CZU 004.056 DOI 10.5281/zenodo.4071173

MANAGEMENTUL INFORMAŢIILOR DE SECURITATE

Liliana CREANGĂ,
doctor în drept, conferenţiar universitar

Anatoli BUZEV,
doctorand

Odată cu înaintarea în timp şi dezvoltarea tehnologiilor informaţionale, procesul de management al informaţiilor de securitate este prezent în majoritatea acţiunilor derulate la nivelul instituţiilor de stat, economiei naţionale, businessului, prestării serviciilor etc. Şi totuşi, când vorbim despre securitatea informaţională, în multe entităţi există un decalaj între conştientizarea nevoilor de securitate şi respectarea măsurilor de securitate. Acest fapt se explică prin abordarea greşită a concepţiilor asupra procesului de management al informaţiilor de securitate, care pot rezulta în implementarea unor soluţii ineficiente. Acest articol îşi propune să cerceteze noţiunea de „management al informaţiilor de securitate" şi să identifice cauzele şi condiţiile care favorizează lezarea siguranţei informaţiilor de securitate, în vederea deducerii recomandărilor privind măsurile de asigurare a securităţii informaţiilor.

Cuvinte-cheie: *management, informaţii de securitate, criptare, acces controlat, standard.*

Introducere. Actualitatea temei rezidă în dezvoltarea şi extinderea proceselor de gestionare a informaţiilor de securitate. Problema managementului informaţiilor de securitate şi sistemelor informatice devine acută din mai multe motive obiective. Progresele ştiinţifice şi tehnologice au transformat informaţiile într-un produs care poate fi cumpărat, vândut sau schimbat. Deseori, costul datelor este de câteva ori mai mare decât costul întregului sistem tehnic care stochează şi procesează informaţii [5, p. 365].

Conceptual, securitatea informaţiei se referă la *„asigurarea integrităţii, confidenţialităţii şi disponibilităţii informaţiei"*. Dinamica tehnologiei informaţiei induce noi riscuri pentru care organizaţiile trebuie să implementeze noi măsuri de control. De exemplu, popularizarea unităţilor de inscripţionat CD-uri sau a memoriilor portabile de capa-

THE MANAGEMENT OF THE SECURITY INFORMATION

Liliana CREANGĂ,
PhD, associate professor

Anatoli BUZEV,
PhD Student

With the time advancement and the development of information technologies, the process of managing security information is present in most of the actions carried out at the level of state institutions, national economy, business, service provision, etc. And yet, when we talk about information security, in many entities there is a gap between awareness of security needs and compliance with security measures. This fact is explained by the wrong approach of the conceptions on the process of managing the security information, which can result in the implementation of some inefficient solutions. This article aims to investigate the concept of security information management and to identify the causes and conditions that favor the safety breach of security information, in order to deduce the recommendations regarding the measures which ensure the security of information.

Keywords: *management, security information, encryption, access control, standard.*

Introduction. The topicality of the theme lies in the development and the extension of security information management processes, the problem of managing security information and information systems becomes acute for several objective reasons. Scientific and technological progresses have transformed the information into a product that can be bought, sold or changed. Often, the cost of data is several times higher than the cost of the entire technical system that stores and processes information [5, p. 365].

Conceptually, information security refers to "ensuring the integrity, confidentiality and availability of information". The dynamics of information technology induces new risks for which organizations have to implement new measures of control. For example, the popularization of high-capacity CD-ROM drivers or portable memory

citate mare induce riscuri de copiere neautorizată sau furt de date [6, p. 6]. Asigurându-se securitatea informației, implicit este protejat și utilizatorul sau destinatarul acelei informații împotriva unor diverse atacuri și amenințări. Informația ca produs al prelucrării automate a datelor și implicit drepturile care derivă din proprietatea intelectuală trebuie protejate indiferent de mijloacele și metodele în care acestea sunt transmise, arhivate sau prelucrate.

