Конфедерация на независимите синдикати в България
София, 1040, пл. „Македония“ № 1, етаж 12, стая 9; тел.: 02/ 40 10 540; e-mail: mnk@knsb-bg.org

ПРОГРАМА за неформално обучение за развитие на специфични дигитални умения

Икономическа дейност	52 (Складиране на товари и спомагателни дейности в транспорта)
Длъжност	31545005 Координатор въздушно обслужване
Име на програмата	Интелигентно управление и сигурност във въздухоплаването
Брой часове	15

Общо представяне на програмата за обучение за всички идентифицирани дигитални умения

Неформалното обучение по програма „Интелигентно управление и сигурност във въздухоплаването“ разглежда приложението на изкуствения интелект (ИИ) при координирането и контролирането на движението на въздухоплавателните средства във въздушното пространство и на земята за безопасно и ефективно осъществяване на полетите. Програмата отразява навлизането на технологиите с ИИ в системите за управление на аварии, осигуряване на безопасност и минимизиране на рисковете за околната среда, както и оптимизиране на въздушните маршрути и ефективността на транспортните коридори. Обучаваните ще придобият специализирани знания за същността на ИИ, видовете ИИ, приложението на ИИ в практиката с цел автоматизиране на процесите и намаляване на грешките, напр. чрез използване на анализ на големи обеми от данни и виртуални асистенти. Обучението включва и запознаване с предимствата и възможностите на облачните технологии.

Цели на обучението

Целта на обучението е да покаже как отговорните лица по координиране на въздушното обслужване могат да подобрят значително своята дейност при вземане на решения чрез възможностите за прогнозиране, заложени в ИИ, големите обеми от данни (Big Data) и дигиталните близнаци (Digital Twins). Обучението цели да се придобият умения и компетентности за работа в споделена облачна среда, както и за възможностите за използване на технологични решения от Интернет на нещата (IoT). Разкрива се същността на IoT за повишаване на транспортната безопасност, по отношение на поддръжка на съоръженията, навигацията и предоставяне на информация за времето и пътните условия. Програмата цели да се получат знания за ролята и значението на критичната инфраструктура, тъй като летищните съоръжения са важна част от нея. Акцент е постигане на умения и компетентности за справяне с увеличаващия се брой компютърни атаки. Обучаваните ще могат да прилагат съвременни технологии за защита и контрол. С цел усъвършенстване на практиките на отчитане и контрол в обучението се предвижда запознаване с техниките на работа със споделени облачни пространства като Google Workspace.

Наименование на темите	
Тема 1	Основи на изкуствения интелект (ИИ). Видове ИИ. Приложение на ИИ за осигуряване на безопасност на полетите. Предизвикателства пред ИИ. Дигитални близнаци. Интернет на нещата (IoT). Big Data. • Знания – за основните направления на изкуствения интелект и дигиталните близнаци. • Умения - за използване на приложения с изкуствен интелект

Проект BG05M9OP001-1.128-0001 „Партньорство в дигитална среда“, финансиран от Оперативна програма „Развитие на човешките ресурси“, съфинансиран от Европейския съюз чрез Европейския социален фонд. Проектът се осъществява от КНСБ в партньорство с КРИБ, БСК, АИКБ, БТПП и МТСП

	за осигуряване на безопасни полети. • Компетентности – за надеждно и сигурно използване на технологии за ИИ.
Тема 2	Рискове и предизвикателства за сигурността на ИТ системите в летищните инфраструктури. Компютърни заплахи. Сигурност и защитни технологии при ИИ. Критична инфраструктура. • Знания – за видовете компютърни заплахи и за същността на критичната инфраструктура и SCADA системите. ▪ Умения - за справяне със Spyware, Adware, Malware, Phishing, уеб-базирани атаки и др. • Компетентности – за изграждане на политики и стратегии за информационна сигурност.
Тема 3	Облачни технологии. Споделени пространства. Google Workspace. Съхраняване на данни в облак. Обработка на данни. Функции за обработка на данни. Проверка. Сортиране. Обобщение. • Знания – за генериране на съдържание и работа с интегрирани документи. • Умения - за работа с Google Workspace. • Компетентности – за изграждане на стратегии за управление в Google Workspace.
Очакваните резултати от обучението	
След завършването на обучението служителите ще познават използването на ИИ при роботизиране на процесите и рационализиране на задачите, които изпълняват отговорните лица за координиране на въздушното обслужване. Резултатите от обучението са свързани с придобиването на основни знания и умения за прилагане на възможностите на ИИ, което ще подобри дейността и ще позволи на работещите да елиминират възможни проблеми, преди те да станат факт, което е и същността на ИИ. Обучените служители ще могат успешно да разрешават проблеми в областта на киберсигурността, ще идентифицират рискове и уязвимости, ще се справят с компютърни заплахи и ще бъдат компетентни при изграждането на защитни механизми и информационни политики за сигурност. Обучаваните ще владеят оптимизирани практики за отчитане и контрол и техники на работа със споделени облачни пространства.	
Методи на обучение	
Чрез различни методи на обучение (лекции, практически занятия, защита на курсови работи и дискусии) у обучаемите ще се формират умения за разбиране на проблемите в сферата на интелигентното управление, Интернет на нещата, сигурността и облачните технологии. Методите за обучение се базират на запознаване на курсистите с теоретичен материал и същевременно практическо му прилагане, за да може те непрекъснато да упражняват и да прилагат предлаганите им технологични инструменти и знания, които да превръщат в лични умения за работа.	
Условия за провеждане	
Лекциите са от съществена важност за разбиране на използването на изкуствен интелект (ИИ) и IoT във въздушния транспорт. Учебната зала за лекционните занятия трябва да бъде	

