Co-funded by the Erasmus+ Programme of the European Union

lmpi licence master professionnel en protection informatique

LMPI - N°573901-EPP-1-2016-1-IT-EPPKA2-CBHE-JP
"Licence, Master professionnels pour le développement, l'administration, la gestion, la protection des systèmes et réseaux informatiques dans les entreprises en Moldavie, au Kazakhstan, au Vietnam»

Raport

Sondaj de identificare a profesiilor țintă și a nevoilor de instruire în domeniul securității informatice în Moldova

Chișinău, 2017

Cuprins

1. Introducere

Raportul este perfectat în conformitate cu cerințele Metodologiei GIP FIPAG (Metodologia de realizare a "Sondajului de identificare a profesiilor țintă și a nevoilor de instruire în domeniul securității informatice în Moldova").

Proiectul Erasmus + LMPI își propune să contribuie la consolidarea securității sistemelor și rețelelor informatice ale companiilor din Moldova prin îmbunătățirea pregătirii profesionale (inițială și continuă, față în față sau la distanță) a resurselor umane în domeniu, precum și a competențelor cetățenilor.

Obiectivele proiectului constau în:

- Depășirea deficitului de competențe privind nivelul de proiectare și de menținere a securității sistemelor și rețelelor informatice ale întreprinderilor, îmbunătățirea capacității de inserție profesională a studenților și perfecționarea în domeniu a angajaților.
- Profesionalizarea programelor de învățământ universitar în dezvoltarea, administrarea, gestionarea și protejarea sistemelor și rețelelor informatice în conformitate cu Procesul de la Bologna și cu Cadrul european al calificărilor și relocarea lor către companii.
- Crearea a două programme noi de învățământ accesibile în IDD (instruirea deschisă la distanță) pentru dezvoltarea și protejarea aplicațiilor, a sistemelor și a rețelelor informatice în companii, adaptate nevoilor acestora:
  - la ciclul I – Licență în administrarea și gestionarea sistemelor și rețelelor informatice;
  - la ciclul II – Mater profesional în administrarea și gestionarea sistemelor și rețelelor informatice în companii;
- Formarea a cel puțin 270 de studenți în primul an al celor două programe noi de învățământ (180 în primul an de licență și 90 în primul an de master) ;
- Perfecționarea a 8 cadre didactice în UE, numerizarea cursurilor și a resurselor didactice;
- Crearea unui sistem modular de formare pe tot parcursul vieții în același domeniu de instruire și formarea a 50 de profesioniști.

- Crearea unui centru de excelență în UTM, centru de resurse în suportul noii oferte.
- Alcătuirea curriculum-ului și a conținutului cursurilor, inclusiv a resurselor numerice care se vor pune la dispoziție în IDD.

Proiectul conține 10 loturi de lucru.

Pentru a răspunde recomandărilor procesului de la Bologna legate de profesionalizarea programelor de studii universitare, luând în considerare corespunderea cunoștințelor predate competențelor cerute de profesie, în al doilea lot al proiectului este prevăzută elaborarea unui chestionar și lansarea unui sondaj privind profesia în cauză.

Având în vedere faptul că toate abilitățile și cunoștințele care trebuie să fie stăpânite de către student la sfârșitul programului de formare, astfel încât acest student să se poată angaja în profesia dată, datele colectate din anchetă trebuie să permită studierea necesităților de competențe generice și specifice în companii (fișele de post), nevoile de formare care vor avea ca rezultat o specializare licență și una de master. Astfel, sondajul trebuie să permită:

- identificarea profesiilor care vor fi vizate de noile programme de studii universitare;
- identificarea competențelor necesare acestor profesii;
- identificarea nevoilor de instruire cerute de aceste profesii.

2. Metodologia utilizată

Pentru sondaj este utilizat chestionarul prezentat în Anexa 1. El a fost elaborat de coordonatorul proiectului, Anne Delaballe, cu implicare reprezentanților tuturor universităților participantge în proiectul LMPI. Chestionarul este a fost plasat pe Internet în Microsoft Forms accesibil online la adresa
https://forms.office.com/Pages/AnalysisPage.aspx?id=SB9tG5OIiUi9vx-4QbyuRvrWeCotU1pMtYzOZpQGFBtUQVk5NlRRUzROVDQ0UUI1NFQ1S0dTTlc4UC4u&AnalyzerToken=3lexxkdmDW4d4OZ8mqg6gR2p2WIZgNd4

El conține 23 de întrebări, ultima referindu-se la informații de contact. Sunt:

- 9 întrebări cu o singură opțiune de selectat: 1, 2, 4, 5, 16, 18, 20-22;
- 10 întrebări cu mai multe opțiuni posibile de selectat: 6-15;
- 4 întrebări deschise: 3, 17, 19 et 23.

Pentru orientare, a fost creată o listă prealabilă din 711 companii: 11 bănci; 153 companii, activitatea de bază a cărora ține de informatică, și 547 companii-furnizoare de servicii de comunicaţii electronice. Solicitarea privind completarea chestionarului de către specialiști în domeniu sau cu tangență la acesta a fost efectuată:

- prin Agenția Națională de Reglementare în Comunicații Electronice și Tehnologia Informației (dl vicedirector Serghei Pocaznoi);
- adresări personale ale participanților la proiect (prin e-mail, la telefon, etc.).

Perioada sondajului: 10 iulie - 31 octombrie 2017.

3. Analiza datelor colectate

Chestionarul a fost completat de 199 persoane. Conform spuselor fostului Președinte al Consiliului de administrație al Asociației Naționale a Companiilor TIC din Moldova, dl Veaceslav

Cunev, este unicul caz în practica Republicii Moldova când un chestionar în domeniu a fost completat de un aşa număr mare de persoane.=

În Anexa 1, opțiunile întrebărilor 6-15 și 21 sunt prezentate nu în ordinea afișării acestora în chestionarul original, prezentat respondenților pentru completare, ci în ordinea descreșterii numărului de selectări a acestora de către respondenți. Aceasta facilitează determinarea preferințelor respondenților.

