SYLLABUS / FIŞA DISCIPLINEI

1. Information on the study programme / Date despre programul de studii

1.1. Institution / Instituția de învățământ superior	Universitatea de Vest din Timișoara
1.2. Faculty / Facultatea	Matematică și Informatică
1.3. Department / Departamentul	Computer Science (Informatică)
1.4. Study program field	Computer Science (Informatică)
1.5. Study cycle/ Ciclul de studii	Masters / master
1.6. Study programme / Programul de studii / calificarea*	Cybersecurity / Securitate Cibernetică / Database administration / *Administrator baze de date - 252101; Computer network administration / Administrator de retea de calculatoare - 252301; Analyst / Analist - 251201; Research assistant in computer science / Asistent de cercetare în informatica - 214918; Programmer / Programator - 251202; Software systems designers / Proiectant sisteme informatice - 251101*

2. Information on the course / Date despre disciplină

2.1. Title of the course / Denumirea disciplinei	Introducere în securitatea cibernetică. Tehnici de prevenire, detecție și mitigare.						
2.2. Teacher in charge of the course / Titularul activităților de curs	Ciprian Pungilă						
2.3. Teacher in charge of the seminar / Titularul activităților de seminar	Ciprian Pungilă						
2.4. Study year / Anul de studii	1	2.5. Semester / Semestrul	1	2.6. Examination type / Tipul de evaluare: E(xam)/C(olloquim)	E	2.7. Course type / Regimul disciplinei: M(andatory)/ E(lective)/ F(acultative)	M / DS

3. Estimated study time (number of hours per semester) /Timpul total estimat (ore pe semestru al activităților didactice)

3.1. Attendance hours per week / Număr de ore pe săptămână	4	out of which din care: 3.2 lecture/ curs	2	3.3. seminar/laborator	2
3.4. Attendance hours per semester / Total ore din planul de învățământ	56	out of which: 3.5 lecture / curs	28	3.6. seminar/laborator	28

Distribution of the allocated amount of time / Distribuția fondului de timp*	**hours/ ore**
Individual study /Studiu după manual, suport de curs, bibliografie și notițe	32
Supplementary documentation at library or using electronic repositories / Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate	20
Preparing for laboratories, homework, reports etc. /Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri	28
Exams / Examinări	7
Tutoring / Tutorat	7

3.7. Total number of hours of individual study / Total ore studiu individual	94
3.8. Total number of hours per semester / Total ore pe semestru	150
3.9. Number of credits (ECTS) / Număr de credite	6

4. Prerequisites (if it is the case) / Precondiții (acolo unde e cazul)

4.1. curriculum / de curriculum	Computer Architecture, Operating Systems I, Operating Systems II, Programming I, Programming II
4.2. skills / de competențe	C1. Programarea în limbaje de nivel înalt C2. Dezvoltarea şi întreținerea aplicațiilor informatice. C4. Utilizarea bazelor teoretice ale informaticii.

5. Requirements (if it is the case) / Condiții (acolo unde e cazul)

5.1. for the lecture / de desfășurare a cursului	• Sală de curs, dotată corespunzător: tablă, laptop/proiector, software adecvat.
5.2. for the seminar, laboratory / de desfășurare a seminarului/laboratorului	• Sală de laborator, dotată corespunzător: tablă, laptop/proiector, calculatoare, rețea, legătură internet, software adecvat.

6. Acquired skills / Competențe specifice acumulate

Professional skills / Competențe profesionale	• C2. Dezvoltarea şi întreținerea aplicațiilor informatice. • C5. Utilizarea şi administrarea sistemelor de calcul, a bazelor de date şi a rețelelor de calculatoare
Transversal skills / Competențe transversale	• CT3. Utilizarea unor metode şi tehnici eficiente de învățare, informare, cercetare şi dezvoltare a capacităților de valorificare a cunoştințelor, de adaptare la cerințele unei societăți dinamice şi de comunicare în limba română şi într-o limbă de circulație internațională

7. Objectives of the course / Obiectivele disciplinei (reieșind din grila competențelor specifice acumulate)

7.1. General objective / Obiectivul general al disciplinei	• Formarea deprinderilor esențiale pentru înțelegerea securității din perspectivă cibernetică. • Însuşirea cunoştințelor generice despre importanța securității informatice şi consecințele neaplicării acesteia. • Însuşirea conceptelor de bază legate de tipurile de atacuri cibernetice existente, de impactul economic, social şi politic al acestora. • Formarea deprinderilor pentru analiza, investigarea şi mitigarea riscului în cazul breşelor de securitate cibernetică.
7.2. Specfic objectives / Obiectivele specifice	• Utilizarea metodologiilor, mecanismelor de specificare şi a mediilor de dezvoltare pentru realizarea aplicațiilor informatice • Utilizarea de criterii şi metode adecvate pentru evaluarea aplicațiilor informatice. • Realizarea şi întreținerea unor aplicații informatice pentru rezolvarea unor

	probleme reale de complexitate medie. • Utilizarea metodologiilor si mediilor de proiectare si administrare a sistemelor de calcul, bazelor de date si retelelor de calculatoare pentru probleme particulare. • Realizarea unor proiecte de sisteme de calcul, baze de date si retele de calculatoare.

