Co-funded by the Erasmus+ Programme of the European Union

licence master professionnel en protection informatique

LMPI - N°573901-EPP-1-2016-1-IT-EPPKA2-CBHE-JP
"Licence, Master professionnels pour le développement, l'administration, la gestion, la protection des systèmes et réseaux informatiques dans les entreprises en Moldavie, au Kazakhstan, au Vietnam"

Dossier d'accréditation

Grade: Mention:	Expert en sécurité informatique Études de maîtrise	Domaine:	061 Technologies de l'information et de la communication

Université:	Université Technique de Moldova	Département:	Ingénierie de logiciels et Automatique
Date de conception:	25.02.2018		

Rédacteurs:	Besliu Victor	Moraru Victor	Bulai Rodica

Co-funded by the
Erasmus+ Programme
of the European Union

lmpi
licence master professionnel
en protection informatique

LMPI - Licence, Master professionnels pour le développement, l'administration, la gestion, la protection des systèmes et réseaux informatiques dans les entreprises en Moldavie, au Kazakhstan, au Vietnam

Project N° 573901-EPP-1-2016-1-IT-EPPKA2-CBHE-JP

PROTOCOL OF PROJECT DOCUMENT VALIDATION

PROCES VERBAL DE VALIDATION DE DOCUMENT DU PROJET

Work Package/lot	3
Activity/Activité	3.3
Name of the activity/ Nom de l'activité	Accreditation files Licence/ Master
Name of the document/ nom du document:	Accreditation files Licence Accreditation files Master
Partner(s) concerne/partenaire(s) concerné(s)	P09 Technical University of Moldova P10 Alecu Russo Balti State University P11 Moldova State University P12 Academy of Economic Studies of Moldova
Referent EU University/université UE réferente	P04 University of West Attica
Person validating the document/personne qui valide le document	
Name/nom	Panayotis Yannakopoulos
Function/fonction	Professor

Date: 21.06.2019

Signature:

I. Contexte

L'humanité connaît aujourd'hui l'une des transformations les plus profondes de toute son existence où l'information joue un rôle déterminant. Nous vivons dans un monde où des centaines de millions d'ordinateurs au service des utilisateurs ayant des exigences différentes, sont reliés entre eux dans une structure informatique mondiale appelée le cyberespace. Les experts cherchent et trouvent, avec une rapidité incroyable, des solutions techniques pour la communication et le renforcement des capacités pour améliorer la qualité des services d'information offerts.

Le développement de l'Internet pendant les dernières années a été fortement alimenté par la perspective de faire des affaires et de communiquer en ligne. Dans ce contexte, la sécurité des informations en général et de celles échangées sur Internet, est le plus grand défi qui se dresse dans le domaine. Pour la plupart des organisations, l'intérêt pour la sécurité de l'information est proportionnel à la façon dont les menaces et les vulnérabilités sont perçues.

La cybersécurité et la sécurité des informations est accentuée par des phénomènes caractéristiques de la société d'aujourd'hui, tels que la globalisation et l'établissement de la société de l'information, les faiblesses de l'économie virtuelle liées à la nature immatérielle des valeurs du cyberespace, l'anonymat et de la nature transfrontalière, l'évolution de la criminalité électronique et sa dynamique.

La criminalité cybernétique coûte les économies du monde entier approximativement 600 milliards de dollars par an, soit 0,8% du PIB mondial selon une étude récente publiée par la société McAfee, spécialisée dans la protection contre les attaques informatiques et par le centre de réflexion Center for Strategic and Internationales Studies (CSIS). Le domaine fait face à une pénurie croissante de professionnels qualifiés et de praticiens expérimentés dans la sécurité de l'information. Pour l'année 2022, près de 1,8 million de postes de sécurité informatique sont estimés mais ils ne devraient pas être couverts. La demande de main-d'œuvre est aiguë, immédiate et croissante. Dans ce contexte, la formation des spécialistes dans le domaine de la sécurité de l'information et des responsables de la sécurité des systèmes d'information est une priorité nationale, demandée à la fois par les médias gouvernementaux ainsi que par l'administration centrale ou locale mais aussi par le secteur privé - entreprises, banques, etc.

Le programme de master vise à atteindre les objectifs suivants :

- Acquérir des connaissances sur les menaces, les vulnérabilités et les risques de sécurité propres aux systèmes d'information ;
- Vous familiarisez avec les dernières technologies avancées utilisées pour assurer la sécurité de l'information ;
- Apprendre des normes et des standards nationaux et internationaux dans le domaine de la sécurité de l'information ;
- Comprendre les méthodologies et les schémas d'audit, de certification et d'accréditation de la sécurité des produits et des systèmes d'information ;
- Identifier et résoudre les problèmes liés à l'acquisition, à la mise en œuvre et a l'exploitation de solutions de sécurité de l'information ;
- Développer des connaissances et des compétences en matière de gestion de la sécurité de l'information, des ressources techniques et humaines nécessaires à l'assurance d'informations ;
- Acquérir la capacité de diriger des groupes de travail ou des équipes de spécialistes en sécurité de l'information ;

- Développer des compétences pour la conception des études et des rapports techniques.

La maîtrise en Sécurité de l'Information est basée sur l'expérience d'enseignement et de la recherche dans le domaine de la sécurité de l'information des enseignants de l'Université Technique de Moldavie. Des professeurs associés des autres universités ou professionnels avec une vaste expérience pratique, qui mènent leurs activités dans des structures commerciales et gouvernementales de sécurité nationale ou dans des entreprises privées seront également invités aux conférences et aux démonstrations pratiques.

L'enquête du projet Erasmus+ "Licence, Masters professionnels pour le développement, l'administration, la gestion, la protection des systèmes et réseaux informatiques dans les entreprises en Moldavie, au Kazakhstan, au Vietnam" a identifié une grande pénurie de professionnels qualifiés dans la sécurité de l'information et une forte demande en spécialistes de haut niveau dans ce domaine, fait qui garantit l'insertion professionnelle des diplômés.

Le master en sécurité de l'information s'adresse aux diplômés universitaires qui souhaitent améliorer la technologie, la réglementation et la gestion de la sécurité des informations. L'admission aura lieu conformément à la réglementation en vigueur, un concours annuel sera annoncé pour le recrutement de 25-50 étudiants, à ce qui concerne l'enseignement à distance, il n'y aura aucune restriction sur le nombre de places disponibles ou d'âge des candidats.

II. Descriptif général du curriculum

• II.1. Description des acquis de formation :

La sécurité de l'information est une spécialité qui implique des technologies, des personnes, des informations et des processus dans le but de permettre des opérations sécurisées dans un contexte incertain en analysant, testant, créant et en exploitant des systèmes d'information sécurisés. C'est une spécialité interdisciplinaire qui comprend des questions liées à la technologie, au droit, à la politique, aux facteurs humains, à l'éthique et à la gestion des risques.

Les acquis de formation	Descriptif
Les savoirs disciplinaires	Connaissance de l'entreprise, ses services/produits, sa structure, son organisation, son environnement juridique. Vision globale et complète des systèmes d'information e l'entreprise, des organisations similaires. Connaissance technique approfondie des concepts et techniques d'architecture des systèmes et réseaux, procédures d'exploitation et des standards d'échange des données employées, procédures de Sécurité informatique, systèmes d'exploitation et langages de programmation associés, bases de données.
Les compétences spécifiques	Les fondements scientifiques et techniques de la sécurité informatique. Les aspects organisationnels et informationnels de la SI. Les mesures de sécurité et de contrôle. Les méthodes et technologies pour développer des solutions de

	sécurité. L'architecture de sécurité et l'infrastructure Savoir-faire pratique et expérience rédactionnelle : actualités/brèves, articles de fond, dossiers. Maîtrise expérimentée «terrain» de l'outil informatique : architecture des systèmes et réseaux, procédures d'exploitation et des standards d'échange des données employées, procédures de sécurité informatique, systèmes d'exploitation (Solaris, Linux) et des langages de programmation associés. Maîtriser les outils bureautiques : traitement de texte, tableur, outil de présentation. Utilisation de logiciels spécifiques : outils de chiffrement de disques durs ou de serveurs, Pare feu (Firewalls), outils d'identification.
Les compétences transversales	"Leadership" et esprit d'entreprise. Adaptabilité et flexibilité. Analyse et synthèse. Communication orale et écrite. Conviction et Influence. Créativité, sens de l'innovation. Gestion de projet. Gestion de la performance. Orientation client. Rigueur et organisation. Sens relationnel. Travail et animation d'équipe.