Rezultatele obținute arată următoarele (pe întrebări).

1. Marea majoritate a persoanelor care au completat chestionarul sunt de vârstă de până la 40 de ani (82.9%), peste jumătate fiind de vârstă de până la 30 de ani (53.8%).

2. Mai mult de o treime din respondenți sunt ingineri sau manageri în domeniu (37.2%). O bună parte sunt șefi de companii (5.5%).

3. Peste 81% din respondenți (162) au specificat succint sarcinile lor de serviciu sistematizate în Tabelul 3.1. Acestea sunt ordonate conform numărului de respondenți respectivi.

Tabelul 3.1 Sarcinile de serviciu ale 81% din participanții la sondaj

ID	Sarcini de serviciu	Nr respondenți
1.	Dezvoltare, mentenanţă şi administrare aplicaţii şi situri Web	18
2.	Proiectarea aplicaţiilor şi sistemelor informatice	13
3.	Administrarea securității informatice, inclusiv: monitorizarea activităților malițioase, identificarea vulnerabilităților și a riscurilor de securitate, prevenirea incidentelor informatice	11
4.	Audit şi consultanţă TI şi securitate informaţională	9
5.	Implementare şi administrare reţele de calculatoare	9
6.	Manager IT	9
7.	Predare cursuri, lucrari practice, cercetare stiintifică	9
8.	Dezvoltatori back-end	8
9.	Prevenirea, identificarea şi combaterea criminalității informatice	8
10.	Proiectare şi administrare baze de date	7
11.	Dezvoltarea si mentinerea aplicatiilor mobile	6
12.	Dezvoltatori Java	6
13.	Cercetări în informatică	4
14.	Support servicii TIC	4
15.	Monitorizarea Internet	3
16.	Testarea aplicaţiilor informatice	3
17.	Administrarea sistemelor informatice	2
18.	Colectarea și analiza datelor privind criminalitatea informatică şi infracţiunile conexe	2
19.	Combaterea fraudelor cu mijloace de plată electronice	2
20.	Folosirea aplicaţiilor informatice în proiectarea construcţiilor	2
21.	Student	2
22.	Suportul tehnic și operațional privind dispozitivele infracțiunilor informatice	1

23.	Testarea mijloacelor şi schemelor de tranzacţii electronice	1
24.	Alte	34

Se poate observa că pe a treia poziție este ”Administrarea securității informatice” (11 respondenți), urmată de ”Audit şi consultanţă TI şi securitate informaţională” (9 respondenți), ”Prevenirea, identificarea şi combaterea criminalității informatice” (8 respondenți) ș.a.

4. Bucură faptul că peste 58% din respondenți (116) au experiență profesională în domeniul securității informatice.

5. Aproape 23% din respondenți reprezintă companii cu peste 500 angajați, iar adăugând la acestea și companiile cu 51-100 angajați obținem aproape 41%.

Totalizând informația privind eșantionul de respondenți ai anchetei, obținută ca răspuns la întrebările 1-5, se poate afirma că acesta este unul reprezentativ.

6. Respondenții consideră că specialiști în securitatea informatică lucrează, în primul rând, în: bănci (73.9%); servicii informatice și societăți de consultanță (72.9%); telecomunicații (72.4%); unități militarizate (60.3%), dar și în gerneral în toate întreprinderile dotate cu calculatoare (54.8%).

7. Cea mai mare nevoie de specialiști în securitatea informatică este în: bănci (72.4%); în toate întreprinderile dotate cu calculatoare (70.9%); telecomunicații (66.8%); servicii informatice și societăți de consultanță (64.3%); unități militarizate (60.8%); administrația publică (56.3%); întreprinderile mari (56.3%).

8. Ca activităţi de bază. ce trebuie să fie în stare să le efectueze specialiştii în securitatea informatică. sunt selectate toate cele 12 activități specificate explicit în întrebarea 8 (peste 66.8%), fiind îndeosebi menţionate aşa activităţi ca:

1) Identificarea vulnerabilităților și a riscurilor de securitate la care este expus sistemul (86.4%);
2) Instalarea sistemelor de detectare și prevenire a intruziunilor (80.9%);
3) Raportarea, analiza și predicția atacurilor de securitate (78.4%);
4) Monitorizarea rețelelor și a sistemelor informatice, reacția la incidente (77.4%);
5) Implementarea procedurilor de codificare informații, autentificare utilizatori și dezvoltare infrastructură PKI (73.9%).

Opţiunea 13 “Alte activităţi“ a fost selectată de doar 5.5% din repondenţi.

9. La problemele de bază privind securitatea informatică întâlnite la serviciu se referă:

1) Nivelul scăzut de conștientizare a importanței securității informatice (50.8%);
2) Probleme de confidențialitate a informației (48.2%);
3) Lipsa strategiei de gestiune a riscurilor (36.7);
4) Dificultăți (timp, bani, personal) în implementarea și aplicarea politicilor de securitate în cadrul companiei (35.2%);
5) Probleme de disponibilitate a informației (34.7%);
6) Probleme de modification a informației (34.2%).
7) Lipsa de resurse pentru a monitoriza / implementa standarde de securitate, cum ar fi ISO 27001 ISO 27002 (27.6%) ș.a.

10. Ca mijloace de securitate informatică (logice şi fizice) folosite de agenţii economici sunt selectate toate cele 9 opţiuni specificate explicit în întrebarea 10 (peste 35.2% din respondenți), fiind îndeosebi menţionate aşa mijloace ca:

1) Acces controlat (71.9% din respondenți);
2) Mecanisme și utilitare de protecție logică (software) (70.4%);
3) Contracarare viruși și produse malware (69.8%);
4) Cifrarea datelor (56.8%);
5) Mecanisme și utilitare de protecție tehnică (hardware) (50.8%);
6) Mecanisme și utilitare de protecție fizică (49.2%).

