Cofinanțat de Uniunea Europeană

Proiect cofinanțat din Fondul Social European prin Programul Educație și Ocupare 2021-2027
Axa prioritara: P07
Titlul proiectului: Practică Racordată Actualității Constănțene în Tehnologia Informației și Comunicații
Contract: PE0/71/PEO _P7 /OP4/ESO4.5/PEO _A49/ G2024-63816/ SMIS 311134

Concursul pentru Elevi și Studenți în Tehnologia Informației

"ESTIC 2026", ediția a XIX-a, 23 mai 2026

Facultatea de Matematică și Informatică
Universitatea "OVIDIUS" din Constanța
PROGRAM

SECȚIUNEA PRACTIC
Sala AB1

Nr. crt.	Ora	Titlul lucrării	Nume şi prenume studenți (an studii) *Profesor îndrumător*	Specializare	Universitate
1.	14:00	SPYE - Toolkit for scraping social platforms	Ioniță Alin-Robert (III) -	Matematică informatică	Universitatea „Ovidius" din Constanța
2.	14:07	CorePass Fan – Secure Digital Ticketing & Access Control System	Horoiu Cezar (I) -	Informatică	Universitatea „Ovidius" din Constanța
3.	14:14	Aplicație informatică pentru realizare backup securizat	Hoțescu Nicolae (III) *Lect. univ. dr. Iordache Dorin*	Informatică	Universitatea „Ovidius" din Constanța
4.	14:21	PhishEye: Intelligent system for detecting and classifying phishing sites	Virgolici Miruna-Teodora (III) *Conf. univ. dr. Pelican Elena*	Informatică (în limba engleză)	Universitatea „Ovidius" din Constanța
5.	14:28	SOC AI Copilot: Threat Intelligence Assistant	Sandu David VIctor (I) -	Securitate cibernetică și învățare automată/Cyber	Universitatea „Ovidius" din Constanța

				Security and Machine Learning	
6.	14:35	Tester Saver	Matei Ștefan (II) *Măceș Andrei*	Informatică	Universitatea „Ovidius” din Constanța
7.	14:42	SmartSecML: Modele Hibride pentru Analiza Statistică și Prevenirea vulnerabilităților	Simion Ana-Bianca (III) *Conf. univ. dr. Pelican Elena*	Informatică	Universitatea „Ovidius” din Constanța
8.	14:49	Sistem Inteligent Pentru Detectarea și Clasificarea Atacurilor Web	Roșca Gabriel (III) *Lect. univ. dr. Iordache Dorin*	Informatică	Universitatea „Ovidius” din Constanța
9.	14:56	RedForge	Bungiu Rareș-Ionuț (I) -	Securitate cibernetică și învățare automată/Cyber Security and Machine Learning	Universitatea „Ovidius” din Constanța
10.	15:03	Veritas Email Analyzer	Jecu Dragoș-Cristian (I) *Conf. univ. dr. Pelican Elena*	Securitate cibernetică și învățare automată/Cyber Security and Machine Learning	Universitatea „Ovidius” din Constanța
11.	15:10	Analiza si detectia modificarilor in imagini folosind tehnici de expertiza tehnico-stiintifica	Solomon Dragoș-Cristian (III) *Lect. univ. dr. Iordache Dorin*	Informatică	Universitatea „Ovidius” din Constanța
12.	15:17	Aplicație informatică pentru monitorizarea prezenței utilizând NFC	Teliman Mihai (III) *Lect. univ. dr. Iordache Dorin*	Informatică	Universitatea „Ovidius” din Constanța

13.	15:24	Detectarea anomaliilor în traficul de rețea prin detecția semnăturilor și a statisticilor	Greceanu Octavian (III) *Conf. univ. dr. Nicola Aurelian*	Informatică	Universitatea „Ovidius” din Constanța
14.	15:31	WiFi Toolkit	Atintisan-Serbulescu Alexandra (II) *Paul Boldeanu*	Securitate cibernetică și învățare automată/Cyber Security and Machine Learning	Universitatea „Ovidius” din Constanța
15.	15:38	Policy as Code Implementation: Auditare si Autoaparare Automatizata a Infrastructurii in Cloud	Pană Dragoș-Andrei (II) *Boldeanu Paul*	Securitate cibernetică și învățare automată/Cyber Security and Machine Learning	Universitatea „Ovidius” din Constanța
16.	15:45	WebGuard Tester	Bugan Andrei (III) -	Informatică	Universitatea „Ovidius” din Constanța
17.	15:52	Sistem de Detectare a Intruziunilor in Retea	Bora Cristian-Vasile (III) *Lect. univ. dr. Iordache Dorin*	Informatică (în limba engleză)	Universitatea „Ovidius” din Constanța
18.	15:59	PhishGuard AI	Leu Alexandra (II) -	Informatică (în limba engleză)	Universitatea „Ovidius” din Constanța
19.	16:06	Sistem expert pentru colectarea, analiza si corelarea datelor	Țugui Tiberiu-Alexandru (III) *Lect. univ. dr. Iordache Dorin*	Informatică	Universitatea „Ovidius” din Constanța

