



Ministerul Educației și Cercetării al Republicii Moldova
Centrul de Excelență în Informatică și Tehnologii Informaționale

"Aprob"

Directorul Centrului de Excelență în Informatică și
Tehnologii Informaționale

_____ Andrei Ciobanu

"__" _____ 2025

Curriculumul stagiului de practică

P.06.O.003 Practica tehnologică

P.04.O.002 Practica tehnologică

Specialitatea: **0611.2 Rețele de calculatoare**

Aprobat:

La ședința Consiliului metodic-științific din 20.06.2025 al Centrului de Excelență în Informatică și Tehnologii Informaționale, proces verbal Nr. 7

Director adjunct _____ Obadă Liuba

La ședința Catedrei de Informatică I din 20.05.2025 al Centrului de Excelență în Informatică și Tehnologii Informaționale, proces verbal Nr. 10

Șef catedra _____ Golub Andrian

Coordonat cu:

Centrul de Excelență în Informatică și Tehnologii Informaționale
Centrul de Excelență în Energetică și Electronică
Colegiul Politehnic din Bălți
Colegiul Universității Tehnice a Moldovei

Autori:

Craițman Liudmila, grad didactic superior, Colegiul Politehnic din Bălți
Dermenji Vasili, grad didactic întâi, Centrul de Excelență în Informatică și Tehnologii Informaționale

Recenzenți:

Sudacevschi Viorica, șefa departamentului Informatică și Ingineria Sistemelor, UTM
Rogojinaru Tatiana, manager serviciul customer, StarLab SRL

Cuprins

I. Preliminarii.....	4
II. Motivația, utilitatea stagiului de practică pentru dezvoltarea profesională.....	4
III. Competențele profesionale specifice stagiului de practică.....	4
IV. Administrarea stagiului de practică.....	5
V. Repartizarea orientativă a orelor.....	5
VI. Sugestii metodologice.....	10
VII. Sugestii de evaluare.....	10
VIII. Resurse necesare pentru atingerea rezultatelor învățării.....	11
IX. Resursele didactice recomandate elevilor.....	13

I. Preliminarii

Perioada de practică tehnologică a elevilor constituie o componentă esențială a procesului educațional, fiind o etapă cheie în pregătirea viitorilor specialiști în domeniul rețelelor de calculatoare. Din acest motiv, formarea profesională ar trebui să fie o prioritate, astfel încât elevul de azi – specialistul de mâine – să fie cât mai bine pregătit pentru a atinge idealul ca „fiecare persoană să devină un profesionist desăvârșit, chiar un expert, în îndeplinirea sarcinilor specifice locului său de muncă”. La încheierea stagiului de practică tehnologică, elevul elaborează și prezintă, conform termenilor stabiliți, raportul practicii și agenda de dezvoltare profesională.

II. Motivația, utilitatea stagiului de practică pentru dezvoltarea profesională

Stagiul de practică tehnologică la specialitatea rețele de calculatoare joacă un rol crucial în dezvoltarea profesională a elevilor, fiind o punte esențială între teoria învățată și aplicarea practică în mediul real de lucru. Motivația pentru participarea la acest stagiul derivă din oportunitatea de a dobândi competențe practice, de a înțelege funcționarea concretă a rețelelor de calculatoare și de a face față provocărilor specifice domeniului. Elevii sunt astfel stimulați să-și dezvolte abilitățile tehnice, să-și cultive gândirea analitică și să-și consolideze încrederea în propriile capacități, pregătindu-se pentru o carieră de succes.

Utilitatea stagiului de practică este evidentă în multiple aspecte. Acesta oferă o experiență directă cu tehnologiile și echipamentele utilizate în industrie, permițând elevilor să-și conecteze cunoștințele teoretice cu cerințele reale ale pieței muncii. Prin implicarea în activități practice, ei învață să configureze, să administreze și să depaneze rețele, dezvoltându-și totodată competențe transversale precum munca în echipă, comunicarea și rezolvarea problemelor. Astfel, stagiul devine un instrument indispensabil pentru formarea unor specialiști bine pregătiți, capabili să răspundă exigențelor profesionale din domeniul rețelelor de calculatoare și să se adapteze rapid la evoluțiile tehnologice.

