Rodica BULAI,
lector al Catedrei ştiinţe reale
şi tehnologii informaţionale a Academiei „Ştefan cel Mare" a MAI, doctorand
Angela PINTILEI,
lector al Catedrei ştiinţe reale
şi tehnologii informaţionale a Academiei „Ştefan cel Mare" a MAI

RISCURILE INFORMAŢIONALE ÎN CADRUL ORGANELOR DE DREPT ŞI PREVENIREA LOR

Dezvoltarea intensivă a mijloacelor tehnice de gestionare a informaţiei şi deservire a telecomunicaţiilor a dus la aplicarea lor pe scară largă în aproape toate domeniile de activitate umană. Amploarea şi sfera de aplicare a tehnicii de calcul sunt de aşa natură încât, împreună cu problemele de fiabilitate şi stabilitate în exploatare, există o problemă şi de securitate informaţională. Această problemă este actuală şi pentru sistemele informaţionale ale organelor de drept ale Republicii Moldova.

Până mai ieri structurile de drept ale ţării deţineau, de regulă, sisteme informaţionale proprii. În urma activităţii desfăşurate erau create anumite resurse informaţionale. Deseori sistemele informaţionale cuprindeau fragmentar activitatea instituţiilor, adică, parţial, evidenţa era ţinută pe suporturi de hârtie (fişe, registre), parţial era automatizată. Totodată, sistemele existente funcţionau autonom, fără integrare reciprocă, dublându-se evidenţa unora şi aceloraşi obiecte informaţionale.

Dezintegrarea resurselor informaţionale nu permitea utilizarea eficientă a informaţiei stocate în combaterea criminalităţii. Pentru a ieşi din situaţia existentă, s-a pus problema formării spaţiului informaţional unic al organelor de drept format atât din resursele informaţionale departamentale, cât şi din resursele informaţionale specializate [1].

Totuşi acest sistem e departe de a fi un sistem integral şi perfect. De aceea nu pot fi neglijate riscurile informaţionale care pot apărea. Ele trebuie cunoscute, evaluate şi pe cât posibil diminuate.

Prin risc informaţional (pericol pentru securitatea informaţională) se înţelege un eveniment sau o acţiune posibilă, orientată spre cauzarea prejudiciului resurselor sau infrastructurii informaţionale a organelor de drept.

Dacă e să facem o clasifcare a riscurilor informaţionale, care pot apărea în cadrul organelor de drept, ele pot fi tehnologice şi organizatorice [2].

Riscurile tehnologice, după natura impactului, pot fi împărţite în riscuri fizice şi riscuri logice (software). Riscurile fizice pot apărea din cauza influenţei fizice asupra componentelor infrastructurii informaţionale şi pot parveni din cauza:

- unei persoane rău intenţionate;
- unor circumstanţe de forţă majoră;

– defectării echipamentelor tehnice.

Riscurile logice (software) pot fi:

– riscurile apărute din partea unei persoane din interior (locale). Riscurile locale sunt direcționate, de obicei, asupra resurselor informaționale: sistemul de operare, programele de aplicație, precum și informațiile stocate. Perturbarea funcționării integrității sau confidențialității oricăror dintre aceste elemente pot duce la pierderea informațiilor valoroase;

– riscurile parvenite din partea unei persoane din exterior (de la distanță). Penetrările exterioare pot afecta atât resursele informaționale locale, cât și resursele canalelor de comunicație: echipamentele de rețea, protocoalele de rețea, sistemele și informațiile utilizate prin intermediul rețelelor de comunicație (de exemplu, virușii, hackerii).

Ca o măsură de contracarare a riscurilor informaționale poate fi protecția în mod adecvat a resurselor informaționale și acțiunile corecte ale personalului și ale utilizatorului. Aici poate apărea întrebarea, dar cum poate un funcționar MAI să realizaze un risc informațional? Persoana rău intenționată poate folosi un impact asupra angajatorului pentru a obține informațiile necesare, sau însuși angajatorul realizează impactul asupra sistemului informațional. Prin urmare, în generarea riscurilor organizatorice rolul principal îi revine factorului uman realizat prin corupere sau intimidare a personalului.