Comisia de organizare:
Conf. univ. dr. Elena Pelican
Conf. univ. dr. Aurelian Nicola
Conf. univ. dr. Gabriela Onu-Badea

Comisia de evaluare pentru secțiunea Studenți - PRACTIC:
Conf. univ. dr. Aurelian Nicola – președinte
Lect. univ. dr. Dorin Iordache
Conf. univ. dr. Elena Băutu

Conf. univ. dr. Cristina Șerban
Lect. univ. dr. Anata-Flavia Ionescu

Conf. univ. dr. Cristina Șerban
Lect.univ.dr. Andrei Rusu
Andrei Măceș – Expert IT Cornerstone Technologies

Notă. Concurenții sunt rugați să se prezinte în sală cu cel puțin 30 minute înainte de ora la care au fost programați.

Ioniță Alin-Robert (III): SPYE - TOOLKIT FOR SCRAPING SOCIAL PLATFORMS, Matematică informatică (Universitatea „Ovidius" din Constanța)
Acest pachet este menit persoanelor care doresc să automatizeze colectarea informațiilor publice (OSINT) de pe platforme sociale (Instagram, TikTok, Twitter, Reddit). Oferă posibilități de împachetare a datelor în formatele JSON și CSV, implică AI pentru detecta topic-ul general al postărilor, pune la dispoziție o bază de date pentru salvarea rezultatelor și un dashboard web pentru vizualizarea datelor și informații suplimentare.

Horoiu Cezar (I): COREPASS FAN – SECURE DIGITAL TICKETING & ACCESS CONTROL SYSTEM, Informatică (Universitatea „Ovidius" din Constanța)
Sistem securizat care previne frauda și accesul neautorizat prin: * tokenuri unice * semnături criptografice * validare în timp real

Hoțescu Nicolae (III): APLICAȚIE INFORMATICĂ PENTRU REALIZARE BACKUP SECURIZAT, Informatică (Universitatea „Ovidius" din Constanța)
Aplicația propune un sistem de backup securizat, structurat în două module care comunică prin cloud file. Pe stația sursă, fișierele sensibile sunt identificate automat utilizând YOLOv11 și PaddleOCR, fiind apoi protejate prin criptare hibridă (simetrică + asimetrică) și transformate în coduri QR. Ulterior, modulul de pe stația destinație preia datele din cloud, le decriptează și reasamblează exact topologia fișierelor originale.

Virgolici Miruna-Teodora (III): PHISHEYE: INTELLIGENT SYSTEM FOR DETECTING AND CLASSIFYING PHISHING SITES, Informatică (în limba engleză) (Universitatea „Ovidius" din Constanța)
„PhishEye: Intelligent System for Detecting and Classifying Phishing Sites" este o aplicație web concepută pentru verificarea securității link-urilor și identificarea rapidă a fraudelor online. La introducerea unui URL suspect, sistemul oferă un verdict, un scor de risc și detalii esențiale precum locația serverului, validitatea certificatului SSL sau lanțul de redirecționări. Proiectul se diferențiază prin modulul care explică pe înțelesul oricui motivele suspiciunii, dar și printr-un chat interactiv care oferă lămuriri despre logica analizei. Utilizatorii pot accesa strategii de apărare, pot descărca rapoarte PDF și au la dispoziție un istoric al scanărilor, aplicația fiind astfel un instrument complet de protecție și educație în mediul digital.

Leu Alexandra (II), Carniceanu Andrei (I): PHISHGUARD AI, Informatică (în limba engleză) (Universitatea „Ovidius" din Constanța)
PhishGuard AI este o aplicație software dezvoltată în Python, destinată detectării tentativelor de phishing din emailuri și linkuri web. Sistemul utilizează tehnici de analiză automată și algoritmi de inteligență artificială pentru identificarea mesajelor suspecte și evaluarea riscului de atac cibernetic. Aplicația oferă utilizatorului explicații și recomandări pentru prevenirea fraudelor informatice.

