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

D.O.008 TECHNOLOGIES DE SÉCURITÉ DE L'INFORMATION

1. Données disciplinaires

Faculté	Ordinateurs, Informatique et Microélectronique				
Département	Informatique et Ingénierie des Systèmes				
Cycle d'étude	Licence, premier cycle				
Programme d'études	**0612.3 Science des données**				
Année d'études	**Semestre**	**Type d'évaluation**	**Catégorie formative**	**Catégorie d'optionnalité**	**Crédits ECTS**
I (éducation à temps plein);	4	E	S – Unité de cours spécialisée	A - Unité de cours obligatoire	4

2. Durée totale estimée

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

3. Les conditions d'accès à la discipline

Selon le programme d'études	Analyse mathématique, Mathématiques discrètes, Programmation informatique, Structures de données et algorithmes, Programmation procédurale, Programmation interactive
Selon les compétences	Informer les étudiants des dernières questions relatives à la sécurité et à la protection de l'information et de l'utilisation des dernières méthodes de protection.

4. Les conditions du processus éducatif pour les

Cours	Un projecteur et un ordinateur sont nécessaires pour la présentation du matériel théorique dans la salle de conférence. Les arrivées tardives et les appels téléphoniques ne seront pas tolérés pendant le cours.
Travaux pratiques / diriges	Les étudiants rédigeront des rapports conformément aux conditions imposées par les lignes directrices méthodologiques. La date limite de remise des travaux de laboratoire est fixée à une semaine après leur achèvement. En cas de remise tardive du travail de laboratoire, le retard sera facturé à raison de 1 % par semaine de retard..

5. Compétences spécifiques accumulées

Les compétences suivantes seront acquises conformément à la grille et à la matrice de corrélation du programme d'études :

CP1. Gestion des niveaux de service

K1 Documentation SLA (Service Level agreement).
K2 Comment comparer et interpréter les données de gestion.
K3 Éléments formant la matrice des accords de niveau de service.
K4 Fonctionnement des infrastructures de prestation de services.
K5 L'impact du non-respect des niveaux de service sur la performance de l'entreprise.
K6 Normes de sécurité en TIC.
K7 Normes de qualité

CP2. Conception et développement

d'applications

K1 Programme/module logiciel adecvate.
K2 Composants matériels, outils et architectures matérielles.
K3 Conception fonctionnelle et technique.
K4 Technologies de pointe.
K5 Langages de programmation.
K6 Bases de données (DBMS).
K7 Systèmes d'exploitation et plates-formes logicielles.
K8 Environnement de développement intégré (IDE - integrated development environment).
K9 Développement rapide d'applications.
K10 Questions relatives aux droits de propriété intellectuelle (IPR).
K11 Technologies et langages de modélisation technique.
K12 Langages de définition d'interface (IDL).
K13 Questions de sécurité

CP3. Intégration des composants

K1 Composants matériels/logiciels/modules, qu'ils soient anciens, existants ou nouveaux.
K2 Impact de l'intégration du système sur l'organisation ou le système existant
K3 Techniques d'interfaçage entre modules, systèmes et composants
K4 Techniques de test d'intégration
K5 Outils de développement (par exemple, environnement de développement, gestion, contrôle des changements et accès au code source)
K6 Bonnes pratiques de conception

CP5. Prestation de services

K1 Comment interpréter les exigences en matière de fourniture de services informatiques.
K2 Meilleures pratiques et normes en matière de fourniture de services informatiques.
K3 Méthodes et modalités de contrôle de la fourniture des services.
K4 Méthodes d'enregistrement de la fourniture des services et de détection des

erreurs.

K5 Meilleures pratiques, normes et standards en matière de gestion de la sécurité de l'information.

K6 Spécificités des technologies des outils web, cloud et mobiles.

.

CP6. Gestion de l'information et de la connaissance

K1 Méthodes d'analyse de l'information et des processus d'entreprise.

K2 Dispositifs et outils informatiques applicables pour le stockage et l'extraction des données.

K3 Défis liés à la taille des données massives (Big Data).

