Contracararea riscurilor și amenințărilor la adresa securității cibernetice a Republicii Moldova

Ghenadie SAFONOV
Academia Militară a Forțelor Armate „Alexandru cel Bun”
gsafonov@gmail.com

Abstract **- Dezvoltarea societății presupune necesitatea edificării societății informaționale și dezvoltării rapide a tehnologiilor moderne de informații şi comunicații, fapt care la rândul său are un impact major asupra mediului social, provoc?nd schimbări esențiale ale cadrului cultural, economic și politic, dar şi asupra vieții de zi cu zi a individului. Astfel accesul liber la tehnologia informației şi comunicațiilor reprezintă una dintre condițiile unei bune funcționări a societății moderne.**

Spațiul cibernetic se caracterizează prin anonimat, dinamism şi lipsa frontierelor. Acest fapt generează atât oportunități de dezvoltare a societății informaționale, cât și riscuri la adresa funcționării acesteia la nivel individual, statal şi interstatal.

Asigurarea securității spațiului cibernetic devine o preocupare majoră a tuturor actorilor implicați, mai ales la nivel instituțional, unde se concentrează responsabilitatea elaborării şi aplicării de politici coerente în domeniu, cea ce prevede necesitatea dezvoltării culturii de securitate cibernetică a utilizatorilor sistemelor informatice şi de comunicații, adesea insuficient informați în legătură cu potențialele riscuri, dar şi cu soluțiile de contracarare a acestora. În consecință una din premizele dezvoltării unei societăți sigure, sănătoase și puternice în Republica Moldova este contracararea riscurilor și amenințărilor la adresa securității cibernetice a republicii.

Cuvinte cheie **- amenințări cibernetice, atacuri cibernetice, contracarare, securitate cibernetică, spațiul cibernetic.**

I. INTRODUCERE

În mai puțin de o generație, revoluția informației şi introducerea calculatoarelor în toate sferele vieții au generat multiple schimbări în societatea contemporană. Lumea se transformă treptat într-un sat global, unde nu mai există hotare pentru afaceri, comunicații sau comerț.

Implementarea activă şi multilaterală a tehnologiilor informaționale a determinat transformarea structurii societății mondiale, conducând treptat spre dispariția frontierelor naționale. În toate domeniile de activitate au apărut noi structuri funcționale, la baza cărora se află rețeaua.

La etapa actuală dezvoltarea societății presupune drept condiție strict necesară a edificării societății informaționale și dezvoltarea rapidă a tehnologiilor moderne de informații şi comunicații, fapt care la rândul său are un impact major asupra mediului social, provocînd schimbări esențiale ale cadrului cultural, economic și politic, dar şi asupra vieții de zi cu zi a individului. Astfel accesul liber la tehnologia informației şi comunicațiilor reprezintă una dintre condițiile unei bune funcționări a societății moderne.

Spațiul cibernetic se caracterizează prin anonimat, dinamism şi lipsa frontierelor. Acest fapt generează atât oportunități de dezvoltare a societății informaționale, cât și riscuri la adresa funcționării acesteia la toate nivelele (individual, statal şi interstatal).

Societatea informațională este o formă nouă a civilizației umane, mult mai perfectă, în care accesul egal şi universal la informație, în corelație cu o infrastructură informațională şi de comunicații dezvoltată, contribuie la o dezvoltare social-economică durabilă, reducerea gradului de sărăcie, îmbunătățirea calității vieții, la integrarea în Uniunea Europeană [1].

Creşterea informatizării societății duce la sporirea vulnerabilității acesteia. În consecință sigurarea securității spațiului cibernetic devine o preocupare majoră a tuturor actorilor implicați, mai ales la nivel instituțional, unde se concentrează responsabilitatea elaborării şi aplicării de politici coerente în domeniu. Astfel este evidentă necesitatea dezvoltării culturii de securitate cibernetică a utilizatorilor sistemelor informatice şi de comunicații, adesea insuficient informați în legătură cu potențialele riscuri, dar şi cu soluțiile de contracarare a acestora.

Cunoaşterea pe scară largă a riscurilor şi amenințărilor la adresa securității cibernetice, precum şi modului de prevenire şi contracarare a acestora necesită o comunicare şi cooperare eficiente între actorii specifici în acest domeniu.

