Investeşte în oameni!
FONDUL SOCIAL EUROPEAN
Programul Operaţional Sectorial Dezvoltarea Resurselor Umane 2007 – 2013
Axa prioritară 1 „Educaţie şi formare profesională în sprijinul creşterii economice şi dezvoltării societăţii bazate pe cunoaştere”
Domeniul major de intervenţie 1.5. „Programe doctorale şi post-doctorale în sprijinul cercetării”
Titlul proiectului: Burse doctorale si postdoctorale pentru cercetare de excelenta
Numărul de identificare al contractului: POSDRU/159/1.5/S/134378
Beneficiar: Universitatea Transilvania din Braşov

ȘCOALA DOCTORALĂ INTERDISCIPLINARĂ

Facultatea: INGINERIE ELECTRICĂ ȘI ȘTIINȚA CALCULATOARELOR

Constantin Adrian MANEA

CERCETĂRI PRIVIND SECURITATEA DATELOR ÎN SISTEMELE INFORMATICE

RESEARCH ON SECURITY DATA SYSTEMS

REZUMAT / ABSTRACT

Conducător ştiinţific

Prof.dr.ing. Sorin-Aurel MORARU

BRAȘOV, 2018

D-lui (D-nei) .....

COMPONENȚA

Comisiei de doctorat

Numită prin ordinul Rectorului Universității Transilvania din Braşov
Nr. 9328 din 24.07.2018

PREŞEDINTE:	Conf.dr.ing. Delia UNGUREANU Universitatea Transilvania din Brașov
CONDUCĂTOR ŞTIINȚIFIC:	Prof.dr.ing. Aurel-Sorin MORARU Universitatea Transilvania din Brașov
REFERENȚI:	Prof. univ. dr. Theodor BORANGIU Universitatea *Politehnica* din Bucuresti
	Prof. univ. dr. Mariana MOCANU Universitatea *Politehnica* din Bucuresti
	Prof. univ. dr. Decebal POPESCU Universitatea *Politehnica* din Bucuresti

Data, ora şi locul susținerii publice a tezei de doctorat: **14 septembrie 2018, ora 10.30, sala V III 9**

Eventualele aprecieri sau observații asupra conținutului lucrării vor fi transmise electronic, în timp util, pe adresa a.c.manea@unitbv.ro

Totodată, vă invităm să luați parte la şedința publică de susținere a tezei de doctorat.
Vă mulțumim.

Cercetări privind securitatea datelor în sistemele informatice

CUPRINS (limba română)

	Pg. teza	Pg. rezumat
LISTA DE ABREVIERI ȘI ACRONIME	6	9
INTRODUCERE	7	10
Motivația și oportunitatea alegerii temei	7	11
Stadiul actual al cercetărilor privind securitatea sistemelor infromatice	11	
Obiective propuse	12	11
Structura tezei	13	12
CAPITOL I SECURITATEA SISTEMELOR INFORMATICE ACTUALE ȘI SECURITATEA DATELOR	16	14
I.1 Importanța securității sistemului informatic și a bazelor de date	16	14
I.2 Securitatea sistemelor informatice vs. securitatea bazelor de date	19	15
I.2.1 Noțiunea de securitatea a informației	21	16
I.2.2 Securitatea sistemelor informatice	23	17
I.2.3 Securitatea bazelor de date	27	19
I.3 Modele de asigurare a securității sistemului informatic	30	21
I.4 Standarde, norme și politici de securitate	34	22
I.5 Vulnerabilitățile sistemelor informatice	45	24
I.5.1 Clasificarea vulerabilităților sistemelor informatice	49	25
I.5.2 Vulnerabilitățile unei rețele de comunicații	51	26
I.5.3 Securizarea rețelelor sociale	55	28
I.6 Concluzii și rezultate obținute	58	28
CAPITOLUL II: ANALIZA PRINCIPALELOR TIPURI DE ATACURI INFORMATICE	63	30
II.1 Evoluția în timp a atacurilor informatice	64	30
II.1.1 Repere în timp privind atacurile informatice	66	31
II.1.2 Tendințe viitoare privind atacurile informatice	72	33
II.1.3 Analiza amenințărilor informatice în România	73	33
II.2 Tipuri de atacuri informatice	75	34
II.2.1 Virușii informatici	76	34
II.2.2 Analiza viermilor informatici	78	35
II.2.3 Analiza cailor troieni	78	35
II.2.4 Programe de tip Adware și Spyware	79	35
II.2.5 IP Sniffing	79	36
II.2.6 Atacuri prin e-mail	80	36
II.2.7 Alte tipuri de atacuri informatice	81	36

II.3 Structura unui arbore de atac informatic 84 37
II.4 Concluzii și rezultate obținute 89 38

CAPITOLUL III: CERCETĂRI PRIVIND PRINCIPALELE METODE DE SECURITATE A SISTEMELOR INFORMATICE 91 39
III.1 Criptografia 93 39
III.2 Canale de comunicații securizate 98 42
III.3 Măsuri de securitate în rețelele virtuale 100 42
III.4 Metode de securitate în comerțul electronic 104 45
III.5 Programe antivirus vs. programe firewall 110 48
III.6 Concluzii și rezultate obținute 114 50

CAPITOLUL IV: CERCETĂRI PRIVIND CADRUL NORMATIV ACTUAL ÎN DOMENIUL SECURITĂȚII INFORMATICE 117 51
IV.1 Confortul siguranței juridice pentru operațiuni prin sisteme informatice..... 119 52
IV.1.1 Reglementarea juridică a comerțului electronic 122 52
IV.1.2 Reglementarea juridică privind protecția și prelucrarea datelor cu caracter personal 124 53
IV.1.3 Reglementarea actuală a infracțiunilor contra siguranței și integrității sistemelor informatice și datelor 129 56
IV.2 Protecția juridică a bazelor de date la nivelul Uniunii Europene 136 58
IV.2.1 Drepturile și obligațiile autorilor de baze de date vs. drepturile și obligațiile utilizatorilor de baze de date 138 59
IV.3 Jurisprudență europeană în domeniul protecției bazelor de date şi a datelor cu caracter personal 140 60
IV.4 Practica instanțelor naționale privind protecția bazelor de date și a autorilor lor 143 62
IV.5 Concluzii și rezultate obținute 144 63

CAPITOLUL V: CERCETARE CALITATIVĂ PRIVIND ASIGURAREA SECURITĂȚII DATELOR CU CARACTER PERSONALE GESTIONATE ÎNTR-UN SISTEM INFORMATIC 147 64
V.1 Metodologia cercetării calitative 150 64
V.2 Prezentarea rezultatelor și propunerea unor măsuri de asigurare a securității datelor cu caracter personal la nivelul unei instituții de învățământ superior 153 65
V.3 Concluzii și rezultate obținute 161 66

.

CONCLUZII ȘI REZULTATE GENERALE, CONTRIBUȚII PERSONALE ȘI LIMITE ALE CERCETĂRII 165 70

Concluziile și rezultate generale 171 71

Contribuții personale 174 74

Perspective de cercetare și dezvoltare ulterioară .....

BIBLIOGRAFIE 175 75

LISTA FIGURILOR 186

LISTA TABELELOR 188

Anexa I - Referințe legislative la nivelul Uniunii Europene și la nivelul României privind folosirea sistemelor informaționale și securitatea cibernetică 189

Anexa II – Tabelul 7 Cercetare calitativă – Matrice răspunsuri interviu semi-structurat 192

Anexa III – Ghid interviu semi-structurat – Cercetare calitativă 215

Anexa IV - Bune practici și recomandări a fi implementate la nivel instituțional pentru asigurarea conformității măsurilor tehnice implementate cu cadrul normativ instituit prin Regulamentul (UE) nr.679/2016 219

Anexa V - Plan de soluții tehnice minimale integrate privind securitatea și protecția prelucrării datelor cu caracter personal în acord cu prevederile Regulamentului 2016/679/UE 221

Scurt rezumat (română/engleză) 223 81

CV 224 82

Cercetări privind securitatea datelor în sistemele informatice

TABEL OF CONTENT

	Pg. Thes.	Pg. Ab.
LIST OF ABBREVIATIONS AND ACRONYMES	6	9
INTRODUCTION	7	10
Reason and opportunity of theme	7	11
Current status of research on information systems security	11	
Proposed objectives	12	11
Thesis structure	13	12
CHAPTER I THE SECURITY OF CURRENT INFORMATION SYSTEMS AND SECURITY OF DATA	16	14
I.1 The importance of security system and database	16	14
I.2 Information systems security vs. database security	19	15
I.2.1 The concept of information security	21	16
I.2.2 Information systems security	23	17
I.2.3 Database Security	27	19
I.3 Models of providing security information system	30	21
I.4 Standards, norms and security policies	34	22
I.5 Vulnerabilities of informatic systems	45	24
I.5.1 Classification vulnerabilities of informatic systems	49	25
I.5.2 Vulnerabilities of communication network	51	26
I.5.3 Securing social networks	55	28
I.6 Conclusions and results	58	28
CHAPTER II: ANALYSIS OF MAIN TYPES OF ATTACKS	63	30
II.1 The evolution of cyber attacks	64	30
II.1.1 Highlights about cyber attacks	66	31
II.1.2 Future trends on cyber attacks	72	33
II.1.3 Analyze on informatic threats in Romania	73	33
II.2 Types of informatic attacks	75	34
II.2.1 Informatic Viruses	76	34
II.2.2 Analysis of informatic worms	78	35
II.2.3 Analysis of Trojan horses	78	35
II.2.4 Adware and Spyware Programs	79	35
II.2.5 IP Sniffing	79	36
II.2.6 Informatic Attacks by e-mail	80	36
II.2.7 Other Informatic Attacks	81	36

II.3 Structure of a tree of virus attack 84 37
II.4 Conclusions and results 89 38

CHAPTER III: CERCETĂRI PRIVIND PRINCIPALELE METODE DE SECURITATE A SISTEMELOR INFORMATICE 91 39
III.1 Cryptography 93 39
III.2 Secure communication channels 98 42
III.3 Security precautions on virtual networks 100 42
III.4 Security methods in e-commerce 104 45
III.5 Antivirus vs. firewall programs 110 48
III6. Conclusions and results 114 50

CHAPTER IV: RESEARCH ON THE NORMATIVE FRAMEWORK IN THE DOMAIN OF INFORMATICS SECURITY 117 51
IV.1 Comfort of legal saftey for operations through computer systems 119 52
IV.1.1 Legal regulation of electronic commerce 122 52
IV.1.2 Legal regulation of protection and processing of personal data 124 53
IV.1.3 Legal regulation of offenses against the security and integrity of information systems and data 129 56
IV.2 Legal protection of databases in the European Union 136 58
IV.2.1 Rights and obligations of authors of databases vs. rights and obligations of users of databases 138 59
IV.3 European law on the protection of databases and personal data 140 60
IV.4 Practice of the national courts on the protection of databases and their authors 143 62
IV.5 Conclusions and results 144 63

CHAPTER V: QUALITATIVE RESEARCH CONCERNING THE SAFETY OF PERSONAL DATA MANAGED IN A COMPUTER SYSTEM 147 64
V.1 Qualitative Research Methodology 150 64
V.2 Presentation of the results and the proposal of measures to ensure the security of personal data at the level of higher education institutions 153 65
V.3 Conclusions and results 161 66

GENERAL CONCLUSIONS AND RESULTS, PERSONAL CONTRIBUTIONS AND PERSPECTIVES OF RESEARCH 165 70
General Conclusions and Results 165 70
Personal Contributions 171 71
Perspectives of Research 174 74

REFERENCES 175 75
LIST OF FIGURES 186

APPENDICES

Appendices 1, References to legislation at EU level and in Romania on the use of information systems and cyber security 189
Annex 2, Table 7 Qualitative research - Matrix answers semi-structured interview 192
Annex 3, Interview guide – qualitative research 215
Annex 4, Best practices and recommendations to be implemented at institutional level to ensure compliance of technical implemented measures with the regulatory framework established by Regulation (EU) nr.679 / 2016 219
Annex 5, Plan of minimal technical solutions integrated security and protection of personal data processed in accordance with Regulation 2016/679 / EU 221

Abstract 223 81
Curriculum Vitae 224 82

Cercetări privind securitatea datelor în sistemele informatice

LISTĂ DE ABREVIERI ŞI ACRONIME

Alin.	Aliniat
Art.	Articol
BD (engl. DB)	Bază de date (engl. data base)
CE	Comisia Europeană
CERT (engl.)	Echipă Răspuns la Urgențe Cibernetice (*Computer Emergency Response Teams)*
DDoS	Distributed Denial of Service
ENISA (engl.)	Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (European Network and Information Security Agency)
GDP**R** (engl.)	General Data Protection Regulation (Regulamentul general privind protecția datelor cu caracter personal)
HTTP	HyperText Transfer Protocol
HTML	HyperText Markup Language
I**S**P	Internet Service Provider
I**P**	Internet Protocol
I**S**O (engl.)	Organizația Internațională pentru Standardizare
I**T**	Tehnologia Informației , acronim engl. *Information Technology*
JO**U**E	Jurnalul Oficial al Uniunii Europene/Comunității Europene
LAN (e**n**gl**)**	Local Area Network
MAC (eng**l**)	Cod de autentificare a mesajului
MDC **(**engl)	Cod de manipualre-detecție
NASA	National Aeronautics and Space Administration (SUA)
OECD (engl)	Organizația pentru Cooperare și Dezvoltare Economică (Organization for Economic Co-operation and Development)
P**I**I	Informații cu privire la Identificarea Personală (ISO27018)
RNCI**S**	Registrul Național al Calificărilor din Învățământul Superior
S**G**BD/D**B**MS	Sistem de gestiune a bazelor de date
S**E**AP	Sistemul Electronic de Achiziții Publice din România
S**M**C	Sistem de Management a Calității
S**M**I	Sistem de Management Integrat
S**MM**	Sistem de Management a Mediului
S**MS**I	Sistem de Management al Securității Informației
S**MS**S**M**/O**H**S**A**S	Sistemul de Management al Sănătății și Securității în Muncă
SNEP	Sistemul Național Electronic de Plată online a taxelor și impozitelor
SSR	Site-uri de socializare în rețea
TFUE	Tratatul privind funcționarea Uniunii Europene
TIC	Tehnologia Informației și Comunicației
TUE	Tratatul asupra Uniunii Europene
UE	Uniunea Europeană
U**E**FISCDI	Unitatea Executivă pentru Finanțarea Învățământului Superior, a Cercetării Dezvoltării și Inovării
U**N**ESC**O**	Organizația Națiunilor Unite pentru Educație, Știință și Cultură
VPN (e**n**gl.)	Rețea Privată Virtuală (engl. Virtual Private Network)
W**W**W/w**w**w	World Wide Web

Cercetări privind securitatea datelor în sistemele informatice

INTRODUCERE

Internetul a devenit în prezent un fenomen social, prin prezența în structura sa a utilizatorilor, din ce în ce mai numeroşi. "*Odată instaurat în fibrele societății, Internetul a produs şi produce consecințe noi pentru societate",* afirma acad. Mihai Drăgănescu susținând faptul că dezvoltarea actuală a Internetului se datorează în egală măsură factorilor sociali care de-a lungul anilor s-au îmbinat cu cei tehnologici, pe fondul procesului de globalizare [28], conturându-se astfel, în prezent, spațiul cibernetic global. Societatea contemporană, dependentă de informație, nu poate subzista în afara spațiului cibernetic, fie cel național, fie cel global, fapt pentru care securizarea spațiului cibernetic, indiferent de nivel, este și va fi permanent o preocupare comună public-privat, deoarece problema securității informațiilor este abordată și din perspectiva partajării informațiilor sau interconectării rețelelor private cu serviciile și platformele publice conținând baze de date.

În egală măsură putem aborda Internetul atât ca o resursă internațională, alături de resursa umană și capital, cât și ca o piață internațională în continuă extindere [26], Internetul fiind în egală măsură un fenomen global, dar și factor al globalizării. Astfel, Internetul, această infrastructură masivă de rețele, a schimbat modul în care societatea actuală abordează educația, mediul de afaceri și activitățile din domeniul public, dându-se noi valențe principiului interconectării.

Internetul, prin resursele sale informaționale și serviciile de comunicații oferite a transformat informația în resursă-cheie și factor de producție în economia digitală, a schimbat coordonatele societății industriale, specifică sfârșitului mileniului II, reașezând între factorii de producție informația, separată de cele mai multe ori de suportul fizic, și asigurând astfel tranziția spre actuala societate informațională.

Preocuparea recentă, atât la nivel juridic cât și la nivelul tehnicilor de securitate IT, în mileniul III, fie că este vorba de activități economice, fie de acțiuni de socializare care se desfășoară prin intermediul Internetului și al rețelelor de calculatoare, este cea a asigurării securității, integrității și confidențialității datelor cu caracter personal ale persoanelor fizice, date gestionate, arhivate și prelucrate într-un sistem informatic. Această preocupare se datorează faptului că prin tehnicile de prelucrare a datelor s-a ajuns la o ingerință în viața privată a utilizatorilor unei rețele, prin folosirea datelor cu caracter personal (bunuri proprii) fie de către operatorii economici, care urmăresc obținerea de profituri financiare, sau manipularea opiniei publice și gestionarea tendințelor comportamentale identificate prin prelucrarea datelor personale, fie de către agenții de amenințare care, accesând ilegal datele personale, le folosesc în scopuri ilegitime, uneori chiar pentru a-și ascunde identitatea.

Din această perspectivă, unul din deziderateleRegulamentului UE nr.2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date, document cunoscut drept *GDPR* (în vigoare pentru statele membre UE din data de 25 mai 2018), este acela că, din punct de vedere tehnologic, trebuie asigurată o protecție

neutră persoanelor fizice și care să nu depindă de tehnologiile utilizate pentru prelucrarea datelor cu caracter personal.

Securitatea sistemelor informatice este în egală măsură o problemă tehnică, deși uneori la echipamente tehnice performante securitatea se poate asigura cu mijloace ieftine (soluții software accesibile), cât și o problemă umană, care impune o anumită viziune managerială privind accesul și controlul accesului la sistemele informatice ale unei organizații.

OBIECTIVELE TEZEI

Primul obiectiv al tezei, pornind de la scopul propus de a demonstra necesitatea și oportunitatea abordării interdisciplinare privind protecția și securitatea informațiilor în sistemele informatice, coroborându-se soluțiile tehnice, adoptate și adaptate în timp în raport cu vulnerabilitățile și atacurile informatice, cu reglementarea juridică a activității în spațiul cibernetic, este de a propune recomandări privind asigurarea securității sistemului informatic în cadrul unui sistem de management integrat (capitolul I.6), precum și recomandări privind principiile și limitele unui cadru normativ minimal necesar, inclusiv la nivel european, care să reglementeze domeniul securității informatice, în scopul diminuării riscurilor vulnerabilității unui atac informatic (capitolul IV.5).

În acest sens, sunt studiate vulnerabilitățile sistemelor informatice și principalele tipuri de atacuri informatice, precum și metode de securitate a sistemelor informatice și a rețelelor. De asemenea, este analizat cadrul normativ european și practica instanțelor de judecată privind bazele de date și drepturile autorilor și utilizatorilor acestora, raportat la legislația națională și la jurisprudența din România, fiind identificate anumite lacune, atât din punct de vedere tehnic (în capitolul III.6), cât și juridic (capitolul IV.1.3 și capitolul IV.2), lacune care necesită concentrarea în viitor a cercetărilor într-o manieră interdisciplinară în domeniul securității sistemelor informatice

Al doilea obiectiv al tezei este reprezentat de propunerea unei soluții integrate privind asigurarea integrității și confidențialității datelor cu caracter personal prelucrate printr-un sistem informatic (formulate sub forma unui set de 15 măsuri tehnice), respectiv a securității informațiilor conținute pe un terminal integrat într-un sistem informatic instituțional princ are se prelucrează date cu caracter personal.

Pornind de la ipoteza că actuala reglementare la nivel european privind protecția datelor cu caracter personal (în vigoare din luna mai 2018), inclusiv în privința prelucrărilor prin sisteme informatice, obligă operatorii, indiferent de domeniul public sau privat, care folosesc în activitatea proprie datele personale ale clienților și ale angajaților la maximă transparență, securizare și protecție în privința prelucrărilor de date cu caracter personal, inclusiv prin regimul sancționator considerabil impus prin Regulamentul UE nr.2016/679, obiectivele cercetării calitative realizate la nivelul celor 12 instituții de învățământ din sistemul național au fost :

- Analiza informațiilor/datelor cu caracter personal cu regim special de securitate în privința colectării și prelucrării lor prin sisteme informatizate;
- Indetificarea măsurilot tehnice și administrative actuale folosite la nivelul operatorilor de date cu caracter personal pentru asigurarea protecției și confidențialității datelor și prelucrărilor;
- Identificarea măsurilor tehnice necesare a fi implementate pentru ca sistemul informatic actual și aplicațiile IT ale universităților prin care se prelucrează date personale să corespundă cadrului normativ al Regulamentului UE nr.679/2016.

STRUCTURA TEZEI

Teza are cinci capitole de bază, la care se adaugă introducerea și, în final, concluziile generale și contribuțiile personale.

Primul capitol abordează problematica securității datelor și informațiilor, precum și a securității actuale a sistemelor informatice, fiind abordate noțiunile de securitate a datelor, ca suport formal al informațiilor și obiect al prelucrărilor automate, și de securitate a sistemelor informatice, în contextul actual al standardelor privind managementul securității informatice. De asemenea, pornind de la analiza vulnerabilităților sistemelor informatice, în scopul asigurării protecției datelor informatice am conturat în capitolul I.5.3 unele măsurile privind securitatea utilizatorilor într-o rețea socială, iar în capitolul I.6 sunt cuprinse recomandări pentru implementarea unui sistem de management integrat, drept soluție de politică organizațională privind securitatea unui sistem informatic.

Scopul principal al analizei realizate în capitolul al doilea este de a surprinde evoluția în timp a atacurilor informatice, urmărindu-se identificarea unei tipologii a amenințărilor pornind de la o analiză tehnică a tipurilor de atacuri informatice (viruși, viermi informatici, cai troieni, atacuri prin e-mail) și evoluția acestora în timp, analiză de care am ținut cont și în soluțiile tehnice pe care le-am propus în capitolul V.2.

În cadrul capitolului al treilea, continuând cercetarea din capitolul anterior privind atacurile informatice și consecințele lor asupra utilizatorilor, am analizat principalele metode de securizare a sistemelor informatice pornind de la criptografiere, ramură a matematicii care se ocupă de securitatea informației concomitent cu măsuri de autentificare și restricționare a accesului într-un sistem informatic, incluzând și semnătura digitală ca mecanism de securitate, continuând cu mecanismele de securitate în rețele virtuale private și canale de comunicații securizate și încheind cu analiza programelor antivirus și de tip firewall.

Și pentru că dezvoltarea atacurilor informatice în timp, generate de exploatarea vulnerabilităților sistemelor informatice, prin modul de operare al agenților de amenințare și efectele produse, la nivelul micro al utilizatorului afectat și la nivelul macro al societății interconectate prin

Internet, au generat fenomenul criminalității informatice, în **ca**pito**lul** al patrulea am realizat o analiză a cadrului normativ actual privind reglementarea națională și europeană în domeniul securității informatice, inclusiv din perspectiva dreptului penal care a instituit măsuri corective în cazul infracțiunilor contra siguranței și integrității sistemelor informatice și a datelor. Din analiza realizată a rezultat că reglementarea juridică a faptelor prin care se săvârșesc atacurile informatice a fost precedată de dezvoltarea și propagarea acestor atacuri în sistemele informatice operaționale, pentru ca ulterior aspectele juridice să se contureze în timp drept metode de probare științifică pentru prelucrarea, interpretarea și utilizarea probelor tehnice care permit descrierea concluzivă a unui atac cibernetic, rezultatele analizei susținând astfel necesitatea abordării interdisciplinare a securității datelor și informațiilor în sistemele informatice actuale.

Capitolul al cincilea cuprinde o cercetare de tip calitativ privind măsurile necesare și adecvate asigurării securității prelucrărilor de date cu caracter personal prin sisteme informatice la nivelul unui operator, sens în care a fost folosit un interviu semi-structurat urmărindu-se identificarea opiniilor, soluțiilor practice și poziției argumentate ale unor angajați din structuri identice la nivelul a douăsprezece instituții de învățământ autohtone (compartiment resurse umane, birou IT/de securitatea tehnologică și secretar șef universitate).

În cadrul capitolului V au fost formulate ipotezele de lucru și obiectivele cercetării calitative propuse, iar prin analiza răspunsurilor primite am formulat concluziile personale privind măsurile necesare a fi implementate pentru asigurarea și tehnică a prelucrărilor de date personale în acord cu dispozițiile Regulamentului UE nr.2016/679. Astfel, am îndeplinit obiectivul al doilea propus prin teză, respectiv am propus o soluție integrată sub forma unui set de 15 măsuri tehnice necesare pentru asigurarea integrității și confidențialității datelor cu caracter personal prelucrate printr-un sistem informatic în cazul instituțiilor de învățământ superior de stat, soluții care pot fi generalizate, coroborat însă cu scopul prelucrării, și la alte sisteme informatice prin care se prelucrează date cu caracter personal de către alți operatori.

În finalul lucrării au fost concetrate într-o secțiune separată concluziile generale și rezultatele obținute conturându-se astfel atingerea obiectivelor propuse, contribuțiile personale și direcțiile viitoare de cercetare, precum și diseminarea rezultatelor obținute în timpul studiilor de doctorat (articolele și participările la conferințele naționale și internaționale).

MULȚUMIRI

Doresc să adresez mulțumiri domnului prof.dr.ing. Sorin-Aurel Moraru pentru ajutorul și sprijinul oferit pe parcursul studiilor doctorale. De asemenea, mulțumirile mele le adresez și cadrelor didactice care prin răbdare și înțelegere m-au îndrumat pe parcursul anilor: prof.dr.ing. Delia Ungureanu, prof.dr.ing. Liviu Perniu și conf.univ.dr. Dominic Kristaly. Nu în ultimul rând, mulțumesc familiei și prietenilor pentru suportul pe care mi l-au oferit pe parcursul elaborării tezei.

Cercetări privind securitatea datelor în sistemele informatice

CAPITOLUL I

SECURITATEA SISTEMELOR INFORMATICE ACTUALE

ȘI SECURITATEA DATELOR

Societatea actuală este dependentă de informația electronică complexă și de comunicarea acesteia, după stocare și prelucrare, prin rețele de comunicare securizate, astfel încât toate organizațiile actuale (de la agenți economici la instituții și autorități publice) folosesc informația digitală, ca resursă informațională a mediului Internet. Și dacă mediul socio-economic actual utilizează informațiile și cunoștințele ca și *capital intelectual* al organizațiilor, ca și resurse intangibile și imateriale generatoare de plus-valoare pe piața serviciilor și produselor, gestionarea acestor informații și cunoștințe necesită instrumente specifice la nivelul proceselor manageriale și operative, respectiv sistemele informatice.

I.1 Importanța securității sistemului informatic și a bazelor de date

În societatea actuală informația este monedă de schimb şi totodată materie primă, iar pentru entitățile juridice este asimilată bunurilor incorporale; granițele fizice în domenii precum comerțul, comunicațiile sau afacerile internaționale sunt desființate de Internet; treptat spațiul cibernetic devine spațiu social, de afaceri, de divertisment, de muncă, şi chiar de educație. Toate aceste transformări sociale, economice şi tehnologice sunt girate, pe de o parte, de către legiuitori, care reglementează cadrul normativ necesar asigurării securității tranzacționării în mediul virtual, gestionării informațiilor organizațiilor şi prevenirii fraudelor informatice, iar pe de altă parte, de către specialiştii IT care caută să dezvolte permanent tehnologiile de accesare, arhivare şi prelucrare a datelor cu ajutorul calculatoarelor, dar şi să crească securitatea sistemelor informatice şi a rețelelor de calculatoare.