II.2. La décomposition du curricula en semestres

Premier semestre

#	Titre du cours /module	Type du cours	Nr. de crédits	Forme de vérification	Nr. d'heures		
					Cours	Lab/Sem	Total
UE 1	Gestion de la sécurité de l'information	Obligatoire	5	E	20	20	40
UE 2	Audit de la sécurité de l'information	Obligatoire	5	E	20	20	40
UE 3	Techniques et méthodes de cryptologie	Obligatoire	5	E	20	20	40
UE 4	Intelligence artificielle	Obligatoire	5	E	20	20	40
UE 5	Gestion de projet	Obligatoire	5	E	20	20	40
UE 6	Tests de pénétration et systèmes d'exploitation	Obligatoire	5	Projet	20	20	40

Deuxième semestre

#	Titre du cours/module	Type du cours	Nr. de crédits	Forme de vérification	Nr. d'heures		
					Cours	Lab/Sem	Total
UE7	La sécurité des transactions électroniques	Obligatoire	5	E	20	20	40
UE8	Architectures cloud	Obligatoire	5	E	20	20	40
UE9	Méthodologie de la recherche scientifique	Obligatoire	5	E	20	20	40
UE10	Sécurité de l'information d'entreprise	Obligatoire	5	Projet		75	75
UE11	Sécurité avancée des réseaux	Obligatoire	5	E	20	20	40

UE12	Application distribuées avancées/ Analyse de logiciels malveillants et enquêtes digitales/ Data Mining	Au choix	5	E	20	20	40

Troisième semestre

#	Titre du cours/module	Type du cours	Nr. de crédits	Forme de vérification	Nr. d'heures		
					Cours	Lab/Sem	Total
1.	Stage de fin d'études, conception du mémoire	Obligatoire	28	E			840
2.	Soutenance de la thèse de master		2	E			60

II.3. Tableau de mise en corrélation entre compétences et unités d'enseignement :

UE 1 : Gestion de la sécurité de l'information (40 heures) (5 ECTS)

- Le cadre de gestion de la sécurité de l'information. Notions de base. Normes internationales sur la gestion de la sécurité de l'information : famille de normes ISO 27000, NIST, PCI DSS.
- Le système de gestion de la sécurité de l'information (ISMS). Composants et mécanismes d'un SGSI. Étapes du processus de mise en œuvre du SGSI selon ISO 27001.
- Analyse et évaluation des risques de sécurité. Concepts généraux sur la gestion des risques liés à la sécurité de l'information. Inventaire des actifs. Menaces et vulnérabilités
- Méthodologies et outils pour l'analyse des risques informationnels.
- Le cadre juridique actuel. Gestion de la sécurité de l'information au niveau de l'État: principes généraux.
- Politiques, modèles et programmes de sécurité.

UE 2 : Audit de la sécurité de l'information (40 heures) (5 ECTS)

- Définition, but, destination, types et emplacement de l'audit;
- Cadre normatif international de référence. Norme internationale d'audit ISO 27001. COBIT. ITIL. ISACA.
- Législation d'audit de la République de Moldova. Règlements internes et instructions.
- Méthodes et outils pour un audit de sécurité de l'information.
- Procédures d'audit de sécurité pour équipements, données, applications informatiques, réseaux/communications internes, sécurité web et attaques Internet externes.
- Audit/évaluation du respect des exigences de la législation nationale sur la sécurité des données personnelles.
- Analyse de l'organisation, gestion de la sécurité de l'information et facteur humain.
- Audit de sécurité des systèmes d'exploitation des entreprises et des systèmes de gestion de bases de données
- Audit de l'infrastructure technique et technologique des systèmes d'information de l'entreprise et des informations confidentielles informatiques.
- Analyse des rapports d'analyse et des suggestions pour capitaliser les résultats

- Évaluation des contrôles de sécurité pour le système de gestion de la sécurité de l'information.
- Structure du rapport d'audit. Élaboration du rapport d'audit et propositions pour la capitalisation des résultats enregistrés. Révision de l'audit du système de sécurité
- Techniques d'audit assistées par ordinateur.
- Exigences du vérificateur professionnel. Code de déontologie de l'auditeur.
- Futur et perspectives de l'audit de la sécurité de l'information

UE 3 : Techniques et méthodes de cryptologie (40 heures) (5 ECTS)

- Techniques et méthodes de conception d'algorithmes et de protocoles cryptographiques.
- Méthodes pour évaluer/casser les codes cryptographiques
- La cryptanalyse des algorithmes asymétriques
- La cryptanalyse d'algorithmes symétriques
- Techniques cryptographiques modernes

UE 4 : Intelligence artificielle (40 heures) (5 ECTS)

- Intelligence artificielle (IA). Avantages et limites de l'IA. Systèmes experts.
- La structure générale d'un SE. Systèmes multi-experts. Résolution de problèmes généraux.
- Méthodes de résolution de problèmes. Raisonnement. Types de raisonnement. Le raisonnement déductif.
- Méthodes heuristiques Réseaux sémantiques Représentation des connaissances à travers des réseaux sémantiques
- Réseaux neuronaux. Réseaux de neurones artificiels.
- Algorithme d'apprentissage Réseaux à couche unique. Sources et règles Techniques de résolution de conflits.
- Typologie des moteurs d'inférence. Conception SE. Le cycle de vie d'une SE. Modélisation conceptuelle Collecte de connaissances
- Générateur EXSYS. Schéma fonctionnel du générateur EXSYS.

UE 5 : Gestion de projet (40 heures) (5 ECTS)

- Notions générales concernant la conception d'un projet.
- Exigences générales et spécifiques. La mise en œuvre du projet.
- Notions spécifiques à la planification d'applications informatiques allant à partir des besoins jusqu'à la maintenance et au support technique.
- Initiation aux techniques de gestion de projet : gestion de la qualité et des risques, communication et gestion des ressources humaines, gestion de coûts.
- Conception d'un plan de projet cohérent. Éléments de gestion des objectifs.
- Éléments de gestion des ressources (financiers, humains).
- Éléments de gestion de la qualité et des risques. Des outils informatiques spécifiques à la gestion de projet. Des outils informatiques pour surveiller la mise en œuvre d'un projet.
- Outils informatiques pour la gestion des ressources. Outils informatiques pour rapporter les résultats.

UE 6 : Tests de pénétration et systèmes d'exploitation (40 heures) (5 ECTS)

- Audit de sécurité et tests de pénétration.
- Phases des tests de pénétration.

- Distributions Linux sécurisées.
- Vulnérabilités et exploits. Les traces. L'écoute.
- Casser le mot de passe par force brute, attaques par dictionnaire.
- Scanneurs réseau, détection des ports ouverts (Nmap). Scaneurs de Vulnerabilité (Nessus). Sniffeurs (Tcpdump). Outils de détection de capture (ifconfig, ifstatus, promiscdetect). Metasploit. Attaques par cross-scripting et attaques par injection SQL.
- Détection des attaques DoS. Détection de backdoors (Netstat, lsof).
- Piratage mobile. IDS, Firewalls & Honeypots.

