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

Fiches métier LICENCE et MASTER

KAZAKHSTAN

8. Fiches métiers

⇨ Intitulés des métiers identifiés :

1. Cybersecurity analyst 2. Secure-software developers 3. Data & information security engineer 4. System security engineer 5. Security managers & architects
After discussing again about the 5 resulting profiles, and taking into account the academic experience of the renovators, 3 job profiles we defined (2 Master level and 2 Bachelor Level) • Engineer on Network security. This is considered a BsC level profile which integrates the sub-profiles 1,3. • Engineer on Data & Application security. This is considered a BsC level profile which integrates the sub-profiles 2, 3. • Expert on System & Data security. This is considered a MsC level profile which integrates the sub-profiles 4, 5 • Expert on Security management. This is considered a MsC level profile which integrates the sub-profiles 5

1	**Intitulé du métier**	Noter l'intitulé du métier et les différentes autres appellations éventuelles
	Secteur professionnel	Noter les types d'entreprises, d'institutions dans lesquelles se trouvent ce métier Domaines d'activité professionnelle d'experts en sécurité de l'information et la protection des données sont les entreprises et les organisations de diverses formes de propriété où il est nécessaire de résoudre un ensemble de problèmes liés à la sécurité de l'information et des systèmes automatisés au sein de leur infrastructure TIC: les institutions financières; Entreprises industrielles; Sociétés de services et de conseils; Petites, moyennes et grandes entreprises; Institutions d'État; Établissements d'enseignement; Armée; Entreprises de télécommunication
2	**Conditions d'accès**	Noter l'ensemble des exigences lors du recrutement (niveau d'études, etc.) **Licence en ingénierie et technologie:** sur la spécialité 5B070400 - " Informatique et logiciels "
3	**Activités professionnelles**	Noter l'ensemble des exigences lors du recrutement (niveau d'études, etc.) • installation, configuration et maintenance de logiciels système, instrumentaux et d'application de systèmes informatiques et de réseaux; • développement, compilation, débogage, test et documentation de programmes dans des langages de haut niveau pour le traitement d'informations numériques et symboliques;

		• utilisation de logiciels et de moyens techniques de collecte et de traitement de données, récupération de données dans la base de données et surveillance, documentation et protection de la base de données • la surveillance du réseau et du système, la réponse aux incidents et la documentation; • assurer la sécurité de l'information grâce aux logiciels et au matériel • application de méthodes de protection cryptographique de l'information • application de normes, matériaux méthodologiques et normatifs qui déterminent la conception et le développement des objets de l'activité professionnelle; • l'analyse des conditions de sécurité de l'information et la sélection des mesures techniques et organisationnelles pour assurer la sécurité de l'information au stade de la conception, de l'exploitation des systèmes de traitement et de gestion informatiques • développement d'outils intellectuels pour résoudre les problèmes de sécurité de l'information;
4	**Compétences génériques**	Lister les compétences génériques (transversales) que doit posséder le titulaire de l'emploi (organisation du travail, maîtrise de l'informatique, compétences relationnelles, etc.) Réparties en savoir, savoir-faire • Travailler dans une équipe interdisciplinaire et communiquer avec des spécialistes d'autres domaines.
5	**Compétences spécifiques**	Lister les compétences spécifiques (propres) au métier Réparties en savoir, savoir-faire C1. Avoir la possibilité d'utiliser un système de gestion de base de données pour les applications professionnelles: utiliser un système de gestion de base de données, SQL Server, Cache, ADO.NET pour la gestion de l'organisation, le stockage, la récupération, la sécurité et l'intégrité des données; processus d'exploration de données, OLAP, suppression de données et standardisation des données: SAS DATA Management, Rapid Miner, Deepsee Cache. C2. Posséder la capacité de mettre en œuvre le développement de logiciels sur la base de la technologie orientée objet en utilisant des langages de programmation modernes Java, C ++, C #, Python. C3. Avoir la possibilité d'utiliser des fins de système logiciel - Système d'exploitation OS Windows, OS Unix, OS Lunix, Ubuntu, la connaissance des réseaux informatiques, ordinateurs de bureau et ordinateurs centraux et leurs applications basées sur le langage assembleur, pour des applications professionnelles; mener des consultations sur l'informatisation de l'organisation. C4. Avoir la capacité de gérer la sécurité des communications: appliquer la connaissance des principes, des politiques et des procédures liés à la sécurité des services et des données de communication, et maintenir l'environnement de communication dans lequel il se trouve; surveiller la sécurité du réseau: XSPIDER, NESSUS, NEXPOSE, Scanner INTERNET. C5. Posséder la capacité d'utiliser des langages de programmation pour développer des logiciels sûrs et fiables. C6. Avoir la capacité d'effectuer des tâches complexes sur une protection de réseau informatique, organisation de la sécurité du réseau: d'appliquer des mesures de protection pour détecter, répondre et protection de l'information, des systèmes et réseaux d'information contre les menaces - netstat Agent, Cisco Packet Tracer, Centre pour la certification MS Windows. C7. Posséder la capacité d'appliquer les dispositions de l'électronique et des circuits pour résoudre des problèmes professionnels; démontrer la connaissance des cartes électroniques, des processeurs, des puces, du matériel informatique et des logiciels, y