III. Competențele profesionale specifice stagiului de practică

În cadrul stagiului de practică tehnologică vor fi formate și dezvoltate următoarele competențe profesionale:

CP7. Realizarea lucrărilor de trasare, mufare, crosare a cablurilor.

CP11. Aplicarea metodelor de securizare a rețelei.

CP13. Întreținerea echipamentelor/dispozitivelor și funcționalității rețelei.

Absolventul programului la atribuirea calificării poate:

RÎ7. Executa lucrările de mufare și crosare a cablurilor conform specificațiilor tehnice, folosind instrumentele necesare și respectând standardele de calitate, finalizând intervenția în termenul stabilit.

RÎ11. Aplica metode de securizare a rețelei conform politicilor de securitate, asigurând protecția datelor, prin monitorizarea constantă a stării de securitate și intervenind în caz de incidente cibernetice.

RÎ13. Efectua operațiuni de întreținere preventivă și corectivă asupra echipamentelor de rețea, aplicând proceduri standard pentru menținerea funcționalității optime.

La finalul stagiului de practică, elevul va fi capabil să:

RÎ1. Aplice legile fundamentale ale circuitelor electrice în analiza circuitelor simple de curent continuu și alternativ.

RÎ2. Realizeze conexiuni corecte între elemente de circuit în montaj serie și paralel, respectând schema electrică.

RÎ3. Calculeze parametrii circuitelor electrice, utilizând formulele corespunzătoare.

RÎ4. Identifice principalele tipuri de amenințări, vulnerabilități și atacuri cibernetice care afectează utilizatorii, rețelele și organizațiile.

RÎ5. Configureze metode de protecție a datelor și comunicațiilor, utilizând criptare, autentificare, control al accesului și măsuri de ascundere a datelor.

RÎ6. Evalueze nivelul de disponibilitate al serviciilor IT și aplică planuri de continuitate, răspuns la incidente și recuperare în caz de dezastru.

RÎ7. Respecte legislația și normele etice specifice domeniului securității cibernetice și contribuie la promovarea unei culturi a securității în organizație.

IV. Administrarea stagiului de practică

Învățământ clasic (4 ani)

Semestrul	Numărul de ore	Forma de evaluare	Numărul de credite
VI	120	Prezentarea raportului de practică	4

Învățământ clasic (2 ani)

Semestrul	Numărul de ore	Forma de evaluare	Numărul de credite
II	150	Prezentarea raportului de practică	5

V. Repartizarea orientativă a orelor

Învățământ clasic (4 ani)

Activități /sarcini de lucru	Produse de elaborat	Modalități de evaluare	Număr de ore
AS1. Analizarea sarcinii.	Conținutul, obiectivele și competențele practicii fixate în agendă.	Prezentare.	2
AS2. Analiza surselor de alimentare pentru echipamentele de rețea.	Studiu comparativ al tipurilor de redresoare utilizate în sursele de alimentare.	Concluzii privind eficiența și utilizarea în echipamente IT (ex: router, switch)	4