UE 7 : La sécurité des transactions électroniques

- Le commerce électronique, les modèles de commerce électronique.
- Application de commerce électronique.
- Classification de systèmes de commerce électronique
- Les systèmes de payement par Internet
- La protection de la messagerie électronique. GPG pour crypter et signer les messages.
- Type et sources de menaces dans le commerce électronique.
- La protection de canaux de communication

UE 8 : Architectures cloud (40 heures) (5 ECTS)

- Architectures cloud. Infrastructure comme service (IaaS)
- Virtualisation de ressources (serveurs, stockage, réseau)
- Études de cas (Amazon, Eucalyptus, etc.)
- Plateforme comme service (PaaS), études de cas (Azure, Google App Engine)
- Logiciel comme service (SaaS). Études de cas
- Déployer des clouds. Couds privés. Sécurité de clouds

UE 9 : Méthodologie de la recherche scientifique (40 heures) (5 ECTS)

- Types de recherche scientifique
- Conditions à remplir par la recherche scientifique. Méthodologie de la recherche.
- Critères dans le choix du domaine et du thème. Sources et façons de choisir le sujet de recherche. Pourquoi la recherche bibliographique est-elle nécessaire ?
- Formulation du problème de recherche. Les hypothèses.
- Collecte de données : méthodes.
- Traitement de données : méthodes statistiques, analyse qualitative.
- Analyse et interprétation des résultats.
- Mémoire de maîtrise: format et contenu.
- Actes normatifs et documents qui déterminent le développement de la recherche scientifique en République de Moldova.

UE 10 : Sécurité de l'information d'entreprise (40 heures) (5 ECTS)

- L'entreprise moderne. Cadre juridique de l'environnement d'information microéconomique
- Menaces du système d'information d'entreprise
- Principes et méthodes d'évaluation des risques liés aux ressources d'information d'entreprise
- Conception de stratégies de sécurité d'entreprise

- Gestion et administration de données personnelles dans le système d'information d'entreprise
- Méthodes de protection du système d'information d'entreprise
- Conception et mise en œuvre de systèmes de sécurité de l'information d'entreprise
- Gestion du système de sécurité de l'information d'entreprise et particularités de l'audit
- Gestion de crise (attaque malveillante) dans la sécurité de l'information d'entreprise
- Meilleures pratiques en matière de sécurité des informations d'entreprise

UE 11 : Sécurité avancée des réseaux (40 heures) (5 ECTS)

- Sécurité des réseaux informatiques : problèmes spécifiques, menaces et vulnérabilités, attaques, solutions et stratégies de sécurité, politiques de sécurité;
- Sécurité périmétrique du réseau. Conception des réseaux sécurisés. Firewalls: principes, fonctionnalités, stratégies, types, configuration.
- Méthodes cryptographiques pour la protection de l'information dans les réseaux informatiques. Éléments de cryptographie: cryptographie symétrique et asymétrique. Algorithmes de chiffrement RSA, DES, IDEA, RC4, AES.
- Confidentialité des sessions de communication, concept de clé de session et protocole Diffie-Hellman.
- Protocoles de contrôle de l'intégrité des données: cryptographie à clé publique, signature numérique.
- Méthodes d'authentification, Authentification unique (SSO), protocoles RADIUS, TACACS, KERBEROS et LDAP.
- Infrastructure à clé publique (PKI): services, acteurs, opérations. Certificats X.509;
- Système de cryptage Pretty Good Privacy (PGP). Norme OpenPGP et son implémentation logicielle GNU Privacy Guard (GPG).
- Sécurité de la couche réseau, protocole IPSec: principes, services, modes de fonctionnement, authentification, format d'en-tête;
- Sécurisation de la couche de transport, protocoles SSL et TLS / SSL. Sécurité Web avec le protocole HTTPS. Protocole SSH;
- Réseaux privés virtuels (VPN): architectures et technologies. IPSec, PPTP, tunnels TLS / SSL.

UE 12/1 : Application distribuées avancées (40 heures) (5 ECTS)

- Conception et utilisation de structures de calcul haute performance parallèles et distribuées. Architectures de cluster et de grille.
- Architectures informatiques distribuées.
- Conception des grappes Beowulf.
- Clusters à haute disponibilité
- Réseaux P2P. Algorithmes d'équilibrage de charge. Architectures de cache distribuées.
- Systèmes de fichiers virtuels.
- Détection et prévention des intrusions
- Bases de données distribuées non SQL

UE 12/2 : Analyse de logiciels malveillants et enquêtes digitales (40 heures) (5 ECTS)

- Utilisez des outils de surveillance du réseau et du système pour examiner la manière dont les programmes malveillants interagissent avec le système de fichiers, le registre, le réseau et d'autres processus dans un environnement Windows.

- Découvrez et analysez les scripts JavaScript malveillants et d'autres composants des pages Web souvent utilisés par les kits d'exploitation pour les attaques au volant
- Contrôlez les aspects pertinents du comportement des programmes malveillants grâce à l'interception du trafic réseau et au code de correction pour effectuer une analyse efficace des programmes malveillants
- Utilisez un désassembler et un débogueur pour examiner le fonctionnement interne des exécutables Windows malveillants
- Contournement et variété d'emballeurs et autres mécanismes défensifs conçus par des auteurs de logiciels malveillants pour détourner, confondre et ralentir l'analyste
- Reconnaître et comprendre les modèles communs au niveau de l'assemblage dans les codes malveillants, tels que l'injection de code L, l'accrochage aux API et les mesures anti-analyse
- Évaluer la menace associée aux documents malveillants tels que les fichiers PDF et Microsoft Office
- Dériver des Indicateurs de Compromission (IDC) des exécutables malveillants pour renforcer la réponse aux incidents et les efforts de renseignement sur les menaces.

UE 12/3 : Data Mining (40 heures) (5 ECTS)

- Introduction à l'exploration de données.
- Data mining et KDD (Knowledge Discovery dans les bases de données). Types de données explorés. Fonctions d'exploration de données.
- Entrepôts de données et technologies OLAP. Architecture de l'entrepôt de données. Mise en place d'entrepôts de données.
- Description des concepts - caractérisation et comparaison. Pré-traitement, nettoyage, réduction des données
- Discrétisation et génération de hiérarchies de concepts. Découvrir les règles d'association (analyse d'association). Algorithmes pour l'extraction de règles d'association booléennes unidimensionnelles à partir de bases de données de transaction - A priori, FP-Growth.
- Algorithmes pour extraire des règles d'association multi-niveaux, multidimensionnelles et contraintes. ODM et analyse des associations dans les OMD.
- Classification et prédiction. Clustering (analyse de cluster) .Extraction de données standard et logicielle - ODM, Microsoft OLE DB.
- Applications et tendances dans l'exploration de données.
- Data mining, sécurité et confidentialité.

Le tableau de mise en corrélation entre compétences et unités d'enseignement est présenté ci-dessous :

	C1	C2	C3	C4	C5
UE1		**x**	**x**		**x**
UE2		**x**	**x**		**x**
UE3		**x**	**x**		
UE4	**x**		**x**	**x**	**x**
UE5				**X**	**x**
UE6	**x**	**x**	**x**	**x**	**x**

UE7	**x**			**x**	
UE8	**x**		**x**	**x**	
UE9	**x**	**x**	**x**	**x**	**x**
UE10	**x**	**x**	**x**		
UE11	**x**		**x**		**x**
UE12/1			**x**	**x**	**x**
UE12/2			**x**	**x**	**x**
UE12/3			**x**	**x**	**x**

II.4. Le projet tutoré

Le projet tutoré s'inscrit pleinement dans la professionnalisation des étudiants. Il permet aux étudiants de s'engager sur un temps long dans un travail collaboratif (de groupe) qui œuvre à la réalisation d'un projet en réponse à une étude de cas proposée par l'encadrant universitaire et par le tuteur entreprise.

Le projet tuteuré comporte trois dimensions complémentaires :

- il implique en effet la conception, la mise en œuvre et l'évaluation d'un projet qui repose sur un problématique validée en formation ;
- il se traduit par la rédaction d'un rapport satisfaisant à l'ensemble des exigences universitaires ;
- il donne lieu enfin à une soutenance comportant un exposé suivi d'un entretien avec le jury.

Plus précisément, il s'agira à travers ce dispositif pédagogique de permettre aux étudiants :

- d'approfondir leur champ de connaissances des secteurs et contextes de la communication publique;
- d'apprendre à gérer un projet de communication de manière autonome dans le cadre de travail en équipe ,
- de gérer le travail de groupe et le calendrier des activités ;
- de développer des capacités d'analyse, d'enquête et de recommandations ;

Le projet tuteuré permet aux étudiants de :

- mettre en pratique les savoirs acquis au cours de la formation,
- travailler au sein d'une équipe sous contrainte de temps et de moyens,
- démontrer leurs capacités d'initiative, d'autonomie et de responsabilité,
- répondre à une demande réelle en analysant une situation et en proposant une solution adaptée.