Tudor Bragaru, Valentin Briceag, Viorel Malcoci și Valeriu Galaicu în articolul *„Securitatea informației vis-à-vis de securitatea informațională"* definesc securitatea informațională ca stare a spațiului informațional, care asigură nevoile informaționale ale subiecților în relațiile informaționale, securitatea informațiilor și protecția subiecților relațiilor informaționale împotriva unor influențe negative. Iar spațiul informațional poate fi definit drept mediu de activitate a subiecților preocupați de crearea, transformarea și consumul de informații. Astfel, conceptul „securitate informațională" este unul acoperitor, care include nu doar securitatea informațiilor, ci și protecția mediului obiectului (statului, organizației, persoanei) împotriva impactului informațiilor negative sau a destabilizării unor componente ale sistemului/obiectului respectiv. Rezumând, securitatea informațională poate fi definită ca protejarea persoanei, organizației, societății și statului în spațiul informațional, a drepturilor și intereselor acestora față de (1) acces, (2) utilizare, (3) divulgare, (4) modificare, (5) dislocare sau (6) distrugeri neautorizate ale atributelor informației, ale IS, TIC și infrastructurilor de procesare, depozitare, acces și transport al informațiilor, inclusiv mass-media, în scopul asigurării intimității persoanei, continuității afacerii, suveranității statului, diminuării pierderilor, dezinformării, inclusiv prevenirii scurgerii de date, spionajului [7, p. 40].

Așadar, putem spune că în situația securității informației ca și concept dat și implementarea lui practică vorbim, înainte de toate, de un interes strategic național, dincolo de cel al oricărei alte entități instituționale.

Tipurile informațiilor de securitate

Securitatea națională este reprezentată de starea de legalitate, de stabilitate economică, politică și socială care conduce la fundamentarea existenței și dezvoltării statului și menținerea ordinii de drept, respectarea drepturilor și libertăților

drivers entails risks of unauthorized copying or data theft [6, p. 6]. By ensuring the information security, implicitly, the user or the recipient of that information is also protected from various attacks and threats. Information as a product of automatic data processing, and implicitly the rights that derive from intellectual property, must be protected regardless of the means and methods in which they are transmitted, archived or processed.

Tudor Bragaru, Valentin Briceag, Viorel Malcoci and Valeriu Galaicu in the article "Information security vis-a-vis informational security" define information security as a state of the informational space, which ensures the informational needs of the subjects in the informational relations, the information security and the protection of information relations' subjects from negative influences. And the informational space can be defined as the activity environment of the subjects concerned with the creation, transformation and consumption of information. Thus, the concept "information security" is a cover, which includes not only the security of information, but also the protection of the environment of the object (state, organization, and person) from the impact of negative information or destabilization of some components of the relative system/object. To resume, the informational security can be defined as protecting the person, organization, society and state in the informational space, their rights and interests from (1) access, (2) use, (3) disclosure, (4) modification, (5) dislocation or (6) unauthorized destruction of the attributes of information, of IS, ICT and the infrastructures for processing, storing, accessing and transporting information, including the mass-media, in order to ensure the privacy of the person, business continuity, state sovereignty, loss reduction, misinformation, including data leakage prevention, espionage [7, p. 40].

Therefore, we can say that in the situation of information security as a given concept and its practical implementation, we speak, first of all, of a national strategic interest, beyond that of any other institutional entity.

Types of information security

The national security is represented by the state of legality, by the economic, political and social stability that leads to the foundation of the existence and the development of the state and the

fundamentale ale omului, de aceea informaţiile cu relevanţă în acest domeniu necesită o atenţie deosebită, manifestată prin secretizarea informaţiilor. De-a lungul timpului au existat categorii de informaţii care au fost exceptate de la accesul liber şi neîngrădit al oricărui cetăţean, limitare justificată de autorităţile statului, dar de multe ori contestată pentru încălcarea drepturilor omului. Mass-media şi opinia publică au contestat în nenumărate rânduri faptul că multe informaţii au fost exceptate de la liberul acces în mod nejustificat sau printr-o clasificare excesivă, dar există şi informaţii care necesită un anumit nivel de protecţie atunci când interesele naţionale, unele măsuri de protecţie a persoanelor, datelor de identificare ale acestora, concurenţa loială, anumite proceduri judiciare, interese economice şi politice strategice ale unui stat, impun luarea acestor tipuri de măsuri.

Măsurile restrângerii liberului acces la informaţii trebuie aplicate într-un mod nediscriminatoriu, realizate în concordanţă cu reglementările internaţionale privind drepturile omului, fiind foarte importantă o educare a cetăţeanului privind aspectele care conduc la restricţionarea liberului acces şi motivarea importanţei limitării. În practică au fost înregistrate cazuri de clasificare excesivă a informaţiilor din partea organelor administraţiei publice cu atribuţii în domeniul apărării, ordinii publice şi siguranţei naţionale.