	Proiectarea unui filtru RC pentru netezirea tensiunii redresate.	Schema electrică a filtrului RC conectat la ieșirea unui redresor.	8
	Montaj practic al unui redresor în punte + filtru.	Montajului realizat pe placa de probă (breadboard). Jurnal de activitate cu observații tehnice	6
	Documentație tehnică a unei surse simple AC-DC pentru echipamente de rețea (5V/12V).	Lista componentelor cu denumiri, valori, marcaje. Recomandări de siguranță (fuzibil, izolare).	6
AS3.Proiectarea unui amplificator de semnal pentru transmisie pe cablu rețea.	Calculul punctului static de funcționare al unui amplificator EC.	Schema electrică a unui amplificator EC.	8
	Simulare a răspunsului în frecvență al amplificatorului EC.	Captură de ecran din simulator cu schema și rezultatele.	6
	Raport de analiză a amplificatorului ca element în lanțul de transmisie de date.	Exemple: amplificatoare în cabluri UTP lungi (>100m). Sugestii pentru reducerea zgomotului (cuplaj capacitiv, reacție negativă).	4
AS4.Integrarea sistemului de protecție și izolare galvanică.	Analiza funcționării transformatorului în sursele switching.	Studiu de caz: transformator într-un adaptor PoE sau UPS.	4
	Proiectarea unui circuit cu optocuplor pentru izolare între două segmente de rețea.	Schemă electrică cu optocuplor între două circuite.	8
	Integrarea diodelor Zener și varicap în circuite de protecție și reglaj.	Circuit de protecție cu diodă Zener (ex: 5.1V) pentru port USB/Ethernet.	4
AS5. Analiza amenințărilor și vulnerabilităților într-o organizație mică.	Studiu comparativ al tipurilor de malware și impactul lor asupra afacerilor.	Tabel comparativ: virus, troian, ransomware, spyware, keylogger. Recomandări de prevenire pentru fiecare tip.	4
	Simularea unui atac de tip phishing.	Ghid pentru utilizatori: cum să recunoască un e-mail periculos.	4
	Analiza vectorilor de atac în rețeaua unei firme.	Hartă logică a rețelei (router, switch, server, stații de lucru) și a punctelor vulnerabile:	6

		Wi-Fi necriptat, parole slabe, porturi deschise. Lista priorităților de remediere.	
AS6. Proiectarea măsurilor de protecție a datelor și accesului.	Aplicarea criptării simetrice (AES) și asimetrice (RSA).	Exemplu practic: criptarea unui fișier cu AES (folosind software gratuit). Diagramă schematică a schimbului de chei RSA în HTTPS.	4
	Configurarea unui sistem de control al accesului (RBAC).	Schemă de implementare pe un server Windows/Linux.	10
	Protejarea bazei de date a firmei.	Plan de backup zilnic + copie offsite. Utilizarea hashing-ului pentru parole (ex: SHA-256). Mecanisme de audit: jurnalizarea acceselor.	6
AS7. Elaborarea planului de răspuns la incidente și continuitate operațională.	Elaborarea unui plan de răspuns la incidente.	Pașii de urmat în caz de atac. Model de raport de incident.	6
	Proiectarea unui plan de recuperare în caz de dezastru.	Scenarii critice: incendiu, inundație, pană generală. Soluții de redundanță: server secundar, cloud backup, generator.	4
	Analiza cadrelor legale și etice în securitatea informației.	Explicația GDPR, NIS, Legea 161/2003 etc. Recomandări pentru conformitate.	4
AS8. Elaborarea raportului stagiului de practică.	Raportul stagiului de practică.	Respectarea standardelor la realizarea raportului stagiului de practică.	6
AS9. Susținerea raportului stagiului de practică.	Raportul (tipărit/în format electronic) și agenda elevului prezentate conducătorului pe practică.	Prezentarea proiectului individual.	6

Învățământ clasic (2 ani)

Activități /sarcini de lucru	Produse de elaborat	Modalități de evaluare	Număr de ore
AS1. Analizarea sarcinii.	Conținutul, obiectivele și competențele practicii fixate în agendă.	Prezentare.	2