		compris les applications et la programmation, les principes de construction de l'espace d'adressage à partir des circuits intégrés de la RAM IC; participer à l'installation, la configuration et le support de l'équipement réseau de l'organisation. C8. Posséder la capacité d'effectuer un ensemble de tâches d'administration de base de données: installation et configuration de logiciels, maintenance de bases de données, surveillance et gestion de sauvegardes de bases de données, sécurité de l'information de bases de données; appliquer la connaissance des principes, des méthodes et des outils pour l'automatisation, le développement, la mise en œuvre ou l'administration de systèmes de bases de données, SQL Server, Cache, ADO.NET. C9. Il a la capacité de prendre en compte et utiliser les principes, concepts théoriques et des outils sous-jacents des systèmes informatiques distribués, y compris les composantes et les normes de communication, la technologie MPI, OpenMP, CUDA, l'organisation de la protection des informations traitées en eux. C10. Posséder la capacité d'appliquer le chiffrement pour assurer la sécurité de l'information de l'objet de protection: RSA, AES, cryptographie elliptique; procédures, outils et applications utilisés pour stocker des données ou protéger des informations, y compris l'infrastructure à clé publique, le chiffrement point à point et les cartes à puce. C11. Posséder la capacité de réaliser des travaux sur l'installation, la configuration et la maintenance du matériel informatique et des moyens techniques de protection de l'information; Démontrer la connaissance des spécifications, de l'utilisation et des types d'équipement informatique. C12. Avoir la capacité d'appliquer les méthodes et procédures de protection des systèmes d'information et des données en assurant leur disponibilité, leur authentification, leur confidentialité et leur intégrité. C13. Posséder la capacité d'effectuer un ensemble de tâches pour assurer la sécurité du réseau de l'organisation et la sécurité du fonctionnement des systèmes d'information; appliquer des méthodes, des outils et des procédures, y compris l'élaboration de plans de sécurité de l'information, la prévention des vulnérabilités des systèmes d'information et la fourniture ou la restauration de la sécurité des systèmes d'information et des services de réseau. C14. Avoir la capacité de décrire l'architecture de la technologie de l'information, les connaissances utilisées des méthodes architecturales utilisées dans la conception et le développement des systèmes d'information, (CALS) technologies, y compris la structure physique du système des opérations internes et de l'interaction avec d'autres systèmes, jeu d'instructions MIPS. C15. Avoir la capacité d'évaluer l'efficacité de la technologie de l'information; appliquer des principes, des méthodes et des outils (par exemple, des enquêtes, des indicateurs de performance du système) pour évaluer l'efficacité et la faisabilité des systèmes informatiques. C16. Avoir la capacité de participer à la surveillance de la sécurité de la gestion et de l'information de l'organisation, à l'organisation et à la conduite du contrôle interne; appliquer des principes, des méthodes et des méthodes pour créer des opérations de contrôle interne (par exemple, autorisation, vérification, rapprochements), surveiller leur utilisation et évaluer leur efficacité (par exemple, identifier les déficiences significatives ou les déficiences significatives). C17. Posséder la capacité de résoudre les tâches standard de l'activité professionnelle basée sur les technologies de l'information de gestion des connaissances: Protégé, OntoEdit, Ontolingua, en tenant compte des exigences de base de la sécurité de