8. Content / Conținuturi*

8.1. Lecture / Curs	Teaching strategies / Metode de predare	Remarks, details / Observații
Introducere. Istoria Internetului: adresele de Internet, DNS, infrastructura Internet, World Wide Web. Introducere în securitatea cibernetică: clasificarea tipurilor de atacuri, motivarea atacurilor, ținte comune ale atacurilor.	Expunerea interactivă, problematizarea, conversaţia euristică, documentarea pe web, exemplificarea.	1 săptămână – 2 ore
Tipuri de atacuri și tehnici de prevenire. Tipuri de atacuri informatice: adware, spyware, browser hijacking, viruși, viermi, cai troieni, scareware, ransomware, exploatări 'zero-day'. **Tehnici de detecție a tipurilor de atacuri.** Tehnici de detecție a tipurilor de atacuri cibernetice. Recunoașterea tipurilor de atacuri cibernetice.	Expunerea interactivă, problematizarea, conversaţia euristică, documentarea pe web, exemplificarea.	2 săptămâni – 4 ore
Tipuri de crime cibernetice. Tipuri de crime cibernetice: cyber-stalking, pornografie infantilă, falsificare și contrafacere, piraterie software, cyber-terorism, phishing, vandalism informatic, hacking cibernetic. **Crearea și distribuirea virușilor prin Internet.** Tipuri de distribuție: spam, cross-site scripting, fraudă licitații online, cybersquatting, bombe logice, web-jacking, furt de timp Internet, atacuri de tip denial-of-service (DoS), atac "salami", alterarea datelor, email	Expunerea interactivă, problematizarea, conversaţia euristică, documentarea pe web, exemplificarea.	2 săptămâni – 4 ore

spoofing.		
Concepte și practici generale de securitate. Concepte și practici de securitate aplicate: autentificare, criptografie și semnături digitale, programe antivirus și firewall, stenografie.	Expunerea interactivă, problematizarea, conversaţia euristică, documentarea pe web, exemplificarea.	1 săptămână – 2 ore
Criminalitate cibernetică. Investigații digitale în criminalitatea cibernetică: cybercrime, impact economic și financiar. Stocarea datelor pe medii externe și interne. Protecția datelor și recuperarea lor.	Expunerea interactivă, problematizarea, conversaţia euristică, documentarea pe web, exemplificarea.	2 săptămâni – 4 ore
Noțiuni de bază în aplicarea securității informatice. Noțiuni de bază a securității informatice. Folosirea unui utilitar pentru gestiunea parolelor. Autentificarea în doi pași. Securizarea sistemelor de calcul folosind programe gratuite antivirus. Configurarea programelor de tip firewall. Selecția unui browser adecvat.	Expunerea interactivă, problematizarea, conversaţia euristică, documentarea pe web, exemplificarea.	1 săptămână – 2 ore
Politici de prevenire a atacurilor informatice. Politici smart pentru guvernanță și management. Controlul aplicațiilor. Controlul utilizatorilor. Controlul rețelelor. Controlul terminalelor informatice. Politici de securitate pentru utilizatori mobili și la distanță. Politici de monitorizare, detecție și înregistrare.	Expunerea interactivă, problematizarea, conversaţia euristică, documentarea pe web, exemplificarea.	1 săptămână – 2 ore
Tehnici de mitigare a atacurilor cibernetice. Tehnici de mitigare a atacurilor cibernetice. Răspunsul adecvat la incidentele ce implică securitatea cibernetică. Tratarea breșelor de securitate. Mitigarea atacurilor de tip	Expunerea interactivă, problematizarea, conversaţia euristică, documentarea pe web, exemplificarea.	2 săptămâni – 4 ore

inginerie socială.		
Tehnici de analiză şi investigare digitală a conţinutului. Analiza fişierelor de tip jurnal. Analiza sistemelor de fişiere. Descoperirea breşelor de securitate.	Expunerea interactivă, problematizarea, conversaţia euristică, documentarea pe web, exemplificarea.	1 săptămână – 2 ore
Studii de caz. Atacuri informatice: primul virus de boot, primul virus informatic, primii viruși polimorfici și metamorfici, primul virus pentru spionaj industrial (Stuxnet).	Expunerea interactivă, problematizarea, conversaţia euristică, documentarea pe web, exemplificarea.	1 săptămână – 2 ore

