

## ПРОГРАМА за неформално обучение за развитие на специфични дигитални умения

Икономическа дейност	52 (Складиране на товари и спомагателни дейности в транспорта)
Длъжност	31546004 Отговорник безопасност на полета
Име на програмата	Киберсигурност и изкуствен интелект за безопасност
Брой часове	15
Общо представяне на програмата за обучение за всички идентифицирани дигитални умения	
<p>Неформалното обучение по програма „Киберсигурност и изкуствен интелект за безопасност“ разглежда приложението на изкуствения интелект (ИИ) и електронното обучение при дейността на специалистите по безопасност на полетите. 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 въздушните 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, дроневи и др.</p>	
Цели на обучението	
<p>Целта на обучението е да покаже как отговорните лица по безопасност на полетите могат да подобрят значително своята дейност при вземане на решения чрез възможностите за прогнозиране, заложи 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 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 в програмата 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.</p>	
Наименование на темите	
Тема 1	<p>Изкуствен интелект (ИИ). Видове ИИ. Приложение на ИИ за осигуряване на безопасност на полетите. Машинно обучение. Методи за машинно обучение. Компютърни системи за управление на работи и интелигентни сензори. Дигитални близнаци. Интернет на нещата (IoT). Big Data.</p> <ul style="list-style-type: none"> <li>• Знания – за основните направления на изкуствения интелект и дигиталните близнаци.</li> <li>• Умения - за използване на приложения с изкуствен интелект за осигуряване на безопасни полети и за работа с алгоритми за машинно обучение и извличане на данни.</li> <li>• Компетентности – за надеждно и сигурно използване на</li> </ul>

	технологии за ИИ.
Тема 2	<p>Рискове и предизвикателства за сигурността на ИТ системите в летищните инфраструктури. Компютърни заплахи. Сигурност и защитни технологии при ИИ.</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>▪ Умения - за справяне със Spyware, Adware, Malware, Phishing, веб-базираните атаки и др.</li> <li>• Компетентности – за изграждане на политики и стратегии за информационна сигурност.</li> </ul>
Тема 3	<p>Критична инфраструктура. SCADA системи.</p> <ul style="list-style-type: none"> <li>• Знания – за същността на критичната инфраструктура и SCADA системите; уязвимостите на HMI, Zero day експлойти, PLC уязвимости и биометрични модалности.</li> <li>• Умения – за работа със SCADA, стратегии за използване на "демилитаризирани зони" (DMZ).</li> <li>• Компетентности – за оценка на системи от съоръжения, услуги и системи, чието спиране, неизправно функциониране или разрушаване би имало сериозно негативно въздействие върху населението, околната среда, националното стопанство и върху ефективното функциониране на държавното управление.</li> </ul>
<b>Очакваните резултати от обучението</b>	
<p>След завършването на обучението обучаемите ще бъдат запознати с използването на ИИ при роботизиране на процесите и рационализиране на задачите, които изпълняват отговорните лица за безопасност на полетите. 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. 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.</p>	
<b>Методи на обучение</b>	
<p>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.</p> <p>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.</p>	

### 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 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 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 финален изпит/курсва работа. Работа със специализиран софтуер за управление и поддържане на превозните средства, работа с комуникационни устройства, контролни системи и електронно оборудване.

## Учебно съдържание

№	I. ТЕМАТИЧЕН ПЛАН НА ЛЕКЦИИ	ЧАСОВЕ
1.	<p>Изкуствен интелект (ИИ). Приложение на ИИ за целите на безопасността на полетите. Машинно обучение. Компютърни системи за управление на работи и интелигентни сензори. Дигитални близнаци. Интернет на нещата (IoT). Big Data.</p> <p>Подтеми:</p> <p>Видове ИИ. Приложения на ИИ. Предизвикателства пред ИИ. Приложения с изкуствен интелект. Методи за машинно обучение. Изкуственият интелект и автоматизацията на процесите. ИИ и безопасност. Интелигентни устройства. Специализирани приложения от IoT и интелигентни ботове за осигуряване на безопасност на полетите. Анализ на приложенията.</p>	3
2.	<p>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. Социално инженерство.</p> <p>Подтеми:</p> <p>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.</p>	4
3.	<p>Критична инфраструктура. Същност и характеристика. Примери. SCADA системи.</p> <p>Подтеми:</p> <p>Видове SCADA системи. Уязвимостите на HMI. Zero day експлойти, PLC уязвимости. Стратегии за използване на "демилитаризирани зони" (DMZ). Препоръки за защита на SCADA системи Оценка на системи от съоръжения и услуги, чието спиране, неизправно функциониране или разрушаване би имало сериозно негативно въздействие върху населението, околната среда, националното стопанство и върху ефективното функциониране на държавното управление.</p>	3
<b>ОБЩО ЧАСОВЕ:</b>		<b>10</b>



ЕВРОПЕЙСКИ СЪЮЗ  
ЕВРОПЕЙСКИ  
СОЦИАЛЕН ФОНД



ОПЕРАТИВНА ПРОГРАМА  
РАЗВИТИЕ НА  
ЧОВЕШКИТЕ РЕСУРСИ



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

№	II. ТЕМАТИЧЕН ПЛАН НА УПРАЖНЕНИЯ	ЧАСОВЕ
1.	Изкуственият интелект за защита и киберсигурност. Приложения, базирани на изкуствен интелект. Примери.	2
2.	Използване на защитни стени и антивирусна защита, защита на уеб трафик	2
3.	Защита на мобилни и облачни приложения	1
<b>ОБЩО ЧАСОВЕ:</b>		<b>5</b>