Din acest punct de vedere, impactul asupra angajatorului poate fi fizic și psihologic, cu scopul de a se obține informații valoroase și/sau secrete sau de a perturba buna desfășurare a activității organelor de interne.

Impactul angajatorului asupra sistemului informațional poate fi intenționat și din imprudență (furtul, acțiuni ale lucrătorilor necinstiți, erori și scăpări ale personalului de deservire și a utilizatorilor) și poate afecta atât informațiile valoroase, cât și buna desfășurare a activității.

O altă clasificare a riscurilor informaționale din cadrul organelor de interne poate fi făcută după standardul COBIT (Control Objectives for Information and Related Technology), elaborat de ISACA (Information Systems Audit and Control Association – Asociația Internațională a Auditorilor de Sisteme Informatice). Conform COBIT, informația trebuie să satisfacă anumite criterii. Aceste criterii sunt: eficiența, eficacitatea, confidențialitatea, integritatea, disponibilitatea, credibilitatea, conformarea. Respectiv, orice activitate ce implică utilizarea resurselor informaționale și poate amenința corespunderea informației acestor criterii constituie un risc informațional. În funcție de criteriul ce poate fi afectat, riscurile informaționale pot fi:

– riscul de ineficiență: încălcarea tehnologiei de prelucrare a informației, elaborarea și răspândirea programelor care afectează funcționarea normală a sistemelor;

– riscul de ineficacitate: accesul nesancționat la resursele informaționale, scurgerea informației prin canale tehnice;

– riscul de compromitere a confidențialității: colectarea și utilizarea ilegală a informației din sistem, compromiterea sistemelor cu parolă, cheilor și mijloacelor de protecție criptografică a informației;

– riscul de compromitere a integrității: implementarea în produsele software și hardware a componentelor care realizează funcții neprevăzute în documentația acestor produse;

– riscul de compromitere a disponibilității: nimicirea, deteriorarea, suprimarea sau distrugerea sistemelor informaționale și a mijloacelor de telecomunicații;

– riscul de compromitere a credibilității: interceptarea informației în rețelele de transmitere a datelor și în liniile de comunicații, decodificarea acestei informații și impunerea informației false;

– riscul de neconformare: încălcarea restricțiilor legale privind răspândirea informației.

De exemplu, o eroare în cadrul unui sistem informatic poate duce la blocarea sistemului, în felul acesta informația necesară activității nu va mai fi disponibilă, pe o perioadă mai scurtă sau mai lungă. Astfel, este afectat criteriul disponibilității informației, iar riscul de erori la nivelul softului constituie un risc de compromitere a disponibilității informației [4].

COBIT este cel de-al treilea standard internațional, prin care se poate realiza dezvoltarea și creșterea securității sistemelor informatice. El reprezintă un set de obiective de control în domeniul informaticii, acceptate pe plan internațional, care se pot aplica în general și în special și care sunt recunoscute în domeniul controlului de securitate și reglementare informatică. În cursul procesului de elaborare a standardului COBIT, s-au luat în calcul mai ales considerentele a trei grupuri profesionale diferite:

– pentru persoanele de conducere la nivel înalt oferă asistență în privința managementului de risc al mediului informatic aflat în mișcare continuă, respectiv în deciziile cu privire la investițiile necesare pentru crearea controalelor.

– pentru utilizatori asigură controlul și securitatea serviciilor informatice.

– pentru controlorii sistemului de informații creează o bază uniformă pentru evaluarea controalelor interne, respectiv pentru activitățile de estimare și consultare pentru management.

În ceea ce privește securitatea informației, cerința de bază este protejarea informației împotriva utilizării neautorizate, a dezvăluirii, modificării, pierderii sau coruperii. Controlul procesului care satisface această cerință se activează prin controlul accesului logic, care să asigure că accesul la sisteme, date și aplicații este permis doar utilizatorilor autorizați, prin metode și practici precum autentificarea, autorizarea și controlul accesului, crearea de profile de utilizatori, cerințele de confidențialitate, administrarea cheilor criptografice, managementul incidentelor, școlarizarea corespunzătoare a utilizatorilor, administrarea centralizată a securității, instrumente de monitorizare etc.

