Dezvoltarea cooperării internaţionale în domeniul securităţii informaţionale

Autor: Tatiana Busuncian
Dr., conferențiar universitar

Chișinău 2023

Conținuturi; Obiective de referință; termeni-cheie

Conținuturi:

1.Dezvoltarea cooperării internaționale în domeniul securității informaționale;
2.Principalele direcții de colaborare în domeniul securității informaționale;
3.Asigurarea securității informaționale, inclusiv în Republica Moldova.

Obiective de referință:

-să identifice căile de colaborare internațională a instituțiilor responsabile de securitatea informațională în domeniul prevenirii și combaterii terorismului și criminalității transfrontaliere;
- să analizeze principalele direcții de colaborare în acest domeniu.
-să inițieze negocierilor privind semnarea acordurilor de cooperare la nivel internațional pentru îmbunătățirea capacității de răspuns în cazul unor atacuri cibernetice majore;
- să determine interesele naționale de securitate informațională în formatele de cooperare internaţională la care Republica Moldova este parte;
- să evalueze activitatea la programe internaţionale care vizează domeniul securităţii informaționale.

Termeni-cheie: *Cooperare, direcții de colaborare, acorduri de cooperare, interese naţionale*.

Începând cu anii 70 - perioada prezumtivă de apariție a criminalității informatice.

Criminalitatea informatică este orice infracțiune care poate fi comisă prin intermediul:

a). unui sistem informatic sau de rețea;

b). ca parte a unui sistem informatic sau de rețea;

c). sau împotriva unui sistem informatic sau de rețea.

ȚINTE

- organizaţiile internaţionale
- autoritățile înalte ale puterii executive și legislative
- instituțiile blocului economic
- universitățile anumitor state
- organizaţii sociale
- sistemul bancar
- Obiecte ale infrastructurii critice

CATEGORIILE SURSELOR CRIMINALITĂȚII INFORMAȚIONALE

Hackerii. Persoanele cu un nivel ridicat de cunoștințe în domeniul tehnologiilor informaţionale și care petrec mult timp la calculator în căutarea vulnerabilităților sistemelor informatice

Hacktiviştii. Termenul «hacktivism» provine dintr-un compus din două cuvinte «hack» și «activism» și este folosit pentru a se referi la noul fenomen de protest social, care este un fel de sinteză a activității sociale, are ca scop să protesteze împotriva la orice

Criminali cibernetici. Persoanele care exploatează rețele de calculatoare pentru profit ilegal

Persoanele implicate în spionaj industrial

Teroriştii

Se presupune că termenul *terorismul cibernetic* a apărut în vocabularul IT în anul 1997.

Agentul special FBI Mark Pollitt a definit acest tip de terorism ca “atacul premeditat, motivat politic impotriva informaţiei, sistemelor informatice, programelor informatice şi datelor, rezultând în violența împotriva țintelor noncombatante, de către grupări sub-nationale sau agenți clandestini".

- Terorismul cibernetic – influienţarea ilicită impotriva sistemelor informaţionale, în scopul de a amenința viața, sănătatea sau proprietățile persoanelor nespecificate prin crearea condițiilor pentru accidente și dezastre tecnogene sau amenințarea reală a unui astfel de pericol.

DEZVOLTAREA COOPERĂRII INTERNAȚIONALE IN DOMENIUL SECURITĂȚII INFORMAȚIONALE

- Societatea actuală este caracterizată de cunoaștere și continuă schimbare. Asistăm astăzi la o lume globală, complexă, dinamică, fapt determinat de mutaţiile ce au loc pe fondul procesului de globalizare și al dependenței informaționale.
- Evoluţia exponenţială a mediului informațional şi valenţele strategice dobândite de ţările dezvoltate au generat riscuri şi vulnerabilităţi, ce sunt sau pot fi exploatate de entităţi rău-voitoare în scopul săvârşirii de infracţiuni, acte de spionaj, ce pun în pericol atât indivizii, cât şi societatea.
- În acest context, provocările în domeniul securităţii informaționale sunt tot mai complexe și mai variate, fiecare stat având obligativitatea de a identifica şi dispune măsuri de dezvoltare a unor mecanisme eficiente de rezilienţă şi răspuns la ameninţările mediului virtual.