Chiar dacă uneori nu recunoaştem, treptat în activitățile noastre cotidiene şi ale entităților juridice suntem dependenți de accesul şi prelucrarea rapidă a informației, tot mai multă informație fiind stocată, prelucrată şi transmisă electronic, fapt pentru care creşte tentația accesării ilegale, însuşirii sau modificării informației în formă electronică, în condițiile în care Internetul preia tot mai mult din activitățile economice ale societății, asigurând profituri economice şi avantaje concurențiale.

Pornind de la aptitudinea individului de a socializa, se găsește răspunsul privind dezvoltarea rapidă şi în ritm exponențial a rețelelor de calculatoare, prin care indivizii comunică şi interacționează pe diverse domenii, și astfel se înțelege evoluția rapidă a conectivității de la LAN –uri (Local Area Network) la Internet.

Recunoscută drept un concept multidimensional, securitatea este întâlnită în majoritatea domeniilor de activitate (în politică, în diplomație, în economie, în domeniul apărării militare, în cultură, în ştiință), iar după specificul fiecărui domeniu se impune adoptarea de măsuri care să promoveze în

siguranță și să garanteze interesele și scopurile specifice fiecăreia. Funcționarea optimă a societății presupune interconectivitatea acestor sectoare, și chiar o dependență între ele, ceea ce sporește necesitatea de securizare sectorială, dublată de o securizare și la nivelul societății.

I.2 Securitatea sistemelor informatice vs. securitatea bazelor de date

Datele, ca seturi de fapte eterogene referitoare la un anumit proces sau eveniment reprezintă suportul formal al informațiilor, deoarece neprelucrarea automată a datelor în informație digitală (formă binară separată de suportul fizic prin codificare și criptarea modalităților de acces și utilizare) reduce relativ considerabil utilitatea datelor în actuala societate. Astfel, informațiile sunt superioare tehnic și calitativ datelor, prezintă grad de noutate, sunt asociate unui anumit scop (economic, social, politic, etc.) și sunt organizate ca și colecții de date, respectiv baze de date, fiind un bun imaterial al unei organizații în activitatea acesteia. Ca și bunurile materiale, informația intangibilă se produce, se prelucrează, se distribuie și se utilizează, se arhivează, devenind astfel perisabilă în timp.

Pe lângă date și informații, specifice societății informaționale, actuala societate a cunoașterii, grefată pe societatea informațională, folosește ca și resursă cunoștințele, în sensul de informație cu înțeles și care acționează [8], deoarece în mediul socio-economic actual informațiile și cunoștințele au devenit resurse de producție imateriale, generatoare de valoare în cadrul proceselor de afaceri, având ca rezultat produse și servicii care utilizează intensiv date și cunoștințe precum cărțile de credit, sistemele de rezervări automate în diferite sectoare sau sisteme de comerț electronic.

Având în vedere procesele tehnice de prelucrare a datelor de intrare cu ajutorul calculatoarelor electronice se poate stabili o relație piramidală între date, informații și cunoștințe [44], relație regăsită în Figura1.

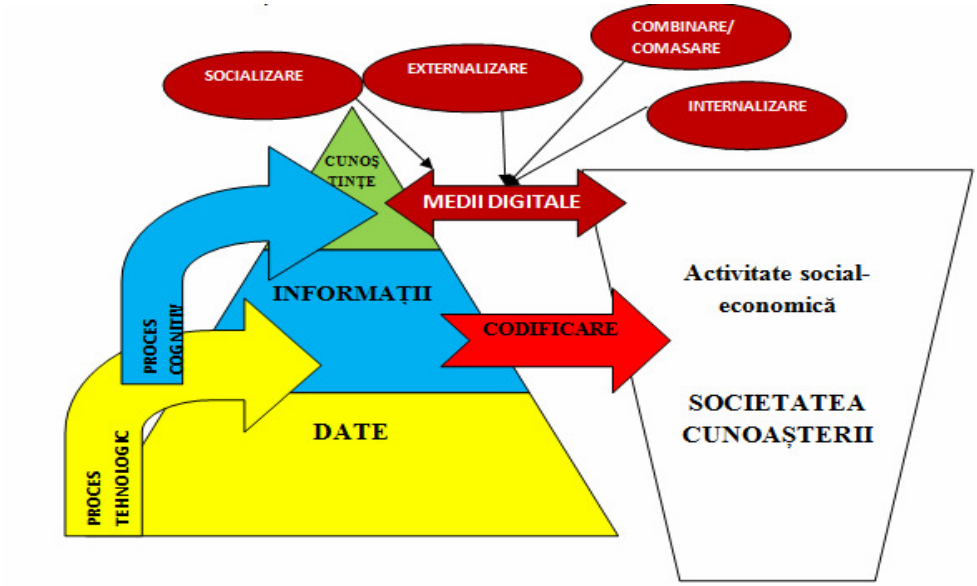

Figura 1 Relația date-informații-cunoștințe în Societatea Cunoașterii

Cercetări privind securitatea datelor în sistemele informatice

În cadrul oricărei activități deciziile sunt luate în baza informațiilor obținute din prelucrarea datelor, fapt pentru care prelucrarea datelor elementare sau de intrare pentru a obține informațiile prelucrate presupune o suită de operații: de la operațiile de identificare sau codificare a datelor prin care sunt generate datele de bază, apoi operațiile de colectare prin diferite criterii a datelor obținându-se datele pentru prelucrare, operațiile de procesare în urma cărora se obțin informațiile brute spuse în final unor operații de transmitere la locul, momentul și în forma dorită a informațiilor prelucrate [36].

I.2.1 Noțiunea de securitate a informației

Conceptual, securitatea informației se referă la "asigurarea integrității, confidențialității şi disponibilității informației"[37]. Asigurându-se securitatea informației, implicit este protejat şi utilizatorul sau destinatarul acelei informații de diverse atacuri şi amenințări. Informația ca produs al prelucrării automate a datelor, şi implicit drepturile care derivă din proprietate intelectuală, trebuie protejate indiferent de mijloacele şi metodele în care acestea sunt transmise, arhivate sau prelucrate.

Având în vedere circulația on-line a informației, problema securității informației trebuie abordată luând în calcul partajarea informațiilor sau conectivitatea rețelelor private cu diferite platforme sau servicii publice on-line [20].

Abordând problema securității informației, indiferent de sistem sau metodă, trebuie urmărite şi menținute trei proprietăți [28] (Figura 2) :

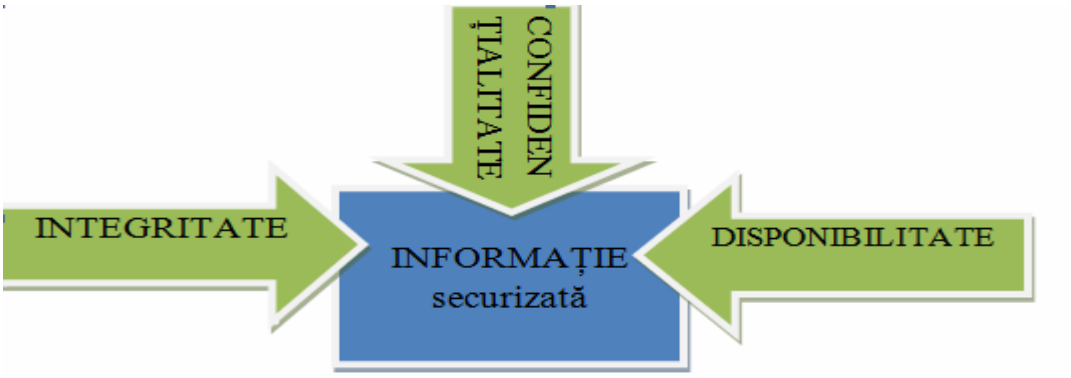

Figura 2 Proprietățile informației securizate

Confidențialitatea informației: proprietatea ca o informație să nu fie dezvăluită sau disponibilă persoanelor sau proceselor neautorizate, sau altfel spus controlarea dreptului ca o informație să fie citită/accesată în mod autorizat de către administratorul sistemului;

Integritatea informației: proprietatea informației de a păstra acuratețea şi completitudinea metodelor prin care se prelucrează informațiile, în condițiile în care identificarea și autentificarea utilizatorilor sunt elemente cheie;

Disponibilitatea informației: proprietatea informației de a fi accesibilă şi utilizabilă la cerere de către o entitate autorizată.

Din perspectiva securității informației, alte două categorii de proprietăți sunt avute în vedere de alți autori [2], și anume :

Legitimitatea folosirii informației: informațiile sunt folosite numai în scopuri legitime de către persoanele autorizate și autentice;

Non-repudierea informației: niciuna din părțile atestate și implicate în folosirea și transmiterea unei informații nu va putea tăgădui participarea sau acțiunile întreprinse.

Asigurarea securității informației nu este doar o problemă de tehnică, ci este totodată o problemă de management ce implică decizia conducerii unei organizații cu privire la politica de securitate și măsurile adoptate în acest sens luându-se în considerare pe de o parte amenințările existente, pe de altă parte metodele de acces și sursele de informații.

I.2.2 Securitatea sistemelor informatice

Conform definițiilor legale (Regulamentul (CE) nr.460/2004), prin „sistem informatic" se înțelege „*calculatoarele şi reţelele de comunicaţii electronice, precum şi datele electronice stocate, prelucrate, regăsite sau transmise de acestea în scopul funcţionării, folosirii, protecţiei şi întreţinerii lor*". În acelaşi ton, Regulamentul (CE) nr. 460/2004 definea inițial în art.4 „securitatea rețelelor informatice și a datelor" drept „*capacitatea unei rețele sau a unui sistem informatic de a rezista, la un nivel de încredere dat, la evenimente accidentale sau la acțiuni ilegale sau răuvoitoare care compromit disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor stocate sau transmise și a serviciilor conexe oferite sau accesibile prin aceste rețele și sisteme*". Prin „rețea" textele legale definesc *sistemele de transmisie și, acolo unde se aplică, echipamentele de comutare sau direcționare și alte resurse care permit transportul semnalelor prin cabluri, prin unde radio, prin mijloace optice sau alte mijloace electromagnetice, inclusiv rețelele de satelit, rețelele terestre fixe* (cu circuite și pachete comutate, inclusiv Internetul) *și mobile, sistemele de cabluri electrice*, în măsura în care sunt folosite în scopul transmiterii de semnale, rețelele folosite pentru transmisiile prin radio și televiziune și rețelele de televiziune prin cablu, indiferent de tipul informațiilor transportate [20].

În legislația comunitară în vigoare la acest moment, Regulamentul (UE) nr. 526/2013, nu mai regăsim definiții ale noțiunilor de sistem informatic sau securitate a rețelelor informatice, însă în legislația românească (Hotărârea Guvernului nr.494/2011, publicată în Monitorul Oficial nr.388 din 02.06.2011, și Hotărârea Guvernului nr.271/2013, publicată în Monitorul Oficial nr.296 din 23.05.2013) întâlnim aceleași definiții cu privire la infrastructuri cibernetice, spațiu cibernetic și securitate cibernetică. Astfel, în art.2 din HG nr.494/2011 infrastructurile cibernetice sunt definite drept "*infrastructuri de tehnologia informației şi comunicații, constând în sisteme informatice, aplicații aferente, rețele şi servicii de comunicații electronice",* în timp ce mediul virtual generat de infrastructurile cibernetice și care include informațiile procesate, stocate sau transmise și acțiunile utilizatorilor reprezintă spațiul cibernetic, un spațiu virtual și nemărginit geografic.

Cercetări privind securitatea datelor în sistemele informatice

Corelată celor două noțiuni și definită după acestea tot în art.2 lit.(e) din HG nr.494/2011, securitatea cibernetică reprezintă o *stare de normalitate, urmărită a fi asigurată prin aplicarea unor măsuri proactive și reactive în scopul asigurării confidențialității, integrității, disponibilității, autenticității și asumării informațiilor în format electronic, a resurselor și serviciilor publice sau private gestionate și desfășurate în spațiul cibernetic*. Asimilând terminologia juridică situațiilor practice, putem conchide că securitatea cibernetică reprezintă situația generală, normală și de drept a spațiului cibernetic, situațiile excepționale fiind reprezentate de atacurile cibernetice.

Abordând problema securității sistemelor informatice avem în vedere trei aspecte ce trebuie combătute simultan de administratorul unui sistem pentru a beneficia de încrederea utilizatorilor acelui sistem: vulnerabilitatea sistemului, amenințarea și atacul potențial. Dacă în privința vulnerabilității unui sistem cele trei puncte slabe ce trebuie avute în vedere sunt deficiențe tehnologice, deficiențele la configurare și deficiențele asupra politicilor de securitate, în privința amenințărilor și atacurilor, acestea sunt imprevizibile, căci nu se poate stabili cu exactitate un profil al persoanei interesate de accesarea neautorizată a unui sistem informatic și nici nu se pot identifica cu precizie, de la un sistem la altul, instrumentele – scripturile și programele – prin care se vor declanșa atacurile.

În cazul sistemului informatic, modelul de securitate poate fi văzut ca având mai multe straturi interdependente ce reprezintă niveluri de securitate (securitate fizică și securitate logică) și care înconjoară subiectul ce trebuie protejat, fiecare nivel izolând subiectul și făcând mai dificil accesul decât modul în care a fost prevăzut și gândit accesul autorizat [28]. La acestea două, am adăuga și nivelul de securitate juridică, nivel care reprezintă cadrul legal național și internațional de norme care reglementează actele de încălcare a nivelelor de securitate fizică și logică și prin care se stabilește regimul răspunderii penale pentru delictul informatic.

Nivelul exterior al modelului de securitate și prima barieră în calea accesului neautorizat este reprezentat de securitatea fizică și constă, în general, măsuri de prevenire a accesului neautorizat la echipamentele de calcul prin asigurarea pazei și controlul accesului în ariile unde sunt amplasate echipamentele sistemului informatic. Tot o problemă de securitate a sistemului la nivel fizic este întreținerea echipamentelor în concordanță cu specificațiile tehnice de folosire și numai de către personal specializat și autorizat.

Cel de-al doilea nivel de securitate în cazul sistemelor informatice, nivelul logic al securității, constă în metode software de control a accesului la resursele și serviciile sistemului, și este împărțit, la rândul său, în două sub-niveluri : nivelul de securitate a accesului la sistem și nivelul de securitate a serviciilor puse la dispoziție de sistemul informatic utilizatorilor săi [29].

Securitatea accesului constă în disponibilitatea de a controla, verifica și stabili drepturi de acces ale utilizatorilor, cel mai înalt nivel de securitate fiind *nivelul de acces la sistem* (NAS), nivel

răspunzător de accesibilitatea rețelei către utilizatori și de gestiunea accesului, putând dispune decuplarea unei stații individuale/utilizator dacă nu-i sunt asociate drepturi de acces [44].

Accesul controlat la serviciile unui sistem (intrările/ieșirile la disc, gestiunea serverului) este asigurat prin nivelurile de securitate a serviciilor, cel mai înalt nivel de securitate fiind *nivelul de control al serviciilor* (NCS) responsabil de raportarea stării serviciilor și de funcțiile de avertizare, putând activa sau dezactiva anumite servicii.

Studiile arată că în medie 90% din breşele de securitate identificate nu sunt datorate problemelor tehnologice, ci instalării şi configurării necorespunzătoare sau datorită nerespectării unor proceduri de utilizare şi administrare a sistemului, instruire deficitară a utilizatorului sau înțelegere greșită a modului de funcționare.

I.2.3 Securitatea bazelor de date (BD)

Aceleași principii fundamentale pe care se bazează securitatea informatică le regăsim și cu privire la securitatea bazelor de date, respectiv confidențialitatea, integritatea și disponibilitatea, asigurate prin intermediul sistemului de gestiune al bazei de date (SGBD/DBMS) care este o interfață între utilizatorii BD-urilor și sistemul de operare.

- Confidențialitatea datelor asigurată prin SGBD presupune blocarea accesului anumitor categorii de utilizatori la date pe care nu trebuie să le acceseze, fie pentru că nu au asociate drepturi de acces (nu au fost cerute, nefiindu-le necesare în activitatea proprie sau SGBD nu permite accesul decât condiționat), fie pentru că nivelul de confidențialitate asociat datelor este ridicat și presupune proceduri de acces de nivel ridicat.
- Disponibilitatea datelor are în vedere caracterul accesibilității simultane de către utilizatori diferiți a bazei de date și într-un timp util, în funcție de operațiunea aplicată asupra bazei de date, astfel încât asigurarea disponibilității datelor este o cerință intrinsecă pentru asigurarea securității unei baze de date.
- Integritatea bazelor de date vizează corectitudinea informațiilor și presupune detectarea, corectarea și prevenirea erorilor care pot afecta datele dintr-o bază de date. Când se fac referiri la integritatea datelor, de fapt se au în vedere regulile definite în majoritatea SGBD-urilor drept constrângeri de integritate care sunt verificate de sistem în legătură cu datele astfel încât baza de date este protejată de operațiile care nu corespund restricțiilor. De asemenea, condițiile de integritate asociate datelor în funcție de obiectivul SGBD–ului numite și constrângeri/restricții de integritate nu permit ca într-o bază de date să fie introduse date aberante, asigurându-se astfel și corectitudinea datelor.

Cercetări privind securitatea datelor în sistemele informatice

O serie de condiții sunt de tip structural, legate de anumite egalități între valori, și exprimate prin dependențe funcționale sau prin declararea unor câmpuri cu valori unice (de cele mai multe ori aceste câmpuri sunt chei). O altă serie de condiții se determină după unitatea la care se aplică restricția și, în acest caz, există restricții pe domenii (acestea privesc anumite valori de același tip având o anumită semnificație din care își iau valori atributele relațiilor) sau restricții pe tabele (relații). La rândul lor, restricțiile pe tabele pot fi unituplu (se referă la fiecare tuplu în parte – listă ordonată de *n* valori) sau multituplu (se referă la combinații de mai multe tupluri).

Constrângerile de domeniu sunt condiții impuse valorilor atributelor, în timp ce constrângerile de tuplu presupun existența unei chei și a unei chei secundare în condițiile în care tuplurile unei relații sunt distincte (nu există două sau mai multe tupluri care să conțină aceeași combinație de valori ale tuturor atributelor).

Un exemplu de restricție de integritate de relație de tip multituplu este restricția referențială care se exprimă prin condiția ca, pentru cheile externe, dacă nu sunt nule, să se admită valori corespunzătoare uneia din cheile primare existente în relația referită. Verificarea acestei condiții are loc ori de câte ori se inserează un nou tuplu ce conține o cheie externă sau se modifică valoarea unei chei externe a unui tuplu, semnalându-se eventualele neconcordanțe și anulând modificările. Verificarea unicității cheii primare și restricțiile rezultate din dependențele funcționale și multivaloare sunt alte exemple de același tip.

Din perspectiva comunicațiilor prin intermediul rețelelor publice, din cauza accesului multiplu și concomitent care poate genera interceptarea și modificarea datelor utilizatorilor, integritatea datelor trebuie asigurată de către sistemul de gestiune al bazelor de date folosite și accesibile în rețea, fapt pentru care administratorii de astfel de rețele trebuie să abordeze integritatea datelor cu maximă importanță. În acest sens, se poate folosi fie tehnica hash, pentru a se preveni modificarea unui mesaj sau pentru a se putea verifica dacă mesajul recepționat este identic cu mesajul transmis, fie tehnica rezumatului, aceasta permițând generarea unei secvențe de identificare a datelor transmise către emitent, denumită „rezumatul datelor".

Rezumatul unui mesaj se construiește prin aplicarea unei funcții de transformare (*funcție hash*), funcție prin care la ieșire se furnizează un șir de date de lungime fixă, respectiv o valoare de transformare, pentru ca la intrare să fie aplicat un șir de date cu lungime variabilă, iar prin sensul unic de transformare funcția asigură imposibilitatea deducerii datelor de la intrare pe baza datelor de la ieșire.

Astfel, funcția *hash* asigură utilizatorii că datele transmise în rețea la intrarea emitentului sunt aceleași cu cele primite la destinație. În urma aplicării unei funcții hash, înaintea transmisie unui pachet de date, va rezulta o valoare fixă, pentru ca la recepție să fie recalculată valoarea, iar din compararea celor două se poate trage concluzia dacă datele au fost alterate din punct de vedere al

securității, caz în care valorile sunt diferite, respectiv obținerea aceleași valori confirmă nefalsificarea datelor pe perioada tranzitului prin rețea. Prin utilizarea unor funcții hash, chiar și o mică modificare a conținutului datelor va crea mari diferențe între valorile de la transmisie și cele de la recepție, denumite valori hash.

Funcțiile hash critpografice sunt utilizate pentru, controlul integrității datelor, autentificarea mesajelor, verificarea parolelor și realizarea semnăturilor digitale.

Funcțiile *hash* pot fi calsificate în două mari categorii:

I. Coduri de detecție modificate (MDC) cunoscute și sub denumirea de coduri de manipulare-detecție sau raportat la scopul lor, mai rar ce-i drept, se întâlnește și sintagma coduri de integritate a mesajului. Scopul unui cod de detecție este de a asigura o imagine hash unui mesaj și astfel, de a garanta, prin mecanisme secundare, verificarea integrității datelor cerută de aplicații specifice. Coduri de detecție modificate (MDC) sunt o subclasă a funcțiilor fără cheie, și pot fi clasificate astfel:

A. *funcții hash inversabile într-un singur sens* (*one-way hush function*) *rezistente la preimagine*, adică pentru o valoare dată (H) este greu de găsit prin aplicarea funcției a unui mesaj (M), transpunerea matematică a funcției fiind de tip: H=hash(M)

B. *funcții hash rezistente la coliziune*, în condițiile în care o coliziune presupune ca două mesaje distincte să aibă aceeași valoare hash (funcțiile de acest tip urmăresc identificarea a două mesaje care să aibă aceeași valoare hash, ceea ce este destul de dificil).

II. Coduri de autentificare a mesajelor (MAC), categorie de funcții care permit asigurarea autenticității sursei și a integrității mesajelor, fără implicarea vreunui mecanism adițional. MAC-urile au funcțional doi parametri distincți: mesajul de intrare și o cheie secretă (subclasă de funcții hash cu cheie).

I.3 Modele de asigurare a securității sistemelor informatice

În funcție de măsurile de securitate stabilite prin politica de securitate, dar și în funcție de specificul sistemului informatic al utilizatorului, se definesc și se aleg în vederea implementării modelele de securitate ale sistemului, modele care conțin mecanismul logic de implementare a politicii de securitate [28]. În funcție de complexitatea sistemului informatic, modelele de securitate sunt de tip multinivel – specifice unui sistem informatic izolat, respectiv de tip multilateral-specifice unei rețele de calculatoare (cum este Modelul zidului chinezesc sau modelului British Medical Association – BMA, analizate în teză).

Modelele de securitate se împart în două categorii, pe de o parte, în funcție de accesul la informație identificăm modelele de securitate multinivel (cum este modelul de securitate propus de David Bell și Len LaPadula, sau modelul de securitate al matricei drepturilor de securitate sau modelul Graham Denning, analizate în teză) securitatea realizându-se pe nivele multiple unde se regăsesc

anumite categorii de informații, pe de altă parte în funcție de modul de organizare a informațiilor din sistemul informatic pe verticală identificăm modelele de securitate multilaterale prin care se controlează fluxul de date între departamentele/compartimentele unei organizații cărora le este permis/restricționat accesul la datele partajate din sistemul informatic.

I.4. Standarde, norme și politici de securitate.

Stabilirea și definirea exactă a politicilor, standardelor și normelor de securitate contribuie la conceperea programului de securitate informațională al unei organizații, care dovedindu-și eficiența și rigurozitatea va asigura buna desfășurare a activităților instituționale.

Existența și implementarea unui standard de securitate conferă unei entități juridice sprijin și repere în efectuarea controalelor interne, iar certificarea implementării standardului îi conferă credibilitate din partea clienților și utilizatorilor externi.

În conturarea unui standard de securitate informațională se va ține cont de scopul și aria de aplicare, de rolurile și responsabilitățile la nivelul organizației privind definirea și aplicarea standardului asumat, identificându-se, astfel, standarde ale cadrului de bază – declarațiile asumate la cel mai înalt nivel aplicabile întregului sistem, standarde tehnologice – declarații și descrieri aferente sistemului și standarde ale administrării – reguli de administrare în timpul exploatării sistemului și aplicațiilor integrate.

Referindu-ne la securitate informațională, noțiunii de politică de securitate îi sunt asimilate mai multe mecanisme, cum ar fi spre exemplu:

- politica de firewall-uri, ca mecanisme de software, utilizate pentru controlul accesului şi configurarea traseelor pe care se regăsesc informațiile în cadrul organizației;
- cardurile de acces, lacătele, camerele de luat vederi, ca echipamente fizice, care permit înregistrarea activității din perimetrele controlate ale organizației prin aceste echipamente.

Primul standard general a fost standardul BS7799 prin implementarea căruia orice organizație obținea certificare privind sistemul de management al securității informației. Standardul BS7799, care în anul 2007 a fost publicat sub numele de ISO/IEC 27002:2005, stă la baza actualului standard oficial de certificare ISO/IEC 27001 care se integrează în seria ISO 27000 de standarde ISMS (Sistem de Management a Securității Informației) dedicate securității informației.

Dacă standardul ISO/IEC 27003:2010 poate fi utilizat și împreună cu standardele ISO/IEC 27001:2005 și ISO/IEC 27002:2005, celelalte standarde pot fi implementate separat, după cum în funcție de specificul activității organizației există în seria ISO/IEC 27000 și standarde speciale, cum ar fi pentru domeniile de audit(ISO/IEC 27006:2007) sau cel de telecomunicații (ISO/IEC 27011:2008).

Indiferent de modul de redactate, politica de securitate a unei organizații trebuie să găsească soluții la următoarele probleme :

- ce amenințări sau riscuri există, natura acestora, care dintre amenințări pot fi eliminate şi care nu;
- ce resurse se pot proteja precum și nivelul de acces la aceste resurse;
- cu ce mijloace interne se asigură securitatea;
- ce costuri presupune pentru organizație introducerea, mentenanța şi actualizarea mecanismelor și procedeelor de securitate.

În contextul lansării în septembrie 2015 a noii ediții, a cincea, a standardului ISO 9001:2015 –Sistemul de Management al Calității, standard cu cea mai mare aplicabilitate actuală la nivel mondial atât ca număr de organizații certificate – peste 1,1 milioane la nivel mondial – cât și ca arie geografică și politică de cuprindere – peste 100 de state au preluat identic standardul ISO 9001:2008, fost ISO 9000:2000 – abordarea integrată în cadrul sistemului de management intern al unei organizații a standardelor internaționale de management, ISO 9001 privind sistemele de management-ul calității (SMC), ISO 14001 pentru sistemele de management-ul mediului, OHSAS 18001 pentru sistemele de management-ul sănătății și securității ocupaționale, ISO 27001 pentru sisteme de management al securității informației (SMSI) este o necesitate impusă de concurența de pe piețele de producție și desfacere, dar și o necesitate internă de eliminare a responsabilităților și relațiilor necorespunzătoare sau a celor dublate prin proceduri individuale.

Pornind de la un Sistem de Management al Calității (SMC) certificat într-o organizație, suprapunând unele proceduri și adăugând procesele specifice necesare sistemelor de management de mediu și/sau de sănătate și securitate ocupațională sau de securitate a informației se poate obține un Sistem de Management Integrat (SMI), care va aduce un plus de valoare organizației și produselor/serviciilor sale.