		l'information; comprendre la valeur de l'information recueillie et les méthodes de partage de cette information dans l'ensemble de l'organisation. C18. Posséder la capacité d'effectuer des tâches complexes de gestion de réseau; gestion des ressources, maintenance des systèmes de réseau et de télécommunication, systèmes et périphériques connexes. C19. Avoir la capacité de montrer des qualités professionnelles personnelles; comprendre les valeurs sociales et éthiques fondées sur les normes sociales et la tolérance aux différentes traditions culturelles et confessionnelles, appliquer diverses structures communicatives et linguistiques pour résoudre divers problèmes qui se posent dans la communication professionnelle. C20. Avoir la capacité d'analyser le cycle de vie des systèmes; utiliser les concepts de systèmes de gestion du cycle de vie utilisés pour la planification, le développement, la mise en œuvre, l'exploitation et la maintenance des systèmes d'information. C21. Avoir la capacité de tester et d'évaluer les systèmes; appliquer des principes, des méthodes et des outils pour l'analyse et le développement de procédures système pour les essais et l'évaluation, les caractéristiques techniques des systèmes informatiques, y compris l'identification des problèmes opérationnels critiques. C22. Posséder la capacité d'exécuter la documentation technique en tenant compte des documents normatifs et méthodologiques existants; utiliser des procédures pour le développement de la documentation technique et opérationnelle, de la documentation à l'appui, de la certification et de l'ICP. C23. Avoir la capacité d'appliquer les développements et les nouvelles applications informatiques (matériel, logiciel, télécommunications), les nouvelles technologies et leurs applications pour les processus métier et les applications, mettre en place des systèmes d'information pour répondre aux exigences organisationnelles. C24. Posséder la capacité d'analyser les tendances de développement des technologies de télécommunication: connaissance des émissions, diffusion, commutation, gestion et exploitation des systèmes de télécommunication, principe du partage secret; formuler la politique de sécurité des objets de protection. C25. Avoir la capacité d'évaluer les vulnérabilités à l'organisation de la sécurité de l'information: appliquer les principes, les méthodes et les outils d'évaluation de la vulnérabilité et le développement ou une recommandation de mesures appropriées pour prévenir les vulnérabilités. Environnement d'analyse VMWare, packages: ProcMon, Wireshark, IDA, Pro gratuit C26. Avoir la capacité de résoudre des tâches de routine des activités professionnelles sur la base des technologies Web et en tenant compte des principales exigences de sécurité de l'information: appliquer les connaissances des principes et des méthodes de technologies web, des outils et des systèmes de distribution, y compris la sécurité Web, la politique de confidentialité et des problèmes avec l'interface utilisateur, JAVA, PHP , AJAX Python, ASP.NET, MVC, MasterPage, LINQ, Entités ADO.NET, DDD, JavaScript; soutenir les processus de modernisation et de promotion des ressources Internet de l'organisation. CG1. Avoir la capacité de s'adapter à de nouvelles situations. CG2. Posséder la capacité de mener ses activités sur la base des principes de l'éthique professionnelle, de la tolérance et de l'humanisme. CG3. Posséder la capacité de communication orale et écrite dans différents contextes: scientifique, social et culturel. CG4. Avoir la capacité de travailler dans une équipe interdisciplinaire et de communiquer avec des spécialistes d'autres domaines.

		CG5. Avoir la capacité de communiquer oralement et par écrit dans l'une des langues étrangères pour résoudre des problèmes d'activité professionnelle.
6	**Connaissances nécessaires**	Domaines de connaissances pour lesquels les étudiants devraient être formés: 1. Terminologie dans le domaine de la sécurité de l'information, des méthodes et des moyens d'assurer la sécurité de l'information, des méthodes de violation de la confidentialité, de l'intégrité et de l'accessibilité de l'information. 2. Contenu des concepts de base sur le support juridique de la sécurité de l'information; les bases de la sécurité du système d'exploitation; les bases de la sécurité des réseaux informatiques; moyens techniques de base et méthodes de protection de l'information; matériel et logiciel principal pour la sécurité de l'information. 3. Analyse des menaces à la sécurité de l'information, les principales étapes de la résolution des problèmes de sécurité de l'information, l'application dans la pratique des principes méthodologiques généraux de base de la théorie de la sécurité de l'information. 4. Les actes juridiques réglementaires nécessaires, les normes informatifs et juridiques dans le système de la législation actuelle, y compris le système d'information juridique; l'application du cadre législatif actuel dans le domaine de la sécurité de l'information; élaboration de projets de textes normatifs réglementant le travail sur la protection de l'information, ainsi que de règlements, d'instructions et d'autres documents organisationnels et administratifs. 5. Fourniture complexe de la sécurité de l'information de systèmes automatisés spécifiques sur la base de programmes et de techniques développés, y compris le respect des exigences des documents réglementaires qui régissent le régime de secret d'Etat; 6. Analyse des matériaux des organisations et des subdivisions du département dans le but de préparer la prise de décision sur la sécurisation de la protection de l'information; 7. Exécution de la gestion opérationnelle des organisations pour la fourniture intégrée de la sécurité de l'information de systèmes automatisés spécifiques basés sur des programmes et des techniques développés. 8. Systèmes matériels et logiciels-matériels dans le domaine de la sécurité de l'information; 9. Recherche professionnelle d'informations nécessaires sur Internet, littérature scientifique et périodique; 10. Choix de l'architecture et intégration du matériel dans le domaine de la sécurité de l'information; 11. Concevoir la politique des systèmes de sécurité de l'information et leurs éléments dans des domaines spécifiques.
7	**Observations**	Autres commentaires pouvant guider la définition du profil de sortie . Le diplômé devrait être compétent sur toutes les questions liées aux étapes du processus technologique de la sécurité de l'information dans la production, la sécurité de l'information.