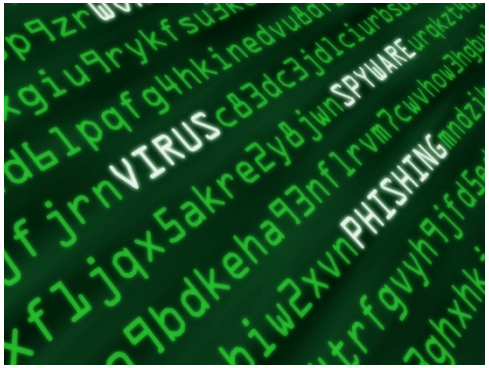
DEZVOLTAREA COOPERĂRII INTERNAȚIONALE IN DOMENIUL SECURITĂȚII INFORMAȚIONALE

În domeniul securităţii informaţionale se înscriu demersurile de creare a unui cadru legislativ şi instituţional corespunzător cerinţelor, cu impact asupra evoluţiilor pe termen mediu şi lung în plan naţional.

DEZVOLTAREA COOPERĂRII INTERNAȚIONALE IN DOMENIUL SECURITĂȚII INFORMAȚIONALE

Existenţa la nivelul fiecărui stat a unui cadru normativ în domeniul securităţii informaţionale este necesară, în condiţiile în care nivelul ameninţării la nivel internaţional este în continuă creştere. În evaluarea nivelului ameninţării informaţionale avem în vedere, pe de o parte, riscurile generate de interesul anumitor entităţi statale şi criminale de a compromite infrastructuri informaţionale/cibernetice şi, pe de altă parte, vulnerabilităţile sistemelor informatice, fie software, fie de natură umană (pe fondul precarităţii culturii de securitate cibernetică).

DEZVOLTAREA COOPERĂRII INTERNAȚIONALE IN DOMENIUL SECURITĂȚII INFORMAȚIONALE



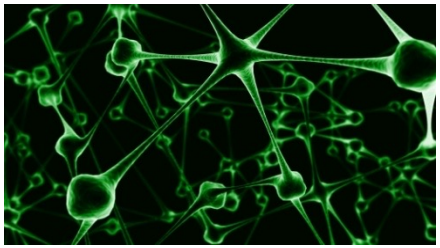
Opiniile pe marginea necesităţii unei legi în domeniul securităţii informaţionale variază, îmbrăcând nuanţe diverse, în tonalităţi diferite.

De exemplu, în registru negativ sunt relevante temerile că aplicarea unui astfel de act normativ ar fi de natură să încalce intimitatea personală şi că, în esenţă, ar conduce la o constrângere din partea autorităţilor competente, înţeleasă în termeni de limitare a exerciţiului unor drepturi şi libertăţi (mai exact limitarea dreptului la viaţă intimă, familială, la secretul corespondenţei, libertatea de exprimare).

DEZVOLTAREA COOPERĂRII INTERNAȚIONALE IN DOMENIUL SECURITĂȚII INFORMAȚIONALE

Calculatorul oricărei persoane fizice, care nu are un minimum de cunoștințe în domeniul securității informaționale/cibernetice, poate fi ținta unui atac sau poate fi folosit pentru un atac cibernetic, fără ca măcar să știe acest lucru.

Educarea societăţii civile în sensul creşterii culturii de securitate, dar şi creşterea încrederii între stat şi societatea civilă sunt puncte esenţiale de atins în obţinerea unui deziderat privind spaţiul cibernetic. În acest sens, modernizarea programelor de studii existente la nivelul învăţământului gimnazial, dar şi pregătirea personalului din administraţia publică şi formarea unor magistraţi cu competenţe în domeniul securităţii informaționale ar putea să soluţioneze câteva din problemele pe care le regăsim la nivelul societăţii civile.