Statul este cel care trebuie să-şi asume rolul de coordonator al activităților desfăşurate la nivel național pentru asigurarea securității cibernetice, în concordanță cu demersurile inițiate la nivel internațional. Deoarece problematica securității cibernetice a devenit prioritară la nivel mondial, organismele internationale au stabilit cadrul de reglementare necesar dezvoltării mecanismelor de apărare cibernetic.

În spațiul informațional (cibernetic) global unic, s-a manifestat o confruntare geostrategică informațională între marile puteri, pentru atingerea superiorității în spațiul informațional mondial. Odată cu dezvoltarea şi sporirea complexității mijloacelor, metodelor şi formelor de automatizare a procesării informației creşte dependența societății de gradul de securitate a tehnologiilor informaționale utilizate, de care, uneori, depinde bunăstarea, iar uneori şi viețile multor oameni [13].

Spațiul cibernetic a devenit un nou mediu de ducere a războiului (al cincilea după uscat, mare, aer, spațiu). Este evident faptul că toate conflictele în viitor vor avea o componentă virtuală, fie în faza inițială a conflictului, fie sub formă de agresiune în sensul direct al cuvântului, fără desfășurarea altor forme de luptă.

?n absența unor acorduri internaționale și a nedoriței de a conveni asupra normelor generale de interpretare a problemei, actorii cu intenții agresive posedă agilitate și flexibilitate în dezvoltarea și punerea în aplicare a potențialilor atacuri cibernetice. Acest potențial fiind suficient pentru a fi categorisit drept armă. Iar odată ce există o armă, se va găsi și un război unde arma respectivă poate fi aplicată.

Astfel una din premizele dezvoltării unei societăți sigure, sănătoase și puternice în Republica Moldova este contracararea riscurilor și amenințărilor la adresa securității cibernetice a republicii.

II. RISCURILE ȘI AMENINȚĂRILE LA ADRESA SECURITĂȚII CIBERNETICE ÎN LUMEA CONTEMPORANĂ

?n anul 2013 s-au realizat modificări semnificative și s-au obținut succese remarcabile în domeniul securității cibernetice. Printre evoluțiile dinamice și schimbările care au avut loc, există un lucru care a rămas stabil: cursa dintre apărătorii și adversari securității cibernetice a continuat și acest proces va continua în viitor. Conform ENISA pe parcursul anului 2013 au avut loc evoluții atât bune, cât și mai puțin bune. Printre cele mai puțin bune se numără:

– agenții de amenințare au crescut nivelul de sofisticare al atacurilor și instrumentelor utilizate;

– a devenit clar că maturitatea în activitățile cibernetice nu este o chestiune de o mână de națiuni membre. Mai degrabă, mai multe state naționale au dezvoltat capacități, care pot fi utilizate pentru a se infiltra în toate tipurile de obiective atât guvernamentale, c?t și private, cu scop de a atinge obiectivele lor;

– amenințările cibernetice au devenit mobile: modelele de atac și instrumente pentru atacarea calculatoarelor vizate în urmă cu câțiva ani, au migrat în ecosistemul mobil;

– au apărut două noi câmpuri de luptă digitale: bazele de date mari și Internetul Obiectelor.

Iar printre cele bune se numără:

– realizarea succeselor impresionante ?n aplicarea legii;

– creșterea numărului de rapoarte și date cu privire la amenințările cibernetice, astfel asigurându-se calitatea informațiilor disponibile. Fapt care a facilitat analiza amenințărilor;

– vânzătorii de produse în domeniul securității cibernetice au crescut viteza de răspuns la amenințări și vulnerabilități prin actualizări ale produselor lor;

– a fost preconizată cooperarea între organizațiile relevante privind evaluarea și protecția de la amenințările cibernetice, urmând a lua amploare în viitorul apropiat [4].

Organismele internaționale specializate ?n securitatea cibernetică realizează analiza amenințărilor cibernetice și elaborează rapoarte anuale. Astfel concluzion?nd datele acestor rapoarte pentru anii 2013 și 2014, în ordinea de importanță, se poate menționa:

1. Perspectiva utilizatorului final trebuie să fie luată serios în considerare de către comunitatea de securitate cibernetică. Este necesar ca utilizatorii finali să se implice mai activ în protecția împotriva amenințărilor cibernetice. Analiza arată, că cunoștințele despre punerea în aplicare a unor măsuri simple de securitate nu este cunoscută de marea parte a utilizatorilor finali. Adoptarea unor măsuri simple de securitate de către utilizatorii finali ar micșora în jumătate din numărul de incidente cibernetice la nivel mondial;

