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	35223015 Оператор радиосъоръжения (наземни)
Име на програмата	Интелигентно управление и сигурност
Брой часове	15

Общо представяне на програмата за обучение за всички идентифицирани дигитални умения
Неформалното обучение по програма „Интелигентно управление и сигурност“ разглежда приложението на изкуствения интелект (ИИ) при наземните комуникационни съоръжения. Програмата отразява навлизането на технологиите на ИИ системите за управление на аварии, осигуряване на безопасност и минимизиране на рисковете за околната среда, както и оптимизиране на транспортните маршрути и ефективността на транспортните възли и логистичните хъбове. 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 виртуални асистенти, анализи на данни, дронове и др.
Цели на обучението
Целта на обучението е да подготви операторите на наземни радиосъоръжения да подобрят значително процесите на вземане на решения, планирането, капацитета и търсенето чрез възможностите за прогнозиране, заложени в ИИ и големите обеми от данни (Big Data). Обучението цели да се придобият умения и компетентности за работа в споделена облачна среда и за възможностите за използване на технологични решения от IoT. Разкрива се същността на IoT за повишаване на транспортната безопасност, по отношение на поддръжка на наземните съоръжения, навигацията и предоставяне на информация за времето и пътните условия. Програмата цели да се получат умения и компетентности за справяне с увеличаващия се брой компютърни атаки. Обучаваните ще могат да прилагат и съвременни технологии за защита и контрол.

Наименование на темите	
Тема 1	Основи на изкуствения интелект (ИИ). Видове ИИ. Приложения на ИИ. Предизвикателства пред ИИ. Дигитални близнаци. • Знания – за основните направления на изкуствения интелект и дигиталните близнаци. • Умения - за използване на приложения с изкуствен интелект. • Компетентности – за надеждно и сигурно използване на технологии за ИИ.
Тема 2	Интернет на нещата (IoT). Интернет на нещата и изкуствен интелект. Big Data. IoT сензори: радиочестотна идентификация, инфрачервени сензори, камери, GPS, сензори за интелигентни устройства.

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

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

	▪ Знания - за IoT сензори: радиочестотна идентификация, инфрачервени сензори, камери, GPS, сензори за интелигентни устройства. • Умения – за работа със софтуер, използван при изграждане на специализирани приложения от IoT и интелигентни ботове. • Компетентности – за оценка на системи от съоръжения, услуги и системи, чието спиране и неправилно функциониране би имало сериозно негативно въздействие.
Тема 3	Рискове и предизвикателства за сигурността на ИТ системите. Компютърни заплахи. Сигурност и защитни технологии при ИИ. • Знания – за видовете компютърни заплахи, като фишинг, мрежови скенери, скенери за слаби страни, разбивачи на пароли, мрежови анализатори (sniffers), подмяна на обекти, модификация на данни, крипто вируси. ▪ Умения - за справяне със Spyware, Adware, Malware, Phishing, уеб-базирани атаки и др. ▪ Компетентности – за изграждане на политики и стратегии за информационна сигурност.

Очакваните резултати от обучението
След завършването на курса обучаемите ще познават използването на ИИ при роботизиране на процесите и рационализиране на задачите и увеличаване на възможностите за достъп до информационни системи и интелигентни бази данни. Резултатите от обучението са свързани с придобиването на основни знания и умения за прилагане на възможностите на ИИ, което ще подобри функционирането на процесите и ще позволи на работещите да елиминират възможни проблеми, преди те да станат факт, което е и същността на ИИ. Работещите 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.
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 и сигурността. Методите за обучение по дисциплината 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 при оперирането на наземните радиосъоръжения.. Учебната зала за лекционните занятия трябва да бъде 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.

Учебно съдържание

№	I. ТЕМАТИЧЕН ПЛАН НА ЛЕКЦИИ	ЧАСОВЕ
1.	Основи на изкуствения интелект (ИИ). Дигитални близнаци. Подтеми: Видове ИИ. Приложения на ИИ. Предизвикателства пред ИИ. Приложения с изкуствен интелект. Изкуственият интелект и автоматизацията на процесите. ИИ и безопастност на радиосъоръженията. Интелигентни устройства. Анализ на приложенията.	3
2.	Интернет на нещата (IoT). Интернет на нещата и изкуствен интелект. Интелигентни IoT системи. Big Data. IoT сензори. GPS. Подтеми: IoT сензори: радиочестотна идентификация, инфрачервени сензори, камери. GPS и сензори за интелигентни устройства. Работа със софтуер, използван при изграждане на специализирани приложения от IoT и	4

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

	интелигентни ботове.	
3.	Рискове и предизвикателства за сигурността на ИТ системите. Компютърни заплахи. Сигурност и защитни технологии при ИИ. Сигурност при IoT. Противодействие и защита. Защита при облачни технологии. Криптиране на данни. 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.	3
	ОБЩО ЧАСОВЕ:	**10**

№	II. ТЕМАТИЧЕН ПЛАН НА УПРАЖНЕНИЯ	ЧАСОВЕ
1.	Приложения, базирани на изкуствен интелект	2
2.	Запознаване и работа с IoT сензори	2
3.	Изкуственият интелект за защита и киберсигурност	1
	ОБЩО ЧАСОВЕ:	**5**

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