⇨ Présenter sur le diaporama, les fiches métiers

Difficultés rencontrées :

Solutions proposées pour les résoudre :

8. Fiches métiers

⇨ Intitulés des métiers identifiés :

1. Cybersecurity analyst 2. Secure-software developers 3. Data & information security engineer 4. System security engineer 5. Security managers & architects
After discussing again about the 5 resulting profiles, and taking into account the academic experience of the renovators, 3 job profiles we defined (2 Master level and 2 Bachelor Level) • Engineer on Network security. This is considered a BsC level profile which integrates the sub-profiles 1,3. • Engineer on Data & Application security. This is considered a BsC level profile which integrates the sub-profiles 2, 3. • Expert on System & Data security. This is considered a MsC level profile which integrates the sub-profiles 4, 5 • Expert on Security management. This is considered a MsC level profile which integrates the sub-profiles 5

La fiche métier (Master) **Intitulés des métiers identifiés 5 pour le Master.**		
1	Secteur professionnel	Les objets de l'activité professionnelle des diplômés du programme de Master dans le programme éducatif sont: Organisations financières; Entreprises industrielles; Sociétés de services et de conseils; Petites, moyennes et grandes entreprises; Institutions d'État; Établissements d'enseignement; Armée; Les entreprises de télécommunication; Institutions de recherche scientifique, Organismes de l'administration d'État.
2	Exigences pour l'éducation de base lors de l'application d'un emploi	**Master en sciences techniques:** spécialisée dans 6M070400 – « Informatique et logiciels »;
3	Activité professionnelle	Planification des processus de gestion de la cybersécurité de l'organisation; Planification des processus de maintenance de la cybersécurité de l'organisation; Planifier des activités pour assurer la cybersécurité de l'organisation; Contrôle des processus de gestion et garantie de la cybersécurité de l'organisation; Assurer la cybersécurité de l'organisation.

4	Compétence générale	- Travailler dans une équipe interdisciplinaire, la capacité d'interagir avec des experts dans d'autres domaines; - Travailler dans un contexte international; - Comparaison, analyse et interprétation d'informations expérimentales complexes et formulation de conclusions; - Résoudre les problèmes théoriques et pratiques des outils informatiques et des logiciels dans différents contextes et la capacité d'établir des relations entre les problèmes et les principes de base; - Résoudre un large éventail de problèmes théoriques et pratiques connus des outils informatiques et des logiciels et mettre en œuvre des solutions aux problèmes implicites et non résolus; - Développement d'expériences informatiques à grande échelle dans des domaines appliqués; - Prévision des faiblesses et risques possibles de la recherche; - Organisation et planification des activités professionnelles, scientifiques et scientifiques-pédagogiques, ainsi que des activités de l'équipe; - Pensée critique, critique et autocritique; - Mener des recherches scientifiques et travailler en tant que chef d'équipe.