Cunoașterea acestor standarde este un prim pas în procesul de organizare a activităților informaționale și a securității, de îmbunătățire a calității serviciilor informaționale și de administrare a riscurilor, în final de atingere a unui nivel superior de calitate în executarea și livrarea acestor servicii.

Adoptarea acestor standarde internaționale oferă o serie de avantaje clare: abordarea securității informației în contextul general, al strategiei, tehnologiei și comportamentului uman, cu efectul adoptării unor decizii mai bune privind politica și implementarea soluțiilor de securitate [3].

În cadrul organelor de drept, informațiile și, prin urmare, gestionarea și furnizarea lor, fără exagerare, sunt printre cele mai importante elemente ale algoritmului de dirijare eficientă ale MAI. În acest context, o importanță deosebită o capătă problemele legate de asigurarea securității sistemului informațional al organelor de drept, stabilirea metodelor prioritare concrete de securitate, precum și

îmbunătăţirea, perfecţionarea continuă a lor [5].

În cadrul organelor de drept, printre punctele vulnerabile pot fi menţionate:

– insuficienţa gradului de pregătire în domeniul securităţii informaţionale;

– nivelul scăzut de coordonare între instituţiile guvernamentale şi publice în domeniul securităţii informaţiionale;

– infrastructură SI săracă: utilizarea parţială sau chiar lipsa utilajului performant şi a programelor necesare asigurării securităţii informaţionale;

– lipsa unei structuri statale specializate de asigurare a securităţii informaţionale [6].

Toate acestea impun desfăşurarea unor măsuri, printre care:

– crearea unei structuri statale specializate de asigurare a securităţii informaţionale, completată cu specialişti de calificare înaltă;

– elaborarea unui regulament eficient şi a unui sistem de control intern, menite să asigure coordonarea instituţiilor guvernamentale şi publice în domeniul securităţii informaţiilor prin implementarea standardelor internaţionale din domeniul securităţii informaţionale: ISO/IEC 27001:2005 Sistemul de Management al Securităţii Informaţionale; ISO/IEC 20002:2005 Codul de practică pentru Managementul Securităţii Informaţionale şi COBIT – descris în acest articol. Procesul de coordonare să fie supravegheat de structura specializată despre care am menţionat mai sus;

– asigurarea unei pregătiri speciale înalte a colaboratorilor organelor de drept, inclusiv a persoanelor cu funcţie de răspundere în problematica securităţii informaţionale, educarea şi instruirea personalului în scopul prevenirii şi contracarării riscurilor informaţionale;

– aplicarea principiului de securitate informaţională pe niveluri multiple prin utilizarea bazelor de date speciale de evidenţă a informaţiei secrete, de dirijare şi analiză a accesului la aceste informaţii, înregistrarea acţiunilor şi auditul vulnerabilităţilor, utilizarea mecanismelor de autentificare şi autorizare, a programelor antivirus, de criptare, arhivare şi restabilire a informaţiei. Acest principiu trebuie să corespundă activităţii organelor de interne, politicii de securitate informaţională din cadrul MAI.

Referinţe bibliografice:

1. Hotărârea Guvernului cu privire la aprobarea Concepţiei Sistemului informaţional integrat al organelor de drept nr. 1202 din 17.10.2006, Monitorul Oficial nr.168-169/1293 din 27.10.2006.
2. http://www.dsectrain.ru/about/articles/dsecct/ Наталья Куканова**,** *Описание классификации угроз DSECCT*.
3. http://www.managementul-riscurilor.ro/COBIT – Securitatea informaţiilor.
4. Marin PRISĂCARU, "Riscurile tehnologiei informaţiei", în *Materialele conferinţei intenaţionale Securitatea informaţională 2007*, ediţia a IV-a, ASEM, Chişinău, 2007.
5. http://www.lib.ua-ru.net/ Максим Валериевич Евдокимов, *Совершенствование организационно-правовой системы защиты компьютерной информации в деятельности органов внутренних дел*.
6. http://www.lib.ua-ru.net/Валерий Александрович Пожилых, *Организационно-правовые особенности защиты информации в автоматизированных информационных системах органов внутренних дел*.