În majoritatea statelor democratice, informaţiile exceptate de la liberul acces vizează:

– informaţiile secrete de stat din domeniul apărării, ordinii publice şi siguranţei naţionale;

– informaţiile secrete de serviciu;

– informaţiile privind datele cu caracter personal, potrivit legii;

– deliberările autorităţilor şi informaţiile de interes economic, dacă sunt clasificate;

– informaţiile privind activităţile comerciale, dacă prin publicarea lor se aduce atingere principiilor concurenţei loiale;

– informaţiile privind procedurile judiciare, dacă furnizarea lor va aduce atingere unui proces echitabil;

– informaţiile care prejudiciază măsurile de protecţie a tinerilor;

– informaţiile privind proceduri de anchetă penală sau disciplinară dacă dezvăluirea lor afectează rezultatul final al anchetei.

maintenance of the order of law, the respect of the fundamental human rights and freedoms, therefore the information relevant in this field requires special attention, manifested by the information conceal. Over time there have been categories of information that have been exempted from the free and unrestricted access of any citizen, a limitation justified by the state authorities, but often challenged for human rights violations. The mass-media and the public opinion have repeatedly challenged the fact that many information has been unjustifiably exempted from free access or over-classification, but there is also information that requires a certain level of protection when national interests, some measures of protection of persons, their identification data, fair competition, certain judicial procedures, economic and political strategic interests of a state, require these types of measures.

The measures to restrict the free access to information must be applied in a non-discriminatory way, realized in accordance with the international human rights regulations, as it is very important to educate the citizen on the aspects that lead to the restriction of the free access and to motivate the importance of the limitation. In practice, there have been cases of excessive classification of information by public administration bodies with responsibilities in the field of defense, public order and national security.

In most democratic states, the information exempted from free access covers:

– the state secret information in the field of defense, public order and national security;

– the secret service information;

– the information regarding personal data, according to the law;

– the deliberations of the authorities and the information of economic interest, if they are classified;

– the information regarding the commercial activities, if by their publication the principles of fair competition are violated;

– the information regarding the judicial procedures, if their provision will affect a fair trial;

– the information that harms the protection measures of young people;

– the information on criminal or disciplinary investigation procedures if their disclosure affects the final result of the investigation.

La nivel național, în conformitate cu Legea nr.LP982/2000 din 11.05.2000 privind accesul la informații, informațiile oficiale cu accesibilitate limitată [8] reprezintă:

– informațiile atribuite la secret de stat, reglementate prin lege organică, a căror divulgare neautorizată sau pierdere poate aduce atingere intereselor și/sau securității Republicii Moldova;

– informațiile confidențiale din domeniul afacerilor, prezentate instituțiilor publice cu titlu de confidențialitate, reglementate de legislația privind secretul comercial, și care țin de producție, tehnologie, administrare, finanțe, de altă activitate a vieții economice, a căror divulgare (transmitere, scurgere) poate atinge interesele întreprinzătorilor;

– informațiile cu caracter personal, a căror divulgare este considerată drept o imixtiune în viața privată a persoanei, protejată de legislația privind protecția datelor cu caracter personal;

– informațiile ce țin de activitatea operativă și de urmărire penală a organelor de resort, dar numai în cazurile în care divulgarea acestor informații ar putea prejudicia urmărirea penală, interveni în desfășurarea unui proces de judecată, lipsi persoana de dreptul la o judecare corectă și imparțială a cazului său, or ar pune în pericol viața sau securitatea fizică a oricărei persoane – aspecte reglementate de legislație;

– informațiile ce reflectă rezultatele finale sau intermediare ale unor investigații științifice și tehnice și a căror divulgare privează autorii investigațiilor de prioritatea de publicare sau influențează negativ exercitarea altor drepturi protejate prin lege.

Informația cu caracter personal face parte din categoria informației oficiale cu accesibilitate limitată și constă din date referitoare la o persoană fizică identificată sau identificabilă, a căror dezvăluire ar constitui o violare a vieții private, intime și familiale.

Amenințări la adresa securității informaționale

Metodele manageriale de asigurare a securității informației includ reglementări interne referitoare la relațiile dintre angajați, care ar exclude sau limita divulgarea, scurgerea sau accesul nesancționat la informații. Aceste metode includ selectarea și instruirea personalului, formularea obligațiunilor referitoare la securitatea informației în contractele individuale de muncă și fișele

At the national level, according to Law no.LP982/2000 of 11.05.2000 on access to information, official information with limited accessibility [8] represents:

1) the information attributed to the state secret, regulated by organic law, whose unauthorized disclosure or loss may prejudice the interests and/or the security of the Republic of Moldova;

2) confidential information in the field of business, presented to public institutions for confidentiality, regulated by the law on commercial secrecy, and related to production, technology, administration, finance, other activity of economic life, whose disclosure (transmission, leakage) can reach the interests of entrepreneurs;

3) personal information, the disclosure of which is considered as an interference in the personal life of the person, protected by the legislation regarding the protection of personal data;

4) information regarding the operative activity and the criminal prosecution of the relevant bodies, but only in cases where the disclosure of this information could prejudice the criminal prosecution, intervenes in carrying out a trial, the person lacks the right to a fair and impartial judgment of his case, or it would endanger the life or physical security of any person – aspects regulated by legislation;

5) information that reflects the final or the intermediate results of scientific and technical investigations and whose disclosure deprives the authors of the investigations of the publication priority or negatively influences the exercise of other rights protected by law.