Într-o abordare grafică conform Figurii 6, Sistemul de Management Integrat asigură planificarea obiectivelor și proceselor necesare obținerii rezultatelor în acord cu strategia organizației și cerințele/așteptările clienților, implementează procesele în condiții de securitate a circulației informațiilor și datelor, verifică, prin indicatori specifici fiecărui sistem de management, procesele și produsul obținut în acord cu politicile, obiectivele și cerințele cerute de calitatea produsului, și întreprinde acțiuni pentru îmbunătățirea performanței proceselor pe baza rezultatelor de audit intern.

Figura 6 Sistem de Management Integrat

Pe fondul evoluției tehnologice, Organizația Internațională pentru Standardizare (ISO) a emis în iulie 2014 standardul ISO 27018, primul standard pentru protecția datelor din cloud, conținând linii

directoare pentru furnizorii de servicii de tip cloud cu privire la Informațiile cu privire la Identificarea Personală ("PII").

Și pentru că deja pe piața IT sunt furnizori de servicii cloud, ISO 27018 oferă specificitate furnizorilor de servicii cloud pentru evaluarea riscurilor și implementarea controalelor pentru protecția PII stocate în cloud.

I.5. Vulnerabilitățile sistemelor informatice

Vulnerabilitatea, din punct de vedere informatic, este o slăbiciune în proiectarea sau implementarea hardware-ului, software-ului, rețelelor sau sistemelor bazate pe calculatoare, inclusiv a procedurilor de securitate și administrare a sistemelor informatice, prin care se permite accesul utilizatorilor neautorizați în sistem [75]. Dacă efectul vulnerabilității asupra sistemului informatic constă în afectarea negativă a organizației, exploatarea vulnerabilității poate fi neintenționată, din neglijență, sau intenționată, voită atât ca acțiune cât și ca efect scontat.

Vulnerabilitatea unui sistem informatic poate fi generată și de o cauză naturală (formă de atac la integritatea fizică a informației) precum cutremure, inundații, incendii sau căderi de tensiune în urma cărora sunt distruse fizic echipamentele de calcul, afectând implicit accesul și prelucrarea informațiilor din rețeaua la care erau conectate aceste echipamente.

Din punct de vedere al software-ului folosit pe un sistem informatic sunt identificate trei grade de vulnerabilitate în funcție de consecințele asupra sistemului informatic astfel afectat [4] prezentate în mod crescător al efectelor:

1) grad de vulnerabilitate C (vulnerabilitatea sistemului de operare) – utilizatorii externi au posibilitatea alterării sistemului informatic sau implicării sistemului într-un atac asupra unui terț utilizator de bună credință;.
2) grad de vulnerabilitate B – utilizatorii locali cu privilegii limitate au posibilitatea măririi fără autorizație a privilegiilor de acces.
3) grad de vulnerabilitate A – utilizatorii externi au posibilitatea accesării neautorizate a sistemului informatic (mod de atac prin viermi informatici sau cai troieni), consecințele fiind cele mai grave prin faptul că breșa în securitatea sistemului poate genera distrugerea sau furtul de date din sistem.

Dacă vulnerabilitățile unui sistem informatic pot avea de la cauze naturale externe, la erori de software sau configurări eronate ale sistemului de operare, și până la erori umane, generate fie de lipsa de cunoștințe sau cunoștințelor limitate ale utilizatorilor și/sau administratorilor de sistem, fie de neglijența utilizatorilor, amenințările asupra sistemelor informatice sunt acțiuni mai grave exercitate asupra sistemelor informatice, cu consecințe care se pot propaga prin Internet la mai multe sisteme informatice interconectate de către terțe persoane neautorizate care speculează vulnerabilitățile sistemului, persoane denumite agenți de amenințare [75].

Cercetări privind securitatea datelor în sistemele informatice

Astfel de agenți de amenințare sunt hackerii, spionii, grupurile de crimă organizată, persoane din interiorul organizației – incluzând chiar administratori de rețea/sistem - și până la statele care organizează acțiuni criminale prin intermediul sistemelor informatice și teroriștii [44].

I.5.1 Clasificarea vulnerabilităților sistemelor informatice

Folosindu-se criterii de clasificare diferite, în literatura de specialitate se consemnează modalități diferite de clasificare, pentru ca din punct de vedere legislativ aceste vulnerabilități să se regăsească și în definirea unor infracțiuni:

1) Interceptarea radiațiilor se realizează prin diferite metode tehnice prin care sunt extrase informațiile existente în radiații electromagnetice transmisibile prin aer (de la un calculator la altul sau de la cablurile de telecomunicații) și care nu pot fi controlate;

2) Interceptarea informațiilor introduse de la tastatură se bazează pe decodarea sunetelor produse de tastatura când este folosită de un utilizator cu ajutorul unui soft care recuperează astfel 96% din caracterele scrise [44].

3) Interceptarea pachetelor sau *spionaj în rețea (network snooping)* este încadrată ca și infracțiune ce vizează comunicațiile prin Internet, operațiune precedând de multe ori atacurile IP (Internet Protocol). Astfel, agenții de amenințare pot intercepta un pachet de date (inclusiv cu mesaje de autentificare, pachete de email, etc.) care călătorește prin Internet între diferite locații.

4)Deturnarea sesiunii reprezintă o tehnică de infracțiune informatică prin care agentul de amenințare se „deghizează" prin detectarea numerelor de secvență, cum ar fi numerele adreselor IP, în cadrul unui trafic informațional, și pătrunde în sistem în locul utilizatorului pe care l-a deturnat, iar calculatorul gazdă al intrusului va fi deconectat, agentul de amenințare punând astfel stăpânire pe fișierele utilizatorului legitim deconectat.

5) Falsificarea adreselor expeditorului (Email spoofing) reprezintă un tip de atac prin care se urmărește obținerea adresei utilizate de Internet Protocol (IP) când se realizează o conexiune în rețea sau se falsifică adresa expeditorului de E-mail, astfel încât utilizatorul care primește mail-ul va răspunde la atac divulgând informații ca răspuns la un mesaj fals.

6) Simularea Web-ului presupune realizarea de către un agent de amenințare a unei copii false și convingătoare a unui întreg Web, cu același număr de pagini și conexiuni ca și Web-ul adevărat, Web-ul fals fiind controlat de către agentul de amenințare care va primi astfel în sistemul său traficul de rețea între browserul victimei și Web-ul fals. Având astfel controlul traficului returnat de serverele Web-ului simulat către utilizatorul victimă, agentul de amenințare paote intercepta traficul de rețea în mod pasiv – *sniffingul* – sau poate simula Web-ul primind în sistemul său informații de la utilizatorul victimă.

7) Interceptarea parolelor se situează printre cele mai preferate tipuri de atacuri [15] în cazul rețelelor on-line. Pentru preluarea parolelor dintr-o rețea agentul de amenințare trebuie să aibă acces

la baza de date cu identificatorii de login și parolele utilizatorilor, iar după ce copiază această bază de date, în care se regăsește funcția hash aferentă, fie se va rula un program cunoscut sub denumirea de *tehnică de spargere a parolelor prin forță brută (brute force password-cracking teghnique)* prin care se generează și încearcă combinații posibile de caractere pentru parole, fie se va rula un program de parole automate, program denumit *atac cu dicționarul (dictionary-based attacks)* [44].

8) Virușii, Caii troieni și Viermii sunt vulnerabilități care au legătură cu alterarea integrității datelor informatice prin modificarea, ștergerea sau deteriorarea lor, precum și prin transferul neautorizat al datelor dintr-un sistem informatic, acțiuni care îmbracă forma infracțiunilor informatice datorită modului de operare și consecințelor lor.

9) Hărțuirea (Harassment) sub forma spam-urilor și bombelor de tip E-Mail par vulnerabilități inofensive deoarece nu alterează integritatea sau confidențialitatea datelor/informațiilor dintr-un sistem, însă pot afecta traficul dintr-o rețea blocând anumite servere care devin de fapt ținta atacurilor. Astfel, agenții de amenințare transmit cantități foarte mari de e-mail-uri, cu conținut nesolicitat de către utilizator, sau mesaje nesolicitate, în general reclame, pe o listă de discuții.

10) *Pirateria software* constă în „spargerea" programelor shareware, modificând codul executabil prin folosirea bibliotecilor de coduri secrete disponibile pe Internet sau inhibând instrucțiunile care cer cheia hardware prin folosirea patch-urilor, de asemenea accesibile pe Internet.

*I.5.2 Vulnera**bi**lită**țile** unei **re**țe**le** de com**u**nica**ț**ii*

O rețea sigură este aceea ale cărei resurse sunt credibile/autentice și securizate, respectiv o rețea care furnizează servicii autentice și de calitate, deși siguranța, ca și securitatea unei rețele nu pot fi garantate 100%.

Deoarece o rețea de comunicații este un sistem complex, exogen, cu foarte mulți utilizatori, ea devine o zonă convenabilă și facilă pentru diferite atacuri, fapt pentru care securitatea rețelei trebuie percepută și implementată ca un obiectiv operațional vital al oricărei rețele de comunicații.

În funcție de vulnerabilitățile rețelei de comunicații identificate și exploatate de către agenții de amenințare, atacurile informatice se pot manifesta astfel:

- accesarea neautorizată a rețelei sau a unor resurse ale acesteia de către un utilizator din interiorul organizației sau extern care nu are anumite drepturi de acces;

- tentative la nivelul fizic al rețelei pentru perturbarea sau întreruperea funcționării (prin factori mecanici precum întreruperea unor cabluri sau scoaterea din funcțiune a unor echipamente din rețea; prin factori electrici, precum acțiuni de bruiaj în cazul rețelelor radio, inducerea de semnale de interferență în rețelele cablate).

- tentative de oprire a traficului sau de încărcare excesivă a traficului din rețeaua vizată prin generarea concomitentă a unui număr foarte mare de pachete de informații către nodurile din rețea.

- atacuri software asupra echipamentelor din rețea care coordonează și dirijează fluxul în noduri critice (router, switch, acces point etc.), fiind modificate fișiere de configurare a drepturilor de acces stabilite exclusiv pentru personalul autorizat.

- afectarea integrității fizice a datelor, fiind astfel modificate sau chiar distruse informațiile,

- afectarea confidențialității datelor prin receptarea și utilizarea neautorizate a informațiilor precum și încălcarea dreptului de autor.

Începând cu anul 2005, revoluția adusă prin Web 2.0 a generat creșterea numerică și dezvoltarea rețelelor de socializare datorită noilor aplicații bazate pe web care au permis utilizatorilor simpli să participe direct și să fie implicați în răspândirea informațiilor și propriilor opinii prin Internet (web), transformându-se astfel din „consumatori" de informații în „creatori" de pagini web cu informații, exemplu edificator în acest sens fiind blog-urile.

Dezvoltarea și răspândirea sistemelor de gestiune a informațiilor în mod automat într-un site/web, numite Content Management Systems, permite stocarea datelor utilizatorilor, în prezent, în direct în web, fără alte partiții intermediare (de exemplu fotografiile private ș.a.), spre deosebire de sistemele anterioare de IT în care datele utilizatorilor erau stocate inițial pe calculatorul utilizatorului de unde erau preluate ulterior în vederea publicării în web. Dezvoltând un concept al legăturii permanente cu web-ul, Content Management Systems permite accesarea tot mai frecventă a aplicațiilor web de către programele locale de pe calculatorul utilizatorului de rețea, unele motoare de căutare fiind capabile și construite pentru a accesa și date locale/personale ale utilizatorului [22].

Tacticile hackerilor de a exploata vulnerabilitățile rețelelor sociale se bazează atât pe cunoștințe IT foarte bune (instalează viruși în rețele sau pe calculatoarele utilizatorilor dând impresia că acești sunt aplicații inofensive ale rețelelor), cât și pe aspecte psihologice precum exploatarea încrederii reciproce a membrilor unei rețele, propagând virușii prin aplicații lansate aparent de unii membri ai rețelei care ulterior sunt accesate (redistribuite, se aplică comentarii sau sunt confirmate prin like/pin) de alți membrii care le consideră legitime.

Speculând latura umană a fiecărui membru al unei rețele de socializare, o altă escrocherie cu aparență de securizare a utilizatorului a fost exploatată, în anul 2013, de către hackeri pe rețeaua Facebook sub forma aplicației *"vezi cine ți-a vizualizat profilul"*, utilizatorii fiind asigurați că vor primi informații despre persoanele care le-au urmărit activitatea și accesat contul propriu pe această rețea. Aplicația frauduloasă nouă, exploatând curiozitatea specific umană, a declasat aplicații de tipul link-urilor frauduloase care încearcă să convingă utilizatorii că pot câștiga diferite premii, de obicei telefoane mobile sau tablete, participând la diferite sondaje sau concursuri, dar în fapt expunându-și propriul calculator accesului virușilor și/sau spam-urilor ascunse în spatele acestor link-uri accesate benevol de către utilizator [22].

I.5.3 Securizarea rețelelor sociale

La sfârșitul anului 2014, la nivel global, cele mai cunoscute și accesate rețele de socializare, în domenii diferite de interes pentru utilizatori, erau: Facebook cu circa 1,4 miliarde de utilizatori; Twitter cu circa 1 miliard de utilizatori cu cont (rețea pentru răspândirea unor știri scurte de maxim 140 de caractere); YouTube – rețea de partajare a videoclipurilor cu circa 1 miliard de utilizatori; LinkedIn cu circa 300 de milioane de utilizatori (rețea pentru managementul carierei și relațiilor profesionale); Pinterest cu circa 70 de milioane de utilizatori (platformă pentru descoperirea și administrarea de imagini și video-uri); Instagram cu circa 30 de milioane de utilizatori [22].

Chiar și în ciuda unor scandaluri de proporții privind lipsa de securitate a datelor cu caracter personal și chiar implicarea în partajarea unor date personale altor aplicații și utilizatori fără acordul persoanelor titulare ale datelor de către rețeaua Facebook în anii 2015 și 2017-2018, statistica utilizării tipurilor de rețele sociale a rămas în prezent în aceeași configurare ca și în anii 2014, cu mențiunea că Twitter este o rețea folosită preponderent pe continentul nord-american, în timp ce rețeaua Instagram folosită la același nivel geografic ca și Facebook-ul a câștigat teren, dublându-și în prezent numărul de utilizatori.

Datorită informațiilor personale pe care membrii unei rețele sociale le schimbă între ei și din cauza aplicațiilor web care accesează direct calculatoarele utilizatorilor, uneori fără știința acestora, toate rețele de socializare sunt vulnerabile în fața atacurilor lansate și exploatate de către hackeri, fie că este vorba de problemele de conectare, erori de tip "cross-site scripting" sau vulnerabilități Java. Tot datorită legăturilor create între membrii rețelei de socializare, banner-ele sau link-urile de pe astfel de rețele pot fi calea prin care un simplu Troian de tip „dropper" ajunge de la un utilizator la altul, se instalează în sistemul descoperit drept vulnerabil și „accesează neautorizat/fură" parole, informații personale și chiar datele de identificare ale cardului bancar folosit de utilizator pentru plăți on-line și memorate pe propriul calculator [22].

I.6 Concluzii și rezultate obținute

- Una din soluțiile cel mai frecvent adoptate și pe care o susținem drept viabilă este cea referitoare la integrarea sistemelor de management al calității şi a unuia sau tuturor celorlalte sisteme de management (SMM, SMSI, SMSSM) într-o variantă de integrare parțială, foarte flexibilă şi adaptabilă unui număr mare de situații.
- Recomandări privind implementarea unui sistem de management integrat prin care se asigură implicit securitatea sistemului informatic operațional prin adoptarea:
  a. Organizația trebuie să stabilească o relație cât mai obiectivă între importanța aspectelor de mediu și/sau de securitate informațională și/sau de sănătate și

securitate ocupațională, pe de o parte, şi a aspectelor de asigurare a calității, pe de altă parte;

b. Trebuie adoptată decizia de realizare a unui sistem de management integrat calitate – mediu/sănătate și securitate ocupațională/securitatea informației, decizie fundamentată pe analiza motivelor esențiale care au stat la baza deciziei de implementare a fiecăruia din sistemele de management din perspectiva organizației;

c. Decizia de implementare sau nu a unui sistem integrat de management trebuie să fie fundamentată pe analiza asemănărilor şi deosebirilor dintre sistemele de management pentru care se optează, precum şi a avantajelor şi dezavantajelor unei posibile integrări.

- Analiza riscului de securitate, ca parte a managementului instituțional, să fie realizată periodic și să fie coroborată cu stabilirea unei politici de securitate și implementarea unui model adecvat de securitate, inculsiv de securitate informațională,
- Sistemul de management al securității informațiilor să fie permanent monitorizat pentru a se identifica la timp incidentele de securitate și posibilele erori, îmbunătățindu-se astfel permanent eficacitatea securității.
- Ca politică de securitate informațională individuală este necesar ca fiecare utilizator să-și securizeze prin programe antivirus și antispam propriul calculator, telefon mobil sau tabletă de pe care accesează Internetul și contul său dintr-o rețea socială, aceste acțiuni putând fi promovate la nivel național prin informări on-line și chiar mesaje mass-media de interes general (cum sunt mesajele de interes public privind sănătatea și alimentația corectă prezentate pe posturi TV în cadrul emisiunilor)

CAPITOLUL II
ANALIZA PRINCIPALELOR TIPURI DE ATACURI INFORMATICE

Indiferent de motivația unei persoane de a interveni neautorizat și de a intercepta, altera sau șterge date și informații dintr-un sistem informatic sau dintr-o rețea publică/privată, consecințele atacului sunt resimțite nu numai de către administratorii rețelei/sistemului informatic ci și de către ceilalți utilizatori care folosesc ca resurse informațiile din sistem.

Frecvența folosirii anumitor tipuri de atacuri informatice este corelată cu consecințele urmărite de către agenții de amenințare, constatându-se potrivit statisticilor, spre exemplu că deși la prima vedere un anumit tip de atac nu este profitabil direct, el este folosit tot mai des prin asociere cu alte fapte de amenințare la care sunt expuși utilizatorii sau organizațiile.

În acest sens se explică de ce au luat amploare, începând cu anul 2005, atacurile prin refuzul serviciilor de tip DoS, atacuri asociate cu șantajul blocării accesului la un anumit site sau la anumite servicii oferite de serverele unei organizații pentru obținerea unor sume importante de bani de către agenții de amenințare pentru a nu duce la capăt amenințarea.

II.1 Evoluția în timp a atacurilor informatice

Exploatând vulnerabilitățile unui sistem informatic pe mai multe niveluri și din nevoia de îmbunătățire pentru a nu fi depistate, atacurile informatice au devenit tot mai complexe, combinând efecte și caracteristici de la mai multe tipuri de atacuri, respectiv aceste malware pot crea breșe în sistem pentru a facilita accesul intrusului (specific cailor troieni), concomitent cu automultiplicarea lor în rețea (caracteristica viermilor) și distrugerea informațiilor (specific virușilor).

Nu se regăsește în literatura de specialitate, nici cea tehnică, nici cea juridică, o definiție unitară a agenților de amenințare, aceștia fiind definiți fie ca actori rău intenționați care declanșează atacuri împotriva structurii informaționale critice [29], fie ca agenți care implementează amenințările în sistemul informatic [44], fie drept atacatori cu mai multe profiluri în funcție de timp, instrumente, scop și riscul asumat prin atac, dar și a modului de acces(extern sau intern) la sistem [28].

În literatura tehnică de specialitate cracker este denumirea generică pentru persoana care are ca ocupație principală lansarea atacurilor asupra sistemelor informatice în mod intenționat prin fapte care se încadrează, de cele mai multe ori, în reglementarea normelor penale, cel mai utilizat termen în mass-media este cel de hacker, termen adoptat în anii ’60, însă acest termen trebuie asociat persoanelor care posedând vaste cunoștințe de programare, fiind chiar specializați în aplicații software și fiind pasionați de dezvoltarea cunoștințelor proprii pătrund neautorizat în sistemele informatice exploatând erorile sistemelor de operare

Spre deosebire de crackeri, hackerii încearcă să dezvolte și metode de securizare a sistemului informatic, nu doar să exploateze vulnerabilitățile din sistem [39], fapt pentru care unii

hackeri sunt susținuți ulterior în demersurile lor de către organizații, în timp ce crackerii ajung în majoritatea cazurilor în fața instanțelor de judecată penale deoarece limitarea cunoștințelor lor nu le permite să șteargă urmele când descarcă programe de pe Internet sau alte instrumente soft pentru atacuri informatice [28].

Un alt termen tehnic care restrânge categoria crackeri-lor este cel de haxori, adică crackeri care nu au cunoștințe tehnice și nici nu sunt animați să-și dezvolte cunoștințele, dar care fiind rău intenționați descărcă de pe Internet aplicații soft pentru atacuri [1].

Atacurile informatice astfel inițiate de către state pot avea de la scopuri politice, precum cele anterior menționate, la scopuri economice și financiare, precum spionajul cibernetic instrumentat de statul chinez asupra mediului de afaceri din Marea Britanie în anul 2007.

În funcție de organizarea atacului și de instrumentele folosite, dar și de experiența autorilor, în literatura de specialitate tehnică sunt identificate trei niveluri de atacuri:

- atacuri oportune: autorul fiind un agent de amenințare ocazional, cu cunoștințe limitate despre sistemul informatic și folosind instrumente existente pe care le folosește pentru atingerea unui obiectiv general, cum ar fi de exemplu atacul unui angajat nemulțumit sau al unui activist înverșunat
- atacuri intermediare: asemănătoare celor ocazionale, doar că atacatorul își va ascunde activitatea cu mai multă pricepere decât autorul unui atac ocazional [30].
- atacuri sofisticate: afectează în mod considerabil serviciile esențiale dintr-un sistem, autorii având obiectivul bine conturat și alocând resurse și timp îndelungat pentru strângerea de informații despre arhitectura sistemului informatic pentru a-și crea propriile instrumente.

II.1.1 Repere în timp privind atacurile informatice

- 1986 a apărut primul virus – virusul Brain – urmat de alți viruși creați de hackeri din dorința de a exploata vulnerabilitățile sistemelor informatice neprotejate la acel moment.
- noiembrie 1988 în Internet este lansat primul atac generalizat de tip vierme de către Robert T. Morris, student la Universitatea Cornell, care s-a automultiplicat afectând un număr de 60.000 de calculatoare de pe teritoriul Statelor Unite ale Americii, calculatoare ale unor centre universitare (Cambridge, Massachusetts, Princeton), ale Centrului de Cercetări NASA din Silicon Valey și ale unor institute de cercetare – nu s-au produs distrugeri de date, dar sistemele afectate au fost încetinite considerabil;
- 1982 spionii sovietici au furat un sistem de control computerizat fără să știe că în soft era introdusă o linie de cod de către specialiștii IT din CIA, pentru ca la accesarea neautorizată să fie generată o explozie masivă, explozie care a fost generată la o

conductă de gaze din Siberia, acesta fiind începutul războiului cibernetic [49], deși opinia publică nu a reacționat cu interes la incident;

- anii '90 acțiuni de vandalism informatic prin care fie erau alterate sistemele de operare la nivelul organizațiilor, fie erau distruse datele de pe sistemele de stocare, fără ca atacatorii să aibă vreun obiectiv economic sau politic, ci doar pentru pură distracție [28];
- 1999 - virusul Melissa a generat primele atacuri de tip spam prin atașarea fișierului infectat de tip text la un mesaj de e-mail transmis automat tuturor contactelor din lista de e-mail;
- în ultimii ani ai primei decade a secolului XXI, (2007 și 2008) când atacurile cibernetice de tip DDoS au vizat sistemele informatice la nivel național din Estonia și respectiv Georgia, ambele atacuri generate dinspre Rusia pe fondul disputelor politice interstatale și afectând activitatea ministerelor, companiilor și băncilor din cele două state, pentru ca atacul din 2008 îndreptat asupra Georgiei să aibă consecințe și mai grave prin pierderea controlului asupra domeniului .ge, situație în care site-urile guvernamentale au fost transferate pe servere din afara țării [49];
- anul 2010 (declarat "Anul vulnerabilității") a fost caracterizat prin atacuri lansate prin rețele P2P (Peer to Peer), secondate ca frecvență de atacurile prin intermediul web-site-urilor și rețelelor de tip botnet;
- anii 2013 și 2014 confirmă faptul că amenințările de natură informatică asupra spațiului cibernetic național prezintă un trend de diversificare a modului de acțiune, sunt în creștere cantitativ, iar majoritatea alertelor primite sesizează cu privire la sisteme infectate cu variante diferite de tip malware;
- ultimii trei ani (2015-2017) din perspectiva nivelului de sofisticare tehnologică (Q1), a complexității (Q2) și a diversității malware-elor, se constată că malwareul rămâne în continuare una dintre cele mai importante amenințări cibernetice și care înregistrează o permanentă evoluție ascendentă;
- Anul 2017 a debutat cu identificarea unei vulnerabilități în sistemul de management de conținut web (CMS - Content Management System) Wordpress, cel mai utilizat sistem pentru publicarea anunțurilor în mediul on-line la nivel global. Vulnerabilitatea depistată rezidă în REST API a WordPress și conducea la o escaladare nedorită de privilegii, prin posibilitatea modificării variabilei ID prin eliminarea caracterelor non-numerice fără ca sistemul să mai verifice apoi drepturile de utilizare. Prin exploatarea acestei vulnerabilități un atacator putea șterge sau

modifica conținutul paginilor unui website neactualizat, și chiar redirecționa vizitatorii site-ului către exploit-uri malițioase.

II.1.2 Tendințe viitoare privind atacurile informatice

Pornind de la trendul anului 2010 în privința securității informatice, se constată că se menține trendul ascendent al valului masiv de atacuri DoS, prin care se suspendă activitatea de procesare a plăților on-line și a website-urilor agențiilor guvernamentale.

Un element vital și exploatat în atacurile informatice îl reprezintă rețelele botnet care sunt folosite pentru a se transmite mesaje de tip spam, pentru a se lansa atacuri de tip DoS sau pentru a găzdui în mod gratuit pagini de phishing sau malware pentru fraude cu card-uri de credit.

În următorii ani, exploatând vulnerabilitatea sistemelor care nu scanează fișierele binare semnate digital, atacurile cu malware se vor concentra prin amenințări mai puțin vizibile și detectabile prin aplicații de malware semnate digital.

Astfel, în anul 2014, numărul total de incidente de securitate cibernetică detectate la nivel global în companii a crescut cu 48% față de anul precedent, atingând 42,8 milioane de evenimente la nivel global, după cum reiese dintr-o analiză făcută de PwC – The Global State of Information Security Survey 2015 [77], iar pierderile financiare cauzate organizațiilor de astfel de incidente au fost estimate la 2,7 miliarde de dolari, în creştere cu 34% față de anul 2013.

La nivel european numărul incidentelor de securitate detectate în anul 2014 a crescut cu 41% față de anul 2013, cu 11% a crescut numărul incidentelor în America de Nord, în timp ce în Asia s-a înregistrat o creştere de 5% față de anul precedent.

America de Sud este singura regiune care a înregistrat o scădere din acest punct de vedere în anul 2014, de aproximativ 9% [77], scăderea numărului de notificări fiind justificată de reducerea cu 24% a bugetelor alocate securității cibernetice în regiune și implicit a surselor financiare a organizațiilor pentru implementarea măsurilor de securitate informatică.

II.1.3 Analiza amenințărilor informatice în România

Atacurile informatice din România nu diferă de cele la nivel internațional, însă cea mai mare amenințare la nivel național este reprezentată de folosirea produselor software contrafăcute sau piratate, atât de către utilizatorii domestici, cât și de către unii operatori, precum și lipsa instalării de programe antivirus, astfel încât multe vulnerabilități nu pot fi remediate în timp util și crește, astfel, riscul infectării sistemului.

