

**MINISTERUL EDUCAȚIEI ȘI CERCETĂRII AL
REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Facultatea Calculatoare, Informatică și Microelectronică
Departamentul Inginerie Software și Automatică**

**Admis la susținere
Șef de departament:
conf. univ.,dr. Fiodorov Ion**

_____ „ ” 2021

**Metode de securizare a Sistemului Informațional
„UNIPASS Frontiera”**

Teză de master

Masterand: _____

**Țurcan Anatolie
gr. SI-201M**

Conducător: _____

**Beșliu Victor
prof.univ., dr.**

Chișinău 2022

ADNOTARE

la teza de master cu tema: **Metode de securizare a Sistemului Informațional „UNIPASS Frontiera”**
a studentului gr. SI-201M, programul de studii „Securitate Informațională”

Țurcan Anatolie

Cuvinte cheie: traversarea frontierei, înregistrarea mijloacelor de transport, politici de securitate, măsuri de protecție, autorități publice, sistem de clasificatori.

Scopul lucrării: cercetarea și analiza sistemului informațional „UNIPASS Frontiera” în vederea stabilirii vulnerabilitățile sistemului.

În cadrul tezei au fost analizate sisteme informaționale analogice sistemului dat utilizate la frontiera statelor vecine Ucraina și România, astfel fiind posibil a actualității și importanța sistemului informațional utilizat de serviciul vamal.

Cele trei capitole prezentate în această lucrare sunt: descrierea funcționalității sistemului informațional, analiza sistemelor informaționale analogice din statele vecine și recomandările privind aplicarea metodelor de securizare, iar în final concluzii și bibliografia.

Primul capitol descrie analiza sistemului în cauză, funcționalitatea, cadrul legal, sarcinile, funcțiile, arhitectura, sursele de informații și interacțiunea cu alte sisteme informaționale.

În capitolul doi sunt analizate sistemele informaționale analogice utilizate de către statele vecine la traversarea frontierei și importanța acestora.

În ultimul capitol sunt prezentate metodele de securitate aplicate sistemului informațional „UNIPASS Frontiera”, un sistem complex de securitate informațională care include măsuri juridico-organizatorice, tehnice și fizice, cu utilizarea mijloacelor tehnologice, dispozitivelor software/hardware și a mecanismelor criptografice de protecție a informației, orientate spre asigurarea nivelului necesar de integritate, confidențialitate și accesibilitate al resurselor informaționale.

Din păcate, nu există un sistem de securitate sigur 100%, dar, prin definirea unei politici de securitate realiste, mereu se va găsi cele mai eficiente căi de evitare a riscurilor la care sunt supuse sistemele informaționale.

ANNOTATION

Master's Thesis **Securing methods for the „UNIPASS Frontiera” Information System**

Turcan Anatolie, gr. SI-201M, *Information Security* study programme

Keywords: customs, import duty, means of transportation, protection measures, security policies, public authorities, system of classifiers.

The aim of the paper: research and analysis of the information system „UNIPASS Frontiera” in order to establish the vulnerabilities of the system.

The Master thesis aims to analyze similar information systems implemented within the customs of the neighboring states and namely, Ukraine and Romania. In the end, it has been concluded that such information systems, meant to provide security methods at the border with other countries, is extremely important within the customs of the country.

The main aspects presented in this paper cover the description of the functionality of the information system, the analysis of similar information systems within the customs of the neighboring states. Finally, some important recommendations on the application of security methods have been shared, conclusions have been made, followed by bibliographic references used.

Chapter one aims at a thorough analysis of the field, the functionality, the legal framework and the importance of implementing the above-mentioned information system.

Chapter two examines the similar information systems used within the customs of neighboring states at the border and their importance.

Finally, chapter three provides recommendations on securing the present information system.

Unfortunately, ensuring information security awareness requires a lot of efforts, time and continuous track of important data. An important point to be made is that realistic security policy, with framed rules and procedures for all individuals accessing it should be thoroughly defined. To conclude with, the most effective ways to avoid the risks, to which information systems are exposed to, will be always identified.

