MD-2045, CHIŞINĂU, STR. STUDENȚILOR, 9/7, TEL: 022 50-99-01 | FAX: 022 50-99-05, www.utm.md

SÉCURITÉ INFORMATIQUE

1. Informations sur l'unité de cours / module

Faculté	Ordinateurs, Génie logiciel et Microeletronique				
Chaire/département	Filière Francophone Informatique, dép. Génie Logiciel et Automatique				
Cycle d'études	Études supérieures, Licence - cycle I				
Programme d'études	526.2 Technologies de l'information				
Année d'étude	**Semestre**	**Type d'évaluation**	**Catégorie formative**	**Catégorie d'option**	**Crédites ECTS**
I(enseignement à plein temps);	7	E	S – Unité de cours de spécialité	O - Unité de cours obligatoire	4

2. Estimation du temps total

Nombre total d'heures dans le programme	Dont				
	Heures dans la salle de cours		Travail individuel		
	Cours	Travaux pratique/dirigés	Projet d'année	Étude du matériel théorique	Préparation de l'application
120	30	30/-		30	30

3. Prérequis pour l'accès à l'unité de cours/module

Selon le programme d'études	Réseaux informatiques ; Algoritmique et Programmation, technologies Web, Administration des réseaux, Programmation réseau.
Selon les compétences	Connaissances et compétences pour développer des applications informatiques, le langage C, .

4. Conditions de déploiement le processus éducatif pour

Cours	Pour présenter le matériel théorique en classe, on a besoin d'un tableau, d'un projecteur et d'un ordinateur.
Travaux pratique/dirigés	Les étudiants rédigeront des rapports selon les conditions formulées dans les indications méthodiques. La durée du soutien d'un travail pratique est une semaine après l'achèvement. La soumission tardive du document est pénalisée : -1 point pour une semaine de retard.

5. Compétences spécifiques accumulées

Compétences professionnelles	✓ Capacité d'identifier et de définir les composants architecturaux hardware, software et des communications, ainsi que ceux nécessaires pour décrire un produit du programme. ✓ Capacité d'identifier, de décrire et d'organiser des activités en équipe; développer les capacités de communication et de collaboration, ainsi que d'assumer différents rôles (exécution et leadership). ✓ Capacité d'appliquer des méthodes de base pour spécifier des solutions architecturales et d'infrastructure pour des problèmes typiques de calcul. ✓ Capacité d'utiliser des critères et des méthodes pour évaluer les caractéristiques fonctionnelles et non fonctionnelles des composants du système. ✓ Capacité de mettre en place une solution d'architecture et d'infrastructure basée sur les contraintes indiquées par le projet.

Compétences	CT1. Appliquer les principes, les normes et les valeurs de l'éthique professionnelle.

transversales	
	CT2. Identifier, décrire et gérer les activités organisées en équipe ; développement des capacités de communication et de collaboration, ainsi que d'assumer les différents rôles (exécution et leadership)
	CT3. Faire preuve de l'esprit d'initiative et d'action pour mettre à jour les connaissances professionnelles, économique et de la culture organisationnelle

6. Objectifs de l'unité de cours / module

Objectif général	**Ce cours apporte les connaissances fondamentales pour analyser les risques qui pèsent sur réseaux et les systèmes informatiques, pour choisir et déployer les contre-mesures appropriées pour réduire les faiblesses face aux menaces et les failles de sécurité.**
Objectifs spécifiques	✓ Analyser les menaces pour protéger les systèmes/données de votre entreprise ✓ Réduire le risque devant les agressions en utilisant les firewalls, le chiffrement et le décryptage de données, etc. ✓ Gérer les risques internes ou connus de l'utilisation d'Internet dans les entreprises et les compagnies ✓ Protéger les utilisateurs de réseaux contre les virus et les applications malveillantes. ✓ Identifier les risques de sécurité menaçant les réseaux et les systèmes informatiques