Ses principales tâches des encadrants (tuteurs universitaire et entreprise) sont :

- valider dès le début la proposition de projet du groupe d'étudiants, notamment sa faisabilité ;
- orienter les étudiants vers des ressources ;
- donner des conseils en terme d'organisation ;
- valider la répartition des tâches au sein du groupe et la planification ;

- évaluer les rapports intermédiaires et les rendus finaux.

Le but principal du projet tutoré est : à partir d'une problématique clairement identifiée (une étude de cas), l'étudiant doit concevoir une réponse cohérente basée sur les connaissances acquises pendant les cours théoriques.

Les étudiants sont évalués sur leur capacité à proposer une solution crédible, réaliste, adaptée. Pour ce faire, il mobilise l'ensemble des connaissances théoriques acquises durant la formation. Ils réalisent l'ensemble des opérations liées à la conception et à la mise en œuvre de leur projet : identification, analyse, recherche des solutions possibles, choix d'une solution, critères et conditions de mise en œuvre, mise en œuvre, mesure d'efficacité, actions correctrices…

Les résultats du projet tutoré sont présentés sous forme d'un rapport écrit qui sera soutenu devant un jury composé de deux enseignants de l'équipe pédagogique et éventuellement du tuteur en entreprise. La soutenance comprend successivement un exposé de l'étudiant suivi d'un entretien avec le jury, elle a pour objectif d'approfondir, compléter, enrichir le rapport.

L'étudiant est donc invité à construire un exposé, appuyé par un diaporama de présentation, qui ne soit pas une répétition du rapport, ni sur le fond, ni sur la forme. Il s'exprime pendant environ dix minutes. A la suite de sa présentation, une dizaine de minutes est consacrée à des questions-réponses avec le jury. Celles-ci peuvent porter sur l'exposé, le rapport, et plus largement sur les acquis de l'étudiant au terme de l'année.

L'entreprise fournit une appréciation qui se traduit par un bonus sur la note globale.

La délibération se fait hors de la présence de l'étudiant. En vue de permettre une harmonisation éventuelle des jurys, les notes ne lui sont pas communiquées à l'issue de la soutenance.

Le projet tutoré se déroule pendant le deuxième semestre d'études et il vaut 5 ECTS.

II.5. Le stage en entreprise

Les stages de fin d'études visent l'approfondissement des connaissances théoriques, l'acquisition des compétences pratiques de travail dans les organisations d´état, publiques ou privées. L'organisation des stages est réalisée en conformité avec les documents normatifs de l'UTM.

Le stage en entreprise est prévu pendant le troisième semestre et vaut 28 ECTS est sa durée est de 15 semaines. Une convention-type entre UTM est l'organisme d'accueil doit être signée avant le début du stage.

Les types d'entreprises d'accueil : institution bancaires et financières, entreprises de production, compagnie du domaine TIC, etc., l'emploi a occuper : expert en sécurité de systèmes d'information et des réseaux

Les modalités de suivi des stages en entreprise : le professeur référent du stage visite régulièrement le stagiaire et l'aide de mettre en place le travail proposé par le tuteur, le

tuteur en entreprise propose les sujets et le cahier de charges pour le stage, surveille quotidiennement le travail du stagiaire, l'aide de surmonter les difficultés rencontrées, veille au respect des règlements en cours, etc.

A la fin du stage l'étudiant présente ses résultats sous forme d'un mémoire du stage in y incluant les résultats les plus pertinents ainsi que l'avis de son tuteur de stage.

Le nombre d'ECTS prévus pour le stage est en adéquation avec le contenu des autres enseignements, les compétences professionnelles visées et l'investissement en temps de travail nécessité par le stage. Une modulation des ECTS peut être opérée, selon sa nature (observation, application, responsabilité...), sa durée et sa période dans l'année.
Une préparation à l'insertion professionnelle et à la recherche de stage est proposée dans les cursus.

Le jury de stage est constitué de deux membres au minimum dont au moins un enseignant de la formation. La participation d'un représentant de l'organisme d'accueil est vivement recommandée.

La note de stage comporte plusieurs évaluations : l'évaluation du rapport écrit et de la soutenance orale, l'évaluation par l'organisme d'accueil des compétences professionnelles et du comportement de l'étudiant. Une pondération peut être prévue entre ces différentes évaluations. Les différents aspects de ces évaluations figurent sur la convention de stage.

L'évaluation des stages réalisés dans le cadre de masters relève de dispositions spécifiques qui doivent être précisées aux étudiants en début d'année universitaire.

II.6. Le stage à l'international

Le stage de fin d'études peut être organisé sous forme d'une mobilité à l'étranger sous financement dans le cadre des projets scientifiques en cours dont UTM fait part (Erasmus +, Horizon 2020 , AUF, etc.) ou par l'obtention des bourses et des grants proposés par des organismes internationaux (tel que AUF, ambassades, etc.). Dans ce but UTM a signé plus de 150 accords de coopération bilatérale avec des universités, des centres scientifiques et des entreprises des pays membres de l'Union européenne (Belgique, République tchèque, Allemagne, Grèce, France, Italie, Grande-Bretagne, Pologne, Portugal, Roumanie, Espagne, Suède, Hongrie), Canada, Biélorussie, Fédération de Russie, Turquie, Ukraine. UTM est membre d'organisations académiques internationales comme l'Agence Universitaire de la Francophonie (1996), le Réseau des universités de la mer Noire (1997), le Réseau international pour l'éducation en matière de sécurité nucléaire, etc.

Le contenu de ce stage, sa durée, le nombre d'ECTS attribués et les modalités de son évaluation sont similaires au stage en entreprise.

II.7. Les mobilités vers les entreprises étrangères (le cas échéant)

Des mobilités vers des entreprises étrangères ne sont pas directement prévues dans le cadre de ce master, mais il est tout à fait possible de les organiser sous réserve d'un financement par un organisme externe, par un projet ou par l'entreprise elle-même.

III Modalités de contrôle des connaissances

Le master est constitué de 90 ECTS. La formation dispensée comprend des enseignements théoriques, méthodologiques et appliqués et un stage, ainsi qu'une initiation à la recherche.

Les études de master sont structurées en semestres et en unités d'enseignement (UE) capitalisables

Dans chaque UE, les aptitudes et l'acquisition des connaissances sont appréciées par un contrôle continu et par un examen terminal. La forme du contrôle (épreuve écrite, orale, pratique, soutenance, etc.) est décidée par l'équipe pédagogique en fonction des spécificités de l'UE.

La prise en compte de l'assiduité aux TD/TP dans l'évaluation de l'UE est laissée à l'appréciation des membres de l'équipe pédagogique ou précisée dans les modalités de contrôle des connaissances spécifiques de la formation.

Une UE est acquise si sa moyenne est supérieure ou égale à 5/10. L'acquisition de l'unité d'enseignement emporte l'acquisition des crédits européens (ECTS) correspondants. Une UE capitalisée ne peut pas être repassée ultérieurement.

Chaque semestre doit être validé par un jury. La validation d'un semestre permet l'acquisition de 30 ECTS. Le contrôle des connaissances des formations définit les modes de validation des semestres notamment les règles de compensation à l'intérieur du semestre et les règles de rattrapage.

L'année est validée lorsque chacun des deux semestres est validé. Il n'y a pas de compensation possible entre les semestres.

Le master est délivré aux étudiants ayant validé toutes les UE constitutives d'un parcours type tel que défini par la maquette.

L'évaluation des mémoires est effectué par un jury de mémoire constitué d'au moins deux enseignants de la formation. L'évaluation du mémoire peut comporter plusieurs notes (mémoire, soutenance orale, etc.). Une pondération peut être prévue entre les différentes notes.

Les soutenances sont publiques sauf en cas de confidentialité.