CLASIFICAREA CRIMINALITĂȚII INFORMATICE

I. Clasificarea ONU

- Crime impotriva sistemelor informatice
- Crime comise pe sau prin intermediul calculatoarelor

Convenţia Consiliului Europei privind criminalitatea informatică clasifică criminalitatea informatică în felul următor:

- Crime impotriva sistemelor informatice
- Crime comise pe sau prin intermediul calculatoarelor
- Infracţiuni referitoare la conţinut
- Infracţiuni referitoare la atingerile aduse proprietătii intelectuale şi drepturilor conexe

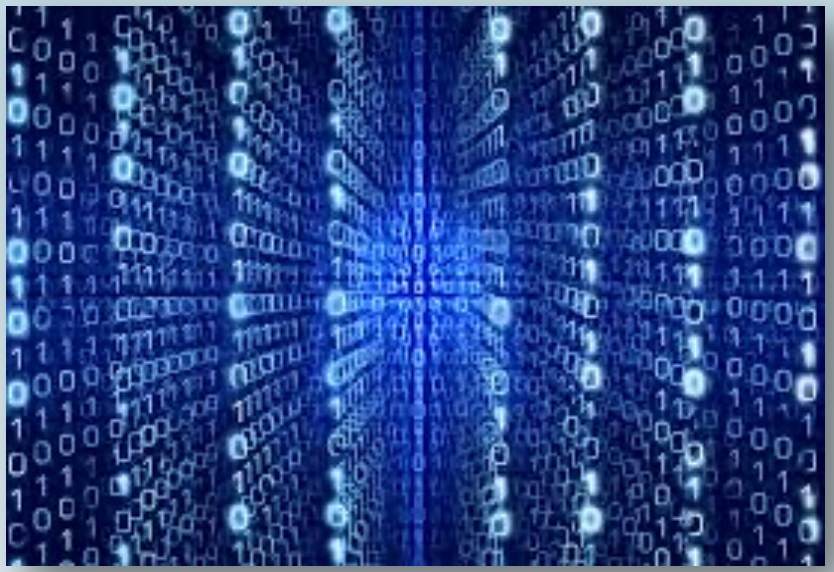
diseminarea informației rasiste și alt caracter, care incită la violență, ură sau discriminare împotriva unei persoane sau a unui grup de persoane pe criterii de rasă, naționalitate, religie sau etnie.

- Convenția CE din 23/11/2001 privind criminalitatea informatică

http://infoeuropa.md/criminalitatea-informatica/

SECURITATEA INFORMATICĂ

Fiecare stat utilizează un set de instrumente, politici, principii, măsuri de siguranță, abordări de gestionare a riscurilor, acțiuni, formarea, experiența, asigurare și tehnologii, care pot fi utilizate pentru protejarea spaţiului informatic, pentru resursele organizației și a utilizatorului.



CONVENȚIA PRIVIND CRIMINALITATEA INFORMATICĂ

Sarcinile principale:

1) adoptarea unei legislații adecvate, precum și prin îmbunătățirea cooperării internaționale, referitor la infracțiuni și dispoziții relevante în domeniul criminalității informatice şi prevederilor în domeniul criminalității cibernetice;