K4 Les défis des données non structurées (par exemple, Data Analytics)

6. Objectifs de la discipline

Objectif général	Étudier les questions de sécurité et de protection de l'information et acquérir les compétences nécessaires pour utiliser les méthodes de protection les plus récentes..
Objectifs spécifiques	Comprendre et décrire les méthodes et techniques de sécurité. Connaître les systèmes et algorithmes de cryptage/décryptage Choisir les procédures appropriées pour développer et analyser le modèle de sécurité.

7. Le contenu de la discipline

Thèmes des activités d'enseignement	**Nombre d'heures**	
	l'enseignement à temps plein	**l'enseignement à temps partiel**
Thème des cours théoriques		
T1. Sécurité de l'information. Concepts et définitions de base. Menaces et attaques. Risque de sécurité. Guildes de sécurité. Méthodes pour assurer l'intégrité de l'information.	6	
T2. Données personnelles. Données institutionnelles. Types d'attaquants. La cyberguerre.	2	
T3. Protéger les données et la vie privée en ligne. Protéger les institutions.	4	
T4. Cube de la cybersécurité. Triade de la CIA. Les états des données et leur signification, La stéganographie en tant que méthode de dissimulation d'informations	4	
T5. Classes et types d'attaques . Contrôle d'accès dans les systèmes d'information - Modèles de sécurité.	2	
T6. Sécurité de l'information et cryptographie. Systèmes de cryptage. Principe de Kerckhoff. Classification des algorithmes de chiffrement. Chiffres de substitution et chiffres de permutation/transposition. Chiffres classiques. Attaques cryptographiques	4	
T7. Cryptographie moderne. Chiffres symétriques et asymétriques. Échange de clés Diifie-Helman. Chiffres symétriques DES et AES. Cryptographie asymétrique : le chiffrement RSA	6	
T8. Signature électronique Infrastructure à clé publique PKI. Certificats numériques.	4	
Total des cours théoriques :	**30**	

Thèmes des activités d'enseignement	**Nombre d'heures**	
	l'enseignement à temps plein	**l'enseignement à temps partiel**

Thèmes des travaux pratiques		
LL1. Contrôler l'intégrité des données à l'aide de fonctions hash	2	
LL2. Failles de sécurité.	2	
LL3. Règles pour créer des mots de passe forts	2	
LL4. Création et gestion de copies de sauvegarde	2	
LL5. Garantir la sécurité des données stockées en ligne	2	
LL6. Détecter les comportements à risque en ligne	2	
LL7. Chiffres mono-alphabétiques	2	
LL8. Cryptanalyse des chiffres mono-alphabétiques	2	
LL9. Chiffres polyalphabétiques	4	
LL10. Chiffre RSA	4	
LL11. Signature numérique	6	
Total des travaux pratiques:	**30**	

8. Références bibliographiques

Principal	1. Gutmann, P., Cryptography and Data Security, http://www.cs.auckland.ac.nz/apgut001. 2. Bellovin, S.M., Security Problems in the TCP/IP Protocol Suite, AT&T Bell Lab. Murray Hill, New Jersey, 07974, 2002. 3. Fergusson, N., Schneier, B., A Cryptografic Evaluation of IP sec., http://www.counterpaine.com, 2000. 4. Gligorovski, D., Markovski, S., Kocarev, L., New Directions in Coding: From Statistical Physics to Quasigroup String Transformation, NOLTA 2004, Japan, Nov 29-Dec 3, 2004
Supplémentaire	1. Dimovski, A., Gligorovski, D., Attacks on the Polyalphabetic Substitution Cipher Using a Parallel Genetic Algorithm, Tech. Rep. SCOPES project, March 2003, Ohoid, Macedonia 2. Dimovski, A., Gligorovski, D., Attacks on the Transposition Cipher Using Optimization Heuristics, Proc. Of ICEST 2003, Oct 2003, Sofia, Bulgaria

9. Evaluation

Forme d'éducation	Périodique		Actuel	Travailler individuel lement	Examen final
	Attestation 1	Attestation 2			
Avec fréquence	15%	15%	15%	15%	40%
Norme de performance minimale					
Assiduité et participation aux cours et aux travaux de laboratoire Obtention d'une note minimale de "5" à chacune des évaluations et à chacun des travaux de laboratoire.					