5	Compétences spéciales	- Connaissance des principes de la cybersécurité utilisés pour gérer les risques associés à l'utilisation, au traitement, au stockage et à la transmission d'informations ou de données. - Capacité à concevoir des mesures de sécurité basées sur les principes de la cybersécurité. - Capacité à dépanner et diagnostiquer les anomalies cybernétiques de l'infrastructure de sécurité en utilisant VoIP, SMS, WAP et HTML mobile. - Aptitude à appliquer des méthodes de cybersécurité, telles que les pare-feux, les zones démilitarisées et le cryptage à l'aide de RSA, El-Gamal. - Possibilité de configurer et d'utiliser des composants de protection informatique (par exemple, pare-feu matériels, serveurs, routeurs, protocoles Bluetooth / Wi-Fi, WiFi Direct, NFC). - Connaissance des méthodes de base, des procédures et des méthodes de collecte de l'information. - Connaissance de la collecte ciblée d'informations et des méthodes de formation opérationnelle et des cycles de vie. - Capacité à effectuer des analyses de vulnérabilité et identifier les faiblesses dans les systèmes de sécurité. - Connaissance des technologies informatiques antivirus et antivirus et des méthodes de piratage (logiciel et matériel). - Capacité d'appliquer des méthodes, des normes et des approches pour décrire, analyser et documenter l'architecture de la technologie de l'information (TI) d'une organisation. - Aptitude à analyser les aspects théoriques et expérimentaux de la virologie informatique et les différentes méthodes et approches utilisées par les pirates. - Connaissance des concepts d'architecture de sécurité et de modèles de référence de l'architecture d'entreprise. - Capacité à concevoir des mesures de sécurité basées sur les principes et principes de cybersécurité. - La capacité de déterminer comment le système de sécurité doit fonctionner et comment les changements dans les conditions, les opérations ou l'environnement affectent ces résultats. - Aptitude à appliquer les concepts d'architecture de sécurité réseau, y compris la topologie, les protocoles, les composants et les principes (VMware ESXi, vSphere Client). - La possibilité d'appliquer des outils de conception de systèmes de sécurité, les techniques et la technologie - la capacité de détecter hôte et la technologie de détection d'intrusion de réseau par l'invasion du pare-feu, Pont, Switch, Internet, Services Internet (Firewall, Bridge, Switch, Internet, Services Internet). - Capacité à configurer et à utiliser les composants de sécurité réseau (par exemple, les pare-feu, réseaux privés virtuels, réseau des systèmes de détection d'intrusion, PAN, LAN, CAN, MAN, WAN, VLAN) - La connaissance des données relatives aux mécanismes de sécurité de chiffrement dans les bases de données, y compris des fonctions intégrées de contrôle de service. - Capacité d'évaluer l'utilisation des normes de cryptage (spécifications standards 28147-89 et dES) .- -- La capacité à développer des logiciels en toute sécurité selon les méthodes de déploiement sécurisé des logiciels, des outils et des techniques dans iOS, Android et Windows Phone.

		- Connaissance des principes et méthodes de la sécurité informatique qui ont trait au développement de logiciels utilisant Java, Java Cryptography Extension. - Connaissance des systèmes de gestion de bases de données et le service de l'information architecture du système de sécurité parlé Server. SQL - Connaître le système d'architecture de sécurité de l'information de l'entreprise. - La capacité à distinguer les besoins de protection (c.-à-d. Mesures de sécurité) des systèmes et réseaux d'information (GSM (2G), UMTS (3G), LTE (4G)).))...
6	Connaissances requises	- Les moyens de l'application des mécanismes protecteurs des logiciels et le matériel de l'organisation; - Principes et méthodologies pour la conception de systèmes d'information; - Des documents normatifs et techniques sur la sécurité de l'information de l'organisation; - Méthodes d'évaluation des résultats de l'utilisation de solutions organisationnelles et techniques pour assurer la sécurité de l'information; - Les bases des moyens de contrôler la mise en œuvre des plans et des activités pour assurer la sécurité de l'information; - Méthodes d'évaluation et de gestion des risques de sécurité de l'information; - Les principes et les moyens d'administration dans l'OS et les mécanismes de protection qui y sont encastrés. - Principes de construction et d'application des outils de sécurité de l'information matérielle et logicielle, des systèmes de surveillance de la vulnérabilité, des systèmes de surveillance de la sécurité de l'information et des systèmes de prévention des fuites d'informations; - Des méthodes pour déterminer, prévenir et éliminer les conséquences des incidents de sécurité de l'information, des situations critiques (d'urgence); - Principes de travail et d'administration des outils de sécurité de l'information matérielle et logicielle; - Principes de travail et d'administration des systèmes de surveillance de la vulnérabilité, des systèmes de surveillance de la sécurité de l'information et des systèmes de prévention des fuites d'informations; - Principes de base et moyens d'effectuer des travaux de développement, de test et d'exploitation de logiciels.
7	observations (commentaires)	Le diplômé devrait être compétent sur toutes les questions liées aux étapes du processus technologique de la sécurité de l'information dans la production, la cyberprotection de l'information.

⇨ Présenter sur le diaporama, les fiches métiers

Difficultés rencontrées :