2. Este clar că este necesară o coordonare mai bună în ce privește colectarea, analiza, evaluarea și validarea informațiilor între organizațiile implicate. Numeroase organizații publice și private lucrează asupra problemelor, care se suprapun, de colectare a informațiilor privind amenințările și de analiză a amenințărilor. Coordonarea crescândă, de exemplu, dintre cei care lucrează cu informații open source și cei care lucrează cu datele operaționale ar putea duce la creșterea calității și vitezei de evaluare a amenințărilor. Mai mult decât atât, activitățile statelor și ale părților interesate din sectorul privat vor fi, de asemenea luate în considerare. Obiectivul este de a evalua fezabilitatea unui astfel de coordonare/cooperare și să se stabilească zonele adecvate și pașii pentru a o obține;

3. Amenințările trebuie să fie extinse cu informații suplimentare cu privire la fluxul de lucru/întreruperea lanțugului de atac și modele de atac. Aceste informații trebuie să fie extrase din analiza incidentelor, stabilindu-se astfel feedback-ul necesar pentru a îmbunătăți calitatea evaluării amenințărilor. Acest lucru va fi de reală valoare adăugată pentru toate părțile interesate, folosind o imagine a amenințării, astfel ca orice descriere a amenințării să conțină informații cu privire la scenariile de atac derivate din incidente reale;

4. Setarea cercetărilor în domeniul amenințărilor cibernetice rămâne una dintre principalele provocări ale comunității de securitate cibernetică și presupune modalități de facilitare a colectării de informații, dezvoltarea de instrumente pentru sprijinul analizei, schimbului de informații, etc. privind amenințările;

5. Experții în securitate au subliniat importanța creșterii vitezei în evaluare a amenințărilor și diseminare prin reducerea ciclurilor de detectare și de evaluare. În

scopul de a realiza acest lucru, părțile interesate trebuie să sinergizeze și sincronizeze activitățile lor;

6. Creșterea sofisticării atacurilor, creșterea complexității arhitecturi tehnologiilor informaționale, creșterea volumului de date și a limitelor neclare ale perimetrului de securitate reprezintă provocări importante pentru apărarea securității cibernetice. Comunitatea de cercetare trebuie să examineze flexibilitatea măsurilor de securitate: în afară de măsuri active (de exemplu firewall-uri, IDS), trebuie să fie dezvoltate mecanisme de securitate pasive (de exemplu generarea automată de politici, validare și aplicare). Infrastructurile de tehnologii informaționale trebuie să fie rezistente și robuste la atacurile de succes, fără a suferi un impact sever în ceea ce privește disponibilitatea, integritatea și confidențialitatea.

III. RISCURILE ȘI AMENINȚĂRILE LA ADRESA SECURITĂȚII CIBERNETICE A REPUBLICII MOLDOVA

Republica Moldova a realizat progrese importante în implementarea tehnologiilor societății informaționale, cota contribuției sectorului tehnologiilor informatice și comunicațiilor la Produsul Intern Brut practic a atins în ultimii ani nivelul de circa 8-10%. Fiecare al doilea cetățean este utilizator de Internet, mai mult de jumătate din gospodării au cel puțin un calculator, majoritatea gospodăriilor conectate au acces la Internet de bandă largă, țara fiind plasată după viteza de acces la Internet printre primele 20 în lume, este implementat pașaportul biometric, buletinul de identitate cu semnătura electronică, sistemul e-Declarații, harta digitală, țara a aderat la inițiativa „Date Guvernamentale Deschise", este în desfășurare proiectul ,,e-Transformare" a Guvernării, etc. Cu toate acestea, în clasificările internaționale țara nu se află printre economiile avansate în acest domeniu, iar nivelul și viteza de dezvoltare a societății informaționale nu corespund cerințelor mediului internațional actual, în care lumea devine tot mai ,,hiperconectată" și mai digitizată [2].

Reieșind din datele sumative privind dezvoltarea tehnologiilor informaționale și de comunicații Republica Moldova ?n anul 2013 a stat foarte bine la capitolul implementării serviciilor on-line a Guvernului, acest fapt fiind asigurat de către promovarea intensivă de către Guvern a tehnologiilor informaționale și de comunicații. Drept consecință la capitolul impactul social, utilizarea de către populație a serviciilor electronice este cea mai bună. ?n anul 2014, la acest capitol Republica Moldova s-a plasat pe poziția 61 din 148 [8].