11. Din cele 15 competenţe generice, care ar putea fi necesare unui specialist în securitatea informatică, specificate în chestionar, cea mai puţin selectată este "Conception et gestion de projets" (31.2% din respondenți), procentajul fiind oricum înalt. Cele mai necesare se consideră:

1) Capacitatea de analiză și sinteză (82.9% din respondenți);
2) Abilitatea de identificare a pericolelor și a riscurilor (77.4%);
3) Capacitatea de a gestiona situațiile de urgență (74.4%);
4) Lucrul în echipă (61.8%);
5) Capacitatea de organizare și planificare (57.3%);
6) Preocuparea pentru calitate (54.8%);
7) Efficaciatea (53.3%);
8) Creativitatea (51.3%).

12. Modalităţile de instruire, ce pot permite obținerea competențelor generice, necesare unui specialist în securitatea informatică, se consideră (toate cele şase specificate în chestionar):

1) Activități practices (91.0% din respondenți);
2) Studii tehnice (80.4%);
3) Studii teoretice (76.4%);
4) Studii de cas (73.9%);
5) Lucrul în echipă (61.3%);
6) Învățământul la distanță (37.2%).

De menţionat că opţiunea "Alte" a fost selectată de doar 5.0% din respondenţi.

13. Ca şi competenţe specifice, necesare unui specialist în securitatea informatică, sunt selectate toate cele 19 specificate în chestionar, cea mai puţin selectată fiind "Faire évoluer les réseaux " (39.7% din respondenți), procentajul fiind oricum înalt. Ca mai necesare sunt selectate:

1) Implementarea sistemelor de securitate (83.9% din respondenți);
2) Diagnosticarea sistemelor informaționale (80.9%);
3) Elaborarea și implementarea soluțiilor de protecție a informațiilor (74.9%);
4) Cunoștințe privind Firewall (74.4%);
5) Cunoștințe privind protocoalele de securitate (73.4%);
6) Cunoștințe privind VPN (72.9%);
7) Identificarea punctelorr slabe (72.9%);
8) Cunoștințe privind criptologia (67.3%).

Opţiunea "Autre" a fost selectată de doar 3.5% din respondenţi.

14. La unitățile de conținut ale disciplinelor, pentru dobândirea competențelor specifice necesare unui specialist în securitatea informatică, se referă:

1) Politici de securitate (77.9% din respondenți);
2) Limbi moderne (engleza) (76.9%);
3) Administrarea serviciilor de rețea (73.9%);
4) Administrarea sistemelor (71.9%);
5) Mijloace (aplicații și echipamente) de securitate (VPN, Firewall, etc.) (70.4%);
6) Supravegherea și administrarea rețelelor (68.8%);
7) Criptographie (68.8%);
8) Rețele fără fir și securitate (67.3%);
9) Securizarea serverelor și a poștei electronice a clienților (65.8%);
10) Metodologia de implementare a politicilor de securitate (60.8%);
11) Auditare/penetrare rețele (60.8%);
12) LSA (Layer Security Application) (57.8%);
13) Configurare rutere (51.3%).

15. Modalităţile de instruire, care ar permite obținerea competențelor specifice, necesare unui specialist în securitatea informatică, sunt (toate cele șase specificate în chestionar):

1) Activități practice (87.4% din respondenți);
2) Studii tehnice (78.4%);
3) Studii teoretice (72.4%);
4) Studii de cas (70.4%);
5) Lucrul în echipă (63.3%);
6) Învățământul la distanță (45.7%).

Opţiunea "Alte" a fost selectată de doar 3.0% din respondenţi. De menţionat că ordinea în cauză coincide cu cea a modalităţilor de instruire, care ar permite obținerea competențelor generice (a se vedea întrebarea 12).

16. Aproape 69% din profesioniştii în domeniu (137 respondenți) au specificat că au nevoie de instruire în securitatea informatică.

17. Optzeci şi opt de profesionişti în domeniu, adică peste 44,2% din respondenţi, au specificat că instruirea (perfecţionarea) lor în securitatea informatică ar trebui să includă unitățile de conținut sistematizate în Tabelul 3.2.

Tabelul 3.2 Unitățile de conținut în securitatea informatică, solicitate de 88 participanți la sondaj - profesioniști în domeniu

ID	Unități de conținut solicitate pentru instruire (perfecționare) în securitatea informatică	Nr respondenți
1.	Toate cele specificate în întrebarea 14	8
2.	Formarea (perfecţionarea) profesională în securitatea informatică, inclusiv privind noile realizări în domeniu	31
3.	Securitate informatică, tehnici si standarte de criptare a datelor, nivele de protectie a datelor, asigurarea protectiei si integritatii datelor	1
4.	Proiectarea şi protectia rețelelor de calculatoare	5

5.	Administrarea și securitatea serviciilor de rețea	1
6.	Firewall, VPN, protocoalele de securitate	1
7.	Rutare avansată interioară și exterioară, supravegherea și administrarea rețelelor, WiFi și securitatea, configurare rutere	1
8.	Securitatea în Rețele Publice de Transport Date	1
9.	Securitatea rețelelor de telecomunicatii	2
10.	Managementul situațiilor de criza în contextul atacurilor cibernetice asupra infrastructurilor critice	1
11.	Metode si tehnci de interconectare securizată a sistemelor electronice de plăți	2
12.	Testarea gradului de siguranță a accesului	1
13.	Obținerea controlului asupra altui dispozitiv de la distanță. Obținerea capacităților de a spiona alte dispozitive și alte capacități ce pot contribui la îndeplinirea atribuțiilor de serviciu	1
14.	Securitatea bazelor de date	2
15.	Securizarea resurselor informaționale proprii, conturilor electronice personale, etc.	2
16.	Aplicarea mijloacelor de securitate informatică, inclusiv în cadrul întreprinderii si in viata personala	3
17.	Metodologii de implementare, politici de securitate informatică	1
18.	Securitatea aplicațiilor și sistemelor informatice	2
19.	Instrumentar pentru asigurarea unui nivel acceptatibl al securitatii informatice in organziatie	1
20.	Solutii IDS/IPS, Solutii pentru filtrarea spamului, Solutii pentru managementul logurilor, Tipuri de atacuri, vulnerabilitati si metode de protectie / prevenire	1
21.	Studii de caz si stagii practice în securitatea informatică	7
22.	Identificarea și tratarea riscurilor de securitate a aplicatiilor inforrmatice	2
23.	Programe pentru analiza informațiilor	2
24.	Documentarea infractorilor în Darknet	1
25.	Proceduri de gestiune a securității pentru utilizatorii finali	1
26.	Alte	7

