 3 februarie 2009 privind prevenirea şi combaterea criminalităţii informatice. Publicat: 26.01.2010 în Monitorul Oficial, nr. 11-12, art nr. 17.
11.http://cert.gov.md/desprecsc/activitatea.html. Vizitat la 18.12.2016.
12. http://papers.duckdns.org/files/2011_IECON_stuxnet.pdf. Vizitat la 18.12.2016.
13. GUZUN, Mihail, COJOCARU, Igor, IONESCU, Răzvan. Management Issues of Information Security. In: Proceedings of the 5th International Conference "Telecommunications, Electronics and Informatics". May 20-23, 2015, Chişinău, Moldova. Chişinău: Ed. Tehnica–UTM, 2015, pp. 343-346. ISBN 978-9975-45-377-6.

Articolul este depozitat în baza de date IBN:
https://ibn.idsi.md/ro/vizualizare_numar_revista/26/2138
Primit la redacţie: 15.03.2017