AS2. Analiza surselor de alimentare pentru echipamentele de rețea.	Studiu comparativ al tipurilor de redresoare utilizate în sursele de alimentare.	Concluzii privind eficiența și utilizarea în echipamente IT (ex: router, switch)	4
	Proiectarea unui filtru RC pentru netezirea tensiunii redresate.	Schema electrică a filtrului RC conectat la ieșirea unui redresor.	10
	Montaj practic al unui redresor în punte + filtru.	Montajului realizat pe placa de probă (breadboard). Jurnal de activitate cu observații tehnice	8
	Documentație tehnică a unei surse simple AC-DC pentru echipamente de rețea (5V/12V).	Lista componentelor cu denumiri, valori, marcaje. Recomandări de siguranță (fuzibil, izolare).	8
AS3. Proiectarea unui amplificator de semnal pentru transmisie pe cablu rețea.	Calculul punctului static de funcționare al unui amplificator EC.	Schema electrică a unui amplificator EC.	10
	Simulare a răspunsului în frecvență al amplificatorului EC.	Captură de ecran din simulator cu schema și rezultatele.	8
	Raport de analiză a amplificatorului ca element în lanțul de transmisie de date.	Exemple: amplificatoare în cabluri UTP lungi (>100m). Sugestii pentru reducerea zgomotului (cuplaj capacitiv, reacție negativă).	6
AS4. Integrarea sistemului de protecție și izolare galvanică.	Analiza funcționării transformatorului în sursele switching.	Studiu de caz: transformator într-un adaptor PoE sau UPS.	6
	Proiectarea unui circuit cu optocuplor pentru izolare între două segmente de rețea.	Schemă electrică cu optocuplor între două circuite.	10
	Integrarea diodelor Zener și varicap în circuite de protecție și reglaj.	Circuit de protecție cu diodă Zener (ex: 5.1V) pentru port USB/Ethernet.	6
AS5. Analiza amenințărilor și vulnerabilităților într-o organizație mică.	Studiu comparativ al tipurilor de malware și impactul lor asupra afacerilor.	Tabel comparativ: virus, troian, ransomware, spyware, keylogger. Recomandări de prevenire pentru fiecare tip.	6
	Simularea unui atac de tip phishing.	Ghid pentru utilizatori: cum să recunoască un e-mail periculos.	6

	Analiza vectorilor de atac în rețeaua unei firme.	Hartă logică a rețelei (router, switch, server, stații de lucru) și a punctelor vulnerabile: Wi-Fi necriptat, parole slabe, porturi deschise. Lista priorităților de remediere.	8
AS6. Proiectarea măsurilor de protecție a datelor și accesului.	Aplicarea criptării simetrice (AES) și asimetrice (RSA).	Exemplu practic: criptarea unui fișier cu AES (folosind software gratuit). Diagramă schematică a schimbului de chei RSA în HTTPS.	6
	Configurarea unui sistem de control al accesului (RBAC).	Schemă de implementare pe un server Windows/Linux.	10
	Protejarea bazei de date a firmei.	Plan de backup zilnic + copie offsite. Utilizarea hashing-ului pentru parole (ex: SHA-256). Mecanisme de audit: jurnalizarea acceselor.	8
AS7. Elaborarea planului de răspuns la incidente și continuitate operațională.	Elaborarea unui plan de răspuns la incidente.	Pașii de urmat în caz de atac. Model de raport de incident.	6
	Proiectarea unui plan de recuperare în caz de dezastru.	Scenarii critice: incendiu, inundație, pană generală. Soluții de redundanță: server secundar, cloud backup, generator.	6
	Analiza cadrelor legale și etice în securitatea informației.	Explicația GDPR, NIS, Legea 161/2003 etc. Recomandări pentru conformitate.	4
AS8. Elaborarea raportului stagiului de practică.	Raportul stagiului de practică.	Respectarea standardelor la realizarea raportului stagiului de practică.	6
AS9. Susținerea raportului stagiului de practică.	Raportul (tipărit/în format electronic) și agenda elevului prezentate conducătorului pe practică.	Prezentarea proiectului individual.	6

VI. Sugestii metodologice

Până la începerea practicii, conducătorul stagiului de practică din instituția de învățământ efectuează instructajul practicii prin informarea elevilor despre scopul și sarcinile practicii, durata practicii, structura și cerințele pentru completarea raportului stagiului de practică.