?n anul 2014, conform, World Economic Forum, The Global Information Technology Report 2014, Rewards and Risks of Big Data, Republica Moldova s-a plasat pe poziția 1 la capitolul Accesibilitate și anumela poziția ce ține de competiția internet&telefonie.

Pe de altă parte, Republica Moldova stă foarte prost la capitolul Mediul politic și de reglementare și anume la pozițiile ce țin de funcționarea și eficacitatea sistemului judiciar și legal. Deasemenea este deplorabilă situația cu referire la utilizarea software-lui piratat, în republică fiind piratate 90% din produsele software instalate.

Reieșind din datele Kaspersky Security Bulletin 2013 Republica Moldova după nivelul de risc la navigarea pe Internet se află în grupul țărilor cu nivel ridicat de infectare pe parcursul anului 2013, atingând nivelul de 47,20% utilizatori unici atacați. Din acest grup fac parte preponderent țările din foste republici sovietice și țările din Asia. Iar în funcție de nivelul de risc al infectării locale a calculatoarelor utilizatorilor prin intermediul memoriilor flash USB, aparatelor de fotografiat și carduri de memorie pentru telefon, hard disk-uri externe, etc. Republica Moldova se află în grupul țărilor cu nivel scăzut de infectare (14 – 24% de utilizatori unici infectați).

În Republica Moldova, în afară de sisteme de infrastructuri critice deținute de către instituțiile statului există și astfel de sisteme deținute de către companiile private. Acești proprietari nu sunt doar întreprinderi mari, dar și întreprinderile mici și mijlocii. Nu sunt suficiente doar măsuri speciale de protecție pentru a preveni atacurile cibernetice moderne asupra infrastructurilor critice ale întreprinderilor. Pentru a preveni astfel de amenințări, este necesar să se implementeze soluții complete pentru protecția rețelelor, care includ soluții de asigurare a securității, soluții de stocare și efectuare a procedurii backup a datelor, precum și procesul de identificare a utilizatorilor și a sistemelor de control al accesului la rețea. La măsurile de securitate trebuie să includem treninguri cu privire la securitate, măsuri privind identificarea riscului asociat vulnerabilității de sistem și de proces al infrastructurilor critice, pericolelor și amenințărilor în adresa acestora, analiză și evaluarea de risc.

Rezultatele unui studiu internațional privind protejarea infrastructurilor critice, denotă că aproximativ 53% din rețelele furnizorilor infrastructurii critice, au fost atacați din motive politice.

Bunăoară, pe parcursul anului 2007 Centrul de Telecomunicații Speciale a identificat un număr mare de atacuri și tentative de atac asupra sistemelor informaționale ale instituțiilor de stat. Printre metodele de atac utilizate se numără Cross-SiteScripting (XSS), Distributed Denial of Service (DDoS), etc.

TABELUL I. PROCENTAJUL ATACURILOR ASUPRA INSTITUȚIILOR DE STAT

Domenul	% de atacuri suportate
border.gov.md	**54 %**
gov.md	**35 %**
cts.md	**4 %**
maia.gov.md	**2 %**
sis.md	**2 %**
moldova.md	**2 %**

În timpul manifestațiilor din aprilie 2009, deasemenea, au fost raportate o serie de atacuri asupra resurselor web ale guvernului, organizațiilor politice. În ultimii ani de către Centrul de Telecomunicații Speciale au fost anunțate o serie de tentative de penetrare a

sistemelor de securitate cibernetică ale instituțiilor de stat.

De exemplu, numai în perioada 17 mai – 21 octombrie 2012, din numărul total de mesaje electronice adresate autorităților publice 986 000 au fost mesaje legitime, pe când majoritatea de aproximativ 8 milioane de mesaje conțineau spam, în conținutul cărora au fost detectate 874 programe malițioase.

Astfel, ?ncep?nd cu 2008, conform datelor Laboratoarelor Kaspersky, instituțiile Republicii Moldova au fost ținta produsului malițios Red October.

Red October este o campanie de spionaj cibernetic care a afectat sute de victime în toată lumea, inclusiv agenții diplomatice și guvernamentale, instituții de cercetare, energetice și nucleare și organizații comerciale și aerospațiale. În Republica Moldova bunăoară, țintele Red October au fost instituțiile guvernamentale, agențiile diplomatice și ambasadele, precum și resursele informaționale ale ministerelor de forță.