7. Contenu de l'unité de cours / module

Thématique des activités didactiques	Nombre d'heures	
	enseignement à temps plein	enseignement à temps partiel
Thème des cours		
T1. Les vulnérabilités, les menaces, les risques, les contre-mesures. Les vraies menaces à la sécurité : Intrus internes et externes ; Observation illicite du trafic sur le réseau ; Cheval de Troie ; Virus ; Mise sur écoute	2	
T2. Une politique de sécurité : les bases de la protection • Définition de vos objectifs de sécurité • Réduire au maximum les menaces • Évaluation des risques Développement d'un plan de sécurité • Nécessité d'un plan viable • Caractéristiques d'un bon plan • Réponse aux incidents	2	
T3. Chiffrement élémentaire. Le code de Cesar, le chiffrement affine, le chiffre de Vigenère	2	
T4. Chiffrement symétrique. Algorithmes : DES, AES, RC4 et autres. Évaluation de la longueur et de la distribution des clés	2	
T5. Chiffrement asymétrique • Génération de clés • Chiffrement avec RSA • Utilisation de PGP et GnuPG • Évaluation du Web of Trust et de PKI	2	
T6. Assurer l'intégrité des données avec le hâchage	2	

• Hâchage avec MD5 et SHA • Protection des données en transit • Création de signatures numériques		
T7. Vérification de l'identité des utilisateurs Évaluation des plans de mots de passe statiques traditionnels • Stratégie pour éviter le vol de mots de passe • Protection contre les attaques d'ingénierie sociale • Chiffrement des mots de passe vs. rejouer les attaques	2	
T8. Authentification des hôtes • Défauts des adresses IP • Problèmes des imitations d'adresses et déploiement de contre-mesures • Solutions pour les réseaux sans fil	2	
T9. Prévention des intrusions système. Découverte des vulnérabilités du système • Failles du système d'exploitation • Problèmes des permissions de fichiers • Limite de l'accès via la sécurité physique	2	
T10. Chiffrement des fichiers pour la confidentialité • Chiffrement avec les outils spécifiques aux applications • Récupération des données chiffrées	2	
T11. Défense contre les intrusions réseau Scan des vulnérabilités • Restriction des accès aux services critiques • Éviter les attaques de type "buffer overflow" Réduction des attaques de type "Deni de Services" • Sécurisation du DNS • Limite de l'impact des attaques communes	2	
T12. Déploiement de firewalls pour contrôler le trafic réseau • Analyse des défauts des filtres de paquets sans états • Analyse comparative entre les filtres de paquets avec état et les proxies applicatifs • Éviter les intrusions grâce aux filtres Création de firewalls réseau • Évaluation des caractéristiques des firewalls • Choix d'une architecture et d'un type personnel de firewall	2	
T13. Assurer la confidentialité du réseau Menaces provenant du réseau local • Observation illicite du réseau • Atténuation des menaces provenant d'hôtes • Partitionnement pour éviter les pertes de données • Identification des faiblesses des LAN sans fil	2	
T14. Confidentialité des connexions externes • Confidentialité grâce au chiffrement • Sécurisation de la couche liaison avec PPTP et L2TP • Assurance de l'information middleware avec SSL et TLS • Déploiement de SSH	2	
T15. Protection des données avec IPsec • Authentification des sites distants • Tunneling entre sites • Échange des clés	2	

Total des cours:	30	

Thématique des activités didactiques	Nombre d'heures	
	enseignement à temps plein	enseignement à temps partiel
Thèmes des travaux pratiques		
TP1 Découverte et vol de mots de passe	4/4	
TP2 La mise en place d'une PKI. Les certificats.	4/4	
TP3 La signature électronique. Utilisation de PGP et GnuPG	4/4	
TP4 Le protocole SSH	4/4	
TP5 Sécurisation du réseau avec IPSEC	4/4	-
TP6 Les réseaux privés virtuels	4/4	
TP7 La configuration d'un firewall sous Linux	6/6	
Total des travaux pratiques:	30/30	

8. Références bibliographiques

Principales	1. Natkin S. , Les protocoles de sécurité, Paris, éditions Dunod, 2001 2. Schneier B., Cryptographie appliquée, algorithmes, protocoles et codes source en C, 2ème édition, Vuibert, France 1996, 3. Berloquin P. Codes : la grande aventure, Michel Lafon, 2010,
Supplémentaires	http://openclassrooms.com/courses/les-premiers-algorithmes-de-chiffrement http://openclassrooms.com/courses/la-cryptographie-asymetrique-rsa

Évaluation

Actuelle		Projet d'année	Examen final
Attestation 1	Attestation 2		
30%	30%		40%
Normes de rendement minimum			
Présence et activité aux cours et travaux pratiques; Obtenez le score minimal de "5" pour chacune des attestations et des travaux pratiques; Démonstration de l'assimilation des informations fournies pendant le cours et des compétences pour dessiner les diagrammes nécessaires à la conception d'un produit de programme à l'examen final.			