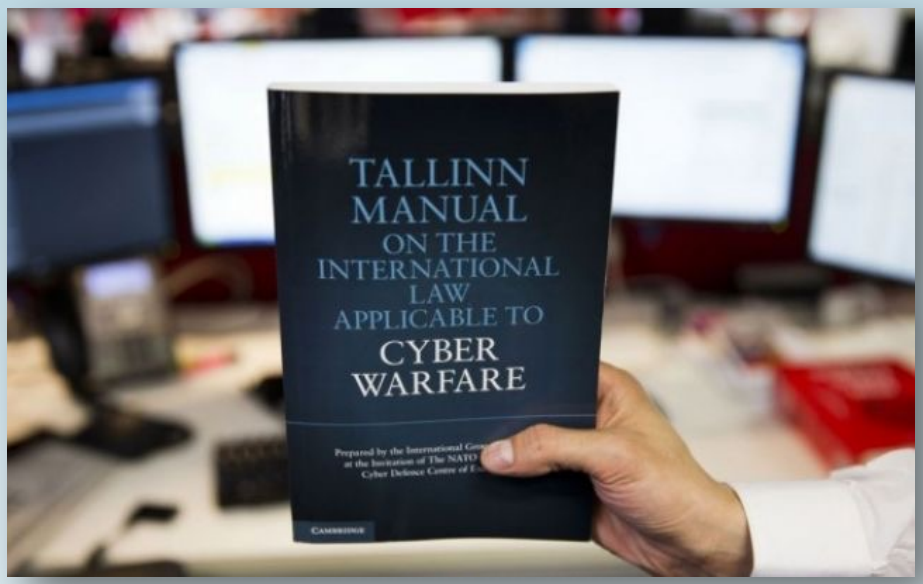
2) stabilirea competențelor și procedurilor necesare pentru investigarea și urmărirea penală pentru aceste infracțiuni, precum și pentru alte infracțiuni săvârșite prin intermediul sistemelor informatice;

3) colectarea probelor în format electronic;

4) elaborarea mecanismelor de cooperare internațională rapide și eficiente.

NATO şi SECURITATEA INFORMAŢIONALĂ

Centrul de Excelenţă pentru Apărare Cibernetică NATO a cărei misiune este sporirea capacităţii de cooperare şi informare între NATO, incluzând şi naţiunile membre, şi alţi parteneri din domeniul apărării cibernetice. De asemenea, Centrul desfăşoară activităţi de cercetare, elaborează lecţii învăţate şi asigură consultanţă de specialitate naţiunilor membre şi partenerilor alianţei



O protecție eficientă a spațiului virtual ar trebui să includă :

- cooperare internațională largă;
- dezvoltarea politicii de coaliție;
- îmbunătățirea capacităților de apărare pentru operațiuni în spațiul virtual.

Vezi publicații de la conferința internaționala a 14: Cyber Conflict: Keep Moving

14th International Conference on Cyber Conflict: Keep Moving

Publicațiile de la conferința a 14 oferă 23 de lucrări alese pentru a reflecta cel mai bine toate fațetele temei din anul trecut pe cele trei piese tradiționale CyCon: lege, tehnologie și strategie/politică.

Alegând „Continuați în mișcare!” ca temă centrală pentru CyCon 2022, Comitetul organizatoric/de program a dorit în primul rând să transmită hotărârea de a nu fi oprit de circumstanțe. Tema, desigur, are și un sens literal, deoarece se acordă din ce în ce mai multă atenție securității cibernetice în industria transporturilor, mediului maritim și lanțului de aprovizionare, precum și tehnologiilor autonome.

Asigurarea securității cibernetice în cadrul Uniunii Europene

STRATEGIA DE SECURITATE A SOCIETĂŢII INFORMAȚIONALE "DIALOG, PARTENERIAT ȘI EXTINDEREA CAPACITĂŢII„.
Această strategie oferă o imagine de ansamblu a stării actuale a amenințărilor la adresa securității societății informaționale și determină măsuri suplimentare pentru a asigura securitate rețelelor și a informațiilor.

PROGRAMUL DE LA STOCKHOLM – O EUROPĂ DESCHISĂ ȘI SIGURĂ ÎN SERVICIUL CETĂȚENILOR ȘI PENTRU PROTECȚIA ACESTORA - prevede măsuri suplimentare pentru îmbunătățirea luptei împotriva criminalității informatice.

AGENȚIA UNIUNII EUROPENE PENTRU SECURITATEA REȚELELOR ȘI A INFORMAȚIILOR (ENISA) - este un centru de expertiză pentru securitatea cibernetică în Europa, ajută UE și statele membre să fie mai bine echipate și pregătite pentru a preveni, detecta și elimina problemele legate de securitatea informațiilor. Oferă sfaturi și soluții practice pentru instituțiile UE și pentru sectorul public și privat din țările membre.