Unitățile de conținut în cauză în Tabelul 3.2 sunt grupate pe domenii. Astfel (ID1), 8 respondenți au specificat direct toate cele 13 unități de conținut din întrebarea 14, iar alții 32 (ID2 și ID3) au specificat, practic, instruirea în securitatea informatică la general, fără a concretiza aparte careva unități de conținut (în total 40 de respondenți, adică 45.5% din cei 88 de respondenți).

Unitățile de conținut cu ID4-ID13 (16 respondenți, 18.2%) se referă la securitatea rețelelor de calculatoare și a componentelor acestora cu unele concretizări față de unitățile de conținut (3), (5), (6), (80, (9) și (13) specificate în întrebarea 13, inclusiv:

a) Managementul situațiilor de criza în contextul atacurilor cibernetice asupra infrastructurilor critice (ID10);
b) Testarea gradului de siguranță a accesului (ID12);
c) Obținerea controlului asupra altui dispozitiv de la distanță (ID13);

d) Metode si tehnci de interconectare securizată a sistemelor electronice de plati (ID11).

Unitățile de conținut cu ID14 și ID15 (4 respondenți) se referă direct la securitatea bazelor de date și a resurselor informaționale proprii ale utilizatorilor.

Aparte este cazul de menționat solicitările privind studiile de caz si stagii practice în securitatea informatică (ID21, 7 respondenți, 0.08%).

18. Aproape 66% din respondenţi (131) au specificat că personal au nevoie de instruire în securitatea informatică.

19. Informațiile privind tipul de instruire în securitatea informatică solicitat de 75 respondenţi este sistematizată în Tabelul 3.3.

Tabelul 3.3 Tipul de instruire în securitatea informatică solicitat de 75 respondenţi

ID	Tipul solicitat de formare în securitatea informatică	Nr respondenți
1.	Teoretică si practică	24
2.	Toate	2
3.	Studii de caz și stagii practice	16
4.	Studii la distanta	7
5.	Lucrul în echipă	4
6.	Exploatarea si administrarea sistemelor de securitate	2
7.	Securitate VoIP și rețele de calculatoare	2
8.	Auditare/penetrare rețele de calculatoare	2
9.	Mijloace (aplicații și echipamente) de securitate (Firewall, VPN, etc.)	1
10.	Securitate Cisco	4
11.	Asigurarea unui Internet mai sigur pentru copii și adulți	2
12.	Securitatea aplicatiilor web	1
13.	Implementare standarde de securitate, cum ar fi ISO 27001 și ISO 27002.	2
14.	Managementul riscurilor de securitate informatică	1
15.	Securitatea bancara	1
16.	Metode de spargere a securitatii sistemelor informatice	1
17.	Auditor sisteme de securitate informatică	1
18.	Cunoştinţe elementare, de precauţie	1
19.	Alte	

Informațiile Tabelului 3.3 arată că cea mai mare parte din respondenții care au răspuns (32%) ar prefera instruirea ”Teoretică si practică” (ID1), 16 respondenți (21%) – ”Studii de caz și stagii practice” și 7 respondenți (9.3%) – ”Studii la distanta”. Unele răspunsuri specifice au completat lista unităților de curs din Tabelul 3.2, cum ar fi: „Securitate VoIP” (ID7), „Securitate Cisco” (ID10), „Implementare standarde de securitate” (ID13) ș.a.

20. Aproape 61% din respondenţi au specificat că organizația în care activează ar accepta studenți la stagii practice în securitatea informatică.

21. Stagiile practice în securitatea informatică pentru studenți, care ar fi acceptate de organizațiile în care activează cei 61% din respondenţi (a se vedea întrebarea 20), se referă la stagii:

a) de observare – 45 răspunsuri (24%);

b) de formare operațională pentru a dezvolta capacitatea de inserție profesională – 72 răspunsuri (39%);
c) funcțional de formare pentru angajare – 70 răspunsuri (37%).

Astfel, posibilitățile de stagii de practică în securitatea informatică pentru studenți sunt promițătoare.

22. Durata stagiului, preferată de organizațiile care ar accepta studenți la stagii practice în securitatea informatică, este de:

1) O lună (28.1%);
2) Trei luni (18.6%);
3) 1-2 săptâmâni (13.6%).

23. Au specificat informaţiile de contact 117 respondenţi. La cele mai cunoscute din acestea se referă: Banca Naţională a Moldovei; Endava; Moldtelecom; Centrul de Cuvernare Electronică de pe lângă Cancelaria Guvernului; Institutul Dezvoltării Societăţii Informaţionale al Academiei de Ştiinţe a Moldovei; Fiscservinform de pe lângă Serviciul Fiscal de Stat; Centrul pentru Combaterea Crimelor Informatice; Trimetrica; Allied Testing; Deeplace; Molddata; Cedacri International; Moore Stephens; Pentalog; Centrul de Telecomunicaţii Speciale; Mobiasbanca – Groupe Société Générale; Agenția Relații Funciare și Cadastru; Tacit Knowledge.

4. Concluzii

Eşantionul de participanţi la sondaj este reprezentativ pentru Republica Moldova. Chestionarul a fost completat de 199 respondenţi, reprezentând şi aşa companii bine cunoscute din domeniu ca: Endava, Moldtelecom, Centrul de Telecomunicaţii Speciale, Centrul de Guvernare Electronică, Fiscservinform ş.a. Aproape 23% din respondenți reprezintă companii cu peste 500 angajați. Peste 58% din respondenți au experiență profesională în domeniul securității informatice.