Cuprins

INTRODUCERE	8
1. DESCRIEREA FUNCȚIONALITĂȚII SISTEMULUI INFORMAȚIONAL „UNIPASS FRONTIERA”	10
1.1 Cadrul Legal.....	12
1.2 Sarcinile Sistemului Informațional.....	14
1.3 Principalele funcții ale sistemului	16
1.4 Arhitectura generală a sistemului.....	19
1.5 Sursele de informații și interacțiunea cu alte sisteme informaționale.....	22
2. ANALIZA SISTEMELOR INFORMAȚIONALE ANALOGICE SISTEMULUI INFORMAȚIONAL „UNIPASS FRONTIERA” STATELOR VECINE.....	29
2.1 Sistemul informațional „Inspector” al Serviciului Vamal de Stat al Ucrainei.....	29
2.1.1 Schimbul de informații în Sistemul Informațional „Inspector”.....	33
2.1.2 Securitatea Sistemului Informațional „Inspector”.....	34
2.2 Sistem informatic utilizat de Serviciul Vamal România	35
2.2.1 Securitatea sistemului informațional ASYCUDA	38
2.3 Practici de securitate informațională	42
3. METODE DE SECURITATE APLICATE SISTEMULUI INFORMAȚIONAL „UNIPASS FRONTIERA”	46
3.1 Sistemul complex al securității informaționale SI UNIPASS Frontiera	47
3.2 Principalele aspecte ale asigurării securității SI UNIPASS Frontiera.....	50
3.3 Modalitatea de conectare/deconectare la SI UNIPASS Frontiera.....	53
3.4 Măsurile de securitate aplicate SI UNIPASS Frontiera	55
CONCLUZII	65
BIBLIOGRAFIE.....	66

Introducere

Dezvoltarea și implementarea pe scară largă a tehnologiilor informaționale și comunicațiilor continuă să producă schimbări pe paliere multiple, fiind elementul caracteristic al societății bazate pe cunoaștere. Se constată infuzarea accelerată cu o componentă informatică a majorității elementelor existenței umane, de la activități care țin de rutina zilnică până la procese critice ce influențează securitatea și apărarea națională. Datorită modului specific de culegere, prelucrare, stocare și diseminare a informațiilor, sistemele și aplicațiile bazate pe tehnologia informațiilor și comunicațiilor contribuie la eficientizarea proceselor și activităților de management și producție din cadrul organizațiilor publice și private.

Aspirațiile actuale de digitizare a societății, precum și implementarea tehnologiilor informaționale în toate domeniile social-economice simplifică mult realizarea unor acțiuni cotidiene, însă implică necesitatea de asigurare a unui nivel înalt de securitate a datelor și sistemelor informaționale contra diverselor atacuri cibernetice. Pentru moment, în pofida existenței cadrului normativ, fiecare operator de date are propria politică de securitate, care adesea nu răspunde unor exigențe simple. Astfel, există pericolul accesului neautorizat la sistemul de evidență a informațiilor confidențiale și al operațiunilor ilegale de prelucrare a acestora sau încălcării principiilor de confidențialitate a datelor, care eventual poate afecta interesul părților vizate de informațiile respective.

Datorită mediului electronic de transmitere, stocare și gestionare a informațiilor din secolul prezent, un secol al vitezei și al globalizării, se pune tot mai des problema securității informatice și implementării metodelor de securitate.

Amenințările de securitate evoluează constant, iar cerințele de conformitate devin din ce în ce mai complexe. Fără o politică de securitate a informațiilor, este imposibil să se coordoneze și să pună în aplicare un program de securitate în cadrul unei organizații și nici să se comunice măsuri de securitate către terți și auditori externi.

Asigurarea unui grad de conștientizare a securității informațională necesită multe eforturi, timp și cheltuieli. Un punct important de subliniat este că o politică de securitate bine definită, cu reguli și proceduri încadrate pentru toți indivizii care o accesează, va ajuta la triajul, investigarea și blocarea

amenințărilor la care sunt expuse sistemele informaționale.