ENISA a publicat un raport cu referire la tehnicile de securitate cibernetică pentru protecția datelor

Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) a publicat un raport despre modul în care tehnologiile și tehnicile de securitate cibernetică pot sprijini implementarea principiilor Regulamentului general privind protecția datelor (GDPR) atunci când partajează date cu caracter personal. Documentul prezintă o analiză a modului în care datele sunt tratate atunci când partajarea face parte dintr-un alt proces sau serviciu. Acesta este cazul când datele trebuie să treacă printr-un canal sau o entitate secundară înainte de a ajunge la destinatarul final. La fel, raportul se concentrează pe diferitele provocări și posibile soluții, spre exemplu dreptul la ștergere și dreptul la rectificare la partajarea datelor. Vizând factorii de decizie politică și practicienii în protecția datelor, raportul oferă o privire de ansamblu asupra diferitelor aspecte ale modului de abordare a partajării datelor cu caracter personal într-un mod eficient

Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) a organizat prima conferință de politică în domeniul securității cibernetice împreună cu Comisia Europeană pentru a discuta evoluția cadrului politicilor de securitate cibernetică a UE. Obiectivul central al reuniunii a fost suportul continuu în dezvoltarea politicilor pentru a atinge un nivel comun ridicat de securitate cibernetică.

Evenimentul a fost menit să abordeze provocările în implementarea noilor prevederi ale NIS 2 în întreaga UE (https://digital-strategy.ec.europa.eu/ro/policies/nis2-directive). De asemenea, a arătat cum să faciliteze procesul de implementare, precum și să discute despre noile evoluții în cadrul politicii UE de securitate cibernetică. Experții au discutat despre o abordare comună a cadrului legislativ actual al UE și au făcut schimb de opinii.

SECURITATEA CIBERNETICĂ în REPUBLICA MOLDOVA

La început a fost Centrul pentru Securitatea Cibernetică - CERT-GOV-MD.

Misiunea Centrului era de a asista beneficiarii în utilizarea sistemelor informaţionale şi de telecomunicaţii al autorităţilor administraţiei publice în implementarea măsurilor proactive şi reactive în vederea reducerii riscurilor de incidente a securităţii IT şi acordarea asistenţei în reacţionarea la incidente. Centrul, de asemenea, examina incidentele apărute în reţele naţionale şi care sunt raportate de către cetăţeni şi instituţii din Republica Moldova, precum şi celor din străinătate.

SECURITATEA CIBERNETICĂ în REPUBLICA MOLDOVA

În 2010, Republica Moldova a lansat procesul de guvernare e-Transformare. Acest program strategic oferă o viziune unificată de modernizare și îmbunătățire a accesului publicului la servicii prin guvernarea IT. Asigurarea de informații - încrederea în securitatea, integritatea și disponibilitatea sistemelor informatice - este, prin urmare, esențială. O dezvoltare logică ar include implementarea unor noi sisteme, împreună cu noi măsuri de protecție. Procesul de dezvoltare rapidă din ultimul deceniu, din păcate, nu a inclus controale suficiente pentru a asigura securitatea cibernetică globală. La nivel guvernamental, au apărut câteva inițiative. Una dintre acestea a fost crearea unei echipe de răspuns la incidentele legate de securitatea calculatoarelor (Computer Emergency Response Team), ce reprezintă o echipă de experţi în securitatea informațională, a cărei sarcină este să răspundă la incidente ce țin de securitatea sistemelor informaționale, cunoscută sub denumirea de Centrul pentru Securitatea Cibernetică CERT-GOV-MD, creată în cadrul Întreprinderii de Stat ”Centrul de telecomunicații speciale”.

SECURITATEA CIBERNETICĂ în REPUBLICA MOLDOVA

Din 18 mai 2018, Întreprinderea de Stat „Centrul de Telecomunicații Speciale” se reorganizează, prin transformare, în Instituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică”. Scopul acesteia este de a asigura administrarea, menținerea și dezvoltarea infrastructurii de tehnologie a informației, sistemului de telecomunicații al autorităților administrației publice, ca parte a rețelei de comunicații speciale și a sistemelor informaționale de stat, gestionarea infrastructurii unice a cheii publice a Guvernului, precum și implementarea politicii statului în domeniul securității cibernetice speciale”.