Raportul trebuie a fi completat cu documentele necesare, perfectat și prezentat de elev la sfârșitul stagiului de practică.

Raportul stagiului de practică va fi întocmit conform *Anexei 1*.

Raportul stagiului de practică se întocmește pe parcursul desfășurării stagiului de practică, iar după finisarea perioadei stagiului de practică, se prezintă pentru control și avizare conducătorului stagiului de practică. În raport urmează a fi reflectate la detaliu toate sarcinile efectuate de elev în cadrul desfășurării stagiului de practică, de asemenea datele, schemele, calculele (distanțelor între echipamente, subrețele, etc.) și documente autentice cu referire la condițiile de aplicare, utilizare a softului și a echipamentelor de rețea, regulamente, instrucțiuni.

La fiecare compartiment al raportului se anexează actele justificative.

De asemenea, sunt incluse documentele și materialele ce confirmă lucrul individual al elevului.

VII. Sugestii de evaluare

Pe parcursul stagiului de practică sunt recomandate tehnici de evaluare la locul de practică și în condiții de lucru simulate.

Competențele sunt evaluate sub aspect teoretic: test oral, în cadrul discuției/consultării și cele sub aspect practic: prin observarea directă în condiții de muncă reale (simularea circuitelor electrice și electronice de bază; verificarea comportamentului mărimilor electrice în diverse condiții; analiza și diagnosticarea funcționării echipamentelor; înțelegerea modului de conectare și funcționare a componentelor pasive și active; simularea unui atac cibernetic; aplicarea criptării; configurarea unui sistem; elaborarea unui plan de răspuns la incidente, etc.).

Evaluările teoretice și practice sunt realizate de conducătorul stagiului de practică tehnologică de la instituția de învățământ.

Conducătorul stagiului de practică implică în procesul evaluării și persoanele terțe din cadrul instituției de învățământ.

Produsele de elaborat sunt prezentate în tabelul ce urmează:

Nr. crt.	Categoria de produs	Criterii de evaluare a produsului
1.	Proiectul sursei stabilizate cu protecție pentru echipamente IT.	– Corectitudinea calculelor și schemelor. – Calitatea documentației tehnice. – Calitatea montajelor practice/simulărilor. – Claritatea expunerii și logică. – Aplicabilitatea în contextul rețelelor de calculatoare. – Respectarea normelor de protecție a muncii. – Creativitatea.

2.	Plan de securitate cibernetică pentru o mică întreprindere IT.	– Corectitudinea tehnică. – Aplicabilitatea soluțiilor într-un mediu real. – Claritatea și structura documentației. – Profunzimea analizei (risc, impact, conformitate). – Respectarea normelor de protecție a muncii. – Creativitatea.
3.	Raportul stagiului de practică.	– Corespunderea raportului stagiului de practică cerințelor stabilite (Anexa 1). – Completitudinea raportului. – Originalitatea. – Creativitatea.
4.	Prezentarea electronică.	– Structurarea conținutului. – Relevanța informației din prezentare. – Formatarea prezentării.
5.	Agenda formării profesionale a elevului.	– Oportunitatea completării agendei. – Veridicitatea conținutului expus. – Completitudinea agendei.

VIII. Resursele necesare pentru atingerea rezultatelor învățării

Activitățile în cadrul stagiului de practică tehnologică se execută în locurile unde sunt situate echipamentele necesare.

Locul pentru stagiul de practică trebuie să fie asigurat cu echipamente tehnologice moderne și mobilier ergonomic, care să asigure un mediu propice desfășurării activităților practice. Dotările esențiale includ aparate de măsură precise (multimetre, osciloscoape, generatoare de semnal), componente electrice și electronice diverse, precum și instrumentar pentru realizarea și testarea circuitelor.