Matei Ștefan (II): TESTER SAVER, Informatică (Universitatea „Ovidius" din Constanța)
Un bot ce face code-review pull request-urile de pe github la un repository public si care poate fi gestionat din interfata.

Simion Ana-Bianca (III): SMARTSECML: MODELE HIBRIDE PENTRU ANALIZA STATISTICĂ ȘI PREVENIREA VULNERABILITĂȚILOR, Informatică (Universitatea „Ovidius" din Constanța)

SmartSecML este o soluție desktop de detecție a fișierelor malițioase care reunește mai multe motoare de analiză complementare, ale căror rezultate sunt agregate printr-un mecanism de decizie bazat pe machine learning și vot ponderat. În contrast cu antivirusurile clasice bazate pe o singură paradigmă de detecție, sistemul propus evaluează fiecare fișier printr-un ansamblu de mecanisme complementare și sintetizează rezultatele într-un verdict unificat. Această strategie multi-strat atenuează punctele oarbe specifice metodelor individuale, asigurând un grad de acoperire superior unui motor monolitic.

Roșca Gabriel (III): SISTEM INTELIGENT PENTRU DETECTAREA ȘI CLASIFICAREA ATACURILOR WEB, Informatică (Universitatea „Ovidius" din Constanța)
Un site educativ pentru securitate cibernetică, care are implementat un sistem inteligent de detectare și clasificare la atacuri web

Bungiu Rareș-Ionuț (I): REDFORGE, Securitate cibernetică și învățare automată/Cyber Security and Machine Learning (Universitatea „Ovidius" din Constanța)
RedForge este o aplicație construită pentru a testa și îmbunătăți securitatea modelelor de inteligență artificială. Mai exact, folosește un AI care generează și lansează automat atacuri (de tip "prompt injection") pentru a vedea dacă le poate păcăli să divulge informații secrete. Aplicația testează două modele în paralel ca să vadă care rezistă mai bine, iar când găsește o vulnerabilitate, folosește un model local pentru a rescrie și repara automat regulile de apărare. Totul funcționează dintr-un dashboard curat și simplu, de unde poți face și teste manuale, poți urmări performanța sistemului și poți descărca rapoarte clare cu rezultatele.

Jecu Dragos-Cristian (I): VERITAS EMAIL ANALYZER, Securitate cibernetică și învățare automată/Cyber Security and Machine Learning (Universitatea „Ovidius" din Constanța)
Analizator de e-mailuri bazat pe transformeri (distilBERT) si procesare avansata a limbajului natural, pentru detectarea si oprirea atacurilor de tip "phishing". Modelul si testele rulează local, fără nevoia de parteneri terți, iar mail-urile rămân mereu pe dispozitivul utilizatorului. Sistemul, sub forma unei extensii pentru clientul de e-mail Mozilla Thunderbird/Betterbird, clasifica mesajele drept "Safe" sau "Phishing". De asemenea, aplicația realizează Sentiment Analysis, validează SPF, DKIM, DMARC s. a, analizează atașamentele din email, semnalează daca mesajul a fost trimis de pe o adresa adesea folosita de atacatori (pe baza de TDL, cu allowlist si blocklist - ex. blochează mesaje trimise din Iran sau de la adrese. loan/. rip).

Solomon Dragoș-Cristian (III): ANALIZA SI DETECTIA MODIFICARILOR IN IMAGINI FOLOSIND TEHNICI DE EXPERTIZA TEHNICO-STIINTIFICA, Informatică (Universitatea „Ovidius" din Constanța)
Lucrarea prezintă o aplicație web pentru detectarea imaginilor generate sau modificate de inteligența artificială, folosind o arhitectură forensică pe cinci straturi de analiză: metadate EXIF, criminalistică la nivel de pixel (ELA, zgomot), domeniul frecvențelor (DCT, wavelets), anomalii vizuale și proveniență. Un orchestrator agregă scorurile ponderat și aplică reguli de corecție pentru a reduce fals-pozitivele pe fotografii reale editate. Aplicația este construită cu FastAPI și OpenCV, oferind un verdict explicabil (LIKELY_REAL → AI_GENERATED), hărți de căldură și un raport detaliat pe fiecare strat.

Teliman Mihai (III): APLICAȚIE INFORMATICĂ PENTRU MONITORIZAREA PREZENȚEI UTILIZÂND NFC, Informatică (Universitatea „Ovidius" din Constanța)
Aplicație de mobile, dezvoltată pentru Android, care se folosește de modulul NFC al dispozitivului pentru a scana tag-urile NFC ale studenților cu scopul de a monitoriza prezența într-un cadru academic.