SECURITATEA CIBERNETICĂ în REPUBLICA MOLDOVA

Pe site-ul „Serviciul Tehnologia Informației și Securitate Cibernetică” găsiți noutăți de ultimă oră din domeniul securității cibernetice.

Spre exemplu: forumul regional ”Her CyberTracks” care a avut loc în Muntenegru. Beneficiare ale forumului au fost femeile implicate în activități naționale și internaționale, procesele și negocierile privind politica de securitate cibernetică din Republica Moldova, Albania, Bosnia și Herțegovina, Georgia, Muntenegru, Macedonia de Nord, Serbia și Ucraina.

Noutăți din domeniul securității cibernetice:

Atacurile de tip phishing pe Messenger generează peste 100.000 de mesaje săptămânale;

Atacul de phishing Microsoft Teams vizează rețelele corporative;

IBM: 90% dintre atacurile cibernetice încep cu phishing prin e-mail și altele.

SECURITATEA CIBERNETICĂ în REPUBLICA MOLDOVA

Anul trecut în perioada 19-23 septembrie 2022 s-a desfășurat la Budapesta, Ungaria exercițiul internațional privind modul de intervenție în cazul fraudelor de plată online și a programelor malware. Această informație o găsiți pe site-ul Serviciului. Exercițiul a fost organizat de Agenția de aplicare a legii a Uniunii Europene (EUROPOL) și Agenția Uniunii Europene pentru Formare în Materie de Aplicare a Legii (CEPOL).

Scopul trainingului regional a fost de a îmbunătăți cunoștințele participanților cu privire la cele mai comune forme de atacuri cibernetice în domeniul Dark Web-ului, investigarea criptomonedelor și a fraudelor de plăți online.

SERVICIUL DE INFORMAȚII ȘI SECURITATE AL REPUBLICII MOLDOVA

Securitatea Republicii Moldova este o parte componentă a securităţii mondiale. Emergenţa ameninţărilor asimetrice în epoca globalizării contemporane implică necesitatea consolidării relaţiilor de parteneriat durabil în cadrul sistemului complex al comunităţii informative în scopul diminuării riscurilor ce pun în pericol securitatea naţională şi regională.

Prevenirea şi contracararea ameninţărilor la adresa securităţii Republicii Moldova este un demers în care Serviciul de Informaţii şi Securitate cooperează cu serviciile speciale şi structurile partenere în plan regional şi internaţional. După anul 1991, odată cu fondarea instituţiei, evoluţia raporturilor de cooperare ale SIS a cunoscut o dinamică pozitivă, îmbrăcând varii forme: schimb de informaţii şi expertiză, participare la evenimente de profil şi realizare de operaţiuni comune cu partenerii externi.

SERVICIUL DE INFORMAȚII ȘI SECURITATE A REPUBLICII MOLDOVA

În contextul politicii de integrare a Republicii Moldova în structurile Uniunii Europene, Serviciul îşi propune ca imperativ aderarea la platformele informative regionale, stabilirea şi promovarea relaţiilor bilaterale şi multilaterale cu instituţiile de profil de pe arena internaţională.

Scopul urmărit în această interacţiune este orientat spre realizarea intereselor fundamentale de securitate naţională şi implicarea activă a SIS în crearea unui climat adecvat de securitate regională şi europeană, având ca finalitate promovarea imaginii Republicii Moldova nu doar în calitate de consumator, dar şi generator de securitate.

COOPERARE MOLDO-NIPONĂ ÎN DOMENIUL SECURITĂȚII CIBERNETICE CU JICA

În iunie, 2022 Viceprim-ministrul pentru digitalizare și directorul Serviciului Tehnologia Informației și Securitate Cibernetică (STISC), au avut o întrevedere la Chișinău cu directorul oficiului Agenției Japoneze pentru Cooperare Internațională (JICA) în Ucraina, Satoshi Sugimoto, care se afla într-o vizită de lucru la Chișinău cu scopul de a discuta despre oportunitățile de finanțare a proiectelor de dezvoltare în anul viitor.