Personal information is part of the category of official information with limited accessibility and consists of data relating to an identified or identifiable natural person, whose disclosure would constitute a violation of private, intimate and family life.

Threats to information security

The managerial methods of ensuring information security include internal regulations regarding the relations between employees, which would exclude or limit disclosure, leakage or unsanctioned access to information. These methods include the selection and training of personnel, the formulation of information security obligations in the individual employment contracts and

postului, organizarea accesului controlat la locurile unde se procesează informații sensibile, elaborarea și păstrarea copiilor de rezervă, lichidarea controlată a informației confidențiale și alte măsuri [9, p. 79].

Informația este vulnerabilă în toate fazele obținerii, stocării și difuzării ei. Spre deosebire de amenințările tradiționale, cele la adresa securității informațiilor impun resurse mai puține și tehnici de contracarare mai ușor de ascuns și de disimulat. Acestea permit o rată de perfecționare și diversificare ridicată, dificil de urmărit și evaluat. De fapt, este motivul pentru care estimările privind amenințările la adresa informațiilor sunt dependente de factorul uman, cu întregul subiectivism și incertitudine pe care le implică [10, p. 42].

Conform lui Sergiu Popovici, director general al Centrului de telecomunicații speciale (CTS), de cele mai multe ori, o eroare banală, neintenționată poate genera un atac cibernetic de proporții. Pe de altă parte, sunt înregistrate nu puține cazuri în care angajații acționează rău intenționat împotriva angajatorului. Datele statistice internaționale prezintă o pondere de 30 % a incidentelor cibernetice cauzate de angajați rău intenționați și 11% din indiferența și neglijența din partea acestora. La nivel global, 40 % din angajați ascund informația cu privire la înregistrarea unui incident cibernetic, fapt care implică, desigur consecințe grave. Astăzi cea mai slabă verigă în procesul de asigurare a securității informaționale sunt angajații, din moment ce majoritatea scurgerilor de date confidențiale sunt legate de acțiunile angajaților rău intenționați, din neglijență sau din necunoaștere.

Conform Legii nr.299 din 21.12.2017 privind concepția securității informaționale a Republicii Moldova [11], principalele amenințări la adresa securității informaționale sunt:

1. acțiunile subversive în scopul influențării politicii interne și externe a statului;

2. amenințările hibride de securitate în scopul subminării securității naționale;

3. dominația informațională externă pe teritoriul necontrolat de către autoritățile constituționale ale Republicii Moldova;

4. elaborarea și aplicarea, de către alte state și entități, a concepției de război informațional;

5. subminarea informațională a campaniilor electorale;

job descriptions, the organization of controlled access to places where sensitive information is processed, the elaboration and retention of back-up copies, the controlled liquidation of confidential information and other measures [9, p. 79].

Information is vulnerable at all stages of its collection, storage and dissemination. Unlike traditional threats, those addressing information security require fewer resources and counter techniques that are easier to hide and dissimulate. These allow a high rate of improvement and diversification, difficult to track and evaluate. In fact, it is the reason why the estimates regarding the threats to the information are dependent on the human factor, with all the subjectivism and uncertainty that it implies [10, p. 42].

According to Sergiu Popovici, General Manager of the Special Telecommunications Center (STC), most of the times, a trivial, unintentional mistake can generate a cyber-attack of large proportions. On the other hand, there are few cases where employees act maliciously against the employer. International statistical data account for 30% of cyber incidents are caused by malicious employees and 11% of their indifference and neglect. Globally, 40% of employees hide information about the recording of a cyber-incident, which of course implies serious consequences. Today, the weakest link in the process of ensuring information security is employees, since most confidential data leaks are related to the actions of malicious employees, negligence or ignorance.