Red October este un produs malițios extrem de sofisticat. Printre altele, acesta include un „mod de înviere", care permite acestuia să re-infecteze calculatoarele. Codul este extrem de modular, care permite atacatorilor ușor a optimiza codul de pentru fiecare țintă în parte.

Red October nu numai recolta informații de pe terminalele tradiționale, dar, de asemenea, de pe dispozitivele mobile conectate la rețelele victimelor. Ceea ce este o recunoaștere clară de către infractorii cibernetici că dispozitivele mobile sunt o componentă de bază a mediului de afaceri de azi și conțin informații valoroase.

În luna martie 2013 un val de atacuri a vizat politicieni și activiști pentru drepturile omului în țările CSI (inclusiv Republica Moldova) și Europa de Est. Atacatorii au folosit instrumentul de administrare de la distanță TeamViewer pentru a controla computerele victimelor lor, astfel încât operațiunea a devenit cunoscută sub numele de „TeamSpy". Scopul atacurilor a fost colectarea informațiilor de la computere compromise. Deși nu la fel de sofisticat ca Red October, NetTraveler și alte campanii, aceasta campanie a fost, totuși, de succes, care indică faptul că nu toate codurile atacurilor orientate de succes necesită a fi construite de la zero.

Deci putem afirma că Republica Moldova în ziua de azi este foarte vulnerabilă la riscurile și amenințările la adresa securității cibernetice, ceea ce necesită o atenție sporită din partea statului. Statul fiind cel care trebuie să-și asume rolul de coordonator al activităților desfășurate la nivel național pentru asigurarea securității cibernetice, în concordanță cu demersurile inițiate la nivel internațional.

IV. CONTRACARAREA RISCURILOR ȘI AMENINȚĂRILOR LA ADRESA SECURITĂȚII CIBERNETICE A REPUBLICII MOLDOVA

Obiectivul tehnologiilor de securitate a informației constă în „protejarea intereselor" celor care se bazează pe informații, sistemele şi comunicațiile care livrează aceste informații împotriva daunelor care pot rezulta din incapacitatea de a se asigura disponibilitatea, confidențialitatea şi integritatea informațiilor.

Scopurile securității informaționale trebuie să fie stabilite pe baza priorităților constante ale securității naționale ce corespund sarcinilor de lungă durată ale dezvoltării mediului informațional al societății, incluzând:

- apărarea intereselor naționale ale statului în condițiile globalizării proceselor informaționale şi formării rețelelor informaționale globale;
- asigurarea organelor puterii şi conducerii de stat, persoanelor fizice şi juridice cu informație veridică, completă şi oportună, necesară pentru luarea deciziilor;
- prevenirea încălcării integrității resurselor informaționale de stat, utilizării lor nelegitime şi ineficiente;
- realizarea drepturilor cetățenilor, organizațiilor şi statului în vederea obținerii, difuzării şi utilizării informației;
- susținerea normelor democratice, în special a principiilor de interacțiune a statului, societății şi persoanei în mediul informațional, în calitate de agenți realmente egali ai relațiilor democratice;
- protecția informațională a cetățenilor.

De asemenea, spațiul cibernetic este în continuă creştere şi dezvoltare, însă odată cu evoluarea acestuia evoluează şi pericolele. O preocupare majoră trebuie să fie contracararea atacurilor cibernetice organizate, capabile să cauzeze o destabilizare critică a infrastructurii naționale, a economiei sau a securității naționale. Se ştie că instrumentele şi metodele de realizare a atacurilor sânt larg răspândite, iar capacitățile tehnice şi numărul utilizatorilor capabili de provocarea unui adevărat dezastru este în creştere.

Atacurile cibernetice asupra rețelelor informaționale ale oricărei țări pot avea consecințe grave, cum ar fi întreruperea funcționării unor componente-cheie, provocarea pierderilor de venituri şi proprietăți intelectuale sau chiar pierderea vieților omenești. Contracararea unor astfel de atacuri necesită crearea unor componente riguroase, cum încă nu există în prezent, dacă se dorește reducerea vulnerabilităților şi prevenirea sau diminuarea forței capacităților îndreptate împotriva infrastructurilor critice.