Discuțiile s-au axat pe intensificarea cooperării moldo-japoneze în domeniul securității cibernetice. Oficialul nipon și-a exprimat disponibilitatea de a oferi suport pentru consolidarea rezilienței cibernetice a Serviciului Tehnologia Informației și Securitate Cibernetică (STISC) și fortificarea sistemelor informaționale guvernamentale.

Principalele subiecte abordate de părți au vizat: suportul necesar pentru consolidarea capacităților STISC și oportunitățile de cooperare în cadrul unor programe de instruire în anul 2023.

Cooperarea va avea loc sub formă de schimb de experiențe, cunoștințe și bune practici, instruirea și dezvoltarea competențelor profesionale ale specialiștilor, precum și crearea parteneriatelor de succes.

Reprezentanții JICA au salutat intenția autorităților moldovenești de a continua cooperarea în cadrul proiectelor de dezvoltare și și-au exprimat disponibilitatea de extindere a domeniilor de interes.

Asigurarea securității în Sistemul financiar global

În economia mondială sunt utilizate, în mod fraudulos, tranzacțiile internaționale drept componentă de bază a spălării banilor şi a finanţării terorismului. Sistemul financiar global, transformat din parte componentă a pieţei într-un factor independent al economiei globale, susține fluxurile băneşti masive, provenite din economia tenebră.

Volumul fraudelor economice transnaționale se conturează tot mai mult. Circulația capitalului, inclusiv fluxurile băneşti de origine suspectă, iau amploare. Sunt pe larg utilizate tehnologiile informaționale alternative pentru transfer, care, în majoritatea cazurilor, privează de informație organele de supraveghere.

Este de menționat faptul că o parte substanțială a capitalurilor provenite din activități ilicite ajung în sectorul economic legal. Avansarea circulației informației, capitalului, persoanelor, bunurilor şi serviciilor, necesită modificarea concepției tradiționale şi a atitudinii fată de crimele transnaționale.

Asigurarea unor măsuri de prevenire a atacurilor cibernetice și de limitare a efectelor acestora sunt absolut necesare, dar este nevoie și de implicarea societății civile, care trebuie să conştientizeze necesitatea colaborării cu autorităţile pe acest palier.

Concluziil

În actualul context de securitate, adoptarea unui cadru legal care să sprijine dezvoltarea capacităţilor elementelor de securitate ale statului, astfel încât să facă faţă ameninţărilor cibernetice este un lucru necesar pentru orice stat şi un pas important în dezvoltarea unui sistem matur de securitate cibernetică.

Deţinerea unui sistem matur de securitate cibernetică reprezintă, de altfel, scopul fiecărui stat, pentru realizarea lui fiind necesară îndeplinirea mai multor obiective, precum: proiectarea unor politici şi a unei strategii de securitate cibernetică; creşterea culturii de securitate cibernetică la nivelul societăţii civile; dezvoltarea unor competenţe cibernetice atât la nivelul utilizatorilor, cât şi la nivelul managerilor; crearea unui cadru legal şi a unor acte normative eficiente; managementul riscului prin organizare; impunerea de standarde şi tehnologie.

Concluzii

Atingerea acestor obiective permite unei entităţi să îşi auto-evalueze capabilităţile de securitate cibernetică şi nivelul la care se situează.

Totodată, constituirea unui sistem matur de securitate implică mai multe etape de la prima fază în care nu există nicio capabilitate de securitate cibernetică, până la etapa finală în care există mecanisme clare privind gestionarea mediului cibernetic, metode dezvoltate de schimbare şi adaptare a strategiei la nevoile actuale de securitate, proceduri de reacţie rapidă, mecanisme de decizie, posibilităţi de realocare de resurse şi de menţinere a atenţiei constante pe schimbările din mediul de securitate.