According to Law no.299 of 21.12.2017 on the conception of information security of the Republic of Moldova [11], the main threats to information security are:

1) subversive actions in order to influence the internal and external policy of the state;

2) hybrid security threats in order to undermine national security;

3) external information domination on the uncontrolled territory by the constitutional authorities of the Republic of Moldova;

4) elaboration and application, by other states and entities, of the concept of informational war;

5) informational undermining of electoral campaigns;

6) altering the content of the information

6. alterarea conținutului informațiilor vehiculate în spațiul public (prin manipulare, dezinformare, prin tăinuirea sau falsificarea informației) cu scopul de a genera panică, tensiuni ori conflicte sociale;

7. îngrădirea accesului la informațiile publice;

8. difuzarea materialelor cu caracter extremist, a pornografiei infantile și a mesajelor psihologic distructive;

9. activitatea organizațiilor extremiste și teroriste, interesul acestora privind posesia și utilizarea armei informaționale;

10. monopolul asupra formării, recepționării și/sau răspândirii informației, inclusiv prin intermediul rețelelor de comunicații electronice;

11. criminalitatea informatică transnațională, activitatea organizațiilor criminale internaționale, a grupurilor sau persoanelor, orientată spre obținerea accesului neautorizat la resursele de rețea și informație;

12. acțiunile de distrugere, deteriorare sau suprimare radioelectronică a resurselor și sistemelor informaționale, a rețelelor de comunicații electronice și a sistemelor de protecție a informației;

13. activitatea ilegală a structurilor politice, economice, militare, activitatea de spionaj a serviciilor speciale străine, a unor grupuri sau persoane, orientate spre obținerea accesului neautorizat la resursele informaționale sau obținerea controlului asupra funcționării resurselor, tehnologiei informației, sistemelor informaționale și rețelelor de comunicații electronice;

14. nivelul redus de utilizare a tehnologiilor informaționale de către autoritățile administrației publice, de către instituțiile financiare de creditare, precum și în domeniul industriei, agriculturii, educației, sănătății, deservirii populației; nivelul redus de instruire a populației privind utilizarea sistemelor informaționale;

15. diversiunile informaționale;

16. lipsa culturii de securitate informațională;

17. alocarea insuficientă a mijloacelor financiare pentru măsurile de asigurare a securității informaționale;

18. delimitarea neclară a atribuțiilor autorităților administrației publice responsabile de elaborarea și realizarea politicii de asigurare a se-

conveyed in the public space (through manipulation, misinformation, concealment or falsification of information) in order to generate panic, tensions or social conflicts;

7) restricting access to public information;

8) dissemination of extremist material, child pornography and psychologically destructive messages;

9) the activity of the extremist and terrorist organizations, their interest regarding the possession and use of the informational weapon;

10) monopoly over the formation, reception and/or dissemination of information, including through electronic communications networks;

11) transnational computer crime, the activity of international criminal organizations, groups or individuals, oriented towards obtaining unauthorized access to network and information resources;

12) the actions of destruction, deterioration or radio-electronic suppression of information resources and systems, electronic communications networks and information protection systems;

13) the illegal activity of the political, economic, military structures, the espionage activity of the special foreign services, of some groups or persons, oriented towards obtaining the unauthorized access to the information resources or gaining control over the functioning of the resources, information technology, information systems and electronic communications networks;

14) the low level of use of information technologies by public administration authorities, financial lending institutions, as well as in the field of industry, agriculture, education, health, population service; the low level of training of the population regarding the use of the information systems;

15) informational diversions;

16) lack of information security culture;

17) insufficient allocation of financial means for information security measures;

18) unclear delimitation of the attributions of the public administration authorities responsible for the elaboration and implementation of the information security policy of the Re-

curității informaționale a Republicii Moldova.

Managementul informațiilor de securitate: proceduri și mecanisme de securitate informațională

Criptarea – metodele de protecție a informațiilor se dezvoltă dinamic, devin mai complexe și se dezvoltă treptat într-o industrie separată a tehnologiilor informaționale și comunicațiilor. Pentru protecția informațiilor de securitate sunt folosite diferite instrumente criptografice [3]. Criptografia este știința și totodată arta ascunderii semnificației unei comunicări în scopul protejării ei față de interceptări neautorizate, iar prin algoritmii folosiți asigură securizarea informației prin autentificarea și restricționarea accesului într-un sistem informatic. Etimologic, cuvântul criptografie este obținut prin contopirea a doi termeni din greaca veche, unde „crypto" înseamnă „a ascunde", iar „grafik" înseamnă „a scrie", rezultând în traducere aproximativă „scriere ascunsă/secretă" [4, p. 421].