Spațiul de lucru trebuie să fie bine iluminat, ventilat și să respecte normele de ergonomie, astfel încât să ofere confort și siguranță elevilor pe durata sesiunilor practice. Întreținerea echipamentelor implică verificarea periodică a funcționării aparaturii, calibrarea instrumentelor de măsură și menținerea curăteniei în laborator.

Este necesară instalarea de software specializat, precum Cisco Packet Tracer, Wireshark, OpenSSL sau aplicații de criptare, semnătură digitală și gestionare a accesului. Mobilierul va fi ergonomic, adaptat lucrului individual sau în echipă, iar spațiile de lucru trebuie să asigure acces facil la echipamente și siguranță operațională.

De asemenea, gestionarea corectă a cablurilor și a conexiunilor electrice este obligatorie pentru prevenirea accidentelor și asigurarea unui mediu de lucru organizat. Utilizarea resurselor trebuie să respecte normele de siguranță electrică, inclusiv măsuri de protecție împotriva electrocutărilor și descărcărilor electrostatice, garantând astfel un cadru sigur pentru elevi și cadre didactice.

Standardul de dotare a laboratoarelor

Suprafața totală a laboratorului – min. 30 m²

Suprafața pentru un elev – min. 2 m²

Numărul locurilor de lucru – min. 15

Nr. crt.	Denumirea	Cantitatea per elev	Cantitatea per atelier
a) Echipamente			
1.	Standuri funcționale compuse din circuite de curent continuu	-	5
2.	Standuri funcționale compuse din circuite de curent alternativ	-	5
3.	Standuri funcționale compuse din circuite cu diverse scheme de amplificare	-	5
4.	Rezistențe	5	80
5.	Inductanțe	5	80
6.	Condensatoare	5	80
7.	Transformatoare monofazate	1	16
8.	Diode semiconductoare	8	128
9.	Tranzistoare bipolare	5	80
10.	Voltmetru	1	16
11.	Ampermetru	1	16
12.	Wattmetru	1	16
13.	Ohmmetru	1	16
14.	Calculator (cu specificații minime: procesor i5, 8 GB RAM, SSD 256 GB)	1	15
15.	Monitor LED 24"	1	15
16.	Router de rețea (ex. Cisco/Juniper)	-	2
17.	Switch gestionabil (24 porturi)	-	2
18.	Access Point Wi-Fi	-	1
19.	Firewall hardware	-	1
b) Mobilier și tehnică sanitară			
20.	Masă de lucru	1	15
21.	Scaun ergonomic reglabil	1	15
22.	Dulap pentru echipamente	-	2
23.	Tabla interactivă/whiteboard	-	1
c) Utilaj tehnologic			
24.	Router profesional	-	15
25.	Access Point Wi-Fi securizat	-	15
d) Instrumente și dispozitive			
26.	Software specializat: Cisco Packet Tracer, Wireshark, OpenSSL, antivirus, VPN client	-	15
27.	Platforme educaționale (Moodle, Google Classroom, Netacad.com, etc.)	-	1
e) Inventar și ustensile			
28.	Manuale și ghiduri de programare	1	15
29.	Markere pentru tablă albă	-	4
30.	Burete pentru tablă albă	-	1