Cunoştinţe generale privind securitatea informatică sunt necesare tuturor utilizatorilor ce folosesc mijloacele informatice. Nevoie de specialiști în securitatea informatică este îndeosebi în: bănci; telecomunicații; servicii informatice și societăți de consultanță; unități militarizate; administrația publică şi întreprinderile mari. Deşi în mai mică măsură, dar de asemenea specialişti poate fi nevoie şi în întreprinderi mijlocii şi chiar mici.

Ca sarcini de bază ale specialiștilor în securitatea informatică sunt selectate toate cele 12 activirţi specificate explicit în întrebarea 8 (peste 66.8%), iar ca mijloace de securitate informatică (logice şi fizice) folosite de agenţii economici sunt selectate toate cele 9 opţiuni specificate explicit în întrebarea 10 (peste 35.2%), din care 5 opțiuni au fost selectate de peste 50% din respondenți.

Din cele 15 competenţe generice, care ar putea fi necesare unui specialist în securitatea informatică, specificate în chestionar, 8 au fost selectate de peste 50% din respondenți, iar din cele 19 competenţe specifice respective, 14 au fost selectate de peste 50% din respondenți. La fel, din cele 24 nominalizate, 13 unități de conținut ale disciplinelor, pentru dobândirea competențelor specifice necesare unui specialist în securitatea informatică, au fost selectate de peste 50% din respondenți.

Aproape 69% din profesioniștii în domeniu (137 respondenți) au specificat că au nevoie de instruire în securitatea informatică o bună parte din care selectând toate cele 13 unități de conținut

din întrebarea 14. Ca și modalităţi de instruire, sunt selectate toate cele şase specificate în chestionar, inclusiv instruirea online (45.7%).

Aproape 61% din respondenţi au specificat că organizația în care activează ar accepta studenți la stagii practice în securitatea informatică.

În ansamblu, rezultatele sondajului pot servi ca bază la elaborarea programelor de studii universitare în securitatea informatică.

Annexe 1. Le questionnaire pour l'Enquête d'identification des métiers cibles et des besoins de formation dans le champ de la sécurité informatique est les réponses obtenu

No	Question	Resp.	%
1.	Votre âge		
	1) 18-30	**107**	**53.8**
	2) 31-40	**58**	**29.1**
	3) 41-50	**13**	**6.5**
	4) 50+	**21**	**10.6**
2.	Votre profession:		
	1) Chef d'entreprise	**11**	**5.5**
	2) Professeur / manageur	**22**	**11.1**
	3) Ingénieur	**74**	**37.2**
	4) IT Technicien	**17**	**8.5**
	5) Autre	**75**	**37.7**
3.	Décrivez brièvement (3-4 phrases) votre tâches de service:	**162**	**81.4**
	1) Dezvoltare, mentenanţă şi administrare aplicaţii şi situri Web	**18**	**9.0**
	2) Proiectarea aplicaţiilor şi sistemelor informatice	**13**	**6.5**
	3) Administrarea securității informatice, inclusiv: monitorizarea activităților malițioase, identificarea vulnerabilităților și a riscurilor de securitate, prevenirea incidentelor informatice	**11**	**5.5**
	4) Audit şi consultanţă TI şi securitate informaţională	**9**	**4.5**
	5) Implementare şi administrare reţele de calculatoare	**9**	**4.5**
	6) Manager IT	**9**	**4.5**
	7) Predare cursuri, lucrari practice, cercetare stiintifică	**9**	**4.5**
	8) Dezvoltatori back-end	**8**	**4.0**
	9) Prevenirea, identificarea şi combaterea criminalității informatice	**8**	**4.0**
	10) Proiectare şi administrare baze de date	**7**	**3.5**
	11) Dezvoltarea si mentinerea aplicatiilor mobile	**6**	**3.0**
	12) Dezvoltatori Java	**6**	**3.0**
	13) Cercetări în informatică	**4**	**2.0**
	14) Support servicii TIC	**4**	**2.0**
	15) Monitorizarea Internet	**3**	**1.5**
	16) Testarea aplicațiilor informatice	**3**	**1.5**
	17) Administrarea sistemelor informatice	**2**	**1.0**
	18) Colectarea și analiza datelor privind criminalitatea informatică şi infracţiunile conexe	**2**	**1.0**
	19) Combaterea fraudelor cu mijloace de plată electronice	**2**	**1.0**
	20) Folosirea aplicaţiilor informatice în proiectarea construcţiilor	**2**	**1.0**
	21) Student	**2**	**1.0**
	22) Suportul tehnic și operațional privind dispozitivele infracțiunilor informatice	**1**	**0.5**
	23) Testarea mijloacelor şi schemelor de tranzacţii electronice	**1**	**0.5**

