**MBA**

**Магістр бізнес адміністрування**

**КІБЕРБЕЗПЕКА КОМПАНІЇ**

**Програма навчання** Американської Асоціації з вищої освіти і акредитації (AAHEA): **Кібербезпека компанії. Результат – професійне звання MBA.**

Студент завершує програму Навчання протягом усього життя відповідно до §60 Закону № 111/98 Sb. **Університет видає своїм випускникам сертифікат про закінчення програми навчання протягом усього життя**.

**Для кого**

Корпоративна кібербезпека являється головним завданням директорів усіх установ, оскільки неякісний кіберзахист підприємства може призвести до його ліквідації. Ось чому кожен працівник повинен знати і практикувати принципи кібербезпеки. Обов’язок курсу - підвищити рівень обізнаності людей щодо безпеки, визначені в Указі про кібербезпеку № 316/2014 Sb. Навчання призначене для директорів, менеджерів та спеціалістів компаній, охорони здоров’я, шкіл, державних установ, кадрових працівників, менеджерів, фахівців. Він призначений для всіх, хто має працівників, зберігає особисті дані про працівників, клієнтів, пацієнтів.

Це навчання також підходить для працівників із захисту даних у рамках GDPR (Загального положення захисту даних), оскільки після переходу управління їх установи до GDPR та освоєння питань конфіденційності кібербезпека їх бізнесу стане надзвичайно серйозною проблемою.

Сучасний стан кібербезпеки в установах показує, що кібербезпека повинна відповідати за всіх працівників компанії. Не лише за працівників ICT, але й користувачів та менеджерів, навіть постачальників.

**Форма навчання:**

За допомогою Інтернет-технологій та технології електронного навчання, з можливістю індивідуального навчання чи роботи в групі з одного робочого місця.

**Цілі навчання**

Метою навчання є формування необхідних знань та навичок для того, щоб випускники мали змогу керувати процесами кібербезпеки свого роботодавця. Студент поступово будуватиме стратегічні плани та детальну планову документацію для всебічного захисту своєї компанії від негативного впливу на захист персональних даних, захист операційних даних та захист від внутрішніх і зовнішніх атак на безпеку компанії. Практиків цього профілю дуже не вистачає на практиці.

**Система навчання:**

Навчання відбувається через Інтернет. У кожному семестрі студент спочатку встановлює час для вивчення навчального матеріалу модуля, продумує застосування набутих знань та розробляє семестральний проект обсягом близько п’яти сторінок. Після завершення всіх модулів студент підготує дисертацію на основі поточних проектів.

Що стосується групи, яка складається з декількох студентів з одного робочого місця, то така група подає спільну дисертацію, яку вони разом захищають. Крім того, всі студенти отримують знижку на вартість навчання за індивідуальною домовленістю.

Навчання всіх студентів завершується урочистою частиною. Додаткову інформацію студент отримає на початку навчання.

**Зміст навчання:**

**М1:** Загальне Положення про захист даних

**M2:** Закони про захист персональних даних у Чехії та Словаччині, їх інновації та застосування GDPR (Загального Положення про захист даних)

**M3:** Інші закони про захист даних, внесенні до GDPR, чеські та словацькі зміни до Закону про захист персональних даних, посадова інструкція співробітника

**M4:** Кібербезпека підприємства

**M5:** Проект застосування кібербезпеки підприємства в стратегії та управлінні бізнесом у співпраці з ІТ та відділом кадрів

**M6:** Варіанти хмар та безпеки даних

**M7:** Інтернет речей, захист даних, безпека операцій

**M8:** Проект застосування технології loT в бізнес-стратегії, управлінні та безпеці експлуатації у співпраці з ІТ-відділом

**M9:** Проект подальшої освіти співробітників установи з питань кібербезпеки **М10:** Дисертація та випускний