În rețelele locale de calculatoare și în sistemul de comunicații, măsurile de securitate trebuie să asigure: autentificarea (verificarea identității unei entități de comunicare la distanță); controlul accesului la resurse; confidențialitatea datelor; integritatea datelor; protecția fizică a echipamentelor tehnice. În general, securitatea sistemelor informaționale reprezintă un domeniu foarte complex, în care este implicat întregul personal și care, prin restricțiile și algoritmii pe care le adoptă și le impune, generează de multe ori contradicții și birocrății în exces. Cu toate neajunsurile și inconvenientele pe care le poate genera, este de preferat să se respecte regulile decât să se pună în pericol îndeplinirea misiunii.

Bibliografie

1. Legea nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal. Accesat octombrie 2021
2. Legea nr. 110 din 9 iunie 2011 privind ratificarea Protocolului adițional la Convenția pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, cu privire la autoritățile de supraveghere și fluxul transfrontalier al datelor Legea nr. 229 din 10 octombrie 2013 pentru aprobarea Strategiei naționale în domeniul protecției datelor cu caracter personal pentru anii 2013-2018 și a Planului de acțiuni privind implementarea acesteia;
3. Legea nr. 271 din 07 noiembrie 2013 privind formularea unor declarații ale Republicii Moldova la Convenția pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal;
4. Hotărâre de Guvern HOTĂRÎRE Nr. 834 din 07-07-2008 cu privire la Sistemul informațional integrat al Poliției de Frontieră; Accesat octombrie 2021;
5. Legea nr. 215 din 04.11.2011 cu privire la frontiera de stat a Republicii Moldova;
6. Legea nr. 284 din 22.07.2004 privind comerțul electronic; Accesat octombrie 2021
7. Legea nr. 171 din 06.07 1994 privind secretul comercial; Accesat octombrie 2021
8. Legea nr.112-XVI din 22.05.2008 pentru aprobarea Concepției securității naționale a Republicii Moldova;
9. Hotărârea Guvernului nr. 1123 din 14.12.2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal.
10. Ghidul practic privind utilizarea datelor cu caracter personal;
11. https://www.legis.md/cautare/getResults?doc_id=69750&lang=ro. Accesat octombrie 2021
12. <https://www.bibliofond.ru/view.aspx?id=601024>. Accesat noiembrie 2021
13. https://ec.europa.eu/taxation_customs/customs-4/customs-security/security_en. Accesat noiembrie 2021
14. <https://www.customs.ro/info-publice/programe-de-dezvoltare-ale-directiei-generale-a-vamilor/programe-fonduri-structurale/proiectul-implementarea-politicii-de-securitate> Accesat

octombrie-noiembrie 2021

15. <https://www.exabean.com/information-security/information-security/> Accesat octombrie-noiembrie 2021
16. <https://asycuda.org/en/project/> Accesat octombrie 2021;
17. Hotărârea Guvernului nr. 1144 din 03.11.2005 cu privire la aprobarea Concepției sistemului de administrare a riscurilor în Serviciul Vamal. Accesat octombrie 2021;
18. [Raport privind progresul înregistrat în implementarea acțiunilor din planul anual 2020.](#) Accesat decembrie 2021;
19. [Propunere de recomandări pentru protecția datelor ce țin de domeniul sănătății;](#) Accesat septembrie 2020;
20. Jurnalul Oficial al Uniunii Europene. REGULAMENTUL nr. 679 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) Disponibil: <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex%3A32016R0679> Accesat noiembrie 2020;
21. Comisia Europeană. Comunicare a Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social și Comitetul Regiunilor. Protecția vieții private într-o lume interconectată. Un cadru european privind protecția datelor pentru secolul 21. Bruxelles, 25.1.2012. COM(2012) 9 final. Disponibil: <https://eur-lex.europa.eu/legal-content/ro/ALL/?uri=CELEX%3A52012DC0009> Accesat noiembrie 2020;
22. Sorina-Elena ANGHELUȚĂ. 2015 Protecția datelor cu caracter personal în contextul angajării. Documentație Internet. Disponibil: <https://www.juridice.ro/401834/protectia-datelor-cu-caracter-personal-in-contextul-angajarii.html> Accesat septembrie 2020;
23. Raportul de audit Sistemului Informațional ASYCUDA pentru 2020: https://asycuda.org/wp-content/uploads/2020/ASYCUDA_Annual_Report_2020.pdf Accesat noiembrie 2020;