La etapa actuală de dezvoltare a sistemelor informaționale, odată cu creşterea cantității de informații vehiculate prin rețelele informaționale, evoluția rapidă a tehnologiilor, şi sporirea numărului de specialişti în domeniul tehnologiilor informaționale precum şi accesibilitatea echipamentelor performante metodele tradiționale de protecție a informațiilor nu mai sunt eficiente. De aceea în ultimii ani se observă o creştere considerabilă a investițiilor în securitatea cibernetică. Acest lucru se datorează nu numai sporirii numărului de atacuri cibernetice asupra instituțiilor, organizațiilor, companiilor atât civile, cât şi celor din sectorul de apărare, dar şi sporirii considerabile a „calității"

atacurilor şi pagubelor materiale şi morale cauzate de către acestea.

Deoarece Republica Moldova este încă la etapa de dezvoltare a unei societăţi electronice avansate infrastructurile critice sunt mai mult sau mai puţin automatizate. Astfel riscurile şi ameninţările la adresa securităţii cibernetice ale acestor infrastructuri pot fi în stare a le afecta funcţionalitatea cu nivele de gravitate diferite, funcţie de nivelul implementării tehnologiilor informaţionale.

Astfel goana după digitizarea serviciilor publice, automatizarea proceselor şi informatizarea Republicii Moldova, fără o atenţie cuvenită apărării cibernetice, duce în cele din urmă la expunerea considerabilă a societăţii informaţionale vulnerabilităţilor şi ameninţărilor cibernetice.

Astăzi sectorul public al Republicii Moldova este dependent de spaţiul cibernetic prin:

- Semnătura digitală;
- MCloud (infrastructura Cloud Computing);
- Mpass (platforma ca serviciu);
- Mpay (sistem de plăţi electronice);
- Guvern fără hârtie;
- Platforma de registre;
- Portaluri de date guvernamentale (servicii, date) etc.

Conform statisticilor pentru anul 2013 şi 2014 marea parte a atacurilor automate au fost lansate din reţelele furnizorilor de servicii tip Cloud, deci odată cu dezvoltarea în Republica Moldova a reţelelor de acest tip (fapt deja constatat) fără atragerea unei atenţii sporite problemelor securităţii acestora infrastructura Cloud Computing poate deveni o sursă pentru atacuri orientate în mâinile peroanelor rău intenţionate.

Totodată accesul în masă la Internetul de bandă largă, utilizarea omniprezentă a reţelelor virtuale de socializare, a mijloacelor mobile de bandă largă şi accesibilitatea conţinutului digital împreună cu lipsa culturii de securitate cibernetică şi utilizarea preponderent a softului piratat (90% din softul instalat) face Republica Moldova o sursă ideală pentru crearea reţelelor botnet [7].

Importanţa deosebită acordată circuitului liber şi protejat al informaţiilor determină necesitatea elaborării în Republica Moldova a unei Strategii Naţionale de Securizare a Spaţiului Cibernetic. În strategie este de a se stabili cinci priorităţi naţionale pentru realizarea scopului propus:

- un sistem de răspuns în caz de perturbare a traficului informaţiilor;
- un program naţional de reducere a vulnerabilităţilor şi ameninţărilor în acest spaţiu;
- un program naţional de pregătire în domeniul protecţiei spaţiului cibernetic;
- securizarea comunicaţiilor guvernamentale;
- cooperarea internaţională în domeniul protejării spaţiului cibernetic.

În anii care vor urma, importanţa spaţiului cibernetic va determina conştientizarea protecţiei lui nu numai de către guverne, dar şi de către firme private şi persoane particulare. Aceasta va conduce la asocierea utilizatorilor în scopul reducerii vulnerabilităţilor combaterii şi eradicării ameninţărilor îndreptate împotriva spaţiului cibernetic. Şi statul în acest efort trebuie să joace rolul cel mai important. Astfel o viziune puternică a statului în dezvoltarea tehnologiilor informaţionale şi a comunicaţiilor ca una dintre domeniile critice pentru economia locală, care continuă a produce efecte bune, atât din punct de vedere economic şi social, cât şi în domeniile unde ţara înregistrează cele mai remarcabile succese de pe glob. Deci Republica Moldova necesită să dezvolte o infrastructură puternică a tehnologiilor informaţionale şi a comunicaţiilor şi să încurajeze o asimilare puternică de către cetăţeni, întreprinderi şi nu în ultimul rând de către Guvern prin extinderea ofertelor sale de servicii on-line. Mergând mai departe, ţara ar putea beneficia mai mult de consolidare a sistemului de inovare, care, la moment, suferă de o serie de deficienţe ce limitează capacitatea de inovare a sectorului privat şi de a beneficia, astfel, de întregul potenţial pe care tehnologiile informaţionale şi a comunicaţiilor îl pot oferi.