IX. Resursele didactice recomandate elevilor

Nr. crt.	Denumirea resursei	Locul în care poate fi consultată / accesată resursa
1.	Guțu, Valentin. Electrotehnica și electronica . Ch., 2010. 671 p.: il. Bibliogr.: p. 670 ISBN 978-9975-63-314-7 621.3 / G-98	Bibliotecă
2.	T. R. Kuphaldt, Lessons on Electric Circuits Volume III – Semiconductors, manual electronic, 2002. 365 p.	Bibliotecă
3.	Blajă V. Electronica, Dispozitive și circuite electronice, Ciclu de prelegeri. Chișinău: U.T.M., 2005	Bibliotecă
4.	Teste electrotehnica și electronică.	http://www.didactic.ro/resurse-educationale/invatamant-profesional-si-tehnic/electrotehnica-aplicata/toate-clasele/teste
5.	Noțiuni fundamentale de circuite electrice.	http://etc.unitbv.ro/~craciun/ElnAn/Curs/C1_Intro.pdf
6.	Buta Adrian, Opincariu Daniel, Bazele electrotehnicii, Lecții de curs.	https://www.google.com
7.	Bazele electrotehnicii, partea 2-a.	http://elth.pub.ro/~vasilescu/bazele_electrotehnicii_2/
8.	Bazele Electrotehnicii.	http://biblioteca.regielive.ro/cursuri/electrotehnica/bazele-electrotehnicii-30035.html
9.	Bazele electronicii.	http://www.hobbytronica.ro/articole/electronica-pentru-incepatori/
10.	Adrian Graur, Bazele Electronicii.	https://ru.scribd.com/doc/122486903/Bazele-Electronicii-Adrian-Graur
11.	E. Cazacu, Bazele electrotehnicii I,II, 2012.	http://www.elth.pub.ro/~cazacu/1.%20Support%20Curs%20BE%20I-TR-%20TET%202015/curs_Bazele%20Electrotehnicii_TET.pdf
12.	CCNA-Routing-and-Switching-Complete-Study-Guide-Exam-100-105-Exam-200-105-Exam-200-125-PDF.	Server local al instituției, format electronic
13.	Donahue, G. Network warrior. – O’Reilly Media, 2011. – 788 p.	Server local al instituției, format electronic
14.	Balchunas, Aaron. Cisco CCNA Study Gide. 2014. – 321 p.	Server local al instituției, format electronic
15.	Tomai, N.; Silaghi, Gh.C. Tehnologii și aplicații mobile. –	Server local al instituției, format electronic

Nr. crt.	Denumirea resursei	Locul în care poate fi consultată / accesată resursa
	Cluj-Napoca: Risoprint, 2012. –	
16.	Moise, G.; Constantinescu, Z.; Vlădoiu, M.; Dumitru, M. Networking și securitate. – Ploiesti: Editura Universității Petrol-Gaze, 2015.	Server local al instituției, format electronic
17.	CCNA-Routing-and-Switching-Complete-Study-Guide- Exam-100-105-Exam-200-105-Exam-200-125-PDF.	Server local al instituției, format electronic

Structura raportului stagiului de practică tehnologică

- I. Foaia de titlu.
- II. Cuprins
- III. Preliminarii
- IV. Descrierea sarcinii
 - 1) Proiectul sursei stabilizate cu protecție pentru echipamente IT
 - i. Conversia AC-DC
 - a) Redresor + filtru + măsurători.
 - b) Documentație tehnică și justificări.
 - ii. Amplificarea și condiționarea semnalului
 - a) Etaj amplificator EC: calcul, simulare, aplicație în rețele.
 - iii. Protecția și izolarea
 - a) Transformator, optocuplor, diode Zener.
 - b) Soluții pentru eliminarea interferențelor.
 - 2) Plan de securitate cibernetică pentru o mică întreprindere IT
 - i. Descrierea firmei (nume, domeniu, număr de angajați, tipul datelor procesate).
 - ii. Amenințări și vulnerabilități
 - a) Analiza riscurilor: malware, phishing, weak passwords.
 - b) Hartă a rețelei și puncte slabe identificate.
 - iii. Măsuri de protecție
 - a) Criptare, control de acces, protecție baze de date.
 - b) Justificări tehnice și economice.
 - iv. Răspuns la incidente și continuitate
 - a) IRP și DRP detaliate.
 - b) Redundanță, backup, testare.
 - v. Conformitate legală și etică
 - a) Respectarea GDPR, NIS, legislație națională.
 - b) Cod de conduită și recomandări pentru formare continuă.
- V. Concluzii
- VI. Bibliografie
- VII. Anexe