	24) Alte	**34**	**17.1**
4.	Votre expérience professionnelle dans le domaine de la sécurité informatique, ans		
	1) Sans expérience	**83**	**41.7**
	2) 1-5	**71**	**35.7**
	3) 6-10	**23**	**11.6**
	4) 10+	**22**	**11.1**
5.	Quelle est la taille de votre entreprise, persons:		
	1) < 10	**34**	**17.1**
	2) 10-50	**69**	**34.7**
	3) 51-100	**15**	**7.5**
	4) 101-500	**36**	**18.1**
	5) 500+	**45**	**22.6**
6.	Selon vous, où travaillent les spécialistes de la sécurité informatique? (plusieurs choix possibles)		
	1) Banques	**147**	**73.9**
	2) Services informatiques et sociétés de consultants	**145**	**72.9**
	3) Télécommunications	**144**	**72.4**
	4) Armées	**120**	**60.3**
	5) Dans toutes les entreprises où il y a des ordinateurs	**109**	**54.8**
	6) Grandes entreprises	**107**	**53.8**
	7) Administrations publiques	**89**	**44.7**
	8) Industries	**79**	**39.7**
	9) Biotechnologies	**63**	**31.7**
	10) Petites et moyennes entreprises de production de services	**62**	**31.2**
	11) Petites et moyennes entreprises de production de produits	**45**	**22.6**
	12) Autre	**16**	**8.0**
7.	Selon vous, où a-t-on le plus besoin de spécialistes de la sécurité informatique? (plusieurs choix possibles)		
	1) Banques	**144**	**72.4**
	2) Dans toutes les entreprises où il y a des ordinateurs	**141**	**70.9**
	3) Télécommunications	**133**	**66.8**
	4) Services informatiques et sociétés de consultants	**128**	**64.3**
	5) Armées	**121**	**60.8**
	6) Administrations publiques	**112**	**56.3**
	7) Grandes entreprises	**112**	**56.3**
	8) Industries	**93**	**46.7**
	9) Biotechnologies	**75**	**37.7**
	10) Petites et moyennes entreprises de production de services	**74**	**37.2**
	11) Petites et moyennes entreprises de production de produits	**62**	**31.2**
	12) Autre	**11**	**5.5**
8.	Précisez les activités, tâches que peuvent réaliser ces spécialistes (plusieurs choix possibles)		
	1) Détection fréquente, détection des vulnérabilités du système	**172**	**86.4**
	2) Mise en place des systèmes de détection, prévention et détection des intrusions	**161**	**80.9**
	3) Rapport, analyse et prédiction des attaque	**156**	**78.4**
	4) Surveillance du réseau et du système, réponse aux incidents	**154**	**77.4**

	5) Mise en œuvre du codage des informations, authentification et construction de l'infrastructure PKI	**147**	**73.9**
	6) Mise en œuvre de la conformité de sécurité	**141**	**70.9**
	7) Assistance régulière des ateliers, des séminaires sur la sécurité de l'information, mise à jour des informations sur les vulnérabilités de sécurité des systèmes/ logiciels	**139**	**69.8**
	8) Audit de sécurité	**139**	**69.8**
	9) Mise en place du système correctif aux pièces des failles de sécurité	**137**	**68.8**
	10) Suggestion et mise en œuvre des normes de sécurité de l'information	**136**	**68.3**
	11) Test de pénétration	**135**	**67.8**
	12) Formation des procédures de sécurité aux utilisateurs des organisations	**133**	**66.8**
	13) Autre	**11**	**5.5**
9.	Précisez quels problèmes vous rencontrer dans votre entreprise concernant la sécurité informatique (plusieurs choix possibles)		
	1) Faible niveau de connaissance de l'ensemble du personnel, de la direction, non seulement des enseignants en informatique sur l'importance de la sécurité de l'information	**101**	**50.8**
	2) Problème de confidentialité de l'information	**96**	**48.2**
	3) Stratégie de gestion des risques adéquate n'est pas encore faite	**73**	**36.7**
	4) Difficultés (temps, argent, personnel) dans la mise en œuvre et l'application des politiques de sécurité au sein de l'entreprise)	**70**	**35.2**
	5) Problème de disponibilité de l'information	**69**	**34.7**
	6) Problème de modification de l'information	**68**	**34.2**
	7) Manque de ressources pour suivre / mettre en œuvre des normes de sécurité telles que ISO 27001	**55**	**27.6**
	8) Ecart entre la sécurité et la facilité d'utilisation	**48**	**24.1**
	9) Manque d'engagement des gestionnaires de haut niveau pour s'assurer que les mécanismes de sécurité sont en place	**41**	**20.6**
	10) Bonne combinaison sur la politique de gestion et la technologie de déploiement n'est pas encore faite	**37**	**18.6**
	11) Problème de substitution d'identité	**32**	**16.1**
	12) Difficultés rencontrées lors de la mise en place des processus de sécurité conformément à la norme ISO 17799	**32**	**16.1**
	13) Difficultés rencontrées de l'ensemble du personnel, de la direction lors de l'élaboration et de la mise en œuvre des processus de sécurité en traitement de l'information, des données et du système d'exploitation	**31**	**15.6**
	14) Manque de coopération entre service commercial et service de sécurité de l'entreprise	**24**	**12.1**
	15) Autre	**26**	**13.1**
10.	Précisez les outils utilisés dans votre entreprise pour la sécurité informatique (logiciels et matériels) (plusieurs choix possibles)		
	1) Accès contrôlé	**143**	**71.9**
	2) Outils de protection software	**140**	**70.4**
	3) Contrer les virus et programmes malveillants	**139**	**69.8**
	4) Encryptage des données	**113**	**56.8**
	5) Outils de protection hardware	**101**	**50.8**
	6) Obstacle physique	**98**	**49.2**

	7) Outils de protection organisationnels	**87**	**43.7**
	8) Outils de protection legaux, moraux, ethiques	**76**	**38.2**
	9) Outils de protection physique	**70**	**35.2**
	10) Autre	**5**	**2.5**
11	Selon vous, qu'elles sont les compétences génériques que doit avoir un spécialiste de la sécurité informatique? (plusieurs choix possibles)		
	1) Capacités d'analyse et de synthèse	**165**	**82.9**
	2) Capacité de vulgarisation des enjeux et des risques	**154**	**77.4**
	3) Capacité à gérer des situations d'urgence	**148**	**74.4**
	4) Travail d'équipe	**123**	**61.8**
	5) Capacité d'organisation et de planification	**114**	**57.3**
	6) Souci de la qualité	**109**	**54.8**
	7) Efficacité	**106**	**53.3**
	8) Créativité	**102**	**51.3**
	9) Esprit critique	**95**	**47.7**
	10) Aptitude à travailler dans un contexte international	**84**	**42.2**
	11) Respect de la confidentialité	**82**	**41.2**
	12) Capacité à communiquer avec des publics divers et variés	**71**	**35.7**
	13) Esprit d'initiative et capacité à entreprendre	**69**	**34.7**
	14) Capacité à manager	**68**	**34.2**
	15) Conception et gestion de projets	**62**	**31.2**
	16) Autre	**8**	**4.0**
12.	Selon vous, quels sont les enseignements qui peuvent permettre d'acquérir ces compétences génériques? (plusieurs choix possibles)		
	1) Stages pratiques	**181**	**91.0**
	2) Techniques	**160**	**80.4**
	3) Théoriques	**152**	**76.4**
	4) Etudes de cas	**147**	**73.9**
	5) Travail de groupe	**122**	**61.3**
	6) Enseignements en ligne	**74**	**37.2**
	7) Autre	**10**	**5.0**
13.	Selon vous, qu'elles sont les compétences spécifiques que doit avoir un spécialiste de la sécurité informatique? (plusieurs choix possibles)		
	1) Mettre en place les différents processus de sécurité	**167**	**83.9**
	2) Réaliser un diagnostic du système d'information	**161**	**80.9**
	3) Apporter différentes solutions de protection	**149**	**74.9**
	4) Connaître les pare-feu	**148**	**74.4**
	5) Maîtriser les protocoles de sécurité	**146**	**73.4**
	6) Maîtriser les VPN	**145**	**72.9**
	7) Recenser les points faibles	**144**	**72.4**
	8) Maîtriser la cryptologie	**134**	**67.3**
	9) Garantir la pérennité des systèmes de sécurité	**129**	**64.8**
	10) Actualiser les systèmes de sécurité en fonction des nouvelles menaces et des dernières technologies	**129**	**64.8**
	11) Rédiger des politiques et des standards de sécurité	**128**	**64.3**
	12) Evaluer la conformité du réseau par rapport aux attentes des métiers	**126**	**63.3**
	13) Concevoir et mettre en œuvre des architectures matérielles et logicielles	**110**	**55.3**