IV Composition de l'équipe pédagogique

a) Le responsable pédagogique général du nouveau curriculum

Nom : **Bulai** Prénom : **Rodica** Fonction : **enseignant-chercheur** Université : **UTM**

b) Les responsables pédagogiques par unités d'enseignement

UE	Responsable d'UE	Université de rattachement
UE1	Maître de conf.,dr. Beslu Victor	UTM
UE2	Maître de conf.,dr. Beslu Victor	UTM
UE3	Prof.univ.,dr.Ferucio Laurențiu Țiplea	Université "Al.I.Cuza" de Iasi, Roumanie
UE4	Prof.univ., dr.Cotelea Vitalie	UTM

UE5	Maître de conf.,dr. Țurcan Iuliu	UTM
UE6	Maître de conf. Catanoi Maxim	Endava
UE7	Prof.univ.,dr. Bolun Ion	ASEM
UE8	Maître de conf.,dr. Pușcașu Veaceslav	Le Centre de Gouvernance Electronique
UE9	Maître de conf.,dr. Ababii Victor	UTM
UE10	Maître de conf.,dr. Cernei Valeriu	BSD Management
UE11	Maître de conf.,dr. Victor Moraru	UTM
UE12/1	Maître de conf.,dr. Ciorbă Dumitru	UTM
UE12/2	Enseignant-chercheur Bulai Rodica	UTM
UE12/3	Enseignant-chercheur Rusu Viorel	UTM

c) Professeurs intervenant dans le curriculum

Nom prénom	Université	Disciplines enseignées	Nombre d'heures d'intervention	UE concernées
Bulai Rodica	UTM		40	UE1, UE2

d) professionnels intervenant dans le curriculum

Nom prénom	Entreprise	Disciplines enseignées	Nombre d'heures d'intervention	UE concernées
Cernei Valeriu	BSD Management		40	UE10
Pușcașu Veaceslav	Le Centre de Gouvernance Electronique		40	UE8
Catanoi Maxim	Endava		40	UE6

NB : le nombre d'heures d'intervention de professionnels doit être de 30% des heures totales.

V Insertion professionnelle

La sécurité de l'information est le sujet très sollicité dans le contexte actuel où la cybercriminalité est devenue omniprésente dans tous les domaines. Pendant les cinq dernières années la demande de professionnels de la sécurité de l'information a augmenté de 3,5 fois plus vite que la demande des autres emplois informatiques et de 12 fois plus vite que tous les autres emplois. Aujourd'hui, les entreprises placent la sécurité de l'information parmi leurs principales priorités et environ 54% des organisations ont un responsable de la sécurité de l'information.

La classification des professions en République de Moldova approuvée le 03.03.2014 par le gouvernement contient, parmi les autres, le grand sous-groupe *25 "Spécialistes des*

technologies de l'information et de la communication" avec des groupes minoritaires *251203 "Analyste pour la sécurité des systèmes d'information" ; 251403 "Spécialiste des procédures et des outils de sécurité pour les systèmes d'information" ; 251903 "Consultant pour la sécurité des systèmes informatiques" ; 252901 "Ingénieur en sécurité de l'information"*, ainsi que d'autres groupes et sous-groupes, tels que *2412 "Spécialistes et consultants dans le domaine de la finance et de l'investissement" - 241233 "Agent de sécurité ; 121113 "Information Security Manager"* couvre les principales fonctions / professions des diplômés du programme de sécurité de l'information.

Tenant compte des compétences du programme de sécurité de l'information, les diplômés du master peuvent occuper d'autres fonctions que celles mentionnées : des enseignants et des chercheurs aux cadres et aux gestionnaires de différents niveaux.

L'équipe pédagogique du programme Sécurité de l'information en accord avec la politique globale adoptée a l'UTM a mis en place une cellule d'aide à l'insertion, dispositif pour aider à l'insertion professionnelle des étudiants et des jeunes diplômés qui inclut la recherche de stage en entreprise, l'organisation périodique d'ateliers sur la technique de recherche d'emplois, une base de données sur les entreprises spécialisées dans le domaine a été mise en place. Chaque année un salon sur la recherche d 'emplois est organisé à l'UTM avec la participation des entreprises et des professeurs du département visant l'établissement des contacts des étudiants et des jeunes diplômés avec le monde professionnel.

VI Le supplément au diplôme

Chaque diplômé obtient le diplôme en deux langues : en roumain et en anglais, et le supplément au diplôme, qui est également rédigé en roumain et en anglais. Le complément est structuré conformément aux recommandations de la Commission européenne et le Règlement sur l'organisation de l'examen final de baccalauréat à l'UTM approuvé par le Sénat. Il contient des informations sur les compétences acquises, les crédits d'études accumulés, les notes de promotion aux sujets étudiés, etc. Diplôme et supplément au diplôme programme d'études master correspondent aux modèles des diplômes et des suppléments dans l'enseignement supérieur approuvé par le ministère de l'éducation de Moldavie.

Annexe 1 : Le partenariat avec les établissements de formation

1.1. Les universités concourant à la formation

Universités	Rôle dans la formation
ASEM	**Enseignement des cours**
USM	**Enseignement des cours**

Joindre les conventions.

1.2. Les collèges concourant à la formation

Collèges	Rôle dans la formation

Joindre les conventions.

Annexe 2 : Le partenariat avec les entreprises

2.1. Les entreprises concourant à la formation

Entreprises	Rôle dans la formation
Endava	**Enseignement des cours, accueil de stagiaires**
Pentalog	**Accueil de stagiaires**
BSD Management	**Enseignement des cours, accueil de stagiaires**

Joindre les conventions.

2.2. Autres entreprises soutenant la formation

Entreprises	Adresses
Fiscservisinform ÎS	
SA Moldotelecom	
ÎCS Red Union Fenosa SA	
SA Moldoincombank	
Dekart SRL	
EST Computers SRL	
MR Crystal System SRL	
BM Public SRL	
Centrul de guvernare	

electronică	
Centrul de Telecomunicații Speciale	
Banca națională a Moldovei	
Reliable Solutions Distributor	
Bitdefender, Romania	
Nec Corporation, Romania	

Joindre les lettres d'appui.

Annexe 3 : Fiche métier

Fiche métier : Expert en sécurité informatique

Intitulé du métier	Expert en sécurité informatique Analyste de la sécurité de l'information
Mission	La mission principale de l'expert en sécurité informatique est d'assurer la protection des données. Il doit mettre en échec les tentatives d'intrusion des pirates informatiques. Pour cela, il évalue le niveau de vulnérabilité du système et établit des solutions pour le sécuriser. Il peut être épaulé dans sa mission par des "hackers éthiques": ces professionnels de l'intrusion l'aident à déceler les failles. Responsable au quotidien de la sécurité des systèmes informatiques, l'expert en cybersécurité exerce son métier en véritable chef de projet. Il est soumis à une obligation de résultat. Il contribue par sa mission à la sensibilisation des collaborateurs comme à la formalisation et au respect des règles. Il contribue, par son expertise, à l'ajustement des niveaux de sécurité aux besoins des différents métiers. Sa mission suppose la compréhension des besoins et des pratiques des différentes typologies d'utilisateurs. Il donne son aval avant toute modification du réseau ou du système en s'alignant sur la politique de sécurité de l'entreprise. Il contribue à définir et à mettre à jour des processus de sécurité, il est responsable du renouvellement des antivirus systèmes et de la sensibilisation des utilisateurs.
Présentation	L'expert en cybersécurité contribue à la mise en œuvre de la politique de sécurité d'une entreprise. Il doit faire remonter les risques en matière de sécurité informatique. Il met en place des contrôles de prévention en amont, de détection en simultané, d'explication et de consolidation en aval, pour contrer des intrusions ou des dysfonctionnements des systèmes informatiques. A ce titre, l'expert en cybersécurité participe à: • La conception, le déploiement et la mise en œuvre des architectures matérielles et logicielles • La rédaction des politiques et des standards de sécurité • La mise en œuvre et le respect de la sécurité • La conformité du réseau par rapport aux attentes des métiers Ainsi, il œuvre pour: • L'intégrité des informations stockées depuis le moment de leur enregistrement • La disponibilité permanente des logiciels et du système informatique • Le respect de la confidentialité des échanges d'information • L'authentification des accès aux documents stockés
Domaines et	L'expert en cybersécurité est rattaché au RSSI (Responsable de la