Recommended bibliography / Bibliografie

1. T.A. Johnson , "Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare" , CRC Press, 2015.
2. P:W. Singe,r A. Friedman, "Cybersecurity and Cyberwar: What Everyone Needs to Know" , Oxford Press, 2014.
3. Kevin D. Mitnick, W.L. Simon , "The Art of Deception: Controlling the Human Element of Security" , 2003
4. A. S. Tanenbaum, "Modern Operating Systems", 2nd edition (cel putin), Prentice Hall International
5. A. Silberschatz, P.B. Galvin, "Operating Systems Concepts", 4th edition (cel putin), Addison Wesley
6. C. Pungilă, website, http://web.info.uvt.ro/~cpungila
7. K. Zetter, "Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon", 2015

8.2. Seminar, lab / Seminar, laborator	**Teaching/learning strategies / Metode de predare/ invățare**	**Remarks, details / Observații**
Introducere în sistemele de operare Windows, Linux și MacOS X. Prezentarea particularităților de securitate ale fiecăruia. Noțiuni introductive de administrare a sistemelor de operare.	Exerciţiul, discuţiile şi dezbaterea, modelarea, proiectul, lucrul în grup organizat.	1 săptămână – 2 ore
Introducere în mașini virtuale. Identificarea unor atacuri virale folosind mașini virtuale dedicate. Evidențierea impactului distructiv și analiza pierderilor de date în urma acestuia.	Exerciţiul, discuţiile şi dezbaterea, modelarea, proiectul, lucrul în grup organizat.	1 săptămână – 2 ore
Analiza și investigarea aplicațiilor de tip antivirus. Particularități de analiză bazată pe semnături.	Exerciţiul, discuţiile şi dezbaterea, modelarea, proiectul, lucrul în grup organizat.	1 săptămână – 2 ore
Analiza și investigarea aplicațiilor de tip antivirus. Particularități de analiză euristică/comportamentală.	Exerciţiul, discuţiile şi dezbaterea, modelarea, proiectul, lucrul în grup organizat.	1 săptămână – 2 ore
Analiza și investigarea aplicațiilor de tip firewall. Particularități de funcționare	Exerciţiul, discuţiile şi dezbaterea, modelarea, proiectul, lucrul în grup organizat.	1 săptămână – 2 ore

bazată pe semnături.		
Analiza și investigarea aplicațiilor de tip firewall. Particularități de funcționare bazate pe euristici/analiza traficului de date.	Exerciţiul, discuţiile şi dezbaterea, modelarea, proiectul, lucrul în grup organizat.	1 săptămână – 2 ore
Administrarea sistemelor de operare Windows din perspective securității. Aspectele generice și particulare pentru prevenirea, detecția și mitigarea riscurilor cibernetice.	Exerciţiul, discuţiile şi dezbaterea, modelarea, proiectul, lucrul în grup organizat.	1 săptămână – 2 ore
Administrarea sistemelor de operare Linux din perspective securității. Aspectele generice și particulare pentru prevenirea, detecția și mitigarea riscurilor cibernetice.	Exerciţiul, discuţiile şi dezbaterea, modelarea, proiectul, lucrul în grup organizat.	1 săptămână – 2 ore
Administrarea sistemelor de operare MacOS X din perspective securității. Aspectele generice și particulare pentru prevenirea, detecția și mitigarea riscurilor cibernetice.	Exerciţiul, discuţiile şi dezbaterea, modelarea, proiectul, lucrul în grup organizat.	1 săptămână – 2 ore
Administrare defensivă a sistemelor de operare Windows. Diferențele între Windows și Windows Server Edition.	Exerciţiul, discuţiile şi dezbaterea, modelarea, proiectul, lucrul în grup organizat.	1 săptămână – 2 ore
Administrare defensivă a sistemelor de operare Linux. Modele și concepte de securitate în Linux (Ubuntu/Debian/CentOS).	Exerciţiul, discuţiile şi dezbaterea, modelarea, proiectul, lucrul în grup organizat.	1 săptămână – 2 ore
Tehnici de analiză a datelor. Recuperarea datelor pierdute ca urmare a atacurilor informatice.	Exerciţiul, discuţiile şi dezbaterea, modelarea, proiectul, lucrul în grup organizat.	1 săptămână – 2 ore
Tehnici de analiză a conținutului. Algoritmi de procesare a conținutului și de regăsire a datelor.	Exerciţiul, discuţiile şi dezbaterea, modelarea, proiectul, lucrul în grup organizat.	1 săptămână – 2 ore
Studiu de caz: virusologie informatică. Analiza bazată pe semnături și cea bazată pe comportament.	Exerciţiul, discuţiile şi dezbaterea, modelarea, proiectul, lucrul în grup organizat.	1 săptămână – 2 ore