Din punctul meu de vedere securitatea cibernetică a Republicii Moldova este lezată de următorii factori importanţi:

- cultura de securitate cibernetică în Moldova nu există. Totul se realizează fragmentar, fără a se asigura o continuitate a măsurilor întreprinse;
- lipsa unei strategii naţionale de dezvoltare a tehnologiilor informaţionale şi securizare a spaţiului cibernetic;
- structurile abilitate în securitatea cibernetică existent reacţionează la ameninţări activ, pe când mult mai eficiente sunt activităţile proactive;
- structuri rudimentare abilitate în managementul crizei şi protecţia infrastructurii critice;
- lipsa bazei legislative adecvate care ar permite executarea (forţarea) legilor cu privire la securitatea cibernetică;
- formularea ?n termeni generali şi vagi a legislaţiei ?n domeniul tehnologiilor informaţionale;
- lipsa unui sistem educaţional în domeniul securităţii informaţionale bine pus la punct.

Contracararea riscurilor şi ameninţărilor la adresa securităţii cibernetice rezidă în soluţionarea factorilor expuşi anterior.

V. CONCLUZII

Ameninţările cibernetice au devenit un lucru obişnuit în societatea noastră. Ele devin tot mai frecvente, mai diverse şi mai complexe reieşind din metodele tehnologice aplicate. Ignorarea lor a devenit imposibilă, deoarece informaţiile au devenit un beneficiu absolut şi vital, iar confruntarea ?n spaţiul cibernetic duce la pagube economice şi fizice considerabile.

Pentru contracararea cu succes a ameninţărilor cibernetice este necesar a se concentra asupra următoarelor:

- stabilirea unui cadru conceptual, instituţional (crearea sistemului naţional de securitate cibernetică, elaborarea legislaţiei, dezvoltarea parteneriatului);

– elaborarea programului național de dezvoltare a potențialului cibernetic (capacităților de prevenire, detectare și contracarare a atacurilor cibernetice, crearea unor structuri specializate, ridicarea nivelului de protecție, dezvoltarea producției produselor de profil);

– consolidarea culturii de securitate informațională (informarea populației, instruirea adecvată a managerilor și a personalului tehnic);

– perfecționarea cooperării internaționale (la nivel de acte normative, schimburi de experiență, de protecție colectivă împotriva atacurilor de amploare).

BIBLIOGRAFIE

[1] Strategia Națională de edificare a societății informaționale „Moldova electronica". Hotărârea Guvernului Republicii Moldova nr.255 din 09.03.2005;

[2] Strategia națională de dezvoltare a societății informaționale ,,MOLDOVA DIGITALĂ 2020", proiect, 36 p.;

[3] M. Drăgănescu, Societatea informațională şi a cunoaşterii. Vectorii societății cunoaşterii, Bucureşti, Academia Română, 95 p.;

[3] И. Завальский, Кибервойна: угрозы и защита, Сборник докладов 7-го симпозиума по вопросам безопасности Черноморского и Каспийского регионов, Одесса, 2012;

[4] ENISA Threat Landscape 2013, Overview of current and emerging cyber-threats, 11 December 2013, 70 p.;

[5] Kaspersky Security Bulletin 2013, 54 p.;

[6] Internet Security Threat Report 2014, Volume 19, Symantec Corporation, 24 p.;

[7] World Economic Forum, The Global Information Technology Report 2013, 409 p.;

[8] World Economic Forum, The Global Information Technology Report 2014, Rewards and Risks of Big Data, 343 p.;

[9] 2013-2014 DDoS Threat Landscape Report, Incapsula, 12 p.;

[10] TrendLabs 1Q 2013 Security Roundup, Zero-Days Hit Users Hard at the Start of the Year, 19 p.;

[11] TrendLabs 1Q 2014 Security Roundup, Cybercrime Hits the Unexpected, 36p;

[12] TrendLabs 2Q 2014 Security Roundup, Turning the Tables on Cyber Attacks, 33p.;

[13] Securitatea informațională în contextul procesului de globalizare, accesat pe http://biblioteca-digitala-online.blogspot.com la data de 04 martie 2014, ora 21.22.;

[14] Cisco 2014. Annual Security Report, 80p.;

[15] Sophos. Security Threat Report 2014, 30p.