périmètre d'intervention	Sécurité des Systèmes Informatiques) qui lui-même est généralement rattaché au Directeur Général ou au directeur informatique, selon la taille de l'entreprise. L'expert en cybersécurité intervient sur l'ensemble du réseau en relation avec les différentes directions ou services. Ses fonctions s'exercent dans le domaine de la sécurité des réseaux, des serveurs, l'ensemble des domaines des systèmes d'information. «Hacker éthique», il cherche et repère les failles du système pour mieux les contrer.
Secteur professionnel	Toutes les entreprises où les systèmes d'information sont utilisés. Un diplôme de niveau master est le minimum requis pour pouvoir postuler au poste *Expert en sécurité informatique* ou *Analyste de la sécurité de l'information*. Le choix se fait alors entre des masters professionnels universitaires dans le secteur de l'informatique (sécurité des systèmes d'information, management de la sécurité des systèmes industriels et des systèmes d'information, etc.)
Activités et tâches professionnelles	Protéger les données et la fiabilité du système informatique d'une entreprise, telle est la mission qui incombe à l'expert en sécurité informatique. Pour cela, l'expert en sécurité informatique est amené à réaliser un diagnostic du système d'information d'une entreprise dans le but de déceler les éventuels points faibles; apporter différentes solutions de protection pour sécuriser les informations et les données d'une entreprise; mettre en place les différents processus de sécurité; garantir la pérennité des systèmes de sécurité; actualiser les systèmes de sécurité en fonction des nouvelles menaces et des dernières technologies. *Activités 1* **Administrer les accès au réseau et aux données** *Tâches* Analyser: • Le fonctionnement de l'ensemble de l'entreprise • Les besoins d'accès aux informations et au réseau de chaque service Qualifier la typologie des contributeurs en fonction des accès autorisés: • Contribution • Validation • Administration *Activités 2* **Contrer les intrusions et les virus** *Tâches* Éviter piratages, vols, destruction de données: • Achat de pare-feu, d'antivirus • Mise en place de tunnels sécurisés • Utilisation de la cryptographie S'assurer de l'emploi des logiciels de protection par les salariés: • Indicateurs de suivi · • Mécanismes d'alerte · • Analyse des logs Mener des audits: ·

	• Recensement des points faibles · • Rédaction des rapports · • Mise à jour des systèmes de protection · • Évolution de la structure du réseau *Activités 3* **Mettre en place les processus de sécurité** *Tâches* Assurer: · • Efficacité des sauvegardes · • Bon niveau de sécurité des serveurs · • Revue et validation des architectures en lien avec les services techniques Créer des alertes: · • Notification de mise à jour · • Programmation d'échéance Mettre en place les processus adaptés: · • Sauvegarde des données sur plusieurs serveurs · • Externalisation des données Lutter contre: · • La sortie d'information de l'entreprise · • Les importations de données potentiellement dangereuses *Activités 4* **Assurer la continuité de l'activité** *Tâches* Définir avec les différents services le plan de reprise d'activité en cas de: • Sinistre (incendie, inondation) · • Mouvement social (grèves des transports, occupation des locaux) · • Acte malveillant (sabotage, terrorisme) Assurer la continuité de l'activité d'un point de vue technique: · • Back up des serveurs · • Accès aux logiciels clés pour l'activité · • Locaux adaptés Assurer la continuité de l'activité d'un point de vue humain: · • Recenser les métiers et les postes clés · • Mettre en place des back up · • Informer les personnes *Activités 5* **Sensibiliser les utilisateurs aux risques** *Activités 6* **Effectuer une veille technologique** *Tâches* Identifier les évolutions nécessaires des réseaux et des systèmes de sécurité: • Adaptations et ajustements • Modifications • Sécurité • Fonctionnalités et services Anticiper les risques:

	• Adaptation et formation • Renouvellement «Benchmarke » les réseaux: • Bonnes pratiques • Références
Compétences génériques	Exécution responsable des tâches professionnelles, dans des conditions restreintes et avec une assistance qualifiée CT1. Appliquer les principes, les normes et les valeurs de l'éthique professionnelle Se familiariser avec les rôles et les tâches spécifiques au travail d'équipe et la répartition des tâches pour les niveaux subordonnés CT2. Identifier, décrire et animer les activités organisées en équipe avec le développement des capacités de communication et de collaboration, ainsi qu'assumer les différents rôles (exécution et leadership) Sensibilisation au besoin de formation continue l'utilisation efficace des ressources et des techniques d'apprentissage pour le développement personnel et professionnel CT3. Démontrer l'esprit d'initiative et d'action pour mettre à jour votre propre culture professionnelle, économique et organisationnelle *Savoir être* Sens de la communication vis-à-vis de différents publics: • Diplomatie • Adaptabilité • Souplesse • Force de persuasion • Curiosité d'esprit • Vif intérêt pour les nouvelles technologies et leurs enjeux Sens pédagogique : • Goût pour l'échange • Aptitude à la communication vis à vis des utilisateurs variés • Capacité de vulgarisation des enjeux et des risques Gestion du stress: • Excellente gestion des situations d'urgence • Hiérarchisation pertinente des priorités Intégrité prouvée: • «Hacker éthique» (il cherche et repère les failles du système pour mieux les contrer); • Respect de la confidentialité • Rigueur Sens de l'engagement : • Implication et motivation • Goût pour le travail en équipe • Charisme et entraînement • Force de proposition
Compétences spécifiques	**C1. Les fondements scientifiques et techniques de la SI**

(professionnelle)	C1.1 Identifier et définir les concepts, théories et méthodes de soutien aux sciences fondamentales et appliquées pour l'ingénierie de la sécurité de l'information C1.2 Expliquer les solutions d'ingénierie en utilisant les techniques, concepts et principes des sciences exactes et appliquées C1.3 Résoudre des problèmes dans les activités humaines en appliquant notamment des techniques et des méthodes de protection C1.4 Choisir les critères et les méthodes pour analyser les avantages et les inconvénients des méthodes et procédures appliquées pour résoudre les problèmes de sécurité C1.5 Modélisation de problèmes typiques en sciences appliquées à l'aide d'un instrument mathématique **C2 Les aspects organisationnels et informationnels de la SI:** C2.1 Identifier et définir les concepts, théories et méthodes utilisés pour effectuer des analyses axées sur la protection des personnes et des informations sur les systèmes opérant au niveau des organisations. C2.2 Expliquer les concepts, théories et méthodes utilisés dans l'analyse des systèmes fonctionnant au niveau organisations C2.3 Application de concepts, de théories et de méthodes de base pour la préparation des informations nécessaires au développement de systèmes de sécurité opérant au niveau des organisations C2.4 Choisir les critères et les méthodes d'évaluation de la qualité, des performances et des limites des systèmes de sécurité en fonction des besoins de l'organisation, y compris ceux requis pour définir un système de gestion de la qualité et de la sécurité C2.5 Élaboration d'un projet (spécification du système) dans les conditions d'un système de gestion de la qualité et de la sécurité. **C3 Les mesures de sécurité et de contrôle** C3.1 Identifier et définir les concepts, procédures et méthodes de sécurité de l'information utilisée pour effectuer les mesures de contrôle découlant des besoins de l'activité humaine C3.2 Expliquer les bonnes technologies pour mettre en œuvre les systèmes de sécurité requis dans les activités des organisations C3.3 Utilisation des technologies modernes dans la définition de solutions de sécurité C3.4 Utilisation de critères et de méthodes basés sur la technologie pour évaluer la conformité aux normes d'interopérabilité C3.5 Développement de mesures de contrôle et de sécurité utilisant des technologies modernes pour la transmission, le stockage et le traitement des données en fonction des besoins d'une organisation **C4 Les méthodes et technologies pour développer des solutions de sécurité** C4.1 Identification et définition de concepts et de méthodes axés sur le développement, la mise en œuvre et l'utilisation de solutions de sécurité C4.2 Explication des concepts et méthodes utilisés pour élaborer, mettre