	14) Sensibiliser et former les collaborateurs aux règles de sécurité	**110**	**55.3**
	15) Elaborer des indicateurs de suivi	**99**	**49.7**
	16) Anticiper les négligences et erreurs lourdes	**97**	**48.7**
	17) Ecrire des rapports	**93**	**46.7**
	18) Evaluer les besoins d'accès aux informations et au réseau de chaque service	**84**	**42.2**
	19) Faire évoluer les réseaux	**79**	**39.7**
	20) Autre	**7**	**3.5**
14.	Selon vous, quels sont les enseignements qui peuvent permettre d'acquérir ces compétences spécifiques?		
	1) Politique de sécurité	**155**	**77.9**
	2) Langes modernes (Anglais)	**153**	**76.9**
	3) Administration de services réseaux	**147**	**73.9**
	4) Administration système	**143**	**71.9**
	5) Dispositifs et équipements de sécurité (VPN-Firewall, etc.)	**140**	**70.4**
	6) Supervision et management de Réseaux	**137**	**68.8**
	7) Cryptographie	**137**	**68.8**
	8) Wireless et sécurité	**134**	**67.3**
	9) Sécurisation de serveur et des postes clients	**131**	**65.8**
	10) Méthodologie de la mise en place d'une PSSI	**121**	**60.8**
	11) Audit/Pentesting réseau	**121**	**60.8**
	12) Sécurité de la couche application (Layer Security Application)	**115**	**57.8**
	13) Configuration des routeurs	**102**	**51.3**
	14) Stage professionnel	**94**	**47.2**
	15) Routage avancé intérieur et extérieur	**93**	**46.7**
	16) Architecture hiérarchique d'interconnexion	**88**	**44.2**
	17) IPV6	**86**	**43.2**
	18) Télécommunications haut débit (3G, LTE)	**76**	**38.2**
	19) Expression et Communication	**75**	**37.7**
	20) Téléphonie sur IP	**69**	**34.7**
	21) Conduite de projet	**68**	**34.2**
	22) Droit	**47**	**23.6**
	23) Projet tuteuré	**41**	**20.6**
	24) Economie et Gestion	**23**	**11.6**
	25) Autre	**5**	**2.5**
15.	Selon vous, qu'elles sont les modalités d'enseignement à privilégier afin d'acquérir ces compétences spécifiques?		
	1) Stages pratiques	**174**	**87.4**
	2) Techniques	**156**	**78.4**
	3) Théoriques	**144**	**72.4**
	4) Etudes de cas	**140**	**70.4**
	5) Travail de groupe	**126**	**63.3**
	6) Enseignements numériques	**91**	**45.7**
	7) Autres	**6**	**3.0**
16.	En tant que professionnel avez-vous des besoins en formation sur la sécurité informatique?		
	1) Oui	**137**	**68.8**

	2) Non	**62**	**31.2**
17.	Si vous, avez des besoins en formation sur la sécurité informatique, précisez vos besoins**:**	**88**	**44.2**
	1) Toate cele specificate în întrebarea 14	**8**	**9.1**
	2) Formarea (perfecţionarea) profesională în securitatea informatică, inclusiv privind noile realizări în domeniu	**31**	**35.2**
	3) Securitate informatică, tehnici si standarte de criptare a datelor, nivele de protectie a datelor, asigurarea protectiei si integritatii datelor	**1**	**1.1**
	4) Proiectarea şi protectia reţelelor de calculatoare	**5**	**5.7**
	5) Administrarea și securitatea serviciilor de rețea	**1**	**1.1**
	6) Firewall, VPN, protocoalele de securitate	**1**	**1.1**
	7) Rutare avansată interioară și exterioară, supravegherea și administrarea rețelelor, WiFi și securitatea, configurare rutere	**1**	**1.1**
	8) Securitatea în Rețele Publice de Transport Date	**1**	**1.1**
	9) Securitatea rețelelor de telecomunicatii	**2**	**2.3**
	10) Managementul situațiilor de criza în contextul atacurilor cibernetice asupra infrastructurilor critice	**1**	**1.1**
	11) Metode si tehnci de interconectare securizată a sistemelor electronice de plăți	**2**	**2.3**
	12) Testarea gradului de siguranță a accesului	**1**	**1.1**
	13) Obținerea controlului asupra altui dispozitiv de la distanță. Obținerea capacităților de a spiona alte dispozitive și alte capacități ce pot contribui la îndeplinirea atribuțiilor de serviciu	**1**	**1.1**
	14) Securitatea bazelor de date	**2**	**2.3**
	15) Securizarea resurselor informaționale proprii, conturilor electronice personale, etc.	**2**	**2.3**
	16) Aplicarea mijloacelor de securitate informatică, inclusiv în cadrul întreprinderii si in viata personala	**3**	**3.4**
	17) Metodologii de implementare, politici de securitate informatică	**1**	**1.1**
	18) Securitatea aplicațiilor și sistemelor informatice	**2**	**2.3**
	19) Instrumentar pentru asigurarea unui nivel acceptatibl al securitatii informatice in organziatie	**1**	**1.1**
	20) Solutii IDS/IPS, Solutii pentru filtrarea spamului, Solutii pentru managementul logurilor, Tipuri de atacuri, vulnerabilitati si metode de protectie / prevenire	**1**	**1.1**
	21) Studii de caz si stagii practice în securitatea informatică	**7**	**8.0**
	22) Identificarea și tratarea riscurilor de securitate a aplicatiilor inforrmatice	**2**	**2.3**
	23) Programe pentru analiza informațiilor	**2**	**2.3**
	24) Documentarea infractorilor în Darknet	**1**	**1.1**
	25) Proceduri de gestiune a securității pentru utilizatorii finali	**1**	**1.1**
	26) Alte	**7**	**8.0**
18.	Seriez-vous personnellement intéressé par une formation en sécurité informatique?		
	1) Oui	**131**	**65.8**
	2) Non	**68**	**34.2**
19.	Si vous personnellement a été intéressé par une formation en sécurité informatique, sur quoi aimeriez-vous être formé?	**75**	**37.7**

