Asigurarea calitativă a sistemului de securitate a informațiilor din Republica Moldova în perioada de criză economică

Ecaterina BARBĂROȘIE,
doctor în științe economice, conferențiar universitar,
Academia de Administrare Publică

Oleg FRUNZE,
doctor în științe tehnice, lector superior universitar,
Academia de Administrare Publică

SUMMARY

The article describes the basic concepts of information security of the country, the principles of information security system. It has been proposed and explained the main directions for managing information security of the country.

Key-words: *national security, economic security, information security, information incident, information security event.*

O parte esențială a strategiei de securitate națională a Republicii Moldova este securitatea economică a statului. Un rol important revine anume securității informaționale.

Pentru început, vom explica conceptele de bază în acest domeniu. Nu există informații sporadice. Există diferite tipuri de date, utilizate pentru analiza economică și prognozarea fenomenelor economice, procese ce au loc la nivel de stat. (1) Aceste date trebuie să asigure veridicitatea, valabilitatea și realitatea informațiilor primite.

Securitatea informațională este protejarea infrastructurii de impactul neașteptat cu caracter artificial sau natural, care ar putea provoca un alt fel de daune. Astfel, este necesar să se asigure disponibilitatea datelor. Cu toate acestea, pot exista incidente informaționale.

În cadrul managementului securității informaționale sunt astfel de termeni importanți, cum ar fi incidentul informațional și evenimentul de securitate informațională. (2)

Evenimentul de securitate informațională este un caz identificat de stare a sistemului sau rețelei, care indică o posibilă încălcare a politicii de securitate informațională, căderea mijloacelor de protecție sau o situație necunoscută anterior, care poate fi importantă pentru securitate.

Evenimentul de securitate informațională, așa cum este arătat în figura 1, reprezintă o legătură logică între acțiune și obiect, spre care este îndreptată această acțiune, și rezultatul acțiunii. Uneori, evenimentele emergente sunt parte din pași, efectuați de atacatori pentru a obține un rezultat neautorizat. Aceste evenimente pot fi văzute ca parte a unui incident de securitate informațională. În cazul în care evenimentul se repetă și poate aduce daune, acesta este un incident de securitate informațională.

Fig. 1. **Structura evenimentului de securitate informațională.**

Evenimentul de securitate informațională			
Subiectul	Acțiunea	Obiectul	Rezultatul

Sursa. Elaborată de autori.

Cuvântul incident este derivat din cuvântul latin *incidentis*, ceea ce înseamnă „incident neplăcut, accident, neînțelegere, confruntare". Incidentul informațional reprezintă o întâmplare (eroare) sau acțiune deliberată, (cu rea-voință) cazul de prezentare a informației incorecte. Acest lucru presupune apariția unui sau mai multor evenimente nedorite sau neașteptate de securitate informațională, iar, ca rezultat, sporește incidența atât a amenințărilor și compromiterilor interne cât și externe. Acest lucru ar putea conduce la o denaturare a realității și, ca o consecință, la analiza de rezultate incorecte. Aceasta, la rândul său, conduce la concluzii greșite și adoptarea unor decizii de gestionare greșite.

De aceea asigurarea calității informației reale este importantă și necesară. Aceste probleme sunt deosebit de acute pe timp de criză în dezvoltarea ciclului economic. Relațiile dintre elementele incidentului informațional sunt prezentate în figura 2.

- conduce la deformarea opiniei publice;
- contribui la distrugerea sistemului de formare și luare a deciziilor la toate nivelurile și nu permite formarea soluțiilor eficiente;
- destabiliza psihicul uman și conduce la comportament inadecvat al persoanei;
- încălca formarea opiniei publice;
- slăbi sau chiar distruge resursele informaționale ale țării;
- distruge și diminua capabilitatea mediului psihoinformațional, ce poate influența distructiv psihicul și comportamentul uman.

O precondiție obligatorie pentru depășirea problemei de asigurare a securității informaționale este gestionarea centralizată a proceselor de prelucrare a informației confidențiale, ceea ce presupune:

- coordonarea acțiunilor administrației publice locale și centrale în realizarea politicilor (complex de măsuri direcționate), asigurarea securității informaționale la nivel central și local;

Fig. 2. **Structura evenimentului de securitate informațională.**

Subiectul	Intrusul externe
Scopul, sarcinile	Producere daune
Metode și instrumente	Atac fizic, mijloace tehnice și organizatorice
Acțiunea	Copiere, furt, distrugere, modificare, ascultare ș. a.
Obiectul	Informații, căi de comunicare
Rezultatul	Producere daune, denaturarea realității ș. a.