În anul 2014, CERT-RO – punct național de contact cu privire la alertele și incidentele de securitate cibernetică – a recepționat şi procesat peste 78 de milioane de alerte de securitate cibernetică, care au vizat peste 2,4 milioane de IP-uri unice din România implicate în diverse tipuri de incidente de securitate cibernetică [76].

Comparativ cu anul 2016, numărul alertelor de securitatea cibernetică în anul 2017 a crescut

cu 20% față de anul 2016 (numeric 138.217.026 de alerte totale colectate și procesate la nivelul anului 2017 comparativ cu 110.194.890 de alerte totale în anul 2016, menținându-se trendul ascendent de creștere anuală a numărului de atacuri cibernetice [78].

Din cauza numărului mare de produse IT contrafăcute existente în România și al folosirii de software piratat, agenții de amenințare profită de vulnerabilitățile de sistem, astfel încât peisajul de malware din România este dominat din anul 2011 și până în anul 2017 de viermele Downadup (în anul 2011 reprezenta 10,24% din total amenințări, pentru ca în anul 2017 procentul să ajungă la 25,36% din totalul alertelor procesate de CERT-RO, care se menține astfel în primele trei locuri de-a lungul timpului, astfel cum rezultă și din tabelul de mai jos (Tabelul 3).

Tabel 3. Evoluția celor mai importante amenințări informatice din România 2011/2016/2017

	TIP MALWARE	PROCENT (%ALERTE)		TIP MALWARE	PROCENT (%ALERTE)		TIP MALWARE	PROCENT (%ALERTE)
2011	Win.Downadup	10,24%	2016	Win.Sality	34,16%	2017	Win.Downadup	25,36%
	Trojan.Autorun	12,23%		Win.Downadup	17,72%		Mirai	15,88%
	Win.Sality	4,48%		Nivdort	13,65%		Win.Sality	15,35%
	Trojan.Crack	3,55%		Ramnit	7,46%		Nivdort	13,72%
	Adware.	1,64%		Dorkbot	5,73%		Ramnit	5,03%
				Mirai	3,60%		Avalanche	3,82%

II.2 Tipuri de atacuri informatice

Încălcând politica de securitate a unui sistem informatic, atacul informatic se desfășoară asemenea unei penetrări a securității unui sistem, autorul său urmărind intenționat să colecteze, să altereze sau să șteargă resursele informaționale din sistemul vizat. Orice act prin care se poate întrerupe o operație în derulare, funcționalitatea, integritatea și/sau disponibilitatea datelor/ informațiilor dintr-un sistem sau a celor transferate prin rețele reprezintă un pericol asupra securității sistemului și/sau a rețelei.

II.2.1 Virușii informatici

Software proiectat pentru a infecta un sistem informatic, virusul informatic este o amenințare cibernetică care are legături și cu infracțiunile informatice privind operațiuni ilegale cu dispozitive sau programe electronice. Caracteristicile de bază ale unui virus informatic sunt auto-executarea și auto-multiplicarea, această din urmă caracteristică având scopul de a afecta și alte sisteme prin înmulțirea lor exponențială în rețelele infectate asemănător virusului din științele medicale.

Virusii altereaza integritatea datelor informatice, respectiv virușii pot modifica, șterge sau deteriora datele existente, pot restricționa în mod neautorizat accesul la aceste date (datele figurează ca fiind șterse, desi în fapt nu sunt șterse real din sistem), dar pot genera și transferuri neautorizate de date dintr-un sistem informatic/mijloc de stocare a datelor informatice [7].

II.2.2 Analiza viermilor informatici

Viermii (worms) sunt programe capabile să se multiplice consumând totodată resursele gazdei, fără însă să se autoexecute, și putându-se transfera și pe alte calculatoare decât cel gazdă pentru a efectua astfel operațiuni distructive.

Astfel, viermii se răspândesc în mod automat, factorul lor de multiplicare fiind exponențial și epuizând resursele calculatoarelor infectate într-un timp determinat.

Dintre acțiunile distructive ale viermilor amintim ștergerea de informații, crearea de uși ascunse pentru a permite accesul neautorizat sau lansarea de atacuri de refuz de servicii. Impactul mare al viermilor prin acțiunilor lor distructive este faptul că propagarea lor creează un refuz al serviciilor ca urmare a traficului de pe Internet [44].

Având în vedere că viermii se copiază de pe un calculator dezactivat în urma infectării pe un alt calculator, folosind protocoale obișnuite, aceștia nu trebuie să modifice un program gazdă pentru a se propaga.

Astfel, viermii informatici au în comun cu virușii capacitatea de multiplicare, însă nu local pe un singur termina, ci de pe un calculator pe altul.

II.2.3 Analiza Cailor Troieni

Având caracteristică comună cu viermii informatici faptul că nu pot infecta un fișier, ci afectează întreg sistemul, caii troieni sunt programe deghizate de tip malware, care urmăresc crearea unor breșe pentru a se permite accesul neautorizat al unui utilizator în sistemul infectat. Spre deosebire însă de virușii informatici, caii troieni nu se pot auto-multiplica, în majoritatea cazurilor după realizarea acțiunilor malițioase aceștia se auto distrug din sistemul infectat.

Troienii sunt alcătuiți din trei elemente: 1) programul Server sau programul propriu-zis al troianului lansat în infectarea calculatorului victimă; 2) programul Client care are drept scop conectarea la un echipament/device infectat, dar și pentru a primi comenzi de accesare neautorizată; și3) programul Build/Edit Server necesar pentru editarea programului Server propriu-zis.

II.2.4 Programe de tip Adware și Spyware

Adware reprezintă acel tip de programe răuvoitoare care se instalează pe calculator şi deschid ferestre pop-up ori noi tab-uri cu reclame, deși utilizatorul nu dorește să acceseze acea formă de publicitate, mai mult apariția reclamei instantaneu distrăgând atenția utilizatorului aplicației.

Programul de tip Adware exploatează astfel vulnerabilități la nivelul browserului, putând chiar schimba adresa de bază a browserului (homepage) ori redirecționa adresele web (URL-urile) scrise greşit ori incomplet în bara de adrese și direcționând astfel pe utilizator, contrar voinței sale, către site-uri de tip jocuri de noroc ori site-uri pornografice.

Cercetări privind securitatea datelor în sistemele informatice

Programele de tip Spyware captează fără știința utilizatorului informații personale și despre comportamentul acestora în mediul virtual, precum site-urile vizitate mai des pe Internet, și în urma analizei lor transmit utilizatorului echipamentului infectat reclame corespunzătoare informațiilor accesate în scop de marketing, reclame nesolicitate de către utilizator.

II.2.5 IP Sniffing

Sniffingul reprezintă procesul de capturare într-un fișier şi analiză a traficului cu scopul de a detecta parole sau date bancare trimise prin rețea. Utilitarele folosite pentru sniffing se numesc sniffere sau analizatoare de protocoale, deoarece prin intermediul lor sunt analizate pachetele transmise prin rețea, apoi sunt capturate parolele, sau alte date confidențiale transmise prin rețea ca informații în format text simplu.

II.2.6 Atacuri prin e-mail

Având în vedere creșterea gradului de utilizare a conturilor de e-mail, atât pentru activitățile profesionale, dar și pentru cele de socializare, în ultimii ani a crescut și numărul atacurilor prin e-mail, agenții de amenințare adaptându-se trendului utilizatorilor.

Folosind ca și cale de intrare contul de e-mail, atacurile se pot clasifica :

1) E-mail bombing
2) E-mail spoofing
3) E-mail spamming
4) E-mail phishing

II.2.7 Alte tipuri de atacuri

Ingineria Socială

Unul dintre cele mai eficiente și simple ca procedură dintre atacurile informatice este Ingineria Socială, tip de atac informatic prin care sunt manipulate anumite persoane cu autoritate în sistemul vizat de atac, astfel încât persoana vizată va face anumite operațiuni ce l-ar putea ajuta pe agentul de amenințare în derularea atacului. Ingineria socială este foarte simplă, nu necesită cunoștințe tehnice aprofundate, fapt pentru care deseori este minimalizată ca incidență dar în cazul atacului pot fi generate pierderi/distrugeri considerabile pentru companie.

Phishingul reprezintă un atac informatic, prin care sunt solicitate direct utilizatorului informații confidențiale sau cu caracter personal prin simularea interogării efectuate de către o organizație legitimă respectiv într-un interes legitim al utilizatorului, cel mai accesibil mod de interogare fiind de exemplu pe e-mailul victimei.

Baitingul reprezintă un tip de atac informatic, în contextul în care utilizatorul-victimă introduce fără a fi notificat în vreun fel, din proprie curiozitate, un cod malițios în calculatorul său, dând astfel drept de acces autorului atacului. Hackerul poate folosi ca momeală un mijloc fizic de acces, respectiv fie un disc, CD, sau un flash drive USB, de pe care se va instala automat codul dăunător în momentul în care

utilizatorul-victimă introduce acel flash pentru a citi/accesa informațiile prezumate a fi conținute pe mediul de stocare, astfel infectând propriul calculator, și chiar dând permisiune de acces hackerului la sistem.

Atacuri de tip SMTP

Atacurile de tip SMTP se bazează pe vulnerabilitatea *buffer overflow,* inserând în textul mesajului un conținut cu o capacitate prea mare, iar în secvența care excede informațiilor comunicate prin contul de e-mail sunt incluse comenzi pentru accesarea serverului e-mail.

Flooding

Flooding-ul ca atac informatic presupune supraîncărcarea unui server prin inundarea sa sau a host-ului cu o cantitate anormală de pachete de informații, și astfel serverul vizat este scos din funcțiune.

SPAM-ul face parte din categoria atacurilor de tip DoS (Denial of Service). Utilizatorii unui server e-mail vor primi deși nu au solicitat mesaje sub forma unor reclame la diferite produse fără interes pentru utilizator, sau vor primi chiar mesaje cu conținut neplăcut.

II.3 Structura unui arbore de atac informatic

Definim un arbore de atac ca o metodă sistematică ce caracterizează securitatea unui sistem informatic, caracterizare ce are la bază analiza unor tipuri distincte de atacuri [28].

Rădăcina arborelui poate reprezenta nivelul de securitate al sistemului informatic.

Arborele de atac se descompune în două modalități:

- Un set de atacuri țintă, fiecare trebuind îndeplinit pentru ca atacul global să fie încheiat cu succes, ceea ce reprezintă o analiză tip AND.
- Un set de atacuri țintă, oricare din atacuri trebuind îndeplinit pentru ca atacul global să fie încheiat cu succes, ceea ce reprezintă o analiză tip OR.

Tipul general de arbore de atac este o reprezentare generică a unor studii, atacuri comune ce au loc în contexte specifice. Fiecare tip de arbore de atac conține:

- scopul principal al atacului specificat de tipul arborelui
- o listă de precondiții ce îi definesc utilitatea
- pașii pentru ducerea atacului la bun sfârșit
- o lista de post-condiții ce sunt veridice dacă atacul este îndeplinit.

Precondițiile reprezintă ipoteze pe care le facem despre atacator sau starea organizației, care sunt necesare pentru îndeplinirea unui atac.

Post-condițiile reprezintă cunoștințele dobândite de către atacator și de starea organizației, indici ce sunt afectați pe măsura îndeplinirii cu succes a etapelor atacului și deținerea precondițiilor de către atacator.

Cercetări privind securitatea datelor în sistemele informatice

În ultimele decenii, cea mai comună formă de vulnerabilitate de securitate a fost manipularea incorectă a "buffer overflow" prin programe de calculator.

II.4 Concluzii și rezultate obținute

- Atacurile informatice au fost generate (la jumătatea secolului XX) din dorința de a sublinia capacitatea tehnică a autorilor de a exploata vulnerabilitățile unui sistem informatic, respectiv ale unei rețele de comunicație.
- Treptat agenții de amenințare au trecut la acte de vandalism informatic, dezvoltând în timp o criminalitate informatică și ajungându-se în prezent la un adevărat război cibernetic.
- În timp, efectele atacurilor informatice s-au modificat, prin schimbarea scopului urmărit de autorul unui atac informatic, de la disfuncționalitatea unui sistem informatic și distrugerea datelor de pe sistemele de stocare la interceptarea datelor confidențiale legate de cărțile de credit, respectiv de la accesarea parolelor la blocarea întregii infrastructuri naționale privind securitatea informațională, în cazul actelor de terorism cibernetic.
- Fiecărui sistem informatic trebuie să îi fie setat un arbore de atac relevant prin care se identifică apoi modul de compromitere a securității sau survivabilității sistemului informatic ca și rădăcină a arborelui de atac.
- Încă de la conceptualizarea arborelui de atac pentru analiza securității organizației trebuie să fie identificate și posibilitățile de perfecționare a arborelui, prin compromiterea nodului rădăcină ca și combinații de extensii manuale și modele de aplicații.

CAPITOLUL III

CERCETĂRI PRIVIND PRINCIPALELE METODE DE SECURITATE A SISTEMELOR INFORMATICE

Prin măsurile de securitate se urmărește în principal minimizarea vulnerabilităților sistemului informatic și ale resurselor, obiectul măsurilor de securitate vor fi deopotrivă: utilizatorii (atât utilizatorul final cât și angajații operatorului), datele și informațiile (inclusiv baze de date și fișiere), echipamentele componente ale sistemului/rețelei și serviciile oferite prin interconectare.

Aceleași trei planuri – procedural, logic și fizic – se identifică și în cazul măsurilor de securitate împotriva atacurilor informatice prin care se urmărește prevenirea, detectarea, eliminarea și refacerea resurselor și a componentelor sistemului/rețelei.

Astfel, orice sistem de protecție eficientă împotriva amenințărilor informatice trebuie:

1. Să identifice utilizatorii care au drepturi și/sau privilegii de acces
2. Să asigure o evidență clară și în timp real a accesului la calculatoare și stații de lucru
3. Să asigure controlul accesului la calculatoare și stații de lucru
4. Să identifice utilizatorii în funcție de aplicațiile și datele la care au acces
5. Să asigure back-up-ul programelor și bazelor de date
6. Să folosească software-uri performante și actualizate împotriva atacurilor informatice.

Constatăm că indiferent de etapa de derulare a unui atac informatic, se impune folosirea software-urilor dedicate protejării împotriva atacurilor informatice, aplicații care combat tipul de atac în mai multe moduri [42]:

- Detectarea semnăturii – cea mai veche metodă de detectare a unui atac informatic, metodă depășită în prezent de noile tipuri de atacuri mai sofisticate tehnic;
- Protecția în timp real – metodă care monitorizează comportamentul software-ului instalat pe un calculator, astfel că dacă se constată că o aplicație încearcă să facă modificări neuzuale la fișiere sau cere permisiuni pe care nu ar trebui să le ceară, se autosesizează și sunt luate măsuri împotriva acelei aplicații;
- Protecția de tip cloud – metodă ce a debutat în anul 2010, odată cu produsele Panda Cloud Antivirus și Norton Internet Security și care se axează pe originea atacului informatic, cum ar fi link-ul sau fișierele specifice.

III.1 Criptografia

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 [35]. 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.*

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 şi coduri.

În criptosistemele cu chei publice/criptare asimetrică fiecare utilizator, deține o cheie care îi permite transformarea publică de criptare, P_A, aceasta putând fi memorată într-un fişier public (cheile pot fi foarte lungi – de ordinul sutelor de caractere) şi o transformare de decriptare secretă, S_A, care nu poate fi obținută direct din algoritmul E_A.

Cheia de descifrare (cheie secretă) se obține prin derivare din cheia de cifrare (cheie publică) printr-o transformare aproape ireversivbilă (one-way). În sistemele de criptare cu chei publice, protecția şi autentificarea sunt operațiuni care se realizează prin transformări distincte, în etape separate.

a) Protecția datelor (confidențialitatea) cu chei publice : utilizatorul A își propune să transmită în condiții de confidențialitate un mesaj (M), unui alt utilizator B. Utilizatorul A va folosi transformarea publică P_B, a lui B. În acest caz A va transmite lui B, un mesaj M sub forma: $C = P_B(M)$. La recepție, B, va descifra mesajul, din C, utilizând transformarea secretă S_B, cunoscută doar de el: $S_B(C) = S_B(P_B(M)) = M$. Schema funcționează ca în Figura 10.

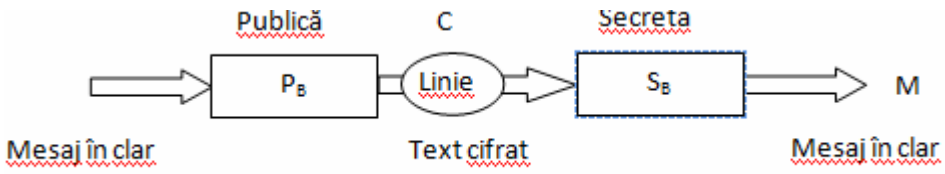

Figura 10 Sistem de criptare cu cheie publică

b) Autentificarea datelor cu chei publice : În vederea autentificării cu cheie publică, în raport cu transformarea lui A, se va aplica direct asupra lui M transformarea secretă S_A a lui A. Utilizatorul va transmite mesajul codificat: $C = S_A(M)$. Utilizatorul B va folosi cheia publică P_A la recepție: $P_A(C) = P_A(S_A(M)) = M$. Schema funcționează ca în figura de mai jos (Figura 11).

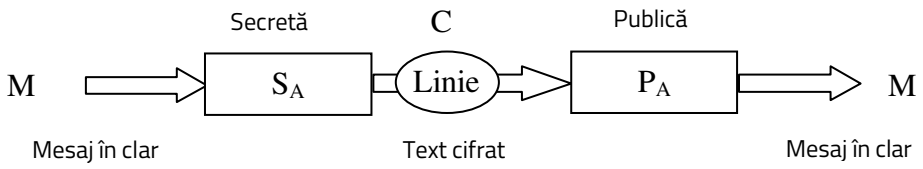

Figura 11 Sistem de autentificare cu cheie publică.

c) Protecția şi autentificarea datelor cu chei publice: În acest caz utilizatorul A va aplica mesajului M transformarea sa secretă (S_A). În etapa următoare A va cripta rezultatul,

utilizând în acest scop transformarea publică a lui B prin aplicarea funcției P_B şi va transmite către B, următorul mesaj: $C = P_B(S_A(M))$.

Receptorul B va obține mesajul în clar M, aplicând propria transformare secretă S_B, apoi transformarea publică a lui A, P_A: $P_A(S_B(C)) = M$.

Transformările (Publică şi Secretă) a fiecărui utilizator sunt una inversa celeilalte:

$\mathbf{P_A(S_A(M) = S_A(P_A(M)) = M}$

$P_B(S_B(M) = S_B(P_B(M)) = M$

Aplicând formulele $P_A(S_A(M)$ şi $P_B(S_B(M)$ asupra formulei $P_A(S_B(C))$ se obține relația regăsită și în Figura 12: $\mathbf{P_A(}S_B(C)) = P_A(S_B(\mathbf{P_B(}S_A(M))))) = P_A(\mathbf{S_A(}M\mathbf{))} = M$

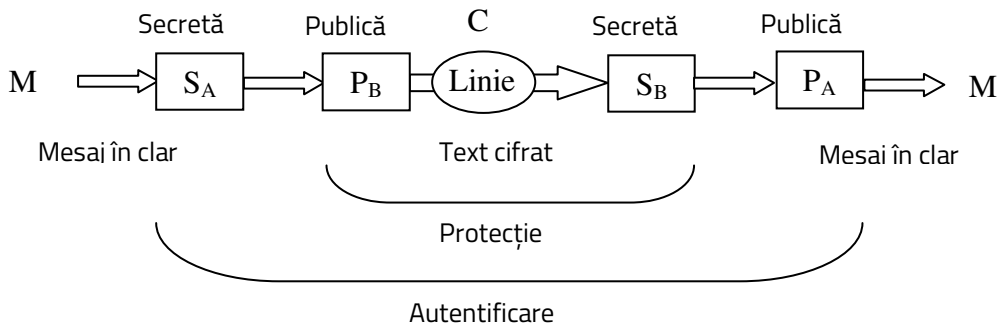

Figura 12 Sistem de protecție și autentificare cu cheie publică.

Semnătura digitală, ramură a criptografiei asimetrice, reprezintă o caracteristică a unui utilizator sau proces, fiind folosită pentru recunoaşterea mesajului emis de acesta și semnat cu cheie privată, asigurându-se astfel autenticitatea mesajului.

Pentru edificare asupra modalității de criptare vom exemplifica astfel: fie B receptorul unui mesaj asupra căruia s-a aplicat de către A o semnătură electronică la momentul emiterii.

Pentru a se garanta securitatea mesajului prin aplicarea semnăturii digitale de către A, semnătura astfel aplicată trebuie să întrunească anumite proprietăți în mod cumulativ:

1. B să aibă capacitate/cunoștințe tehnice de validare a semnăturii aplicate de către A;
2. Semnătura sofisticată aplicată de către A trebuie să fie imposibil de falsificat pentru oricine, inclusiv pentru B;
3. În cazul în care A nu va recunoaşte mesajul M prin aplicarea semnăturii, trebuie să existe un intermediar, un „judecător" care să soluționeze disputa dintre emitentul A și receptorul B.

Semnătura digitală rezolvă astfel problema autentificării atât a emițătorului cât şi a autenticității datelor cuprinse în mesajul semnat. Semnăturile digitale sunt implementate mult mai facil în cazul sistemelor de autentificare cu chei publice.

Spre deosebire de algoritmii de criptare, semnătura digitală ajută la identificarea și autentificarea utilizatorilor într-o comunicare prin Internet, astfel încât prin imposibilitatea renegării ulterioare a mesajului transmis, semnătura digitală conferă servicii de securitate prin utilizarea atât a criptării cu cheie publică (asigurând confidențialitatea), cât și a utilizării funcțiilor hash [41] care vor

depista orice modificare precum ștergerea sau adăugarea unui caracter prin diferențe mari între valorile hash [35], fapt pentru care mesajul nu poate fi repudiat.

III.2 Canale de comunicații securizate

Comunicațiile criptate între două echipamente aflate într-o rețea nesigură, cum este și Internetul, se asigură prin canale de comunicații securizate, cum este și programul Secure Shell (SSH), în timp ce standardul S/MIME (Secure/Multipurpose Internet Mail Extensions) oferă soluții de securizare în trimiterea mesajelor între echipamente dintr-o rețea de calculatoare, verificându-se totodată integritatea mesajului și nerepudierea informațiilor prin folosirea semnăturilor digitale [28].

Protocolul SSH (SSH = Secure SHell)

SSH este un protocol care permite crearea unei sesiuni de lucru la distanță, transferul de fișiere și crearea unor canale de comunicație pentru alte aplicații, toată transmisia fiind sigură împotriva atacurilor intrușilor. Pachetul SSH este compus din program server – SSHD, un program client – SSH și câteva utilitare pentru manevrarea cheilor de criptare [28].

Confidențialitatea transmisiei este asigurată prin criptare. Integritatea este asigurată prin trimiterea unor sume de control criptografice. Autentificarea serverului se face prin criptografie asimetrică, serverul având o cheie secretă și clienții dispunând de cheia publică corespunzătoare.

Autentificarea clientului se face fie prin criptografie asimetrică, ca și în cazul autentificării serverului (dar bineînțeles folosind alta pereche de chei), fie cu parola clasică, dată de client după autentificarea serverului.

Conexiunea de tip SSH oferă următorul mecanism:

- Se lansează aplicația intitulată *agent de autentificare*, aplicație care va citi cheia secretă criptată, apoi va solicita mașinii client fraza-cheie de decriptare și ulterior va decripta cheia secretă, pe care o va reține pentru siguranță în memoria RAM
- Dacă aplicația *agent de autentificare* rulează în momentul lansării unui client de tip SSH, acesta va încearcă să intre în contact cu aplicația *agent de autentificare* transmițând date către aceasta. Comunicația se face local prin funcții primitive oferite de sistemul de operare al mașinii client - de exemplu, prin FIFO UNIX.
- Opțional, la deschiderea unei sesiuni de tip SSH, se poate seta forwardarea conexiunii către aplicația din sistem intitulată *agent de autentificare*.

III.3 Măsuri de securitate în rețelele virtuale

O rețea privată virtuală (VPN) permite crearea unei rețele private independente ca existență în spațiul unei rețele publice, cum ar fi Internetul, astfel încât cele două părți ale conexiunii să comunice în condiții de securitate similare unei rețele locale.

Modul de lucru în VPN facilitează derularea comerțului electronic.

Cercetări privind securitatea datelor în sistemele informatice

Din punct de vedere al securității, VPN permite autentificarea utilizatorilor, identitatea fiind stabilită prin utilizarea de parole sau alte procedee, și codificarea tuturor datelor trimise între două puncte ale rețelei publice, procedeu cunoscut sub numele tunneling [5].

Un serviciu VPN este format dintr-un server VPN (implementat în diferite locații), protocoale VPN (pentru a crea tunelul) și criptare (pentru a asigura comunicarea).

Beneficiile utilizării unei VPN sunt:

-înlocuirea IP-ului original cu unul anonim

-evitarea cenzurei

-criptarea datelor prin protocoale criptografice fiabile (exemplu Point-to-Point Tunneling Protocol – PPTP, IP Security – IPSec, VPN-Q, Layer 2 Tunneling Protocol – L2TP)

-protejarea și asigurarea conexiunii WiFi.

Securitatea rețelei este reprezentată prin orice activitate concepută pentru a proteja integritatea și gradul de utilizare a rețelei și a datelor transmise între utilizatori. Acestea includ atât tehnologii hardware cât și software.

Securitatea rețelei combină mai multe straturi de apărare pe lângă și în rețea. Fiecare strat de securitate a rețelei implementează politici și controale. Astfel, dintre programele client ale unei rețele VPN mai multe programe de acest tip pot fi configurate astfel încât, în intervalul de timp necesar unei conexiuni VPN active, programele client configurate să solicite trecerea întregului trafic IP printr-un protocol de tip Cryptografic tunneling, sporind astfel siguranța conexiunii.

Având în vedere asigurarea confidențialității în rețeaua VPN a datelor, terminalele care folosesc conexiunea VPN trebuie să folosească aceeași cheie pentru criptarea și decriptarea datelor, fiind astfel într-un procedeu de criptare simetrică cu chei prestabilite.

Astfel, folosirea cheii statice, prestabilite, este punctul sensibil al securității VPN, fapt pentru care soft-ul de criptare al VPN, cum este IPSec-ul, va schimba la anumite intervale cheile prestabilite.

III.3.1. Moduri de securizare a rețelelor VPN:

1. Controlul accesului Nu toți utilizatorii ar trebui să aibă acces la rețeaua VPN. Pentru a împiedica atacatorii potențiali, trebuie să autentificat atât fiecare utilizator, cât și fiecare dispozitiv. Astfel, prin politici de securitate se pot bloca dispozitive de punct final care nu sunt conforme sau li se poate oferi acces limitat.
2. Software antivirus și antimalware

Uneori, programele malware vor infecta o rețea, dar înainte de asta pot sta latente în dispozitiv și/sau rețea zile sau chiar săptămâni. Cele mai bune programe antimalware nu numai că scanează programe malware la intrare, ci și continuă să urmărească fișierele ulterior pentru a găsi anomalii, a elimina programele malware și a repara pagubele. Astfel, fiecare utilizator conectat trebuie să ruleze pe dispozitivele proprii programe antivirus și antimalware.

3. Analiza comportamentală

Pentru a detecta comportamentul anormal al rețelei trebuie definit un comportament normal. Instrumentele de analiză comportamentale discern în mod automat activitățile care deviază de la ceea ce este stabilit drept normalitate. Identificarea indicatorilor de compromis care prezintă o potențială problemă reprezintă primul pas în acțiunile de remediere.