În vederea obținerii unei criptograme, asupra cuvintelor, caracterelor sau literelor conținute într-un mesaj inițial, denumit „Plain Text (PL)" se aplică o funcție criptografică/ funcție de criptare, aceasta fiind o funcție dependentă de un parametru fix numit cheie și se obține astfel mesajul criptat pe care îl vom denumi „Cipher Text (CT)". Criptogramele prezentându-se sub forma unor mesaje neinteligibile, în general, sunt împărțite în cifruri și coduri.

Controlul accesului – confidențialitatea vizează protejarea informațiilor împotriva oricărui acces neautorizat. Uneori este interpretat în mod greșit că această cerință este specifică domeniului militar și serviciilor de informații care trebuie să-și protejeze planurile de luptă, amplasamentul depozitelor de muniție sau al rachetelor strategice, notele informative. Este însă la fel de importantă pentru o organizație care dorește să-și apere proprietatea intelectuală, rețetele de producție, datele despre personalul angajat etc. Pentru o instituție publică, datorită caracterului informației pe care o gestionează, este important să asigure în primul rând integritatea și disponibilitatea datelor.

Accesul la facilitățile și serviciile oferite de sistemul informațional trebuie controlat în funcție de specificul și cerințele mediului în care își desfășoară activitatea organizația.

Controlul accesului în sine prevede în general

public of Moldova.

The Management of the Security Information: procedures and mechanisms for information security

Encryption - information protection methods are developing dynamically, becoming more complex and are developing gradually into a separate industry of information technologies and communications. Different cryptographic tools are used for the protection of security information [3]. Cryptography is the science and at the same time the art of hiding the meaning of a communication in order to protect it from unauthorized interceptions, and through the algorithms used it ensures the information security by authenticating and restricting access in a computer system. Etymologically, the word cryptography is obtained by merging two Old Greek terms where "crypto" means "to hide" and "grafik" means "to write" resulting in approximate translation of hidden/secret writing [4, p. 421].

In order to obtain a cryptogram, on the words, characters or letters contained in an initial message, called "Plain Text (PL)", a cryptographic function/ encryption function is applied, this being a function dependent on a fixed parameter called key and this result in the encrypted message we will call "Cipher Text (CT)".Cryptograms appearing in the form of unintelligible messages are generally divided into numbers and codes.

Access Control - confidentiality aims to protect information against any unauthorized access. Sometimes it is misinterpreted that this requirement is specific to the military and intelligence services that must protect their battle plans, the location of ammunition depots or strategic missiles, informative notes. However, it is equally important for an organization that wants to defend its intellectual property, production recipes, data about the employees, etc. For a public institution, due to the nature of the information it manages, it is important to ensure first and foremost the integrity and availability of data.

The access to the facilities and services offered by the information system must be controlled according to the specificity and the requirements of the environment in which the organization operates.

The access control itself generally provides

neral o gamă de reguli de acces corelate cu atribuțiile fiecărui utilizator al sistemului informatic, pentru a împiedica potențialii atacatori.

Sisteme de management al securității informației – actualitatea creării Sistemului de Management al Securității Informației (SMSI) reprezintă una dintre pietrele unghiulare cu care se confruntă oricare organizație internațională (și ar trebui să preocupe și organizațiile naționale), una dintre cele mai prioritare sarcini ale sistemului managerial de gestionare a organizațiilor. Standardele „ISO/IEC 27001:2005 (fost BS 7799-2) Sistemul de Management al Securității Informației" și „ISO/IEC 27002:2005/ Cor 1:2007 (fost BS 7799-1, ulterior, ISI/IEC 17799), Codul de practică pentru Managementul Securității Informației" sunt cele mai importante, până la ora actuală, în domeniul securității informației. Ele stabilesc un limbaj internațional comun pentru securitatea informației.

În anul 2003, Banca Națională a Republicii Moldova a fost prima din spațiul sovietic care a început să implementeze în practică cerințele ISO 17799 și BS 7799:2, obligând toate băncile să îndeplinească cerințele lui, creând SMSI pe baza standardului. Un SMSI elaborat în conformitate cu cerințele standardului ISO/IEC 27001:2005 reprezintă un sistem complex care include atât mecanismele de gestionare, cât și mecanismele de protecție a informației. Modelul procesului de realizare a SMSI presupune un ciclu perpetuu de măsuri, și anume: planificarea, realizarea, verificarea și menținerea [2].