Sursa. Elaborată de autori.

Astfel, incidentul include următoarele elemente: atacatorul, metodele și instrumentele, acțiunile și obiectele asupra cărora sunt îndreptate aceste acțiuni.

Ar trebui de remarcat că suprimarea securității informaționale poate:

- focusarea tuturor resurselor statului spre soluționarea problemelor prevăzute în strategia de securitate națională;
- controlul asupra oportunității și eficacității realizării politicilor de securitate informațională.

Astfel, sistemul de securitate informațională se bazează pe următoarele principii:

a) prognoza și detectarea timpurie a amenințărilor de securitate a resurselor informaționale, cauzelor și condițiilor, ce produc daune financiare, materiale, morale, și fac funcționarea dificilă și dezvoltarea lentă;

b) crearea condițiilor de funcționare cu probabilitate minimală de realizare a amenințărilor securității resurselor informaționale și producerea daunelor;

c) crearea mecanismului și condițiilor de răspuns rapid la amenințarea securității informaționale și apariția tendințelor negative în funcționare, suprimarea eficientă a atentatelor la resursele pe bază legală, a măsurilor organizaționale și tehnice și mijloacelor de asigurare a securității naționale;

d) crearea condițiilor pentru maximalizarea posibilității de recuperare a daunelor produse de persoane fizice sau juridice prin acțiuni cu impact negativ asupra securității informaționale, prevenirea urmărilor și riscurilor atacului informațional planificat și implementat printr-un scenariu dezvoltat de hackeri.

Este necesar de menționat faptul că protecția informațională efectivă în mediul economic actual este, practic, ireală exclusiv prin metode tehnice. Fraudele cu utilizarea ingineriei sociale reprezintă calea cea mai ușoară și rapidă de compromitere a securității informaționale și cel mai dificil de depistat. Pentru realizarea atacurilor sociale atacatorii folosesc naivitatea, trândăvirea, vicleșugul, amabilitatea și chiar entuziasmul oamenilor care sunt abordați.

Sistemul de măsuri profilactice care vor spori eficiența de prevenire a accesului neautorizat la informație se poate prezenta prin următorul algoritm:

- depistarea eventualelor amenințări de acces neautorizat la fiecare sursă de informare;
- identificarea persoanelor cu starea fragilă în condiții de distribuție normală de loialitate a populației statistice;
- prestarea către populație a activităților și instrumentelor de prevenire, pentru îmbunătățirea eficienței în prevenirea accesului neautorizat la informațiile confidențiale;
- aplicarea măsurilor de formare educațională și existențială, a evenimentelor de training, creșterea nivelului de loialitate a populației până la situația de repartiție normală.

Astfel, securitatea informațională este starea de protecție a mediului informațional, a societății și instituțiilor de stat de atacurile interne și externe ce asigură formarea, utilizarea și dezvoltarea în interesul cetățenilor, societății și a statului în general.

O aplicație complexă în metodologia de gestionare a securității informaționale a măsurilor preventive, bazată pe algoritmul menționat, în combinație cu alte măsuri necesare, va contribui la sporirea educației populației în direcția securității informaționale a statului. Acest lucru va diminua folosirea irațională a resurselor și va îmbunătăți indicatorii economico-sociali ai statului, la fel, va îmbunătăți calitatea asigurării sistemului de securitate informațională în perioada de criză.

În plus, aceste măsuri vor contribui nu doar la sporirea calității asigurării informaționale, dar și la procesul decizional privind gestionarea resurselor umane.

BIBLIOGRAFIE

1. Барбарошие Е. А., Назар Н. М. Значение информационного обеспечения в финансовом менеджменте организации. В: Проблемы информационной безопасности. 1–я Международная научно-практическая конференция. 26-28 февраля 2015, Симферополь-ГУРЗУФ, стр. 4-5, 0,25 с. а.
2. ISO/ IEC 27001 2005 Information technology, security techniques incident management.
3. CCMU/SEI-2004-TR-015 Dafining incident management processes for CSIRT.

Prezentat: 07.mai.2015.
E-mail: ec_barbaros@yahoo.com
frunze_oleg@yahoo.com