4. Prevenirea pierderilor de date

Organizațiile trebuie să se asigure că personalul lor nu trimite informații sensibile în afara rețelei. Tehnologiile de prevenire a pierderilor de date sau tehnologiile DLP pot împiedica persoanele să încarce, să retransmită sau chiar să tipărească informații critice într-un mod nesigur.

5. Protecția e-mailului

Folosirea e-mailului reprezintă vectorul de amenințare numărul unu pentru o încălcare a securității. Atacatorii folosesc informații personale și tactici de inginerie socială pentru a construi campanii sofisticate de phishing pentru a înșela destinatarii și pentru a îi direcționa către site-uri care oferă programe malware. O aplicație de securitate a e-mailurilor blochează atacurile primite și controlează mesajele de ieșire pentru a preveni pierderea datelor sensibile.

6. Firewall-uri

Firewall-urile au ca scop "ridicarea"unei bariere între rețeaua de încredere internă și rețelele externe deschise și nesigure, cum ar fi Internetul. Ele folosesc un set de reguli definite pentru a permite sau bloca traficul. Un paravan de protecție poate fi hardware, software sau ambele.

7. Securitatea dispozitivelor mobile

Se estimează că numărul utilizatorilor de telefoane mobile din întreaga lume va depăși cifra de cinci miliarde până în 2019. Această creștere rapidă, din păcate, este direct proporțională cu numărul infractorilor cibernetici care se adaptează și își schimbă metodele pentru a profita de numărul din ce în ce mai mare de potențiale victime.

Datele utilizatorilor reprezintă o țintă majoră a infractorilor cibernetici - de la credențialele cardurilor de credit la parolele de e-mail și listele de contacte, iar furtul lor de pe dispozitivele mobile este facil dacă se coroborează cu accesare rețelelor WiFi de pe telefoanele mobile. Criminalii cibernetici vizează tot mai mult dispozitivele mobile și aplicațiile mobile, sens în care se preconizează că în următorii 3 ani, 90% din organizațiile IT vor oferi sprijin pentru aplicații corporative pe dispozitive mobile personale.

8. Securizarea traficului web

O soluție de securitate web este reprezentată prin controlarea modului de utilizare a Internetului de către personalul unui operator. Se pot bloca amenințările web și se va refuza accesul la site-uri web rău intenționate de pe dispozitivele operatorului. Acesta va proteja gateway-ul web pe

site sau în cloud. "Securitatea Web" include, de asemenea, și măsurile necesare a fi implementate pentru a se proteja propriul site web.

9. Securitatea wireless

Rețelele wireless nu sunt la fel de sigure ca cele cu fir. Abilitatea de a intra într-o rețea de pe un laptop mobil spre exemplu are avantaje deosebite. Cu toate acestea, rețelele fără fir sunt predispuse la anumite probleme de securitate. Hackerii au descoperit că rețelele wireless sunt relativ ușor de accesat și chiar utilizează tehnologia fără fir pentru a intra în rețelele cu fir.

III.4 Metode de securitate în comerțul electronic

Enunțând avantajele comerțului electronic, Luckling-Reiley D. și Spulber D.F. [17] menționau că prin comerțul electronic se asigură accesul la piețe sau clienți inaccesibili fără mijlocirea echipamentelor electronice datorită locației geografice diferite, se reduc costurile de funcționare sau aprovizionare, se mențin disponibile continuu ofertele în mediul on-line, se pot realiza oferte personalizate și crea noi oportunități pentru export.

Comerțul electronic include două tipuri de activități: *comerț electronic indirect* (comandă prin mijloace electronice de bunuri tangibile care ajung de la operator la consumator prin canale tradiționale de distribuție – poștă sau servicii de curierat, plata fiind efectuată fie prin mijloace electronice, fie tradițional la momentul recepției bunurilor) și *comerț electronic direct* (comandă, plată și distribuție electronică de bunuri intangibile, cum ar fi programe informatice, filme sau cărți în format digital sau bilete la diferite spectacole, tot în format de coduri de bare).

Pentru a face viabile din punct de vedere legal, afacerile electronice trebuie să asigure prin mijloace tehnice autenticitatea, legalitatea și securitatea tranzacțiilor și/sau comunicațiilor on-line. Astfel, atât din punct de vedere legal, cât și tehnic (IT) se pune problema autenticității și non-repudierii contractului electronic care stă la baza tranzacției electronice prin folosirea semnăturii electronice, respectiv integritatea, confidențialitatea și disponibilitatea asigurate tranzacției prin mijloacele de plată on-line.

Dintre avantajele aduse activității on-line a operatorului amintim:

1) extinderea activității la nivel local, național și chiar internațional coroborat cu reducerea costurilor pentru desfășurarea activităților firmei,

2) reducerea costurilor de transport și a costurilor de marketing,

3) modelarea facilă și rapidă a ofertelor corespunzător nevoilor cumpărătorilor (prin folosirea anumitor programe de tip cookies).

Totodată și avantajele consumatorilor (utilizatorii finali în cazul comunicațiilor de comerț electronic) sunt numeroase:

1) posibilitatea de a efectua tranzacții sau cumpărături indiferent de locație sau de oră;

2) posibilitatea de alegere, inclusiv prin compararea produselor de la mai mulți operatori;

3) posibilitatea de comparare a prețurilor;

4) livrarea rapidă la locația specificată;

5) urmărirea stadiului comenzii;

6) interacțiunea utilizatorilor-cumpărători fie pe forum-uri specializate, fie prin recenzii chiar pe site-ul de unde se achiziționează [13].

Pentru a face viabile din punct de vedere legal, afacerile electronice trebuie să asigure prin mijloace tehnice autenticitatea, legalitatea și securitatea tranzacțiilor și/sau comunicațiilor on-line. Astfel, atât din punct de vedere legal, cât și tehnic (IT) se pune problema autenticității și non-repudierii contractului electronic care stă la baza tranzacției electronice prin folosirea semnăturii electronice, respectiv integritatea, confidențialitatea și disponibilitatea asigurate tranzacției prin mijloacele de plată on-line.

Semnătura aplicată unui document în formă electronică va fi definită de lege drept semnătură digitală dacă norma juridică este dependentă de tehnologia criptografică cu chei publice folosite, iar dacă abordarea legiuitorului nu presupune legătura cu o tehnologie anume, vorbim de o legislație neutră în care termenul de semnătură electronică este folosit cu predilecție [18].

Avantajul unei legislații dependente de tehnologia semnăturii digitale, prin raportarea strictă a normei juridice la tehnologia de criptare, rezidă în stabilirea exhaustivă a capacităților și limitărilor tehnologiei respective, cu implicații juridice stricte, ce nu pot fi aplicate prin analogie, constituie totodată și un dezavantaj față de legislația care abordează semnătura electronică, pentru că este limitată circulația liberă a produselor și serviciilor bazate pe tehnologii diferite.

Definind **semnătura electronică** drept "*date în format electronic atașate sau asociate logic cu alte date electronice și care servesc ca modalitate de autentificare*", Directiva 1999/93/CE a stabilit (în art.5 Directivă) că numai semnătura electronică avansată, confirmată printr-un certificat calificat și generată cu ajutorul exclusiv al dispozitivului securizat de creare a semnăturii este echivalentă din punct de vedere juridic cu semnătura olografă, generând aceleași efecte juridice și având aceeași forță probantă [18].

Și în reglementarea în vigoare, Regulamentul UE nr. 910/2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE, definiția semnăturii electronice se menține - art.3 pct.10 Regulament 910/2014: "*date în format electronic, ataşate sau asociate logic cu alte date în format electronic şi care sunt utilizate de semnatar pentru a semna*".

Pornind de la enumerarea cuprinsă în art.4 al Legii nr.455/2001 privind definirea conceptelor utilizate înțelegem că datele în formă/format electronică sunt „*reprezentări ale informației într-o formă convențională adecvată creării, prelucrării, trimiterii, primirii sau stocării acesteia prin mijloace electronice*", în timp ce înscrisul în formă/format electronică reprezintă "*o*

colecție de date în formă electronică între care există relații logice şi funcționale şi care redau litere, cifre sau orice alte caractere cu semnificație inteligibilă, destinate a fi citite prin intermediul unui program informatic sau al altui procedeu similar". Deci, informațiile cuprinse într-un înscris electronic care poartă și o semnătură electronică nu sunt neapărat criptate, nu sunt protejate la citire, ele putând fi accesate de oricine.

Folosirea semnăturilor electronice presupune executare următorilor pași:

1) Utilizatorul obține o pereche de chei criptografice unice (privată și publică);
2) Transmițătorul pregătește mesajul, spre exemplu un mesaj tip poștă electronică;
3) Transmițătorul creează semnătura electronică a mesajului folosind un algoritm de criptare și cheia privată;
4) Transmițătorul atașează semnătura electronică mesajului;
5) Transmițătorul expediază mesajul și semnătura electronică către recipient;
6) Recipientul folosește cheia publică a transmițătorului pentru verificarea semnăturii digitale, certificându-se astfel proveniența mesajului și integritatea sa.

Legea nr.365/2002 privind comerțul electronic consacră în terminologie juridică, astfel cum sunt definite în art. 1 pct. 11-13 din lege, drept instrumente pentru plăți electronice:

- *instrumentele de plată electronică* – instrumente tehnice care permite titularului efectuarea următoarele tipuri de operațiuni: a) transferuri de fonduri realizate fără intervenția instituțiilor financiare; sau b) retrageri de numerar, precum şi încărcarea şi descărcarea unui instrument de moneda electronică;

- *instrumente de plată cu acces la distanță* - instrumentele de plată electronică prin mijlocirea cărora titularul instrumentului poate să îşi acceseze liber fondurile disponibile aflate într-un cont personal la o anumită instituție financiară şi sa autorizeze efectuarea unei plăți, utilizând în acest scop un cod personal de identificare sau un alt mijloc similar prin care instituția financiară care primește ordinul de plată să poată identifica pe titularul operațiunii în persoana titularului contului;

- *instrument de monedă electronică* - instrument de plată electronică reîncărcabil, diferit de instrumentul de plată cu acces la distanță, și în cazul căruia unitățile de valoare sunt stocate în format exclusiv electronic, asigurând titularului instrumentului posibilitatea de a efectua toate tipurile de operațiuni posibile și recunoscute prin instrumentele de plată electronică.

Pornind de la cardurile bancare, metodele de plată electronice actuale s-au diversificat, însă toate presupun folosirea protocoalelor de plată prin care se realizează o verificare on-line despre deținătorul de card din cadrul unei tranzacții on-line. Spre exemplu, protocolul SSL este standardul pentru comunicația client-server securizată în Web, fiind integrat în toate serverele și browserele, deoarece utilizează criptografia cu chei publice, asemenea protocolului SET (*Secure Electronic Transaction*) și iKP (*Internet Keyed Payments Protocol),* dar, de regulă, serverele (operatorii

comerciali) au certificate în timp ce cumpărătorii sunt anonimi.

Protocoalele de tip iKP se ocupă de tranzacții de plată, operațiuni în care sunt implicați trei participanți: cumpărătorul, operatorul comercial și banca, astfel încât principala protecție criptografică se referă la criptarea fișei de plată cu cheia publică a băncii și cu semnătura sa pe autorizație, contul cumpărătorului fiind menținut secret [34].

Protocolul SET (*Secure Electronic Transaction*) este o metodă de plată securizată, un standard deschis ce poate fi aplicat la orice serviciu de plată, având ca suport al plăților cardurile de credit.

III.5 Programe antivirus versus programe firewall

Antivirus sau software antivirus (adesea abreviat ca AV), uneori cunoscut sub numele de software **anti-malware**, este un software de calculator folosit pentru a **preveni, detecta și elimina** software-ul rău intenționat dintr-un sistem de operare.

Software-ul antivirus a fost inițial dezvoltat pentru detectarea și eliminarea virușilor de pe computer, de unde și numele. Cu toate acestea, odată cu proliferarea altor tipuri de malware, software-ul antivirus a început să ofere protecție împotriva altor amenințări la adresa calculatorului. În special, software-ul antivirus modern poate proteja calculatoarele impotriva : obiectelor de ajutor pentru browser rău-intenționate (BHO), atacatori de browser, ransomware, keyloggers, backdoor, rootkits, cai troieni, viermi,malware LSPs, dialere, tool-uri frauduloase, adware și spyware.

Există mai multe metode pe care antivirus-ul le poate utiliza pentru a identifica programele malware:

- Detectarea sandbox-urilor: este o tehnică specială de detectare bazată pe comportament care, în loc să detecteze amprenta comportamentală la timpul de execuție, execută programele într-un mediu virtual, înregistrând ce acțiuni desfășoară programul. În funcție de acțiunile înregistrate, motorul antivirus poate determina dacă programul este rău intenționat sau nu, iar dacă nu se identifică un comportament dubios atunci programul este executat în mediul real. Aceată tehnică eficientă ca detecție este greoaie deoarece încetinește fucționarea sistemului de operare pe timpul rulării programului anit-virus, fiind astfel rar utilizată
- **Tehnicile de extragere a datelor**: sunt una dintre cele mai recente abordări aplicate în detectarea malware-ului. Minerii de date și algoritmii de învățare a mașinilor sunt folosiți pentru a încerca să clasifice comportamentul unui fișier (fie ca fiind malware fie ca fiind benign) dat o serie de caracteristici de fișier care sunt extrase chiar din acel fisier.
- Rootkit detection. Software-ul anti-virus poate încerca să scaneze pentru rootkit-uri. Un rootkit este un tip de malware conceput pentru a obține control la nivel administrativ asupra unui sistem informatic fără a fi detectat.

Cercetări privind securitatea datelor în sistemele informatice

Pornind de la reguli predefinite, un firewall, ca mecanism de protecție pentru rețelele de calculatoare, este un dispozitiv sau o serie de dispozitive configurate în vederea filtrării accesului utilizatorilor, în scopul criptării informațiilor transmise în rețea dar și în vederea gestionării unui trafic securizat între diferite nivele de securitate prestabilite pentru siguranța rețelei de calculatoare.

O altă definiție dată programelor firewall este de ansamblu de componente hardware și software care se interpun între două rețele pentru a regla și controla traficul dintre ele [37].

Un **firewall** va asigura utilizatorului și chiar rețelei față de care acționează:

- m**o**nitorizare**a** căilor de pătrundere neautorizată în rețeaua privată, inclusiv monitorizarea traficului în rețea și asigurând astfel implicit o detectare mai facilă a încercărilor de infiltrare și/sau acces neautorizat;
- **blocarea** traficului în şi dinspre Internet, în cazuri de alerte/incidente de securitate, asigurând un acces controlat al echipamentelor din rețea la adresele din Internet;
- s**e**lectarea accesului în spațiul privat luându-se în considerare informațiile conținute în pachetele lansate în trafic.
- **permiterea sau interzicerea** accesului la rețeaua publică de Internet din anumite stații specificate și interconectate și la rețeaua privată;
- i**z**olare**a** spațiul privat de cel public, în scop de protecție în fața atacurilor informatice depistate şi realizarea unei interfețe între cele două spații ale mediului virtual.
- m**o**nitorizeze **traf**icul dintre rețeaua locală și Internet, creând filiere jurnal pentru orice eveniment observat.

În funcție de nivelul modelului OSI sau TCP/IP la care operează firewall-ul se identifică: fi**re**wall-uri de filtrare (nive**l** 3) care execută filtrarea traficului dintre rețeaua locală și Internet, blocând accesul anumitor elemente care pot reprezenta factori de risc pentru rețeaua locală [16]; **firewall-uri porți de circuit** (nivel 5) care monitorizează sesiunile TCP dintre rețeaua locală și Internet, având viteză sporită de filtrare, însă filtrarea se face doar în funcție de titlu și nu de întregul pachet [4]; fi**re**wa**ll-u**ri interme**d**iare (nivel 7) care nu permit trecerea directă a traficului între calculatoarele locale și Internet [28], programul executând el însuși unele din serviciile de rețea, ascunzând astfel existența rețelei locale față de Internet.

Cercetări privind securitatea datelor în sistemele informatice

III.6 Concluzii și rezultate obținute

- Criterii de care trebuie ținut cont în alegerea unui program antivirus:

1) Rata de detecție – fiind recomandat să optăm pentru un produs antivirus cu o detecție de peste 97%;

2) Viteza de reacție la o nouă amenințare, fiind de optat pentru o soluție de protecție care să recunoască noile amenințări într-un timp cât mai scurt;

3) Suportul tehnic oferit de dezvoltator - astfel utilizatorii își pot clarifica nelămuririle privind configurarea și setările programului. Serviciile de suport tehnic trebuie să aibă un spectru larg al canalelor de livrare, cum ar fi baze de date FAQ, forum-uri, newsletter, e-mail-uri, rețele sociale, telefon, etc.;

4) Gradul de utilizare a resurselor calculatorului utilizatorului este de dorit să fie cât mai redus pentru a nu se încetini activitatea sistemului în timp ce programul antivirus își efectuează scanările de rutină și operațiunile de dezinfecție. Din aceste motive programele antivirus sunt dotate cu moduri speciale tip GAME MODE (opțiune folosită în timpul unui joc care suspendă scanările automate, notificările sau up-date-urile antivirusului);

5) Viteza de scanare poate cântări considerabil în alegerea unei soluții de protecție antivirus, în condițiile în care volumul de informații stocate și complexitatea operațiunilor efectuate impun dimensiuni tot mai mari ale hard diskurilor.

- Din perspective de securitate informațională, propunem folosirea de către instituțiile bancare, pentru efectuare plăților prin sistemele informatice, a protocoalelor precum iKP (Internet Keyed Payments Protocol), SET (Secure Electronic Transaction dezvoltat de Visa și Mastercard), OPT (Open Trading Protocol), SNPP (Simple Network Payment Protocol), SEPP (Secure Electronic Payment Protocol) sau STT (Secure Transaction Technology).

CAPITOLUL IV
CERCETĂRI PRIVIND CADRUL NORMATIV ACTUAL ÎN DOMENIUL SECURITĂȚII INFORMATICE

Directiva UE 1148/ 2016 (NIS, Network Internet Security) privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune, act ce trebuie implementat și aplicat la nivelul statelor membre UE până la data de 9 mai 2018, este considerată drept un deziderat necesar în vederea atingerii obiectivelor *Strategiei europene pentru o piață unică digitală* asumată de Comisia Europeană.

Cadrul minimal asigurat prin Directiva UE nr.1148/2016 stabilește astfel legiuitorilor din statele membre Uniunii, printre care şi România, cerințele minimale pentru instituirea la nivel național a cadrului legislativ adecvat, astfel încât prin măsurile implementate să fie responsabilizați deținătorii/proprietarii de infrastructuri cibernetice cu privire la funcționarea acestora în condiții de maximă securitate, respectiv nivelul necesar pentru implementarea măsurilor tehnice privind creşterea capacităților de reacție și intervenție la incidentele cibernetice și în scopul diminuării impactului acestora asupra societății informaționale actuale.

În acest scop, în reglementarea Directivei NIS se regăsesc ca principii și condiții minimale obligatorii pentru statele membre UE :

- obligativitatea stabilirii pentru toate statele membre UE a necesității de adoptare a strategiei națională privind securitatea rețelelor și a sistemelor informatice;
- necesitatea constituirii unui grup de cooperare pentru sprijinirea și facilitarea cooperării strategice și a schimbului de informații între statele membre UE precum și pentru a dezvolta încrederea parteneriatelor dintre acestea în privința securității cibernetice;
- necesitatea constituirii unei rețele europene a echipelor de intervenție în caz de incidente de securitate cibernetică pentru a promova cooperarea operațională rapidă și eficace;
- stabilirea cerințelor de securitate cibernetică și notificarea pentru operatorii de servicii esențiale și pentru furnizorii de servicii digitale;
- stabilirea pentru statele membre a obligațiilor de desemnare a autorităților competente la nivel național pentru securitate cibernetică, a punctelor unice de contact și a CSIRT/CERT-urilor cu atribuții legate de securitatea rețelelor și a sistemelor informatice de la nivel național.

Din perspectiva reglementărilor cadrului minimal prin Directiva NIS, statele membre trebuie să actualizeze lista operatorilor de servicii esențiale în domeniul securității comunicațiilor şi tehnologiilor informațiilor, criteriile minimale pentru identificarea furnizorilor de servicii esențiale care trebuie să se regăsească și în legislațiile naționale fiind următoarele:

- furnizorii trebuie să asigure furnizarea unui serviciu esențial pentru susținerea activităților societale și/sau economice de cea mai mare importanță;

- furnizarea serviciului în cauză depinde exclusiv de tipul de rețea precum și de caracteristicile sistemelor informatice;
- furnizarea serviciilor nu trebuie perturbate de nici un incident de securitate.

IV.1 Confortul siguranței juridice pentru operațiuni prin sisteme informatice

Informația în format electronic a devenit o resursă de producție, o proprietate națională vitală pentru configurarea infrastructurilor din domenii de interes național, o valoare strategică pentru dezvoltarea instituțională, o valoare economică și juridică care dacă nu este protejată printr-un sistem juridic și prin mecanisme tehnice și proceduri tehnologice, poate fi accesată în mod neautorizat, contrafăcută și chiar distrusă.

Deși din punct de vedere tehnic, sistemele informatice actuale și tehnologiile privind securitatea informațiilor în mediul virtual reprezintă tipologii de tehnologii caracteristice dezvoltării contemporane, la nivel de reglementare juridică a tehnicii și tehnologiilor informaționale în prezent România nu a atins maximul de reglementare legislativă, deși cadrul normativ este conturat (legea privind comerțul electronic, legea privind semnătura electronică, legea privind securitatea datelor și prelucrării datelor cu caracter personal, anumite infracțiuni privind securitatea tehnologică și folosirea neautorizată a echipamentelor tehnologice cuprinse în codul penal și în legi penale speciale).

Un sistem normativ de drept informatic îşi găseşte o prelungire firească într-un sistem de drept al informării şi comunicării. În mod tradițional, dreptul informării este conceptualizat în strânsă legătură cu libertatea de exprimare, libertate de circulație și libertate de opinie, iar obiectul său de reglementare este limitat la ceea ce devine public și respectiv informație publică prin mijlocirea diverselor instrumente: scris, imagine şi sunet.

Dreptul informatic sau dreptul Internetului este susținut și conlucrează (având în acest scop un loc bine determinat) cu întregul sistem tehnologic la nivel național care ține de tratarea (prelucrarea) datelor şi serviciilor dedicate informației prin sisteme informatice competente.

Dacă la origini Internetul nu a fost reglementat prin norme juridice adică reguli cu caracter general obligatoriu a căror nerespectarea angajează răspunderea celui care nu respectă regula cauzând prejudicii unei alte persoane, nefiind previzionat la actualul grad de dezvoltare și implementare în activitățile societății contemporane, începând cu secolul XX s-a resimțit necesitatea implementării unor reguli de conduită obligatorii pentru reglementarea relațiilor sociale cu privire la Internet.

IV.1.1 Reglementarea juridică a comerțului electronic

Dezvoltarea exponențială a folosirii Internet-ului în activitate curentă a fost percepută de diferite medii de afaceri drept o necesitate și oportunitate funcțională. Trebuie însă conștientizat că alături de oportunitățile de afaceri într-un mediu deosebit, Internetul prezintă și o serie de

dezavantaje sau „capcane" care trebuie luate în considerare per ansamblul activității pentru a se evita astfel pierderi considerabile, în primul rând sunt avute în vedere pierderile financiare.

Cele mai mari amenințări care se ridică în fața comerțului electronic sunt:

- *securitatea, încă precară, a tranzacțiilor în mediul on-line;*
- *lipsa unor reglementări juridice clare şi armonizate la nivel global*

Marketingul direct, operațiune aferentă şi de susținere a dezvoltării comerțului electronic, justificat prin interesul legitim al consumatorului în calitate sa de utilizator al unei baze de date, trebuie gestionat proporțional cu scopul propus de operator, deoarece transmiterea (masivă) de mesaje comerciale nesolicitate, justificate prin nevoia de promovare, este plasată la granița tehnică a atacului informatic sub forma *spam*-ului. Protecția reală a consumatorului impune aplicarea sistemului opțiunii de intrare *(option-in)*, ceea ce presupune ca în cazul unui mor prealabil al destinatarului contului, în calitate sa de utilizator al poștei electronice. În lipsa acestor măsuri tehnice, intimitatea virtuală a utilizatorului, drept ce derivă din interesele sale legitime va rămâne la nivelul unui concept pur teoretic.

Prin raportare la principiile implementate de actualul Regulamentul GDPR, principalul argument adus pentru excluderea marketingul direct din conceptul acoperit prin sintagma „interes legitim", nici chiar din perspectiva reglementării regulamentare, este acela al protecției vieții private a persoanei vizate. În unele legi naționale (inclusiv Legea nr.365/2002 privind comerțul electronic) de transpunere a directivelor europene referitoare la comerțul electronic (Directiva 2000/31/CE) și cea referitoare la protecția vieții private în sectorul comunicațiilor electronice (Directiva 2002/58/CE), este consfințit sistemul obținerii în mod prealabil prelucrării datelor personale a consimțământului valabil exprimat de către persoana vizată în momentul transmiterii comunicărilor comerciale.

Se constată că reglementarea normativă națională privind comerțul electronic instituie respectarea celor două reguli necesare pentru garantarea intimității virtuale: legalitatea comunicărilor comerciale care întrunesc calitatea de servicii ale societății informaționale și *option-in-ul* (sistemul opțiunii de confirmare a acordului la momentul intrării). Comunicările promoționale/comerciale în mediul on-line, respectiv prin poșta electronică sunt calificate drept servicii ale societății informaționale, fiind astfel asimilate unor activități de prestări de servicii prin care se constituie, se modifică, se transferă ori este stins un drept real asupra unui bun corporal sau necorporal.

IV.1.2 Reglementarea juridică privind protecția și prelucrarea datelor cu caracter personal din bazele de date

Dacă Directiva 1995/46/CE a prezentat dezavantajul aplicării neuniforme a dispozițiilor sale prin preluările în sistemele naționale (prin implementarea în legislațiile naționale a cadrului minimal din directivă, dar și prin reglementări proprii în scopul armonizării cu sistemul național juridic) în funcție de nivelul de reglementare juridică la nivel național privind sistemele informatice și a

operațiunilor cu sisteme informatice, Regulamentul UE nr.2016/679 (GDPR) îndeplinește misiunea de armonizare normativă, garantată și prin aplicarea imediată, directă și prioritară în cadrul normativ al statelor membre.

În cadrul acestui nou mediu digital, persoanele au dreptul să beneficieze de un control efectiv asupra informațiilor cu caracter personal. Protecția datelor personale este un drept fundamental în Europa, reglementat și adus la nivel de principiu al demnității umane atât prin textul articolului 8 din Carta drepturilor fundamentale a Uniunii Europene cât și a articolului 16 aliniatul (1) din Tratatul privind funcționarea Uniunii Europene (TFUE), care trebuie protejat în mod corespunzător, inclusiv din perspectiva procesării acestor categorii de date prin sisteme informatice automatizate sau care necesită intervenție umană (anumite aplicații, platforme locale și/sau regionale/globale).

Comisia Europeană a adoptat din anul 2016 o reformă fundamentală a cadrului normativ european privind protecția datelor cu caracter personal, asigurând și o etapă de tranziție prin prorogarea intrării în vigoare pentru cursul lunii mai 2018, fiind adoptate două acte:

- un regulament (de înlocuire a Directivei 95/46/CE), care stabilește un cadru general la nivel european și uniformizat la nivelul statelor membre UE privind protecția datelor Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (GDPR) , cu aplicare directă și obligatorie în toate statele membre, inclusiv în România, începând cu data de 25 mai 2018, fără a fi necesară vreo transpunere.