Totuși, la crearea SMSI, este necesară luarea în considerare nu doar a regulilor enumerate mai sus, nu doar atingerea tuturor proprietăților resurselor informaționale, ci și a specificului activității. De exemplu, pentru sectorul bancar, scopul-cheie în direcția SI este asigurarea integrității informației financiare; pentru operatorii sectorului de telecomunicație – accesul la resursele informaționale, începând cu canalele de transmisie și până la serverele comerciale; pentru companiile de stat, este importantă menținerea confidențialității informațiilor etc. Acest lucru nu înseamnă că băncile nu iau în calcul accesibilitatea datelor sau că sectorul de stat nu are nevoie de menținerea integrității datelor.

În ajutorul managementului care intenfor a range of access rules correlated with the attributions of each user of the computer system, to prevent potential attackers.

Information security management systems – the actuality of the creation of the Information Security Management System (ISMS) is one of the cornerstones that any international organization (and national organizations should also concern), one of the most priority tasks of the managerial system of organizations' administration. The standards "IOS/ECI 27001: 2005 (formerly BS 7799-2) Information Security Management System" and "IOS/ECI 27002: 2005/ Cor 1: 2007 (formerly BS 7799-1, subsequently, ISI/ECI 17799), The Code of practice for the Management of Information Security" are the most important, until now, in the field of information security. They establish a common international language for information security.

In 2003, the National Bank of the Republic of Moldova was the first in the Soviet area, which began to implement the requirements of IOS 17799 and BS 7799: 2 in practice, forcing all banks to meet its requirements, creating ISMS based on the standard. An ISMS developed in accordance with the requirements of IOS/ECI 27001: 2005 represents a complex system that includes both management mechanisms and information protection mechanisms. The model of the process of carrying out the ISMS involves a perpetual cycle of measures, namely: planning, implementation, verification and maintenance [2].

However, when creating ISMS, it is necessary to take into consideration not only the rules listed above, not only the attainment of all the properties of the information resources, but also of the specific activity. For example, for the banking sector, the key purpose in the direction of IS, is to ensure the integrity of the financial information; for telecommunication operators – the access to information resources, starting with transmission channels and up to commercial servers; for state-owned companies, it is important to maintain the confidentiality of information, etc. This does not mean that banks do not consider data accessibility or that the state sector does not need to maintain data integrity.

In order to help the management that intends to ensure its continuous availability and to protect

ționează să-și asigure disponibilitatea continuă și să-și protejeze integritatea și confidențialitatea informației vine Organizația Internațională de Standardizare (ISO) cu familia de standarde ISO/IEC 27000, care oferă îndrumări bazate pe bunele practici acumulate în domeniu privind implementarea, menținerea, îmbunătățirea, evaluarea (auditul) și certificarea unui sistem de management al securității informației [1, p. 79].

Din aceste considerente, de la bun început, se iau în considerare aspectele critice cele mai importante și specifice ale instituției și prin crearea unei arhitecturi corecte, în final, poate fi obținut un SMSI eficient și sigur.

Concluzii și recomandări. Procedurile și mecanismele de management al informațiilor de securitate includ reglementări interne referitoare la relațiile dintre angajați, care ar exclude sau limita divulgarea, scurgerea sau accesul nesancționat la informații. Aceste proceduri și mecanisme includ selectarea și instruirea personalului, formularea obligațiunilor de serviciu referitoare la securitatea informației cu stipularea în contractele individuale de muncă și fișele postului, organizarea accesului controlat la locurile unde se procesează informații sensibile, elaborarea și păstrarea copiilor de rezervă, distrugerea autorizată a informației confidențiale și alte măsuri.

Problema temei cercetate constă în alinierea politicilor și procedurilor ce reglementează programul de securitate informațională și responsabilitățile de serviciu, pentru a garanta o arhitectură generală a securității informaționale. Aceste mecanisme trebuie implementate pentru a se atinge obiectivele specifice ale securității și pe cele generale ale instituției.

Practica confirmă că managerii care au implementat proceduri și mecanisme de protecție corespunzătoare, au instruit personalul privind metodele corespunzătoare ce trebuie respectate pentru a proteja informațiile împotriva amenințărilor, ca rezultat au doar beneficii. Procedurile de securitate a informațiilor trebuie să fie integrate în activitatea zilnică, iar angajații ar trebui să conștientizeze procesul de securizare ca un factor de favorizare, decât ca o limitare.

În cele din urmă, conceptul sistemului de management al informațiilor de securitate poate fi definit drept un set de norme juridice,

the integrity and confidentiality of the information, the International Organization for Standardization (IOS) comes with the IOS/ECI 27000 family of standards, which provides guidance based on the good practices accumulated in the field regarding implementation, maintaining, improving, evaluating (auditing) and certifying an information security management system [1, p.79].

From these considerations, from the beginning, the most important and specific critical aspects of the institution are taken into account and by creating a correct architecture, finally, an efficient and safe ISMS can be obtained.