Конфедерация на независимите синдикати в България
София, 1040, пл. „Македония“ № 1, етаж 12, стая 9; тел.: 02/ 40 10 540; e-mail: mnk@knsb-bg.org

оборудвана с мултимедиен проектор и интернет достъп. За всяко лекционно занятие трябва да е разработена Powerpoint презентация, в която има множество примери, за да могат обучаемите да усвоят по-лесно и трайно теоретичния материал и да го превърнат в практическо умение.

Практическите занятия са от основно значение за трайно усвояване на умения и практики за използване на приложения за ИИ. По всяка тема от лекционния материал трябва да има специално подготвено практическо задание, което обучаемите да изпълняват по време на практическите занятия в компютърна зала под ръководството и насоките на преподавателя, който да им помага да се справят с възникнали в процеса на работа трудности, неясноти или допуснати грешки.

Критерии за оценяване

Подготовка на курсова работа. Разработката включва представяне на тема от курса по избор.

Критерии за оценяване на проекта:

Пълнота и логическа завършеност
Значимост на темата за сектора
Актуалност на използваните източници

Средства за оценяване

Използва се точкова система за оценяване:

Пълнота и логическа завършеност - 20 точки
Значимост на темата за сектора - 20 точки
Актуалност на използваните източници - 20 точки

Условия за провеждане на оценяването

Достъп на обучаемите до настолен или персонален компютър за провеждане на финалния изпит/защита на курсова работа. Работа със специализиран софтуер за управление и поддържане на комуникационни устройства, контролни системи и електронно оборудване

Конфедерация на независимите синдикати в България
София, 1040, пл. „Македония“ № 1, етаж 12, стая 9; тел.: 02/ 40 10 540; e-mail: mnk@knsb-bg.org

Учебно съдържание

№	I. ТЕМАТИЧЕН ПЛАН НА ЛЕКЦИИ	ЧАСОВЕ
1.	Основи на изкуствения интелект (ИИ). Приложение на ИИ за целите на безопасността на полетите. Дигитални близнаци. Интернет на нещата (IoT). Big Data. Подтеми: Видове ИИ. Приложения на ИИ. Предизвикателства пред ИИ. Приложения с изкуствен интелект. Изкуственият интелект и автоматизацията на процесите. ИИ и безопастност. Интелигентни устройства. Специализирани приложения от IoT и интелигентни ботове за координиране на полетите. Анализ на приложенията.	3
2.	Рискове и предизвикателства за сигурността на ИТ системите в летищните инфраструктури. Компютърни заплахи. Сигурност и защитни технологии при ИИ. Сигурност при IoT. Противодействие и защита. Защита при облачни технологии. Криптиране на данни. Критична инфраструктура. Подтеми: Видове компютърни заплахи, Spyware, Adware, Malware, Phishing, уеб-базирани атаки и др. Мрежови скенери, скенери за слаби страни, разбивачи на пароли, мрежови анализатори (sniffers), подмяна на обекти, модификация на данни, крипто вируси. Защита от разрушаване: антивирусна защита, контрол за автентичност на данните и програмите, защита от хардуерни и софтуерни грешки, защита от грешки на персонала. Излагане на информация пред неоторизиран достъп; изтичане на информация; загуба на информация; уязвимост към кибератаки. SCADA системи.	4
3.	Облачни технологии. РПредизвикателства на облачните изчисления. Споделени пространства. Google Workspace. Подтеми: Съхраняване на данни в облак. Обработка на данни. Функции за обработка на данни. Проверка. Сортиране. Обобщение.	3
	ОБЩО ЧАСОВЕ:	**10**

№	II. ТЕМАТИЧЕН ПЛАН НА УПРАЖНЕНИЯ	ЧАСОВЕ
1.	Изкуственият интелект за защита и киберсигурност. Приложения,	2

Проект BG05M9OP001-1.128-0001 „Партньорство в дигитална среда“, финансиран от Оперативна програма „Развитие на човешките ресурси“, съфинансиран от Европейския съюз чрез Европейския социален фонд. Проектът се осъществява от КНСБ в партньорство с КРИБ, БСК, АИКБ, БТПП и МТСП

	базирани на изкуствен интелект. Примери.	
2.	Използване на защитни стени и антивирусна защита, защита на уеб трафик	2
3.	Защита на мобилни и облачни приложения	1
	ОБЩО ЧАСОВЕ:	**5**