	1) Teoretică si practică	**24**	**32.0**
	2) Toate	**2**	**2.7**
	3) Studii de caz și stagii practice	**16**	**21.3**
	4) Studii la distanta	**7**	**9.3**
	5) Lucrul în echipă	**4**	**5.3**
	6) Exploatarea si administrarea sistemelor de securitate	**2**	**2.7**
	7) Securitate VoIP și rețele de calculatoare	**2**	**2.7**
	8) Auditare/penetrare rețele de calculatoare	**2**	**2.7**
	9) Mijloace (aplicații și echipamente) de securitate (Firewall, VPN, etc.)	**1**	**1.3**
	10) Securitate Cisco	**4**	**5.3**
	11) Asigurarea unui Internet mai sigur pentru copii și adulți	**2**	**2.7**
	12) Securitatea aplicatiilor web	**1**	**1.3**
	13) Implementare standarde de securitate, cum ar fi ISO 27001 și ISO 27002.	**2**	**2.7**
	14) Managementul riscurilor de securitate informatică	**1**	**1.3**
	15) Securitatea bancara	**1**	**1.3**
	16) Metode de spargere a securitatii sistemelor informatice	**1**	**1.3**
	17) Auditor sisteme de securitate informatică	**1**	**1.3**
	18) Cunoştinţe elementare, de precauţie	**1**	**1.3**
	19) Alte	**1**	**1.3**
20.	Seriez-vous intéressé par accueillir des stagiaires en formation sécurité informatique?		
	1) Oui	**121**	**60.8**
	2) Non	**78**	**39.2**
21.	Si votre organisation accepte des stagiaires, pour quel type de stage?		
	1) Le stage opérationnel pour développer son employabilité	**72**	**36.2**
	2) Le stage fonctionnel pour embaucher	**70**	**35.2**
	3) Le stage d'observation	**45**	**22.6**
22.	Si votre organisation accepte des stagiaires, sur quelle durée accueillerez-vous des stagiaires?	**75**	**37.7**
	1) 1 à deux semaines	**27**	**13.6**
	2) 1 mois	**56**	**28.1**
	3) 3 mois	**37**	**18.6**
	4) Plus de 3 mois	**14**	**7.0**
23.	Souhaitez-vous nous laisser vos coordonnées afin de recevoir des informations sur nos formations ?	**117**	**58.8**
	Molddata, Chirev Pavel, pavel.chirev@gmail.com		
	Cedacri International, Andrei Anghelov, Cell.: +37379854798 e-mail: andrei.anghelov@cedacrinternational.md		
	Universitatea Agrară de Stat din Moldova, l.vacarciuc@uasm.md, tel: +373 69043418, str. Mircesti, 46, Chisinau.		
	Centrul de Guvernare Electronica de pe lângă Cancelaria de Stat, Igor Bercu, igor.bercu@egov.md		
	Centrul de eGuvernare de pe lângă Cancelaria de Stat, Mihail Croitoru, mcroitor@gmail.com		
	Moore Stephens, Valeriu Cernei, valeriu.cernei@bsdm.md		
	Endava SRL, str. Sfatul Tarii 15, MD 2012, info.chisinau@endava.com, avanovski@gmail.com		

	Centrul pentru Combaterea Crimelor Informatice		
	Centrul de Telecomunicaţii Speciale		
	BC „Mobiasbancă – Groupe Société Générale” S.A., Lilian Rusu, lilian.rusu@mobiasbanca.md rusu.lilian.l@gmail.com		
	Tacit Knowledge, antonioprepelita@gmail.com		
	Pentalog		
	Trimaran SRL, Sergiu Gafton, sgafton@gmail.com, t. 069112300		
	Info-Trust Consulting, Marin Prisacaru, marin.prisacaru@infotrust.md		
	Info-Trust Consulting, Alexandru Plesca, alex.plesca@infotrust.md		
	Allied Testing		
	Institutul Dezvoltării Societății Informaționale a Academiei de Științe a Moldovei, Igor Cojocaru, idsi@asm.md		
	Institutul Dezvoltării Societății Informaționale a Academiei de Științe a Moldovei, Ion Coșuleanu, cosuleanu.ion@gmail.com		
	Institutul Dezvoltării Societății Informaționale a Academiei de Științe a Moldovei, Irina Cojocaru, irina.cojocaru@idsi.md		
	Agenția Relații Funciare și Cadastru a Republicii Moldova, Mihail Nișcii, m.niscii@gmail.com		