	en œuvre et utiliser des mesures de contrôle et de sécurité C4.3 Application des langages de programmation, environnements de modélisation et de développement, méthodologies de création de systèmes de sécurité C4.4 Utilisation de critères et de méthodes pour évaluer le processus de développement de systèmes de sécurité en termes de qualité et de performance C4.5 Développement et implémentation de logiciels de sécurité pour des problèmes concrets dans divers domaines de l'activité humaine **C5 L'architecture de sécurité et l'infrastructure** C5.1 Identification et définition du matériel architectural, des logiciels et des composants de communication, ainsi que de ceux qui sont nécessaires pour décrire une infrastructure de protection C5.2 Expliquer l'interaction et le fonctionnement des composants architecturaux et de sécurité C5.3 Application de méthodes de base pour spécifier des solutions architecturales et d'infrastructure pour des problèmes de sécurité typiques C5.4 Utilisation de critères et de méthodes pour évaluer les caractéristiques fonctionnelles et non fonctionnelles des composants du système de sécurité C5.5 Mise en place d'une solution architecturale et d'infrastructure basée sur les contraintes imposées par les projets de sécurité *Savoir faire* Pratique et expérience rédactionnelle: • Actualités/brèves • Articles de fond • Dossiers Maîtrise expérimentée «terrain» de l'outil informatique: • Architecture des systèmes et réseaux • Procédures d'exploitation et des standards d'échange des données employées • Procédures de Sécurité Informatique • Systèmes d'exploitation (Solaris, Linux) et des langages de programmation associés Maîtriser les outils bureautiques: • Traitement de texte, tableur, outil de présentation Utilisation de logiciels spécifiques: • Outils de chiffrement de disques durs ou de serveurs • Pare feu (Firewalls) • Outils d'identification
Compétences transversales	"Leadership" et esprit d'entreprise. Promouvoir sa vision auprès des décideurs internes et externes, et encourager la prise d'initiative de ses équipes. Adaptabilité et Flexibilité. Evaluer l'impact des changements et proposer les réponses ou les solutions adéquates. Analyse et Synthèse. Identifier les informations / sources nécessaires à

	la réalisation des activités de l'entreprise et conduire une analyse critique. Présenter l'essentiel sur un sujet donné dans une logique de préconisation. Communication orale et écrite. Communiquer de façon habile et fine dans des situations complexes (message sensible, public difficile, situation imprévue…). Conviction et Influence. Identifier et décrypter les positions des différents interlocuteurs stratégiques internes et externes, repérer et toucher les bons relais d'influence auprès des personnes à convaincre. Créativité, sens de l'innovation. Concevoir et mettre en œuvre des solutions nouvelles et efficaces. Gestion de Projet. Diriger un projet majeur ou coordonner plusieurs projets opérationnels simultanément. Gestion de la performance. Mettre en place de nouveaux indicateurs pertinents en fonction des objectifs. Partager et promouvoir les meilleures pratiques en interne comme en externe. Orientation client. Etre force de proposition par rapport au besoin exprimé tout en mobilisant les parties prenantes nécessaires (internes – externes). Rigueur et Organisation. Hiérarchiser et établir des priorités d'actions selon les enjeux des activités. Sens Relationnel. Adapter son comportement et son attitude en fonction de l'interlocuteur pour maximiser la qualité des échanges. Travail et animation d'équipe. Accompagner un ou deux collaborateurs sur une activité opérationnelle ou un projet de l'entreprise.
Connaissances nécessaires	*Savoirs* Connaissance de: • L'entreprise • Ses services/produits • Sa structure • Son organisation • Son environnement juridique Vision globale et complète des systèmes d'information • De l'entreprise • Des organisations similaires Connaissance technique approfondie des: • Concepts et techniques d'architecture des systèmes et réseaux · • Procédures d'exploitation et des standards d'échange des données employées • Procédures de Sécurité Informatique • Systèmes d'exploitation et langages de programmation associés • Bases de données
A sortir	Des connaissances approfondies des systèmes de sécurité informatique, un très large panneau de connaissances informatiques (cryptologie, pare-feu, limitation des accès au réseau) et surtout régulièrement mises

	à jour. Esprit de synthèse et vision d'ensemble d'un système. Extrêmement réactif tout en étant capable de réagir très rapidement à un problème de sécurité, être pédagogue et un très bon communicant pour entretenir de bonnes relations de travail avec ses collaborateurs.
Conditions d'accès	Master en Informatique avec une spécialisation en Sécurité Informatique.

Annexe 4 : L'accord de collaboration avec ICS Endava S.R.L.

ACORD DE COOPERARE

Mun. Chişinău **Septembrie 2016**

Prezentul Acord este încheiat între:

1. **ICS ENDAVA" S.R.L**, reprezentată prin Vasile Nedelciuc, având funcţia de Director, cu sediul în Chişinău, Moldova, Str. Sfatul Tarii, nr. 15, posesoarea certificatului de înregistrare nr. IDNO 1002600023471, codul fiscal nr. 7800076, având contul nr. MFO RNCBMD2X504, denumita in continuare **Partener**

şi

2. **Universitatea Tehnică a Moldovei**, reprezentată de domnul Ion Balmuş conf. univ., dr., decan al facultăţii Calculatoare, Informatică şi Microelectronică, cu sediul bd.Stefan cel Mare,168, MD-2004, Moldova, Chisinau, codul fiscal nr.1007600001506, codul bancar AGRNMD2X723, Banca beneficiara BC Moldova-Agroindbank SA, fil.Chisinau-Centru cu sediul bd.Stefan cel Mare,168, MD-2004,Moldova,Chisinau denumită în continuare **Universitate**

denumite în continuare Părţi, care au convenit să semneze prezentul acord cu intenţia realizării următoarelor obiective:

- să colaboreze în vederea ridicării nivelului de pregătire al specialiştilor în domeniul tehnologiilor informaţionale;
- să avizeze şi să propună îmbunătăţiri ale programelor de studii în conformitate cu cerinţele pieţii IT;
- să ofere posibilitatea desfăşurării unor stagii de practică (internship) în cadrul ÎCS Endava SRL pentru studenţi şi colaboratori ai Universităţii Tehnice din Moldova, selectaţi de ÎCS Endava SRL în conformitate cu cerinţele şi posibilităţilor acesteia.

Articolul 1. Obiectul Acordului de colaborare îl reprezintă stabilirea unui parteneriat reciproc avantajos între Părţi în scopul ajustării procesului de formare profesională a studenţilor Universităţii la necesităţile pieţei muncii, prin corelarea asistenţei ştiinţifico-consultative cu cea practică.

Articolul 2. Drepturile şi angajamentele Universităţii:

- punerea la dispoziţie a programelor de studii la disciplinele de specialitate şi revizuirea acestora, după necesitate, conform recomandărilor propuse de către Partener;
- crearea condiţiilor privind implicarea specialiştilor Partenerului la predarea unor lecţii privind ultimele evoluţii în domeniile legate de dezvoltarea de software şi cerinţele de bază pentru angajare la companiile din domeniul TIC;
- înaintarea propunerilor privind efectuarea de către studenţi a stagiilor de practică şi supravegherea sistematică a procesului de stagiere a studenţilor;
- recomandarea, la solicitarea Partenerului, a celor mai performanţi absolvenţi sau viitorilor absolvenţi ai Universităţii în vederea includerii acestora în procesul de selectare pentru angajare în câmpul muncii, inclusiv prin participarea Partenerului la Târgurile locurilor de muncă vacante, organizate regulat de către Universitate;

- organizarea, cu participarea specialiştilor Partenerului, a meselor rotunde pentru familiarizarea studenţilor şi cadrelor didactice cu activitatea acestora, cu posibilităţi de stagiere a studenţilor şi de angajare la lucru după absolvire.