Recommended bibliography / Bibliografie

1. T.A. Johnson , “Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare” , CRC Press, 2015.
2. P:W. Singe,r A. Friedman, “Cybersecurity and Cyberwar: What Everyone Needs to Know” , Oxford Press, 2014.
3. Kevin D. Mitnick, W.L. Simon , “The Art of Deception: Controlling the Human Element of Security” , 2003
4. A. S. Tanenbaum, “Modern Operating Systems”, 2nd edition (cel putin), Prentice Hall International

5. A. Silberschatz, P.B. Galvin, "Operating Systems Concepts", 4th edition (cel putin), Addison Wesley
6. C. Pungilă, website, http://web.info.uvt.ro/~cpungila
7. K. Zetter, "Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon", 2015

9. Correlations between the content of the course and the requirements of the IT field / Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatorilor reprezentativi din domeniul aferent programului

- Conținutul disciplinei corespunde curriculei din alte centre universitare, din țară sau Uniunea Europeană. Conținuturile practice (lucrări de laborator) corespund cerințelor de pe piața muncii locală.

10. Evaluation / Evaluare*

Activity / Tip de activitate	10.1. Evaluation criteria / Criterii de evaluare**	10.2. Evaluation methods / Metode de evaluare***	10.3. Weight in the averaged mark / Pondere din nota finală
10.4. Lecture / Curs	Evaluarea are în vedere următoarele categorii de cunoștințe: • cunoștințe generale, evaluate printr-un test cuprinzând întrebări cu variante multiple de răspuns sau definiții de bază • cunoștințe de detaliu, evaluate printr-un test cuprinzând întrebări orientate spre noțiunile cheie predate • utilizarea algoritmilor, evaluate printr-un test cuprinzând un set de probleme pe baza algoritmilor prezentați la curs.	Examinare scrisă; participare activă la activitățile de curs.	35
	Lucrările de control periodice acoperă părți ale materiei, în condiții similare examenului scris final.	Examinare scrisă intermediară	15
10.5. Seminar/ lab	Evaluarea are în vedere următoarele categorii de cunoștințe: • cunoștințe generale: utilizarea și înțelegerea utilitarelor de administrare defensivă • cunoștințe de detaliu: aplicarea conceptelor de securitate ale sistemelor de operare, în contextul	Evaluarea temelor, activităților adiționale; Evaluarea activității la laborator; Participarea activă la activitățile de laborator	20

	detecției și mitigării riscurilor informatice • cunoștințe avansate: realizarea de scenarii de reacție și mitigare complexe, eventual folosind unelte diferite pentru rezolvarea unor sarcini de dificultate medie sau sporită, ca urmare a atacurilor informatice.		
	Temele/referatele sau proiectele acoperă părți ale materiei prezentate la laborator, în condiții similare examinării de laborator.	Proiect individual, proiect de grup.	30

10.6. Minimal knowledge for passing / Standard minim de performanță

Examinare scrisă:

- Pentru nota 5 este necesară obținerea unui punctaj superior (minim 60%) pentru cunoștințele generale, precum și dovedirea unui nivel minim de înțelegere și aplicare a unora dintre algoritmii prezentați la curs (minim 40%)
- Pentru nota 10 este necesară obținerea unui punctaj superior (minim 75%) pentru cunoștințele generale și cunoștințele de detaliu, precum și o bună înțelegere a algoritmilor prezentați

Probe practice și activitate de laborator:

- Pentru nota 5 este necesară obținerea unui nivel superior (minim 60%) pentru cunoștințele generale, precum și a unui nivel minim de înțelegere și utilizare a cunoștințelor de detaliu prezentate anterior.

Pentru nota 10 este necesară dovedirea unui nivel superior (minim 80%) pentru cunoștințele avansate, precizate anterior.

Date/ Data completării

Signature (lecture) /
Semnătura titularului de curs

Signature (seminar)
Semnătura titularului de seminar

Signature (director of the department)
Semnătura directorului de departament
Conf.dr. Victoria Iordan