și

- o directivă (de înlocuire a Deciziei-cadru 2008/977/JAI), care definește normele privind protecția datelor cu caracter personal prelucrate în scopul **prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor, precum și în scopul activităților judiciare** conexe: Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului, acest act normativ având termen limită de implementare în ordinea juridică națională a statelor membre data de 06 mai 2018.

Principalele noțiuni din Regulamentul UE 2016/679, grefate pe terminologia consacrată încă din Directiva 1995/46/CE, asimilează un plus de reglementare cantitativă și calitativă în cuprinsul lor, completările, respectiv adaptările conținutului noțiunilor incluzând aspectele validate după anul 1995 din aplicarea Directivei inițiale și astfel sunt înlăturate și anumite dificultăți de interpretare.

Pentru exemplificarea clarificărilor nou aduse de textul actualului Regulament este calificarea legală a noțiunii-cadru „*date cu caracter personal*", care, în enumerarea art. 4 pct. 1 din Regulamentul GDPR, abordează pe lângă elemente clasice de identificare și identificatorii online (cont de e-mail și IP asociat), datele genetice și datele de localizare.

Doctrina de specialitate a susținut vocația Directivei 1995/46/CE de a se aplica în privința prelucrărilor de date personale prin intermediul Internetului, respectiv a folosirii Internetului, ca mediu virtual, pentru transferul datelor personale și în acest sens se poate extrage art. 17, text în care se stabilește necesitatea implementării măsurilor necesare de protecție a datelor personale de către responsabilul prelucrării, mai ales în contextul în care prelucrarea presupunea transmiterea datelor într-o rețea deschisă (cum este și Internetul).

Regulamentul GDPR stabileşte obligatoriu cerințe minimale pentru prelucrarea datelor cu caracter personal, unele dintre acestea fiind nou introduse comparativ cu vechea reglementare, pe care le prezentăm mai jos:

- posibilitatea de a obține informații cuprinzătoare asupra scopului și temeiului legal în care sunt colectate și prelucrate datele cu caracter personal;

- obligativitatea definirii de către operatorii care prelucrează date personale și a informării persoanei vizate asupra perioadei de stocare a datelor și drepturile de care aceasta beneficiază în acest interval în acord cu interesele operatorului pentru stocarea datelor;

- dreptul de a fi uitat, drept ce poate fi exercitat și în privința prelucrărilor de date în mediul on-line (excepție în cazul în care prelucrarea este necesară pentru respectarea libertății de exprimare și a dreptului la informare la persoanei vizate, respectiv pentru respectarea unei obligații legale a operatorului de date, sau pentru aducerea la îndeplinire a unei sarcini care servește unui interes public legitim.

- obligația operatorului de date de a proba obținerea neviciată a consimțământului pentru prelucrările de date personale în care consimțământul persoanei fizice vizate trebuie exprimat fără echivoc;

- portabilitatea datelor personale;

- posibilitatea de a cere transferul datelor de la un operator la alt operator de date menționat expres coroborată cu obligativitatea operatorului inițial de a transfera datele într-un format structurat în acord cu scopul solicitării transferului, astfel încât operatorul la care se realizează transferul să poată utiliza în mod curent, interoperabil și accesibil inclusiv prelucrărilor automat a datelor în structura în care a fost solicitat și obținut transferul.

Reglementarea cadrului necesar pentru evaluarea impactului asupra protecției datelor personale conferă acțiunilor operatorilor de date, cu impact asupra responsabilizării lor sociale :

- demonstrarea că prelucrarea de date cu caracter personal s-a efectuat cu respectarea dreptului la demnitate și viață privată a persoanei vizate;
- asigurarea estimării impactului prelucrărilor asupra vieții particulare a persoanelor vizate;
- demonstrarea respectării și asumării principiilor fundamentale ale Regulamentului nr. 679/2016 de către operator.

În acest sens au fost introduse 2 noi concepte, *privacy by design* și *privacy by default*. Principiul „Confidențialitatea / protecția datelor prin proiectare" se bazează pe abordarea privind confidențialitatea încă de la începutul procesului de proiectare a sistemelor și este o strategie preferabilă în comparație cu încercarea de adaptare a unui produs sau serviciu într-o etapă ulterioară.

IV.1.3 Reglementarea actuală a infracțiunilor contra siguranței și integrității sistemelor informatice și datelor

Abordând problematica infracțiunilor din domeniul IT, se constată în literatura de specialitate [46], [11], [12] preocuparea pentru definirea unitară a noțiunii de *criminalitate informatică*, definiție care ar asigura o uniformizare a incriminărilor în materie, astfel încât limbajul juridic să surprindă întocmai procesele tehnice. De asemenea, preocupările pentru impunerea unei definiții și terminologii care să descrie infracțiunile din domeniul informatic continuă și în prezent, fiind și subiect al cercetărilor științifice doctorale[45], [29].

Nici din perspectiva textelor legale nu există un consens la nivel internațional în privința terminologiei privind criminalitatea informatică, iar definiția legală a infracțiunii informatice lipsește cu desăvârșire (a se vedea în acest sens și textul Directivei 2013/40/UE privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului). Constatăm, la nivel internațional, folosirea alternativă a mai multor termeni pentru descrierea infracțiunilor comise asupra și/sau prin intermediul calculatoarelor sau sistemelor informatice precum computer-related-crime, cyber crime, high-tech crime, e-crime sau electronic crime.

În esență, dacă analizăm infracțiunile informatice, astfel cum au fost ele definite inițial în Legea nr. 161/2003 dar şi în actuala reglementare penală [Cod Penal Român], constatăm că suntem în prezența unor infracțiuni de drept comun la săvârşirea cărora autorul, de cele mai multe ori persoană specializată cu cunoştințe în domeniul informatic, foloseşte sistemele informatice. Astfel, calculatorul sau rețeaua, pe de o parte, şi programele informatice, pe de altă parte, sunt fie ținta directă a unor fapte penale (infracțiunea de acces ilegal la un sistem informatic sau cea de interceptare ilegală a unei transmisii de date informatice), fie instrumentul sau mijlocul de manipulare al unei fapte penale (efectuarea sau acceptarea de operațiuni financiare frauduloase, fraude legate de comerțul electronic) sau mijlocul de stocare a unor eventuale probe privind săvârşirea unor fapte penale (pornografia infantilă).

Cercetări privind securitatea datelor în sistemele informatice

Chiar dacă definiția standard a infracțiunii informatice nu este stabilită unanim, fenomenul infracțional există şi ia amploare, fapt pentru care această conduită dezvoltată prin intermediul sau în legătură cu utilizarea sistemelor informatice şi/sau a rețelelor de comunicații trebuie incriminată penal. Dintre definițiile reținute în doctrină [33], [12], optăm pentru definirea *lato sensu* a criminalității informatice drept ansamblul infracțiunilor comise într-un interval temporal și spațial determinat prin intermediul sau în legătură cu utilizarea sistemelor informatice sau rețelelor de comunicații, care pot fi instrumentul, obiectul-țintă sau locația acestor infracțiuni.

Înțelesul noțiunilor de *sistem informatic* și *date informatice* prin preluarea definițiilor din art.35 alin.1 lit.(a) și lit.(d) din Legea nr.161/2003, adoptarea Legii nr.187/2012 nu au abrogat expres dispozițiile anterior menționate, deși prin art.130 din Legea nr.187/2012 sunt aduse modificări exprese la Legea nr.161/2003 privind abrogarea integrală a Secțiunilor 1, 2 și 3 ale Capitolului III din Titlul III destinat prevenirii și combaterii criminalității informatice, însă numai a textelor privind incriminarea infracțiunilor informatice. Astfel, menținându-se definițiile din art.35 al Legii nr.161/2003 acestea își vor găsi aplicabilitate în domeniul răspunderii contravenționale cu privire la nerespectarea obligațiilor legale pentru prevenirea criminalității informatice, aspecte reglementate de art.52 raportat la art.41 din Legea nr.161/2003.

Un sistem informatic include echipamente (elemente de hardware) și programe informatice (elemente de software), alcătuind subsistemul tehnic și subsistemul social care asigură furnizarea informației [39], astfel încât cele două componente – tehnic și social – formează o rețea socio-tehnică unitară.

Lipsa definiției legale a noțiunii de program informatic din textul art.181 al actualului Cod penal pentru a avea elementele de incriminare în situația reglementată de art.365 din Codul penal se complinește, paradoxal, prin trimiterea la textul art.35 alin.1 lit.(d) și (h) din Legea nr.161/2003, text în vigoare conform art.130 din Legea nr.187/2012, și potrivit căruia prin *program informatic* se înțelege „*un ansamblu de instrucțiuni care pot fi executate de un sistem informatic în vederea obținerii unui rezultat determinat*", respectiv prin *măsuri de securitate*]n sens juridic sunt vizate „*folosirea unor proceduri, dispozitive sau programe informatice specializate cu ajutorul cărora accesul la un sistem informatic este restricționat sau interzis pentru anumite categorii de utilizatori*".

Gravitatea, dimensiunea transfrontalieră și impactul general asupra societății al infracțiunilor informatice, luând în considerare că rețelele de calculatoare și informația electronică ar putea fi utilizate pentru comiterea de infracțiuni, dar și pentru stocarea și transmiterea probelor incriminatoare, au determinat statele membre ale Consiliului Europei se adopte în anul 2001 Convenția privind criminalitatea informatică [Convenția Consiliului Europei 2001], act juridic care oferea cadrul minim pentru definirea și incriminare faptelor prin și a disponibilității datelor şi implicit a

sistemelor informatice, pentru ca infracțiunile informatice să fie circumscrise în domeniul fraudei informatice și a falsului informatic.

Directiva 2013/40/UE urmărește asigurarea protecției sistemelor informatice în fața atacurilor și vulnerabilităților sistemelor informatice în condițiile în care tehnologiile contemporane devin valoare socială ocrotită de norma penală datorită rolului său în dezvoltarea actualei societăți informaționale.

Art.362 Cod penal incriminează fapta de alterare a integrității datelor informatice, ceea ce se poate realiza prin acțiuni alternative de modificare, ștergere, deteriorare sau restricționare a accesului la acestea inducând percepția că datele au fost șterse din sistem, deși ele sunt în continuare dar nu mai este permisă accesare lor. Prin aceste acțiuni se generează efecte negative asupra stării datelor care nu mai servesc scopului lor, datele fiind modificate față de cele inițiale care prezentau importanță pentru un anumit utilizator.

Acțiunea de transfer de date informatice neautorizat, incriminată la art.364 Cod penal este în fond tot un tip de intervenție direcționată asupra datelor, însă autorul nu modifică conținutul datelor sau reprezentarea lor binară, ci modifică doar locația inițială a datelor fie în cadrul aceluiași sistem informatic, fie de pe un suport de stocare curent pe un alt suport de stocare extern. În cazul transferului de date în același sistem doar prin schimbarea locației se poate crea și impresia alterării datelor prin ștergere, faptă incriminată de art.362 Cod penal, însă încadrarea juridică se va face în raport cu conținutul datelor informatice care diferă în cazul celor două acțiuni menționate.

Tot datele informatice sunt obiectul material și în cazul infracțiunii de perturbare a funcționării sistemelor informatice – art.363 Cod penal – deși alături de date acțiunea poate fi orientată și asupra celorlalte componente ale sistemului informatic, datele nefiind alterate.

Conduita incriminată de textul art.363 Cod penal constă fie în acțiuni de alterare a datelor informatice dar care au ca efect și alterarea funcționării sistemului în care sunt modificate aceste date, fie în acțiunea de introducere în sistem a anumitor programe malițioase, aparent inofensive – viruși, viermi, cai troieni – care sunt plasate în sistemul informatice de la distanță, prin interconectările existente în rețelele de comunicații și prin intermediul cărora se transferă date din sistemul informatic afectat sau se descarcă anumite programe care defectează funcționarea sistemului, acesta generând erori funcționale și nemaiputând în unele cazuri fi recuperat nici sistemul, nici datele stocate în el.

IV.2 Protecția juridică a bazelor de date la nivelul Uniunii Europene

Conform articolului 8 al Convenției Europene a Drepturilor Omului este consacrat dreptul de protecție împotriva colectării şi utilizării datelor cu caracter personal, drept circumscris sferei protecției vieții private a persoanelor fizice, respectiv a vieții de familie și a vieții particulare, sfera extinzându-se și asupra dreptului la domiciliu și la confidențialitatea corespondenței, dreptul astfel

reglementat derivând din dreptul de autor (autor și titular asupra propriilor date care îl identifică ca și individ).

Definit juridic ca un drept *sui generis* al autorilor bazelor de date, protecția juridică asupra bazelor de date are ca reper aspectul creativ și cel pecuniar al activității de realizare al unei baze de date (în scopul realizării bazei de date au fost realizate acțiuni de colectare, sortare și grupare pe diferite criterii a datelor în baza de date obținută ca produs final), și nu pornește ca argumentare juridică de la actul propriu-zis de creare al bazelor de date, acesta din urmă fiind circumscris dreptului de autor. Din această perspectivă juridică, dacă un operator urmărește să investească timp și resurse proprii (atât resurse umane, cât și resurse financiare) pentru obținerea, verificarea sau prezentarea conținutului unei baze de date, originalitatea produsului final, respectiv baza de date astfel create, constă în modul de realizare (prin aplicarea criteriile de selectare și/sau organizare) și a celui de prezentare a bazei de date, mai ales în condițiile în care realizarea bazei de date pornind de la criteriile astfel conturate era strict necesară derulării propriei activități a operatorului.

La nivel european se constată conturarea unui cadru legislativ consolidat în privința protecției juridice a invențiilor, mărcilor și drepturilor de autor (Directiva 89/104/CEE din 21 decembrie 1988, de apropiere a legislațiilor statelor membre privind mărcile, publicată în Jurnalul Oficial nr. L 40/11.02.1989; Directiva Consiliului 91/104/CEE din 14 mai 1991, respectiv Directiva Consiliului 91/250/CEE din 14 mai 1991 privind protecția juridică a programelor pentru calculator, publicată în Jurnalul Oficial nr. L 122/17.05.1991; Directiva Consiliului 92/100/CEE din 19 noiembrie 1992, privind dreptul de închiriere şi de împrumut şi anumite drepturi conexe dreptului de autor în domeniul proprietății intelectuale, publicată în Jurnalul Oficial nr. L 346/24.11.1992; Directiva Consiliului 93/83/CEE din 27 septembrie 1993, privind armonizarea anumitor dispoziții referitoare la dreptul de autor şi drepturile conexe aplicabile difuzării de programe prin satelit şi retransmisiei prin cablu, publicată în Jurnalul Oficial nr. L 248/06.10.1993; respectiv Directiva Consiliului 93/98/CEE din 29 octombrie 1993, privind armonizarea duratei de protecție a dreptului de autor şi a anumitor drepturi conexe, publicată în Jurnalul Oficial nr. L 290/24.11.1993), context în care în anul 1996 a fost adoptată și Directiva Parlamentului European şi a Consiliului 96/9/CE din 11 martie 1996, fiind actul normativ care definește și garantează ca drept distinct dreptul *sui-generis* al autorilor de baze de date.

IV.2.1. Drepturile și obligațiile autorilor de baze de date vs. drepturile și obligațiile utilizatorilor de baze de date

Din perspectivă tehnică şi juridică, sintagma prelucrarea datelor cu caracter personal acoperă semantic orice operațiune sau set de operațiuni care se realizează direct asupra datelor cu caracter personal, prin mijloace automate sau neautomate (atât operațiuni cu baze de date, cât şi operațiuni realizate în formă scriptică prin folosirea unor registre/agende de lucru), cum ar fi:

colectarea, înregistrarea, sistematizarea, arhivarea, modificarea, extragerea, utilizarea, divulgarea prin transfer către terțe părți, promovarea, alăturarea ori combinarea, blocarea, ştergerea parțială sau distrugerea datelor.

Dreptul la informare al persoanei vizate trebuie asigurat cu maximă diligență mai ales în cazul în care datele nu provin în mod direct de la persoana vizată, situație în care aceleaşi informații anterior menționate trebuie sa fie furnizate persoanei vizate de către operator obligatoriu fie în momentul colectării datelor, fie cel mai târziu până în momentul primei dezvăluiri, în situația în care scopul prelucrării necesită dezvăluirea datelor către terți, cu excepția cazului în care persoana vizată se afla deja în posesia reperelor cuprinse în informarea realizată.

Oricărei persoane vizate îi este recunoscut și garantat dreptul de a obține de la operatorul care îi prelucrează datele personale, pe bază de manifestare expresă a voinței (prin cerere scrisă) şi în mod gratuit pentru o solicitare pe an, confirmarea stagiului prelucrării datelor care o privesc.

Prin asigurarea legală a acestui drept, persoana vizată ia cunoștință de stadiul prelucrării datelor sale, pe de altă parte persoana în cauză se asigură astfel că datele folosite de operatorul față de care și-a exprimat consimțământul în privința prelucrării sunt actuale şi conforme scopului declarat la momentul colectării în vederea prelucrării (acest drept este reglementat ca fiind dreptul de acces în codificarea Regulamentului UE 679/2016).

IV.3 Jurisprudență europeană în domeniul protecției bazelor de date şi a datelor cu caracter personal

În acord cu prevederile art. 3 din Directiva 96/9/CCE, bazele de date obținute prin desemnarea sau ordonarea elementelor constitutive ca și elemente de originalitate creativă, reprezintă o creație intelectuală proprie a autorului/operatorului care a prelucrat în acord cu anumite criterii bazele proprii de date, situație în care intersele de prelucrare și gestionare a acestor baze de date sunt protejate ca atare în virtutea dreptului de autor, fără ca acest drept să se extindă și asupra conținutului informațiilor din acea bază de date. Pe același argument juridic, în art.4 din Directivă este stabilită calitatea de autor al unei baze de date, fie a persoanelor fizice, fie a persoanelor juridice, prin raportare la activitatea concretă de colectare și de creare a bazei de date propriu-zisă.

De la data de 1 ianuarie a anului calendaristic care urmează finalizării conturării unei baze de date, pentru o perioadă de de 15 ani autorul/creatorul bazei de date este protejat prin dreptul sui-generis astfel consacrat de legislație, fără a fi necesară constatarea acestei protecții de către o autoritate anume (art.10 Directiva 96/9/CCE).

În virtutea drepturilor sale sui-generis, producătorul bazei de date are recunoscută prerogativa de a interzice terților extragerea și reutilizarea ansamblului sau ale unei părți substanțiale, evaluată calitativ sau cantitativ, a conținutului bazei de date astfel create și protejate, atunci când obținerea, verificarea sau prezentarea acestui conținut atestă o investiție pecuniară

consistentă din punct de vedere calitativ sau cantitativ (art.7 alin.1 Directiva 96/9/CCE). Producătorul bazei de date, în virtutea aceluiași *drept sui-generis,* dacă constată că un terț îi încalcă interdicția stabilită de utilizare și folosește baza sa de date, are dreptul conferit de lege de a se adresa instanței judecătorești în vederea protejării dreptului său *sui-generis* și de a obține totodată obligarea celui care i-a încălcat astfel dreptul de a respectării dreptului său sui-generis și obligarea la eventuale daune-interese dovedite, conform principiului răspunderii juridice patrimoniale delictuale [25].

Prin soluțiile pronunțate în intervalul noiembrie 2004 - ianuarie 2005 s-a stabilit ca și principiu și criteriu unitar de aplicare a dispozițiilor minimale din Directiva 96/9/CCE a regulii potrivit căreia protecția prin recunoașterea dreptului sui-generis al autorului unei baze de date se referă la obținerea, verificarea și prezentarea conținutului bazei de date realizate, respectiv adunarea și ordonarea după anumite criterii proprii a datelor, activitatea astfel desfășurată nu se va confunda cu crearea sau generarea de date într-o bază, inclusiv nu va interfera cu activitatea de verificare a datelor înaintea introducerii în baza de date [25].

În speța soluționată de către Curtea Europeană de Justiție *British Horseracing Board ("BHB") v. William Hill ("WH"),* persoana juridică BHB realizase o bază de date privind cursele de cai, bază de date în care ordonase ca și criterii de selecție în funcție de numele cailor, numele proprietarilor, antrenorilor și ale jocheilor, grupate într-o bază intitulată *liste de prindere,* pentru ca o firmă concurentă în piață, WH, să preia baza astfel creată și să o rearanjeze în vederea difuzării pe site-ul propriu de pariuri, ca liste proprii, ceea ce a fost considerat și reclamat de către BHB drept încălcarea a drepturilor sale asupra bazei de date create inițial de aceasta.

În speța *Fixtures Marketing Ltd v. Oy Veikkaus AB* (C-46/02), firma Fixtures Marketing Ltd. acorda, în numele organizatorilor meciurilor, licență de preluare în afara Marii Britanii a listelor meciurilor din Premier League, pentru ca înainte fiecare campionat să realizeze o listă cu echipele participante, în ordinea cronologică a meciurilor și a rezultatele obținute, pentru ca ulterior trei operatori de pariuri sportive din Suedia, Grecia și Finlanda să preia și să folosească listele procesate ca și baze de date.

În argumentarea soluțiilor exprimate, Curtea de Justiție Europeană, urmărind și o aplicare unitară a textului Directivei 96/9/CCE, a definit *"parte substanțială, evaluată calitativ, din conținutul unei bazei de date"* la care face trimitere art.7 alin 1 din Directivă – prin aplicarea criteriului astfel : *investiția autorului bazei de date în resurse umane, tehnice sau financiare în vederea obținerii, verificării sau prezentării acelei părți a bazei de date care este subiect al extragerii și/sau reutilizării nu se referă la valoarea intrinsecă a conținutului datelor extrase și/sau reutilizate*, în timp ce pentru aprecierea drept *"parte substanțială, evaluată cantitativ, din conținutul unei bazei de date"* – criteriul care diferențiază protecția bazei de date realizate de alte operațiuni de prelucrare este circumscris

volumului de date extrase și/sau reutilizate, prin raportare și la volumul total de date din baza de date inițială, prin stabilirea unei relații direct proporționale [25].

Referitor la protecția juridică privind prelucrarea datelor cu caracter personal, la nivelul jurisprudenței europene, Curtea Europeană de Justiție, a consacrat legalitatea dreptului utilizatorului, titular al datelor cu caracter personal, de a solicita ștergerea acestor date care stabilesc legătura cu persoana sa din motoarele de căutare pe Internet.

Fie că se regăsesc menționate explicit în cuprinsul textelor normative, fie că nu se regăsesc în directivele incidente în materie de prelucrare a datelor personale, aceste operațiuni trebuie calificate prin raportare la sintagma „*prelucrare a datelor cu caracter personal*" fiind întrunite atât elemente tehnice de prelucrare prin sisteme informatice, cât și prezența unor date care permit identificarea unei persoane fizice determinate. Chiar și în contextul în care informațiile ce au format obiectul unei noi prelucrări, au fost în prealabil accesibile publicului pe Internet ca urmare a unui alt tip de prelucrare (realizarea paginilor web ale unui cotidian), calificarea drept operațiuni de prelucrare a datelor cu caracter personal se menține prin raportare la specificul noilor operațiuni și la caracterul indubitabil de date personale, chiar și în condițiile în care au fost publicate în prealabil în mass media, deoarece nu s-a pierdut caracterul personal. [14].

IV.4 Practica instanțelor naționale privind protecția bazelor de date și a autorilor lor

Anterior anului 2004, din statistica jurisprudenței naționale, nu rezultă demararea procedurilor judiciare pentru protecția drepturilor sui-generis a autorilor/producătorilor de baze de date, de notorietate fiind speța aflată în anul 2007 pe rolul Tribunalului București, dosar înregistrat ca având drept obiect încălcarea dreptului de autor al reclamantului (inițiatorul și administratorului site-ului de Internet ghj.ro, care are drept obiect publicarea de creații din domeniul fotografiei artistice) de către pârâtă, care administrând la rândul ei un site, a extras și reutilizat în cadrul unui articol propriu despre localitatea C, una din fotografiile publicate inițial pe site-ul ghj.ro, fără autorizarea reclamantului, autorul inițial al fotografie și având drepturi *sui-generis* asupra conținutului site-ului ghj.ro unde s-a regăsit inițial postată fotografia în cauză.

Astfel, a fost întemeiată acțiunea introductivă de instanță pe dispozițiile art.122^1 și art.139 din Legea nr.8/1996, drept încălcarea a drepturilor sui-generis și au fost solicitate prin petit adiacent daune în cuantum de 2000 lei, reclamantul arătând că acest cuantum acoperă prejudiciului moral ce i-a fost cauzat prin fapta ilicită a pârâtei, respectiv pentru angajarea răspunderii delictuale a intimatei.

Tribunalul București a respins în fond acțiunea ca neîntemeiată, reținându-se în considerente, practica Curții de Justiție Europeană, privind aplicarea criteriilor de apreciere în sensul interpretării prevederilor art.7 alin.1 Directiva 96/9/CCE, astfel că în speța dedusă judecății s-a constatat că partea extrasă din baza de date (site-ul ghj.ro) nu are caracter substanțial, nici din punct de vedere cantitativ (faptic este o poză dintr-un album de peste 200 de instantanee), nici din punct de

vedere calitativ (era vorba de folosirea individuală a unei poze, obținute prin extragerea dintr-o bază de date cu aproximativ 2000 de fotografii de același tip, rezultând astfel un procent de 1/2000, apreciat drept nesemnificativ pentru a se invoca încălcarea dreptului sui-generis care protejează întreaga bază de date cu fotografiile reclamantei).

Apreciem că prin soluția pronunțată de Tribunalul București în acord cu textul Legii nr.8/1996 privind protecția drepturilor sui-generis ale autorilor bazelor de date și cu practica instanțelor europene, nu a fost negată calitatea reclamantului din speță ca și autor al bazei de date realizate de aceasta pe site-ul propriu - site-ul ghj.ro - argumentul instanței raportându-se strict la modul de protecție al drepturilor recunoscute sui-generis autorilor în cazul reutilizării substanțiale sau a reutilizării nesubstanțiale dar prin acte repetate a bazei proprii de date de către terțe persoane fără drept.

IV.5 Concluzii și rezultate obținute

- În corelare cu spațiul virtual (cyberspațiu), în care utilizatorii internetului interacționează, propunem de *lege ferenda* reglementarea unei jurisdicții statale asupra cyberspațiului din perspectiva cetățeniei sau a locului de acces al utilizatorului de Internet
- Cyber-spațiul devine cel de-al cincilea element în cadrul noțiunii juridice de *teritoriu statal*, alături de solul, subsolul, apele teritoriale și spațiul aerian al unui stat și trebuie avut ca atare în vedere de legiuitor în reglementarea raporturilor cu elemente de extraneitate
- Adoptarea unui cod al dezvoltării şi utilizării tehnologiilor informației și mecanismelor de securitate este oportună, evitându-se astfel denumirea de cod informatic, pentru a se elimina o posibilă confuzie cu conceptul tehnic.
- Legiferarea prin norme cu caracter de sinteză este oportună pentru reorganizarea cadrului normativ național privind securitatea informațională.
- Din analiza cadrului normativ actual și a practicii instanțelor la nivel național și european, susținem că este necesară elaborarea și integrarea în ordinea juridică internă și de la nivel european a unor acte normative de nișă, specializate, cu caracter integrator în domenii conexe și cu impact major asupra societății informaționale .