Articolul 3. Drepturile şi angajamentele Partenerului:

- furnizarea materialelor publicitare proprii în scopul familiarizării corpului profesoral şi a studenţilor cu privire la activitatea Partenerului, inclusiv prin plasarea informaţiei pe portalul web al Universităţii şi pe panourile informaţionale plasate la facultate sau la catedrele de profil;
- suportarea, după caz, a cheltuielilor legate de organizarea unor cursuri de instruire speciale cu studenţii selectaţi de către Partener pentru angajarea ulterioară a acestora la lucru;
- înaintarea, după caz, a propunerilor privind perfecţionarea programelor de studii la specialităţile IT;
- oferirea posibilităţii de efectuări de către studenţii selectaţi de către Partener a stagiilor de practică, supraveghind şi validând activitatea acestora;
- selectarea din rândul studenţilor de la specialităţile IT a celor mai performanţi pentru eventuala lor angajare, inclusiv prin participarea la Târgurile locurilor de muncă organizate de către Universitate;
- acceptarea stagierii unor cadre didactice ale Universităţii, care corespund cerinţelor Partenerului, în cadrul ÎCS Endava SRL.

Articolul 4. Cesiunea Acordului

Una dintre părţile prezentului Acord poate transmite unei terţe persoane, total sau parţial, drepturile şi obligaţiile ce i se cuvin prin acest Acord, numai dacă a obţinut acordul scris prealabil al celeilalte părţi.

Articolul 5. Forţa majoră

Forţa majora exonerează de răspundere partea care o invoca, cu condiţia ca aceasta să notifice cealaltă parte în termen de cel mult 5 zile de la data la care a intervenit cauza de forţă majoră, termen care se decalează corespunzător în cazul în care, prin natura ei, situaţia de forţă majoră împiedică inclusiv comunicarea. Efectul este suspendarea obligaţiei părţii în cauză de îndeplinire a prestaţiilor asumate în prezentul Acord a căror executare este împiedicată, sub condiţia dovedirii situaţiei de forţă majora în condiţiile legii. În înţelesul prezentului Acord "forţa majoră" înseamnă orice eveniment imprevizibil şi insurmonabil (în afara puterii de control a părţilor), care se petrece în perioada de derulare a Acordului şi care împiedică pe una din părţi, în mod obiectiv, să îşi îndeplinească obligaţiile din Acord, cum ar fi, de exemplu, conflicte armate, actele de terorism, dezastrele naturale şi alte asemenea, fără a include însă grevele, modificarea cursurilor de schimb, creşterea fiscalităţii sau înrăutăţirea situaţiei socio-economice. În caz de forţă majoră, întregul Acord încetează sau negociază după cum vor stabili părţile pe cale amiabilă.

Articolul 6. Încetarea Acordului

Prezentul Acord încetează în conformitate cu art. 4 din prezentul contract sau în baza acordului părţilor şi în celelalte cazuri prevăzute de lege şi de prezentul contract.

În cazul în care oricare dintre părţi nu-şi îndeplineşte sau îşi îndeplineşte necorespunzător obligaţiile asumate prin prezentul Acord, partea care se considera prejudiciată va transmite celeilalte părţi o

notificare, ce constituie şi punerea în întârziere, semnalând încălcarea constatată şi termenul de remediere, neremedierea sau remedierea neadecvată în acel termen dau dreptul părţii care a făcut notificarea să declare, printr-o nouă notificare, încetarea Acordului prin rezoluţiune unilaterala.

Articolul 7. Dispoziţii finale
- Relaţiile dintre Părţi vor fi guvernate de principiul echităţii, bunei voinţe şi dezvoltării relaţiilor de colaborare durabilă.
- Prezentul Acord de colaborare se întocmeşte pe un termen de 1 an, prelungirea lui realizându-se prin consensul Părţilor.
- Modificările şi completările în prezentul Acord de colaborare se vor efectua prin consensul Părţilor.
- Eventualele litigii între Parţi vor fi soluţionate pe cale amiabilă.
- În cazul reorganizării, schimbării locului de reşedinţă, a numerelor de telefon, fax sau a altor date prezentate în Acordul de colaborare, Părţile vor informa despre aceasta cealaltă parte în termeni utili.

Articolul 8. Acordul de colaborare este redactat în două exemplare originale, cîte unul pentru fiecare Parte şi intră în vigoare din momentul semnării ei de către Părţi.

ÎCS ENDAVA SRL
Director, Vasile Nedelciuc

Universitatea Tehnică a Moldovei
Decan FCIM conf. univ., dr. Ion Balmuş

Annexe 5 : L'accord de collaboration avec l'Université Alexandru Ioan Cuza de Iasi, Romania

Biroul Executiv al Consiliului de Administrație
în ședința din 18/20.01.2016
HOTĂRĂȘTE
SE APROBĂ
RECTOR

Nr. intregistrare UTM
22.01.2016 / 01-63

Nr. inregistrare UAIC
600 / 15/01/2016

ACORD DE COLABORARE
pentru desfășurarea de activități de cercetare comune
în domeniile: CHIMIE, STIINTELE VIETII SI ALE PAMANTULUI si INFORMATICA

între

UNIVERSITATEA "Alexandru Ioan CUZA" IAȘI-ROMÂNIA
Biroul pentru Studii Doctorale Universitare
și
UNIVERSITATEA TEHNICĂ A MOLDOVEI
Departamentul "Școli Doctorale"

CAP. I. PARTILE

CSUD al Universității "Alexandru Ioan CUZA", cu sediul în Iași, Blvd. Carol I nr. 22, Iasi, reprezentat prin Directorul Consiliului pentru Studiile Universitare de Doctorat, prof.univ.dr. Ovidiu CÂRJĂ, având ca domeniu principal de activitate coordonarea studiilor doctorale.

si

Departamentul "Școli Doctorale" al Universității Tehnice a Moldovei, cu sediul in Chișinău, bl Ștefan cel Mare, 168, biroul 303, reprezentat prin doamna Galina Marusic, conf. univ. dr., șef departament, având ca domeniu principal de activitate organizarea și desfășurarea studiilor superioare de doctorat,

convin prin prezentul protocol să colaboreze pe baza de parteneriat activ pentru organizarea mobilităților doctoranzilor din cadrul UTM în scopul realizării cercetărilor științifice prin utilizarea laboratoarelor de cercetare științifică din cadrul ***Universității "Alexandru Ioan CUZA"***.

CAP. II. PRINCIPII DE COLABORARE

- transparența și profesionalism în valorificarea cunoștințelor și a experienței în domeniul fiecăruia de activitate;
- confidențialitate, în schimbul de informații și păstrarea secretului profesional.

CAP. III. PARTEA FINANCIARĂ

Pe durata derulării activităților la Universitatea "Alexandru Ioan CUZA" din Iași, România, doctorandul va putea beneficia de:

- acoperirea cheltuielilor de tur-retur din partea UTM;
- acoperirea cheltuielilor privind cazarea din partea Universității "Alexandru Ioan CUZA" din Iași.

Pe durata derulării activităților la UTM, Republica Moldovaa, doctorandul va putea beneficia de:

- acoperirea cheltuielilor de tur-retur din partea UAIC Iași;
- acoperirea cheltuielilor privind cazarea din partea UTM Republica Moldova.

CAP. IV. DURATA MOBILITĂȚII

Mobilitatea doctoranzilor poate fi desfășurată cu o durată maximă de 10 zile calendaristice pe un an de studii.

CAP. V. DISPOZIȚII FINALE

Prezentul ACORD de colaborare are caracterul unui document cadru și acoperă întreaga activitate de realizare a obiectivelor comune convenite.
Prezentul ACORD poate fi modificat sau completat cu acordul scris al părților semnatare ori de cate ori acestea convin asupra amendamentelor propuse.
Acordul are valabilitate de un an, cu prelungire automată pentru noi perioade de cîte un an, dacă nici una din părți nu notifică celeilalte părți cererea de încetare a valabilității sale.

Încheiat în doua exemplare, ambele cu valoare de original, câte un exemplar pentru fiecare parte.

Universitatea "Alexandru Ioan CUZA"din Iași, Iași, România

RECTOR,
prof. univ. dr. Vasile ISAN

Director CSUD,
Prof.univ.dr. Ovidiu CÂRJĂ

Universitatea Tehnică a Moldovei

RECTOR,
prof. univ. dr. hab. Viorel BOSTAN

Șef departament "Școli Doctorale",
conf. univ. dr. Galina MARUSIC