Greceanu Octavian (III): DETECTAREA ANOMALIILOR ÎN TRAFICUL DE REȚEA PRIN DETECȚIA SEMNĂTURILOR ȘI A STATISTICILOR, Informatică (Universitatea „Ovidius" din Constanța)
O aplicație ce ruleaza local pe masina gazda, monitorizeaza traficul ce trece prin interfata de retea prin stocarea pachetelor captate intr-o baza de date, iar pe baza unor interogari obtine traficul anormal posibil existent, si notifica utilizatorul de existenta anomaliilor.

Atintisan-Serbulescu Alexandra (II): WIFI TOOLKIT, Securitate cibernetică și învățare automată/Cyber Security and Machine Learning (Universitatea „Ovidius" din Constanța)
O interfață educațională și ghidată pentru învățarea instrumentelor de securitate wireless. Aceasta include utilitare utilizate în mod obișnuit, cum ar fi airmon-ng, aircrack-ng, kismet, fiecare cu explicații clare și câmpuri de introducere ușor de utilizat care corespund opțiunilor din linia de comandă. Interfața este concepută pentru a ajuta utilizatorii să înțeleagă ce face fiecare instrument și cum funcționează.

Pană Dragoș-Andrei (II): POLICY AS CODE IMPLEMENTATION: AUDITARE SI AUTOAPARARE AUTOMATIZATA A INFRASTRUCTURII IN CLOUD, Securitate cibernetică și învățare automată/Cyber Security and Machine Learning (Universitatea „Ovidius" din Constanța)
Proiectul prezinta un sistem modern de DevSecOps bazat pe conceptul de Policy as Code, utilizand Terraform si Open Policy Agent pentru auditarea automata a securitatii infrastructurii in Microsoft Azure. Elementul central al lucrarii este implementarea unui algoritm de Self-Healing intr-un script de orchestrare PowerShell; acesta intercepteaza vulnerabilitatile cibernetice (porturi SSH deschise, Key Vault public, lipsa tag-urilor) in faza de dezvoltare (Shift-Left) si aplica automat patch-uri corectoare direct pe codul sursa inainte de deployment, garantand o infrastructura sigura prin design.

Bugan Andrei (III): WEBGUARD TESTER, Informatică (Universitatea „Ovidius" din Constanța)
WebGuard Tester este o soluție hibridă de testare a securității cibernetice, formată dintr-o extensie de browser intuitivă și un motor de scanare (API) dezvoltat în Python. Lucrarea automatizează auditul non-intruziv al aplicațiilor web, identificând instantaneu vulnerabilități critice de infrastructură (porturi expuse), configurări greșite (SSL, Headere HTTP) și scurgeri de date sensibile. Prin transformarea analizelor tehnice complexe într-un scor vizual clar și prin generarea automată a rapoartelor PDF pentru clienți, aplicația democratizează accesul la securitate web, oferind companiilor un instrument de evaluare a riscurilor rapid, etic și gata de utilizare în mediul comercial.

Bora Cristian-Vasile (III): SISTEM DE DETECTARE A INTRUZIUNILOR IN RETEA, Informatică (în limba engleză) (Universitatea „Ovidius" din Constanța)
Un NIDS ce ajuta la detectarea intruziunilor in retea pe baza de semnatura, ML sau hybrid

Sandu David VIctor (I): SOC AI COPILOT: THREAT INTELLIGENCE ASSISTANT, Securitate cibernetică și învățare automată/Cyber Security and Machine Learning (Universitatea „Ovidius" din Constanța)
SOC AI Copilot: Threat Intelligence Assistant este o platformă inteligentă destinată asistării analiștilor SOC în procesul de investigare și triere a alertelor de securitate. Aplicația analizează loguri și artefacte asociate incidentelor cibernetice, extrage indicatori de compromitere (IOC), identifică tipare specifice atacurilor și oferă explicații, clasificări de severitate și recomandări pentru răspuns la incidente folosind tehnologii AI și reguli de detecție.

Țugui Tiberiu-Alexandru (III): SISTEM EXPERT PENTRU COLECTAREA, ANALIZA SI CORELAREA DATELOR, Informatică (Universitatea „Ovidius" din Constanța)
Platformă web inteligentă de analiză OSINT (utilizând date publice) orientată spre threat intelligence.