CAPITOLUL V
CERCETARE CALITATIVĂ PRIVIND ASIGURAREA SECURITĂȚII DATELOR CU CARACTER PERSONAL GESTIONATE ÎNTR-UN SISTEM INFORMATIC

Pornind de la interpretarea semnificației datelor colectate prin metoda interviului aplicat, se propune să se evidențieze modul în care pornind de la măsurile și tehnicile deja implementate în acord cu vechea reglementare juridică privind protecția datelor cu caracter personal (Directiva 95/46/CE), se impune adaptarea acestor măsuri și implementarea unor noi tehnici care să fie în acord cu cerințele actuale de securitate și protecție din Regulamentul nr.679/2016 - GDPR.

V.1 Metodologia cercetării calitative

Optându-se pentru o cercetare de tip calitativ, deoarece prin analiza răspunsurilor primite de la personalul de specialitate din cadrul instituțiilor în care s-au aplicat interviurile, se pot contura obiectiv concluziile situațiilor practice din instituțiile de învățământ privind prelucrările de date cu caracter personal prin raportare la ipotezele conturate de noi, vom enunța în continuare ipotezele de lucru avute în vedere:

1. Regulamentul UE 679/2016 asigură o protecție crescută şi uniformă la nivel european datelor cu caracter personal şi prelucrării acestora prin mijloace electronice şi/sau integrate într-un sistem informatic de către operatori, indiferent de domeniul de activitate sau de mărimea acestuia.
2. Prelucrarea datelor personale/cu caracter personal necesită fie existența unui temei legal (principiul legalității prelucrării datelor cu caracter personal) sau a unui temei juridic (existența unui contract a cărui executare necesită strângerea datelor cu caracter personal de la persoana fizică vizată în vederea prelucrării lor în acord cu clauzele contractuale), fie obținerea consimțământului persoanei vizate în mod clar, neechivoc şi transparent
3. Eliminându-se notificarea şi înregistrarea calității de operator de date cu caracter personal a operatorilor în registrul național al operatorilor autorizați, registru gestionat de către autoritatea națională cu competențe în supravegherea prelucrărilor în domeniu (astfel cum era reglementat anterior în Directiva 95/46/CE și în Legea nr.677/2001), instituțiile/operatorii trebuie să demonstreze prin politica şi măsurile implementate că respectă principiile esențiale ale prelucrării datelor cu caracter personal (legalitate, scop legitim şi determinat, necesitate şi proporționalitate, transparență şi securitate), în acord cu prevederile Regulamentului UE 679/2016.

În cadrul cercetării calitative pentru care s-a optat și prin structurarea interviului folosit în rândul instituțiilor de învățământ superior de stat selectate din sistemul național de educație, s-a

pornit în demersul cercetării de la situația concretă că în acest domeniu, specific ca şi activitate şi reglementare prin norme legale speciale a raporturilor juridice de şcolarizare, există două categorii de persoane vizate a căror date necesită prelucrarea pentru desfăşurarea activității instituției: proprii angajați şi studenții.

Opțiunea pentru cele 12 instituții de învățământ superior a avut în vedere şi faptul că acestea sunt reprezentative ca număr de studenți, programe de studii, cicluri de studii şi bază didactică în sistemul de învățământ superior de stat din România, care au implementate diferite aplicații, platforme şi programe cu care prelucrează baze de date ale studenților, de la cele pentru repartizarea locurilor la admitere, la cele privind acordarea burselor studențeşti, la cele privind registrul matricol şi al gestionării mobilităților de studiu, dar care au şi un aparat administrativ considerabil în raport cu activitatea desfăşurată (număr de angajați şi structuri administrative).

S-a ales metoda interviului individual cu reprezentanți din instituțiile selecționate care sunt direct implicați în procedurile de prelucrare și în operațiunile cu date personale, iar ca instrument de lucru s-a folosit interviul semi-structurat şi semi-directiv, permițându-se în cadrul răspunsurilor ca respondenții să ofere informațiile din perspectiva propriilor experiențe și cunoștințe pentru validarea ipotezelor de lucru, și folosindu-se chiar sugestiile respondenților pentru conturarea unor măsuri tehnice unitare prin care să fie asigurată respectarea principiilor de securitate minimale impuse prin Regulamentul UE nr.679/2016, indiferent de obiectul de activitate al operatorului care gestionează date cu caracter personal.

V.2 Prezentarea rezultatelor și propunerea unor măsuri de asigurare a securității datelor cu caracter personal la nivelul unei instituții de învățământ superior

Din analiza informațiilor obținute prin interviul semi-structurat, pentru o analiză succintă s-a folosit o grilă de sinteză în care s-au structurat în funcție de temă și obiective răspunsurile primite de la reprezentanții celor 12 instituții ce au format obiectul cercetării, grilă în care pe orizontală regăsim categoriile de teme şi la fiecare temă separat subtemele/obiectivele – esența din întrebările aferente temei – iar pe verticală s-au sintetizat răspunsurile primite, fiind astfel prin efectul matricei surprinse aprecierile fiecărei instituții în care s-au aplicat interviurile semi-structurate.

Sintetizând şi analizând răspunsurile prin folosirea matricei de mai sus, constatăm că la nivelul fiecărei instituții de învățământ superior structurile organizaționale implicate în colectarea, prelucrarea şi arhivarea datelor cu caracter personal ale studenților caută să adopte şi să actualizeze politicile de securitate şi să implementeze noi măsuri tehnice şi operaționale (instrucțiuni/proceduri de lucru) prin care să se asigure confidențialitatea datelor cu caracter personal gestionate şi arhivate.

Din perspectiva răspunderii ce trebuie angajate în cazul încălcării protecției datelor cu caracter personal, respectiv a confidențialității prelucrărilor cu acest tip de date, şi din punct de vedere al nivelului la care trebuie angajată răspunderea s-a identificat pe baza răspunsurilor primite

în cadrul cercetării că majoritatea reprezentanților instituțiilor au optat pentru angajarea răspunderii funcționarului/ofițerului (terminologie din traducerea termenului din limba engleză Data Protection Officer – DPO) responsabil cu datele cu caracter personal sau a răspunderii conducerii structurii instituționale care răspunde de implementarea tehnologiilor de securitate informatică în universitate.

Analizând tipurile de platforme şi aplicațiile IT cu care instituțiile care au fost supuse cercetării operează prelucrările de date necesare derulării activităților proprii, concluzia susținută de majoritatea celor cu care s-a discutat din structura instituțiilor privind măsurile IT a fost necesitatea, şi în contextul viitoarei reglementări juridice europene privind protecția datelor cu caracter personal, de a se folosii servicii şi tehnologii de cloud în privința gestiunii bazelor de date conținând date cu caracter personal ale studenților/foştilor studenți, volumul acestora fiind în creştere de la an la an coroborat cu obligativitatea arhivării permanente a numitor date cu caracter personal derivată din obligativitatea arhivării pe perioadă nedeterminată a actelor de studii emise şi eliberate absolvenților.

Dintre măsurile obligatorii a fi implementate la nivelul instituțiilor de învățământ superior pentru asigurarea colectării, gestionării, prelucrării şi arhivării în condiții de maximă securitate a datelor personale ale persoanelor vizate, inclusiv constituirea de baze de date, conform prevederilor legale (inclusiv ale Regulamentului UE nr.679/2016), pe baza cercetării efectuate am identificat şi conturat, în acord cu al doilea obiectiv al tezei un set de bune practici și recomandări a fi implementate la nivel instituțional pentru asigurarea conformității măsurilor tehnice implementate practic într-o universitate cu cadrul normativ instituit prin Regulamentul UE nr.679/2016, inclusiv cu privire la actualizarea anumitor proceduri şi măsuri de tehnică informațională prin care să se asigure conformarea la cadrul legislativ stabilit prin Regulamentul GDPR a aplicațiilor şi tehnologiilor deja implementate.

V.3 Concluzii și rezultate obținute

- Au fost identificate soluțiile tehnice, care pot fi implementate și la alți operatori, respectiv soluții tehnice și de politică informațională în acord cu prevederile legale în vigoare privind securitatea sistemelor informatice, dovedind totodată oportunitatea stabilirii obiectivului al doilea al tezei: **plan de soluții tehnice minimale integrate**:

1. Datele personale ale studenților și/sau angajaților universității nu se vor transmite de la o persoană la alta sau de la un birou la altul pe stick, CD sau alt suport extern, ci exclusiv prin poșta electronică, folosindu-se contul de email-ul instituțional.

2. Dacă datele sunt solicitate de către alte instituții publice, gen administrații financiare, ministere, bănci, autorități administrative locale și regii autonome colaboratoare, solicitarea fiind comunicată via e-mail, această transmisie și comunicarea răspunsului se vor face exclusiv prin folosirea conturilor instituționale, fiind excluse comunicările pe adrese personale de e-mail.

3. În momentul în care sunt solicitate din exterior date cu caracter personal din bazele proprii, trebuie verificată identitatea și scopul pentru care sunt solicitate aceste date, sens în care anterior formulării răspunsului se vor solicita date suplimentare dacă din datele inițiale nu se poate stabili aceste informații pe baza cărora se verifică legalitatea scopului solicitării și a condițiilor transferului de informații.

4. Toate calculatoarele care stochează date cu caracter personal trebuie parolate.

5. Toate persoanele care utilizează calculatoare/laptopuri în universitate trebuie să se autentifice pe aceste calculatoare/laptopuri cu un nume de utilizator personal și o parolă individualizate.

6. Se implementează un sistem care după introducerea greșită a unei parole de cinci ori să refuze automat și să fie chiar blocat accesul unui utilizator, chiar identificat prin cont de utilizator valabil.

7. Calculatoarele/laptopurile în funcțiune în mod obligatoriu vor fi oprite în momentul în care nu se mai folosesc aplicațiile pentru o anumită perioadă de timp (15-20 minute).

8. Aplicațiile care stochează conturi de utilizatori (conturile candidaților la admitere, conturile cadrelor didactice și ale studenților pe intranet) trebuie să rețină username-ul și parola criptate în baza de date.

9. Se va folosi un sistem centralizat de stocare a datelor cu caracter personal, partajate pe un server special, și toate aplicațiile care au nevoie de aceste date le vor prelua din aceeași bază de date centralizată, fără să mai fie nevoie de introducerea datelor despre studenți, angajați, etc. în mai multe aplicații de prelucrare.

10. Bazele de date care stochează informații cu caracter personal vor avea implementat un sistem care să înregistreze orice tranzacție care se efectuează pe baza de date (citire de date, copiere de date, modificare de date, ștergere de date), identitatea utilizatorului care a efectuat tranzacția, data și ora efectuării operațiunii, toate acestea urmând a se regăsi într-un jurnal de acces la date.

11. Se generează zilnic, la sfârșitul programului de lucru, un back-up la bazele de date pentru o eventuală recuperare a datelor.

12. Aplicațiile/programele prin care se prelucrează date cu caracter personal și care nu mai sunt folosite o perioadă de timp prestabilită, trebuie să închidă automat sesiunea de lucru, anterior salvării ultimei intervenții în aplicație.

13. Se vor instala oblgiatoriu pe calculatoare programe antivirus și firewall-uri și se vor actualiza periodic a aceste programe de securizare (cel puțin la 6 luni).

14. Se vor realiza copii de siguranță ale datelor care fie stocate pe calculatoare/terminale diferite și în locații diferite față de calculatoarele care stochează sau prelucrează datele; eventual calculatoarele ce păstrează copiile de siguranță să fie poziționate în spații securizate ca și acces prin

folosirea anumitor sisteme de siguranță și evidență a accesului (carduri de acces, încăperi monitorizate video, etc.).

15. Se evită salvarea pe desktop de fișiere ce conțin date cu caracter personal, precum și scurtături către aplicații ce accesează sau prelucrează în mod curent date cu caracter personal; acestea se vor salva într-un fișier care să fie eventual parolat.

- Set de bune practici și recomandări a fi implementate la nivel instituțional pentru asigurarea conformității măsurilor tehnice implementate practic într-o universitate cu cadrul normativ instituit prin Regulamentul UE nr.679/2016, inclusiv cu privire la actualizarea anumitor proceduri şi măsuri de tehnică informațională prin care să se asigure conformarea la cadrul legislativ stabilit prin Regulamentul GDPR a aplicațiilor şi tehnologiilor deja implementate.

Recomandarea I: Având în vedere obligativitatea informării complete, clare, transparente şi integrale prin raportare la scopul prelucrării datelor proprii ale persoanelor vizate şi pentru obținerea în condițiile informării a consimțământului expres pentru prelucrarea acestor date în cadrul colectării lor prin sisteme informatice (exemplu platforme de înscriere on-line la procedura de admitere la studii, platforme de semnare on-line a contractelor de admitere, spre exemplu) trebuie ca sistemele informatice să asigure on-line/prin mijloace electronice informarea completă a utilizatorilor (spre exemplu a candidații la admitere care folosesc o platformă on-line de înscriere) anterior accesării nivelului de încărcare în platformă a datelor cu caracter personal şi să se obțină tot on-line/prin mijloace electronice consimțământul clar și expres al persoanei vizate.

Recomandarea II: Accesul angajaților la datele cu caracter personal din aplicațiile unui operator se face exclusiv prin autentificarea utilizatorilor respectivi în sistemele informatice ale Universității. Astfel, autentificarea în cadrul sistemelor informatice se face prin introducerea credențialelor de autentificare unice și netransmisibile dobândite în urma procesului de înrolare și management al identității electronice, proces guvernat de politicile de securitate în vigoare .

Recomandarea III: În cazul studenților, se impune ca măsură de securitate tehnică dezactivarea și chiar distrugerea codurile de identificare/conturilor de utilizator alocate pe perioada studiilor, operațiuni tehnice care se vor face la terminarea studiilor nemaiexistând necesitatea comunicării între instituția de învățământ și titularul contului (fostul student).

Recomandarea IV: Se va ține o evidență distinctă (sub forma unu registru) a conturilor utilizatorilor care realizează operațiuni de prelucrare a datelor cu caracter personal și care vor fi obligatoriu însoțite de parole individuale, folosite drept chei de autentificare în aplicații. Parolele sunt înşiruiri de caractere – litere și simboluri - adecvate din punct de vedere al securității ca lungime – minim 8 caractere- și structură. La introducerea parolelor sistemul trebuie setat astfel încât acestea să nu fie afişate în clar pe monitor.

Cercetări privind securitatea datelor în sistemele informatice

Recomandarea V: Se impune schimbarea periodică (la intervale de cel puțin șase luni/durata unui semestru) a parolelor, măsură tehnică ce trebuie prevăzută în politicile de securitate ale oricărei instituții de învățământ, fiind consiliați în acest sens toți utilizatorii, indiferent de nivelul de acces în bazele de date. Schimbarea sistemică a parolelor conturilor de utilizator se face sub coordonarea administratorilor de rețea.

Recomandarea VI: Sistemul informațional trebuie să blocheze automat accesul în cazul unui utilizator care a introdus în mod greșit după un număr fix de chei de autentificare prestabilit, urmând ca intervenția administratorului de rețea să decidă accesul în continuare în rețea de pe contul asociat cheii de autentificare eronat introduse.

Recomandarea VII: Utilizatorii codurilor de identificare care acționează într-o rețea a unui operator, cum este o instituție de învățământ superior, vor asigura păstrarea confidențialității datelor de autentificare, cât și a datelor personale din bazele de date la care au acces ca și obligație de serviciu, stabilită și asumată clar prin fișa postului, urmând ca în cazul unor incidente de securitate dacă se identifică IP-ul său ca responsabil de incident să răspundă atât disciplinar față de angajator, cât și patrimonial în limitele prejudiciului astfel cauzat prin divulgarea datelor cu caracter personal.

Recomandarea VIII: Computerele şi terminalele de acces la bazele de date cu caracter personal din sediul Universității vor fi instalate în încăperi cu acces restricționat și fără ca prin poziționarea lor să se permită accesul (inclusiv vizual) neîngrădit al terților persoane. Fiecare computer sau partiția în care sunt gestionate bazele de date de acest fel vor fi accesate numai de către utilizatorii autorizați cu user-ul stabilit și parola cunoscută.

Recomandarea IX: Scoaterea din instituție a mediilor de stocare mobile (CD/DVD, USB Stick, Portable HDD) care conțin date cu caracter personal trebuie notificată și aprobată în prealabil de către responsabilul IT, în privința securității mediului de stocare, respectiv de către un reprezentant al instituției, din perspectiva scopului în care este necesar transferul extern.

Recomandarea X: Solicitarea și transmiterea de date sensibile între angajații Universității pentru efectuarea diferitelor operațiuni se face doar prin e-mailul instituțional, rețeaua intranet fiind securizată și supravegheată din perspectiva vulnerabilităților inclusiv prin instalarea și actualizarea programelor antivirus și firewall-urilor.

Recomandarea XI: Periodic se va avea în vedere, la nivel instituțional, instituirea obligativității cartografierii periodice a tipurilor de date cu caracter personal şi a structurilor din instituție care colectează, prelucrează şi arhivează în scopuri diferite date cu caracter personal coroborat cu activitatea reglementată prin procedura internă adoptată, sens în care după identificarea unor noi categorii de date supuse prelucrării sau a unor scopuri noi de prelucrare se vor identifica şi aproba şi instrumentele scriptice pentru obținerea consimțământului persoanei vizate, respectiv a procedurile de implementare a mijloacelor electronice prin sisteme informatice de prelucrare a datelor.

CONCLUZII ȘI REZULTATE GENERALE, CONTRIBUȚII PERSONALE ȘI LIMITE ALE CERCETĂRII

Ca într-o ecuație (Figura 14) a căror necunoscute sunt vulnerabilitățile și riscurile la adresa sistemelor informatice (caracterul de variabile necunoscute se datorează modului de operare al agenților de amenințare) analizate în capitolul I, măsurile de securitate informațională încearcă să apere utilizatorii și bunurilor acestora, incluzând informațiile deținute, datele cu caracter personal și nu în ultimul rând propriul echipament, de acțiunile agenților de amenințare. Acest algoritm adaptat în urma cercetărilor din capitolele I și II, a fost folosit de noi în special pentru atingerea celui de-al doilea obiectiv propus: promovarea unor soluții tehnice integrate într-un set de 15 măsuri necesare prelucrării datelor cu caracter personal în cadrul unui sistem informatic în acord cu prevederile legale în vigoare privind transparența, integritatea și confidențialitate prelucrărilor, respectiv a datelor.

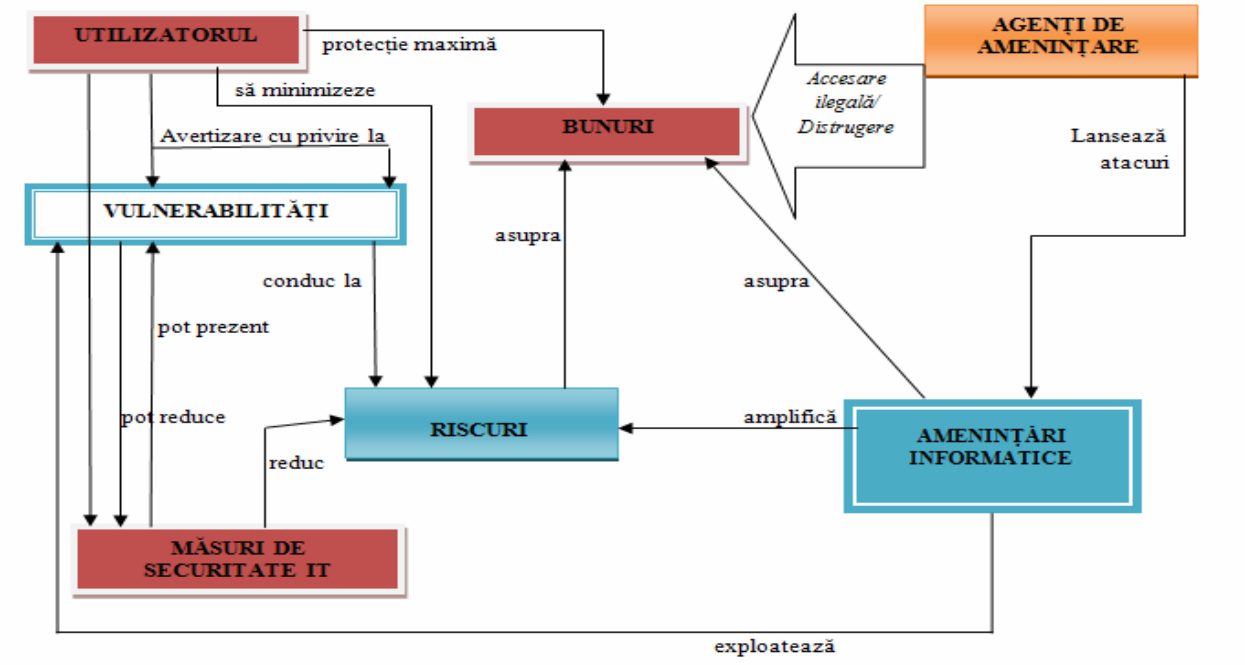

Figura 14 Ecuația amenințărilor informatice-riscuri-vulberabilități
(adaptare Standard Common Criteria for Information Tehnology Security Evaluation)

Asimilând în ecuația de mai sus bunurile cu informațiile (bunuri intangibile), ajungem să definim riscul sistemelor de informații ca fiind suma vulnerabilităților (aspecte sensibile) și amenințărilor (evenimente viitoare posibile) la care se adaugă valoarea informațiilor. Posibilitatea ca sistemele informatice să fie insuficient protejate împotriva anumitor atacuri sau pierderi de informații este numită de Straub D.W. și Welke R.J. drept *risc de sistem* [43].

Metodele și tehnicile de securitate pornesc de la obiectivele de securitate și trebuie armonizate de la nivelul aplicației informatice, a bazei de date folosite și a programelor care rulează, până la nivelul tuturor utilizatorilor și echipamentelor lor, a echipamentelor periferice conectate la sistem, respectiv de la nivel logic la cel fizic, de la nivelul informației și până la nivelul organizației (Figura 15).

Cercetări privind securitatea datelor în sistemele informatice

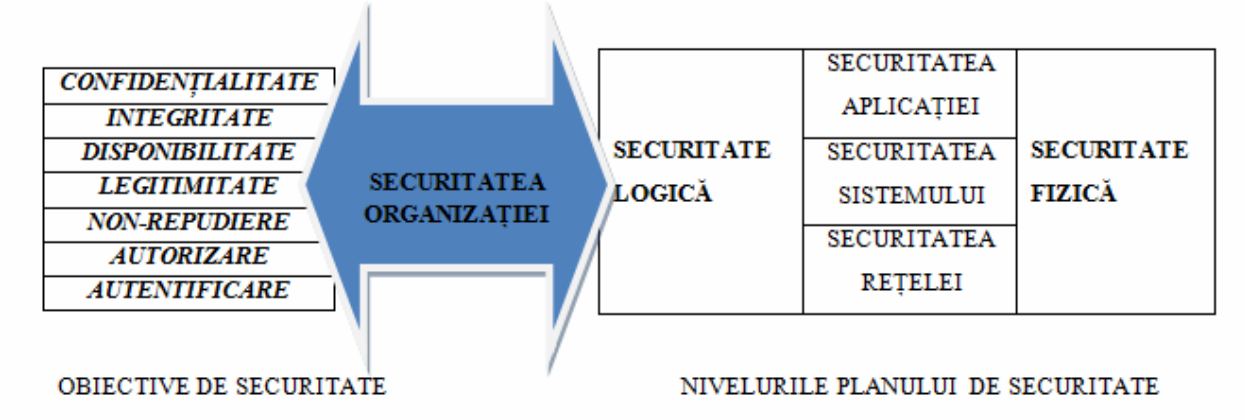

Figura 15 Implementarea obiectivelor de securitate în planurile de securitate

Securitatea unui sistem informatic urmărește definirea, conform standardelor și practicilor în domeniul securității tehnologice, și implementarea politicii de securitate prin măsuri simultane și coroborate de securitate fizică a componentelor hardware cu cele de securitate a componentelor software raportat la măsuri de securitate administrativă și a resursei umane din organizație, luându-se în considerare și aspectul utilizării sistemului informatic într-o rețea locală sau în mediul Internet.

Obiectivul de securitate este împiedicarea pătrunderii intrușilor, indiferent de formă, în sistem, iar ca back-up, dacă din cauza vulnerabilității exploatate pătrunderea neautorizată în sistem se produce atunci trebuie să intervină bariere de stopaj temporar sau de întârziere a atacului, astfel încât să fie asigurate integritatea, confidențialitatea și disponibilitatea informațiilor.

Contribuții personale

Contribuțiile personale în planul cercetării fundamentale aduse prin tema propusă și analiza efectuată pot fi sintetizate astfel:

- Am stabilit conținutul conceptelor fundamentale *date, informații* și *cunoștințe* în contextul actual al societății cunoașterii, etapă ulterioară de dezvoltare tehnică, economică și socială bazată pe societatea informațională, concepte necesare unei analize interdisciplinare;
- Am conturat în capitolele I.5 și II.1. definiții proprii cuprinzătoare a agenților de amenințare, ca autori morali și/sau fizici ai atacurilor informatice, și am realizat o ierarhizare în sens crescător a celor șase categorii de agenți de amenințare actuali având ca reper scopul în care sunt lansate atacurile: 1)hackeri (scop de distracție sau ca provocare intelectuală); 2)vandali (scop de a produce pagube nu neapărat cu impact economic pentru autor); 3)atacatori în scop economic (scop obținere de câștiguri financiare sau poziție de piață); 4)infractori de profesie (scop obținere de câștiguri financiare personale); 5)spioni (scop politic și/sau militar) și 6)teroriști (scop politic și/sau militar asumat cu generarea unui climat colectiv de teamă sau pentru discreditarea unui sistem guvernamental sau a unei autorități publice), aceste demersuri putând fi preluate și ca propuneri de legiferare;

- Am susținut și am dovedit necesitatea unei abordări simultane interdisciplinare juridico-tehnice a securității informațiilor și a securității sistemelor informatice deoarece în procesul de investigare a atacurilor cibernetice sunt coroborate aspectele juridice cu identificarea tehnică a urmelor din sistem și atribuirea responsabilității în scopul determinării identității sursei unui atac cibernetic, pentru ca prin agregarea măsurilor întreprinse să fie limitate efectele atacului cibernetic asupra sistemului informatic victimă, să fie identificat în vederea sancționării autorul atacului și să fie identificate vulnerabilitățile noi ale sistemului care au facilitat amenințarea.
- În privința dezvoltării tehnicilor pentru identificarea urmelor dintr-un sistem informatic, în special în cazul accesării neautorizate, considerăm că este deschisă în continuare calea cercetărilor, soluțiile tehnice noi ce vor fi identificate urmând, însă obligatoriu să se regăsească și în cadrul normativ, concluzie ce susține obiectul prim al tezei.
- Susținem, prin obiectivul prim propus și pe baza rezultatelor cercetărilor din capitolul I.5.3, dezvoltarea în sistemele de educație a cursurilor dedicate securității informatice, chiar și la nivel preuniverstiar cum ar fi spre exemplu cursuri despre riscurile de securitate a rețelelor deschise și soluții eficiente, cursuri despre protecția juridică și tehnică a prelucrărilor automatizate de date cu caracter personal, deoarece considerăm că dezvoltarea unei culturi de securitatea cibernetică trebuie să înceapă încă din sistemul de învățământ, având pe termen lung menirea de a dezvolta încrederea şi siguranța individului în tehnologiile informației şi comunicațiilor, instrumente viitoare ale dezvoltării societății actuale.
- Atingându-ne primul obiectiv prin cercetările din capitolul I și II coroborate cu cele din capitolul IV, am identificat în capitolul IV.5 beneficiile aduse de existența unei reglementări juridice naționale privind securitatea cibernetică și susținem continuarea demersurilor legislative pentru adoptarea și în România a unei legi privind securitatea cibernetică. Reforma legislativă în domeniul securității informatice este necesară pe de o parte datorită declarării prin Decizia nr.17/21.01.2015 ca neconstituțional a proiectului de lege nr.580/2014 privind securitatea cibernetică a României votat de Parlament, în urma controlului de constituționalitate anterior promulgării, control efectuat de către Curtea Constituțională a României cu privire la obiecția de neconstituționalitate, pe de altă parte datorită intensificării atacurilor informatice asupra sistemelor informatice din România care proliferează în lipsa unui cadru normativ sancționator.
- Am susținut, prin argumente teoretice în capitolul I.4, dar și prin setul de soluții tehnice integrate propus în capitolul V.2, necesitatea implementării la nivel organizațional a unui Sistem de Management Integrat (SMI) Calitate –Mediu - Sănătate și Securitate Ocupațională – Securitatea Informațiilor suprapunând unele proceduri și adăugând procesele specifice necesare sistemelor de management de mediu și de sănătate și securitate ocupațională cu

proceduri specifice de securitate a informației, sistem de management care va aduce un plus de valoare organizației și produselor/serviciilor sale.