Conclusion and recommendations. Procedures and mechanisms for managing security information include internal regulations regarding employees' relations, which would exclude or limit disclosure, leakage or unsanctioned access to information. These procedures and mechanisms include the selection and training of personnel, the formulation of service obligations related to information security, stipulated in the individual employment contracts and job descriptions, the organization of controlled access to the places where sensitive information is processed, the elaboration and retention of the backup copies, the authorized destruction of the confidential information and other measures.

The problem of the researched topic consists in aligning the policies and the procedures that regulate the information security program and the service responsibilities, in order to guarantee general information security architecture. These mechanisms must be implemented to achieve the specific objectives of the security and the general objectives of the institution.

The practice, confirms that the managers who have implemented appropriate procedures and protection mechanisms, have trained the staff on the appropriate methods to be followed to protect the information against threats, as a result they have only benefits. Information security procedures should be integrated into daily activity, and employees should be aware of the security process as a factor rather than a limitation.

Finally, the concept of security information management system can be defined as a set of legal, organizational, administrative and technical norms, meant to counter the threats against

organizaționale, administrative și tehnice, menite să contracareze amenințările la adresa scurgerilor de informații, pentru a minimiza impactul negativ asupra utilizatorilor și entității în ansamblu.

Considerăm că măsurile de protecție ar trebui să fie adecvate gradului de amenințare, precum și corespunzătoare importanței informației care este păstrată. Numai o analiză minuțioasă a amenințărilor și a tipurilor informațiilor de securitate poate oferi o siguranță relativă.

leaks, to minimize the negative impact on users and the entity as a whole.

We believe that the protection measures should be appropriate to the degree of threat, as well as to the importance of the information that is kept. Only a thorough analysis of threats and types of security information can provide a relative security.

Referințe bibliografice

Bibliographical references

1. Guzun Mihail, Friptuleac Lilian, Metode tehnice și manageriale ale securității informației, în revista Tehnologiile societății informaționale, p. 79.
2. http://security.ase.md/publ/ro/pubro35/Bulai_Rodica%20.pdf
3. Claudia Hlopeanicov, Mecanisme și protocoale de protecția informației în rețele și sisteme informaționale, în Revista Militară, p. 421.
4. Patriciu V.V., Ene-Pietroșanu M., Bica I., Văduva C., Voicu N. (2007) Securitatea comerțului electronic. București: Ed. All.
5. Colun Tatiana, Securitatea sistemelor informatice – pilon de bază al siguranței informaționale - 6 th International Conference ,,Telecommunications, Electronics and Informatics" ICTEI 2018, p. 356.
6. Stelian Popa, Securitatea sistemelor informatice – note de curs și aplicații, Bacău: Alma Mater, p. 6.
7. Bragaru Tudor, Briceag Valentin, Malcoci Viorel, Galaicu Valeriu, Securitatea informației vis-à-vis de securitatea informațională, în revista Studia Universitatis Moldaviae 2019, p. 40.
8. https://www.legis.md/cautare/getResults?doc_id=85988&lang=ro
9. Dr. Mihail Guzun, ing. Lilian Friptuleac, metode tehnice și manageriale ale securității informației, în revista Tehnologiile societății informaționale, p. 79.
10. Mr. conf. dr. Roceanu Ion, lt. col. Buga Iulian, Amenințări, riscuri și vulnerabilități la adresa informațiilor din sistemele de comunicații și informatice, în Revista Forțelor Terestre nr. 5-6/2003, p. 42.
11. https://www.legis.md/cautare/getResults?doc_id=105660&lang=ro

Despre autori

Liliana CREANGĂ,
doctor în drept, conferențiar universitar,
șef al Catedrei „Drept public și securitate a frontierei" Academia „Ștefan cel Mare" a MAI
e-mail: creanga_liliana@gmail.ru
tel.: 069313116

Anatoli BUZEV,
doctorand, șef adjunct direcție,
Inspectoratul General al Poliției de Frontieră a MAI al Republicii Moldova
e-mail: anatolbuzev@mail.ru
tel.: 069823874

About authors

Liliana CREANGĂ
PhD, Associate Professor, Head of the "Public Law and Border Security" Chair ,
Academy "Stefan cel Mare" of MIA
e-mail: creanga_liliana@gmail.ru
tel.: 069313116

Anatoli BUZEV
PhD Student, Deputy Chief of the Department, Border Police General Inspectorate of MIA of the Republic of Moldova
e-mail: anatolbuzev@mail.ru
tel.: 069823874