Schimburile de informații, instruirile comune concentrate pe îmbunătățirea abilităților profesionale de a detecta și investiga criminalitatea cibernetică prin utilizarea metodelor și tehnicilor de investigare online în conformitate cu legislația internațională poare spori numai printr-o colaborare, comunicare și conlucrare eficienă. Astfel, pentru a spori cooperarea, comunicarea și conlucrarea cu experții în criminalitate cibernetică, este nevoie de instruiri prin intermediul prezentărilor practice, învățarea experiențelor interactive, inclusiv, exercițiilor practice individuale și lucru în grup.

Sarcini de autoevaluare

- Identificați acorduri de cooperare la nivel internațional pentru îmbunătățirea capacității de răspuns în cazul unor atacuri cibernetice majore;
- Determinați interesele naționale de securitate cibernetică în formatele de cooperare internațională la care Republica Moldova este parte;
- Evaluați activitatea la programe internaţionale care vizează domeniul securităţii cibernetice.

Teme pentru lucrul individual

- Provocări actuale în domeniul securității cibernetice – impact și contribuția Republicii Moldova în domeniu;
- Importanța cooperării în aria securității informaționale/cibernetice;
- Bune practici pentru prevenirea și limitarea efectelor atacurilor cibernetice la nivelul instituțiilor publice din Republica Moldova;
- Mecanisme de cooperare la nivel european/internațional;
- Dezvoltarea cooperării naționale și internaționale.

Bibliografie

1. 14 th International Conference on Cyber Conflict: Keep Moving, CCDCOE Publications. 2022. https://ccdcoe.org/uploads/2022/06/CyCon_2022_book.pdf 1.
2. ENISA a publicat un raport cu referire la tehnicile de securitate cibernetică pentru protecția datelor https://www.enisa.europa.eu/publications/engineering-personal-data-sharing
3. ENISA a organizat prima conferință de politică în domeniul securității cibernetice https://www.enisa.europa.eu/news/supporting-policy-developments-to-achieve-a-high-common-level-of-cybersecurity
4. Parteneriatele NATO și Republica Moldova în fața noilor amenințări la adresa securității regionale. Chișinău, 2014, p. 47-49.
5. Cooperare pentru securitate cibernetică. https://cybersecuritytrends.ro/cooperare-pentru-securitate-cibernetica/
6. Conferinţa Internaţională cu genericul "Securitatea Cibernetică în Republica Moldova: Provocări, Tendinţe şi Soluţii". http://cert.gov.md/news/noutati/article//conferinta.html
7. Problematica securităţii cibernetice în cadrul organizaţiilor internaţionale şi implicarea României ca membru al acestora. https://www.mae.ro/node/28369
8. Starea Uniunii 2017 – Securitatea cibernetică: Comisia consolidează răspunsul UE la atacurile cibernetice. Comisia Europeană - Comunicat de presă. file:///D:/USERS/Corina.Arhiri/Downloads/IP-17-3193_RO.pdf
9. Programul de Securitate Cibernetică. http://www.mtic.gov.md/ro/projects/programul-de-securitate-cibernetica
10. Securitatea cibernetică: reguli de protecție împotriva amenințărilor online. http://www.rfi.ro/politica-88178-securitatea-cibernetica-reguli-de-protectie-impotriva-amenintarilor-online
11. Мазуров В. Кибертерроризм: понятие, проблемы противодействия. Доклады ТУСУРа, № 1 (21), ч. 1, июнь 2010. с. 41-44
12. Смирнов А. Обеспечение информационной безопасности в условиях виртуализации общества: опыт Европейского Союза. Москва: ЮНИТИ-ДАНА, 2011.
13. Шрайер Ф., Викс Б., Винклер Т. Кибербезопасность: дорога, которую предстоит пройти. Женева: Женевский Центр демократического контроля над вооруженными силами, 2013. 62 с.
14. Tielidze G., Bagge D., Spinu N. and Ivanović Z. Regional Cyber Security. B: per Concordiam, Vol. 5, issue 2, 2014. p. 24-34
15. Initiative de contracarare a banilor publici, Chisinau, 2015, 86 p.