În planul ***cercetării aplicative***, pornind de la concluziile cercetării calitative realizate în teză în capitolul V cu privire la importanța securizării prelucrării datelor cu caracter personal în contextul legislației europene în vigoare, Regulamentul UE nr.679/2016 cu directă aplicare în sistemele juridice naționale ale statelor membre UE analizat în capitolul IV.1.2, contribuțiile personale pot fi sintetizate astfel :

- Am identificat incidentele și riscurile în gestiunea datelor cu caracter personal prelucrate și arhivate într-un sistem informatic, în cazul instituțiilor de învățământ superior din România
- Am constatat din situația faptică rezultată din cercetarea realizată în capitolul V necesitatea coroborării măsurilor tehnice de securizare cu prevederile legale în vigoare privind protecția datelor personale pentru prevenirea și împiedicarea actelor neautorizate de titularii drepturilor
- Am adus argumente privind necesitatea abordării holistice, sistemice și multi-level a problematicii protejării tehnice a prelucrărilor de date cu caracter personal în cadrul unui sistem informatic, prin crearea unui sistem de detectare și blocare a atacurilor similar cu sistemul imunitar al acțiunii leucocitelor prin definirea clară a barierelor de intrare în sistem,
- Susținem conștientizarea necesității prelucrării legitime a datelor cu caracter personal în sistemele informatice sub imperativul răspunderii juridice materiale și penale, realizarea periodică a analizelor riscului de atac asupra sistemelor informatice și evaluarea oportunităților de atac prin identificarea potențialelor vulnerabilități, inhibitori și amplificatori specifici activității în care sunt prelucrate datele cu caracter personal și detectarea intruziunilor la nivel de rețea și/sau device în scop de atac cibernetic prin implementare unor tehnici de avertizare și contramăsuri pentru anihilarea tentativei de atac informatic.
- Pornind de la noul cadru juridic privind protecția juridică și tehnică a datelor cu caracter personal prelucrate prin sistemele informatice actuale, stabilindu-se ca principiu juridic necesitatea implementării măsurilor tehnice și a politicii de securitate informațională de către fiecare organizație în parte, în calitate de operator de date personale, am constatat că este necesar ca măsurile tehnice concrete adoptate în funcție de specificul activității să asigure informarea completă, clară și fără echivoc a persoanei ale cărei date personale sunt prelucrate, inclusiv cu privire la scopurile prelucrării, astfel încât și exprimarea consimțământului privind prelucrarea propriilor date manifestat prin mijloace electronice să fie valabil, clar exprimat și comunicat în condiții de securitate, sens în care am făcut în capitolul V.2 și unele recomandări privind aplicațiile identificate ca fiind folosite la nivelul instituțiilor de învățământ superior din România.

Cercetări privind securitatea datelor în sistemele informatice

Perspective de cercetare și dezvoltare ulterioară

Cercetările teoretice și aplicative realizate pe parcursul elaborării tezei de doctorat au evidențiat necesitatea continuării cercetărilor și dezvoltărilor ulterioare de alte măsuri de securizare astfel încât capabilitățile IT ale unui sistem informatic să susțină cadrul normativ în scopul creșterii gradului de securizare a rețelelor și sistemelor informatice. Din aceste perspective cumulate, și susținând argumentat primul obiectiv al tezei (necesitatea abordării interdisciplinare a securității sistemelor informatice), susținem ca având au un mare potențial de cercetare, dezvoltare și inovare următoarele aspecte, pe care le putem chiar concentra ca viitoare direcții de cercetare:

1. Abilitatea tehnică a sistemelor informatice de a identifica urmele lăsate de utilizatori și echipamente atunci când Internetul este accesat prin intermediul diferiților ISP (*Internet Service Provider*) și a diferitelor adrese IP, și în special în cazul rețelelor private în care proprietarii de rețea nu doresc să coopereze;
2. Efectuarea de investigații criminalistice live și prezervarea de evidențe digitale de la distanță prin intermediul Internetului, ceea ce ar permite pe de o parte o reacție în timp real pentru limitarea efectelor unui atac și prezervarea unor potențiale probe care sunt încă în memoria sistemului înainte de a se genera alte operațiuni în sistem, inclusiv cele de autoprotecție;
3. Dezvoltarea cadrului de legiferare în privința rețelelor, astfel încât normele legale să stabilească condițiile generale în care sunt disponibile informații substanțiale referitoare la o rețea, precum și să incrimineze accesul neautorizat la datele gestionate într-o rețea;
4. Dezvoltarea unor tehnici de conservare și prelevare a probelor în cazul unui atac cibernetic care să asigure totodată confidențialitatea informațiilor și rezultatelor în scopul identificării autorilor;
5. Necesitatea și oportunitatea perfecționării arborelui de atac, respectiv analiza posibilității de prioritizare a ramurilor unui arbore de atac în funcție de impactul atacului.

Cercetări privind securitatea datelor în sistemele informatice

BIBLIOGRAFIE SELECTIVĂ

[1] Albert R., Jeong H., Barabasi A. (2002) The Internet's Achilles Heel: Error and Attack Tolerance of Complex Networks, format electronic http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=B2C34DF6485AE9118A624CB053C36244?doi=10.1.1.33.2606&rep=rep1&type=pdf. Accesat la 25.04.2017.

[2] Amor D. (2000) *The E-Business (R)evolution, Living and Working in an Interconnected World*, Hewlett-Packard Professional Books.

[3] Anderson R. (2001) *Security Engineering: A Guide to Building Dependable Distributed Systems,* New York: John Wiley&Sons Inc.

[4] Burtescu E. (2004) Teză doctorat *Securitatea datelor în sistemele informatice economice* Academia de Studii Economice București, Facultatea de Cibernetică, Statistică și Informatică Economică.

[5] Clark R.K., Greenberg I.B., Boucher P.K., Lund T.F., Neumann P.G., Wells D.M., Jenson E.D. (2003) Effects of Multilevel Security on Real-Time Applications, *Proceedings of Ninth Annual Computer Security Applications,* Orlando, 06-10 December 2003

[6] Cohen F. (1987) Computer Viruses: Theory and Experiments. În *Computers and Security,* Vol.6, p.22-35

[7] Dobrinoiu, M. (2006). *Infracțiuni în domeniul informatic* format electronic https://www.e-crime.ro/ecrime/site/files/93361241097364Infractiuniindomeniulinformatic.pdf. Accesat la 20.12.2017.

[8] Drăgănescu, M. (2001). *Societatea informațională și a cunoașterii. Vectorii societății cunoașterii.* Proiect SI-SC (Societatea Informațională-Societatea Cunoașterii) al Academiei Române, București, 09 Iulie 2001. Format electronic disponibil: http://www.academiaromana.ro/pro_pri/pag_com01socinf_tem.htm, http://www.racai.ro/~dragam, Accesat la 30.05.2017.

[9] Drăgănescu, M. (2004). *De la societatea informațională la societatea cunoașterii*, București: Editura Tehnică.

[10] Groza B. (2012). *Introducere în criptografie. Funcții Criptografice, Fundamente Matematice și Computaționale*. București: Editura Politehnică.

[11] Hotca M.A., Dobrinoiu M. (2009) *Elemente de Drept Penal al Afacerilor.* București: C.H. Beck.

[12] Ioniță Ghe.I. (2011) *Infracțiuni cibernetice. Criminalitate, prevenire și combatere.* București: Universul Juridic.

[13] Ivan I., Milodin D., Zamfiroiu A. (2013) Securitatea tranzacțiilor de M-Comerț. În *Economie teoretică și aplicată* Vol.XX nr.7 (584), p.57-36, format electronic http://store.ectap.ro/articole/880_ro.pdf Accesat 05.06.2017.

[14] Jugastru C. (2018). Tradiție și inovație în materia protecției datelor cu caracter personal În *Revista Universul Juridic* – ISSN 2393-3445, Nr.4/aprilie 2018, format electronic http://revista.universuljuridic.ro/traditie-si-inovatie-materia-protectiei-datelor-cu-caracter-personal/ Accesat la 10.05.2018.

[15] Klander L., Renehan E. J. Jr. (1997) *Hacker Proof : The Ultimate Guide to Network Security* New York: Jamsa Press.

[16] Knorr K., Rohrig S. (2001) Security Requirements of E-Business Processes, Towards the E-Society: E-Commerce, E-Business and E-Government. In *First IFIP Conference on E-Commerce, E-Business, E-Government,* Zurich, Elveția, 4-5 october 2001.

[17] Luckling-Reiley D., Spulber D.F. (2001) Business-to-business electronic commerce. In *Journal of Economic Perspectives.*

[18] Manea C.A. (2014) The electronic signature – Technical and legal implications *In Bulletin of Transilvania University of Brasov,* Series VII, nr.2/2014 Vol.7(56)

[19] Manea C.A. (2015) Information Security Policy. În *The 2end International Conference for Doctoral Students – IPC 2015*, 5-6 iunie 2015, Sibiu- Universitatea Lucian Blaga

[20]Manea C.A. (2015) Crimes against Security and Integrity Systems and Computer Data in Criminal Current Regulation. În *The 2end International Conference for Doctoral Students – IPC 2015*, 5-6 iunie 2015, Sibiu- Universitatea Lucian Blaga

[21] Manea C.A. (2015) Information Security Management - part of the integrated management system. În *The 7th International Conference on Manufacturing Science and Education – MSE 2015,* 3-6 iunie 2015, Sibiu - Universitatea Lucian Blaga.

[22] Manea C.A. (2015) Social Networks and Information Security in Virtual Environment, În *The International Scientific Conference Globalization, Intercultural, Dialogue and National Identity,* Universitatea Petru Maior Târgu Mureș, 28-29 mai 2015.

[23] Manea C.A. (2015) Presentation of Outstanding Software Solutions available for Computer Protection against Security Threats on the Internet, *In Bulletin of Transilvania University of Brasov,* Series I, nr.1/2015 Vol.8(57)

[24] Manea C.A. (2016) European and Romanian jurisprudence in the field of databases security, În *The International Scientific Conference Globalization, Intercultural, Dialogue and National Identity,* Universitatea Petru Maior Târgu Mureș, mai 2016.

[25] Manea C.A. (2016) The virtual theft and the illegal use of a communication terminal *In Bulletin of Transilvania University of Brasov,* Series VII, nr.1/2016 Vol.9(58)

[26] Manea C.A. (2017) The Security of personal data of users in on-line socialization networks. Legal Aspects. *In Bulletin of Transilvania University of Brasov,* Series VII, nr.1 Vol.10(59)

[27] Manea C. A. (2018) coautor Home Assisted Living of Elderly People using Wireless Sensors Networks in a Cloud System, - ISSI'2018 International Conference on Sensing and Instrumentation in IoT Era IEEE Conference, 6-7 sept. 2018. http://issi2018.csp.escience.cn/dct/page/1, (lucrare acceptata pentru prezentare si publicare)

[28] Mihai, I.C. (2012) *Securitatea Informațiilor.* Craiova: Sitech Press.

[29] Moise A.C. (2010) *Metodologia investigării infracțiunilor cibernetice* Teză doctorat susținută la Universitatea București

[30] Moore A.P., Ellison R.J., Linger R.C. (2001) *Attack Modeling for Information Security and Survivability,* Pittsburgh PA: Software Engineering Institute.

[31] Oprea D., Protecția și securitatea informațiilor, Iași : Polirom, 2007.

[32] Patriciu V.V (1994), *Criptografia și securitatea rețelelor de calculatoare cu aplicații în C și Pascal*, București: Editura Tehnică.

[33] Patriciu V.V, Vasiu I., Patriciu Ș.-G. (1999) *Știință și Drept* București: All Beck.

[34] Patriciu V.V., Ene-Pietrosanu M., Bica I., Priescu J. (2006) *Semnături electronice și securitate informatică- Aspecte criptografice, tehnice, juridice și de standardizare,* București: Editura All.

[35] Patriciu V.V., Ene-Pietrosanu M., Bica I., Vaduva C., Voicu N. (2007) *Securitatea comerțului electronic.* București: Editura All.

[36] Perniu, L. (2013) *Procesarea datelor. Volumul I.* Brașov: Libris.

[37] Popa, S.E. (2007) *Securitatea sistemelor informatice – note de curs şi aplicații,* Bacău : Alma Mater.

[38] Popescu, M. (2007) *Jurisprudența în domeniul protecției bazelor de date,* format electronic www.wipo.int/edocs/mdocs/mdocs/en/wipo_ip.../wipo_ip_mng_10_ref_t15.pptx, Accesat 28.04.2016.

[39] Raymond E.S. (2002) *The New Hacker's Dictionary ,* Massachutes: The MIT Press.

[40] Rose J. (2000) *Information systems development as action research – soft systems methodology and structuration theory,* PhD Thesis Management School, Lancaster University, UK

[41] Sarcinschi A. (2009) *Vulnerabilitate, risc, amenințare. Securitatea ca reprezentare psihosocială.* București : Editura Militară.

[42] Schiller-Ionaș, E., Ionescu, C. (2011) *Elemente de inginerie software și guvernare IT,* București: Editura Pro Universitaria

[43] Straub D.W., Welke R.J. (1998) Coping with systems risk: security planning models for management decision making. In *MIS Quarterly* no.22(4) 1998.

[443]. Șerb, A., Baron, C., Isăilă, N., Ionescu, C., Defta C.L. (2013). *Securitatea informatică în societatea informațională,* București : Pro Universitaria.

[45] Vară O. (2014) *Criminalitatea informatică.* Teză doctorat susținută la Academia de Poliție *Alexandru Ioan Cuza* București.

[46] Vasiu I. (2001) *Cybercriminalitate*. București: Nemira.

[47] Vasiu I., Vasiu L. (2005) Protecția datelor personale. În *Revista Română de Drept Penal* Nr.2 București.

[48] Vasiu I., Vasiu L. (2007) *Afaceri electronice – aspecte legale, tehnice și manageriale* Cluj-Napoca: Editura Albastră.

[49] Vevera A.V. (2014) Amenințări cibernetice globale și naționale. În *Revista Română de Informatică și Automatică,* vol.24, nr.3 an 2014, disponibil electronic www.rria.ici.ro .

Surse legislative și electronice

[50] *** Directiva 95/46/CE a Parlamentului European și al Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, publicată în Jurnalul Oficial nr.L281/31 din 23.11.1995, format electronic https://eur-lex.europa.eu/legal-content/ro/TXT/?uri=CELEX%3A31995L0046 Accesat la 03.10.2015

[51] ***Directiva 1999/93/CE a Parlamentului European și a Consiliului din 13 decembrie 1999 privind

un cadru comunitar pentru semnăturile electronice, publicată în Jurnalul Oficial nr.L13/12 din 19.01.2000, format electronic https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:31999L0093&from=RO Accesat la 25.03.2018.

[52] *** Directiva 2000/31/CE a Parlamentului European și a Consiliului din 08 iunie 2000 privind aspectele juridice ale societăților informaționale, în special ale comerțului electronic pe piața internă, publicată în Jurnalul Oficial nr.L178/1 din 17.07.2000, format electronic https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32000L0031&from=RO Accesat la 25.11.2017.

[53] *** Convenția Consiliului Europei din 23 noiembrie 2001 privind criminalitatea informatică, publicată în Jurnalul Oficial nr.343 din 20.04.2004.

[54] *** Directiva 2002/19/CE a Parlamentului European și a Consiliului din 7 martie 2002 privind accesul la rețele de comunicații electronice și la infrastructura asociată, precum și interconectarea acestora, publicată în Jurnalul Oficial nr.L108 din 24.04.2002, format electronic http://www.ancom.org.ro/uploads/links_files/Directiva_2002_19_consolidata_RO. PDF Accesat la 25.02.2018

[55] *** Directiva 2002/21/CE a Parlamentului European și a Consiliului din 7 martie 2002 privind un cadru de reglementare comun pentru rețelele și serviciile de comunicații electronice, publicată în Jurnalul Oficial nr.L108 din 24.04.2002, format electronic http://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex:32002L0021 Accesat la 25.02.2018.

[56] *** Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor cu caracter personal și protecția intimității în sectorul comunicațiilor electronice, publicată în Jurnalul Oficial nr.L201 din 31.07.2002, format electronic https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex%3A32002L0058, Accesat la 25.02.2018.

[57] *** *Tratatul privind Uniunea Europeană și Tratatul privind funcționarea Uniunii Europene* - Tratatul privind Uniunea Europeană (versiune consolidată) - Tratatul privind funcționarea Uniunii Europene (versiune consolidată) – Protocoale – republicat în J*urnalul Oficial C 326 , 26/10/2012*, format electronic http://eur-lex.europa.eu/legal-content/RO/TXT /?uri=celex%3A12012E%2FTXT. Accesat la 18.01.2018.

[58] *** Regulamentul UE nr.526/2013 din 21 mai 2013 al Parlamentului European și al Consiliului privind Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA) și de abrogare a Regulamentului (CE) nr.460/2004, publicat în Jurnalul Oficial nr.L165 din 16.08.2002, format electronic https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32013R0526, Accesat la 25.02.2018.

[59] Regulamentul UE al Parlamentului European și al Consiliului nr.910/2014 din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE, publicat în Jurnalul Oficial nr.L257 din 28.08.2014.

[60] *** Directiva UE nr.2015/1535 din 9 septembrie 2015 a Parlamentului European și a Consiliului din 9 septembrie 2015 referitoare la procedura de furnizare de informații in domeniul reglementarilor tehnice și al normelor privind serviciile societății informaționale, publicată în Jurnalul Oficial nr.L241 din 17.09.2015, format electronic https://eur-lex.europa.eu/legal-

content/RO/TXT/?uri=OJ%3AJOL_2015_241_R_0001 Accesat la 26.02.2018.

[61] ... Regulamentul UE 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) , publicat în Jurnalul Oficial nr.L119/1 din 04.05.2016, , format electronic https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32016R0679 Accesat la 26.11.2016.

[62] ... Legea nr.455/2001 privind semnătura electronică, republicată în Monitorul Oficial nr.316 din 30 aprilie 2014

[63] ... Hotărârea Guvernului nr.1259/2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea *Legii nr. 455/2001* privind semnătura electronică, publicată în Monitorul Oficial nr.487 din 28 decembrie 2001

[64] ... Legea nr.365/2002 privind comerțul electronic, republicat în Monitorul Oficial nr.959 din 29 noiembrie 2006.

[65] ... Legea nr.161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice şi în mediul de afaceri, prevenirea şi sancționarea corupției, publicată în Monitorul Oficial nr.279 din 21 aprilie 2003.

[66] ... Legea nr.286/2009 privind Codul Penal Român, publicată în Monitorul Oficial nr.510 din 24 iulie 2009.

[67] ... Legea nr.187/2012 pentru punerea în aplicare a Legii nr. 286/2009 privind Codul penal, , publicată în Monitorul Oficial nr.757din 12 noiembrie 2012.

[68] ... Comunicarea Consiliului European din 23-24 martie 2001 privind eEurope 2002, nepublicată în Jurnalul Oficial, [format electronic http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52001 DC0140&from=EN, Accesat :01.02.2015]

[69] ... Comunicarea Comisiei către Parlamentul European a programului eGovernment 2011/2015, nepublicată în Jurnalul Oficial, [format electronic http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri= CELEX:52010DC0743&from=EN, Accesat :01.02.2015]

[70] ... Comunicarea Comisiei către Parlamentul European a Strategiei în domeniul securității cibernetice, „Un spațiu cibernetic deschis, sigur și securizat", nepublicată în Jurnalul Oficial, format electronic Accesat : 30.01.2015 http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667,

[71] ... Court of Appeal from Craiova, *Prosecution Decision no.930/07.07.2004.* Available at: http://www.hamangiu.ro/upload/cuprins_extras/infractiuni-economice-practica-judiciara_extras.pdf. Accesat la: 22.03.2016.

[72] ... *Hotărârea pronunțată de Curtea Europeană de Justiție la data de 09 noiembrie 2004 în dosarul C-203/02;* http://www.consiliermarci.ro/2013/03/Actiune-incalcarea-dreptului-de-autor-asupra-unei-fotografii-conditiile-incalcarii-drepturilor-baze-de-date.html; Accesat la 30.04.2016.

[73] ...*British Horseracing Board v. William Hill*: The race is never lost, till won: 08. 02.2005; http://www.twobirds.com/en/news/articles/2005/british-horseracing-board-v-william-hill Accesat la: 28.04.2016.

[74] ***ISO/IEC 27002:2005 Standard Internațional Tehnologia informației – Tehnici de securitate - Codul de practică pentru managementul securității informației

[75]*** *Federal Plan for Gyber Security and Information Assurance Research and Development (FPGSIARD)* – Report by the Interagency Working Group on Cyber Security an Information Assurance, S.U.A. (2006), format electronic https://www.nitrd.gov/pubs/csia/csia_federal_plan.pdf. Accesat la 30.01.2018.

[76]*** CSIR Guide: *Cyber Security Incident Response Guide – version 1,* http://www.crest-approved.org/wp-content/uploads/CSIR-Procurement-Guide.pdf, Accesat la: 30.03.2015

[77] *** AV: *Independent Tests of Anti-virus Software 2014,* http://chart.av-comparatives.org/awards.php?year=2014 Accesat la: 15.03.2015

[78]*** CERT-RO: *Raport privind evoluția amenințărilor cibernetice în 2017,* https://www.cert.ro/vezi/document/raport-alerte-2017 Accesat 25.02.2018.

[79] *** www.cert-ro.eu/ecsm.php, Accesat la 30.04.2015

[80] *** PwC : *Global State of Information Security Survey 2015,* http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml# Accesat la: 20.03.2015.

Cercetări privind securitatea datelor în sistemele informatice

REZUMAT

Actualitatea și complexitatea ridicată a domeniului privind sistemele informatice, cât și abordarea neunitară în legislațiile naționale, inclusiv la nivel european, a problematicii securității informatice și tratarea diferențiată a infracționalității informatice, deși este vorba despre același flagel indiferent de infrastructura IT, ne-au determinat să abordăm protecția și securitatea informațiilor în sistemele informatice printr-o cercetare interdisciplinară, raportând soluțiile tehnice adoptate și adaptate în timp în raport cu vulnerabilitățile și atacurile informatice la cadrul normativ existent privind securitatea rețelelor și a sistemele informatice.

Al doilea obiectiv al cercetării a fost de a se determina o serie de bune practici/recomandări la nivel organizațional pentru creșterea gradului de securitate a sistemului informatic, aplicabile inclusiv în privința prelucrării datelor cu caracter personal, și respectiv identificarea unei soluții integrate sub forma unui set de măsuri tehnice necesare pentru asigurarea integrității și confidențialității datelor cu caracter personal prelucrate printr-un sistem informatic în cazul instituțiilor de învățământ superior de stat (conform cercetării efectuate), soluții care pot fi generalizate, coroborat însă cu scopul prelucrării, și la alți operatori și la sistemele lor informatice prin care se prelucrează date cu caracter personal în condiții de maximă transparență, securizare și protecție.

Concluziile tezei, atât de natură teoretică cât și empirică, evidențiază faptul că se impune abordarea simultană a celor două laturi (tehnică și juridică) în momentul în care se dorește implementarea unui mecanism de securizare a unui sistem informatic, deoarece soluția tehnică se coroborează cu instrumentele juridice actuale pentru evitarea atacurilor cibernetice asupra sistemelor informatice.

ABSTRACT

The actuality and high complexity of the field Computing Systems, and also uneven approach in national legislation, including at European level, of the issue of cyber security and the treatment of cyber crime differentiated, led us to address the protection and security of information systems through an interdisciplinary research, reporting the technical solutions adopted and adapted against vulnerabilities and attacks with the existing regulatory framework regarding the network security systems.

The second objective of the research was to determine a set of best practices recommendations for enhancing organizational level security system, which are applicable also to the processing of personal data, and respectively identifying an integrated solution as a set of technical measures necessary to ensure the integrity and confidentiality of personal data processed by a computer system for institutions of higher education (according to conducted research), solutions that can be generalized, but in conjunction with the purpose of processing, and other operators and to their computer systems which process personal data in conditions of maximum transparency, security and protection.

The conclusions of thesis, both theoretical and empirical, shows that need to be addressed simultaneously the two sides (technical and legal) when you want to implement a mechanism for

securing a computer system, because the technical solution is supported by tools legal to combat cyber attacks against information systems.

Cercetări privind securitatea datelor în sistemele informatice

FORMAT EUROPEAN CURRICULUM VITAE

Informații personale

Nume / Prenume	MANEA CONSTANTIN ADRIAN
Adresă(e)	
E-mail(uri)	a.c.manea@unitbv.ro
Naționalitate(-tăți)	Română
Data naşterii	

Experiența profesională

Perioada	2003 - prezent
Funcția sau postul ocupat	Consilier juridic IA
Numele şi adresa angajatorului	Universitatea *Transilvania* din Brașov, Brasov, Bd.Eroilor, nr.29, jud.Brașov
Perioada	2005 - prezent
Funcția sau postul ocupat	Asistent universitar doctorand/ Asistent cercetare
Numele şi adresa angajatorului	Universitatea *Transilvania* din Braşov, Bd. Eroilor 29, 500036 Braşov

Educație şi formare

Perioada	**2007- 2010**
Numele si tipul institutiei	Universitatea *Transilvania* din Braşov-Facultatea de Drept şi Sociologie
Domeniul studiat/aptitudini ocupaționale	Master Drept Public şi Instituții Publice
Perioada	**2000**
Numele si tipul institutiei	Universitatea din București – Facultatea de Drept

Aptitudini şi competențe personale	Engleză – scris, vorbit nivel de bază Membru al asociațiilor profesionale: Colegiul Consilierilor Juridici Brasov Membru fondator Asociatia Master.Conference.Awards.Law

Cercetări privind securitatea datelor în sistemele informatice

FORMAT EUROPEAN CURRICULUM VITAE

Personal Information

Name	MANEA CONSTANTIN ADRIAN
Address	
E-mail	a.c.manea@unitbv.ro
Nationality	Romanian
Date of birth	

Professional Experience

Period	2003 - present
Office or post	Legal Adviser IA
Employer name and address	*Transilvania* University of Brașov, Brasov, Bd.Eroilor, No. 29, Brașov County
Period	2005 - present
Office or post	Assistant Professor PhD/ Research Assistant
Employer name and address	*Transilvania* University of Brașov, Brasov, Bd.Eroilor, No. 29, Brașov County

Education and Training

Period	2007- 2010
Name and type of educational institution	*Transilvania* University of Brașov - Law Faculty
Period	2000
Name and type of educational institution	Bucharest University – Law Faculty
Competents and Professional Skills	English language Associate Member : Professional Legal Advisers College Founding Member : Association Master Conference Award Law Romania