

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

Икономическа дейност	49.10 Пътнически железопътен транспорт
Длъжност	13243017 Началник превозна служба
Име на програмата	Специфични дигитални умения и компетентности за Началник превозна служба
Брой часове	16
Общо представяне на програмата за обучение за всички идентифицирани дигитални умения	
<p>Курсът разглежда приложението на информационните технологии при изпълнение на служебните задължения на Началник превозна служба. Програмата отразява навлизането на специализирани бази от данни, възможностите на Интернет технологии при извършване на регулярните дейности по осигуряване на превозната дейност и комуникацията с клиентите. Обучаваните ще придобият знания за специализираните документно информационни системи и софтуера за търговската експлоатация.</p>	
Цели на обучението	
<p>Обучението цели да се придобият умения и компетентности за работа с Microsoft Office пакет, създаване и оформяне на цифрово съдържание на дигитални документи, за работа със специализиран софтуер при комуникация с клиенти и оформяне на митнически документи, както и взаимодействие чрез дигитални технологии посредством изпращане на електронни писма и онлайн комуникация. Обучаваните ще могат да прилагат съвременни технологии за защита и контрол.</p>	
Наименование на темите	
Тема 1	<p><b>Сътрудничество чрез дигитални технологии.</b></p> <p><b>Знания</b></p> <p>Представяне на възможностите за използване на Microsoft Office пакет. Запознаване със информационни технологии за онлайн комуникации за обмен на файлове, специализиран софтуер за търговската експлоатация. Запознаване с използването на дигитални технологии за управление на цифрова идентичност.</p> <p><b>Умения</b></p> <p>Извършва дейности по изготвянето на дигитални документи и регистри, като осигурява управление на цифровата идентичност. Оценява, избира и използва цифрови инструменти, с които се оформя цифрово съдържание на дигитални документи.</p> <p><b>Компетентности</b></p> <p>За работа с цифрова идентификация (цифров подпис). Използва достъп до различни обществени услуги, чрез онлайн</p>

	<p>удостоверяване. Прилага дигиталните знания и умения при набиране на информация и изготвяне на документи и техния обмен във вътрешноведомствена мрежа и с клиентите.</p>
<p>Тема 2</p>	<p><b>Защита на данни и поверителност в дигитална среда.</b></p> <p><b>Знания</b></p> <p>Рискове и предизвикателства за сигурността на ИТ системите. Запознаване с прилагането на общите политики и механизми за осигуряване на безопасност и сигурност. Познаване на общ регламент за защита на данни (GDPR).</p> <p><b>Умения</b></p> <p>За работа със защитни стени и антивирусни програми. Изпълняване на процедури осигуряващи предотвратяването на загуба на данни. Използване на облачни технологии позволяващи съхранение на данни и организира процедури по архивиране или репликация на данни.</p> <p><b>Компетентности</b></p> <p>За изграждане на политики и стратегии за информационна сигурност. Разпознава рисковете и заплахите в дигитална среда за сигурността на личните данни и запознат е със специфични мерки за безопасност и сигурност, прилагани в съответствие с изискванията на нормативна база.</p>
<p>Тема 3</p>	<p><b>Идентифициране на нуждите и технологични решения</b></p> <p><b>Знания</b></p> <p>Познава основните принципи на функциониране на използваните системи в транспорта. Начини за запис и съхранение (архивиране) на дигитално съдържание. Има възможност да прави оценка на потребностите и идентифицира, оценява и избира дигитални инструменти и възможни технологични решения.</p> <p><b>Умения</b></p> <p>При идентифициране на основни комуникационни проблеми да намери най-подходящите начини за настройване и персонализиране на дигиталната среда и да избере съответните дигитални инструменти и възможни технологични решения за изпълнение на поставените задачи.</p> <p>За работа със системите за общо предназначение и ИСУ (Интегрирана система за управление). Притежава умения и средства за комуникация при идентифициране на необходимостта от промени в настройките и опциите на специализирания софтуер. Да анализира и използва техническа документация и инструкции. Настройва и персонализира дигиталната среда за лични нужди (напр. свързани с достъпността).</p> <p><b>Компетентности</b></p>

	Да следи техническото състояние на поверената му техника и спазването на технологичната и трудовата дисциплина. Да идентифицира грешки и откази от хардуер или от софтуер и да намира решения за подобряване на ефективността на компютрите.
<b>Очакваните резултати от обучението</b>	
След завършване на курса обучаваният служител следва да може: <ul style="list-style-type: none"><li>- да използва дигитални инструменти и технологии за съвместни процеси при работата с клиенти и вътрешнофирмена комуникация;</li><li>- да идентифицира проблеми със сигурността и да прилага методи за защита на информацията;</li><li>- да оценява собствените или на другите нужди и да идентифицира, оценява, избира и използва цифрови инструменти и възможни технологични отговори за решаването им. Да регулира и персонализира цифровите среди спрямо личните си нужди (напр. достъпност).</li></ul>	
<b>Методи на обучение</b>	
<p>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.</p> <p>За теоретичната част от обучението се използва лекция, презентация и беседа с обучаемите, мултимедийно представяне на учебно съдържание, свързано с различните типове информация, демонстрация на примери от практиката.</p> <p>За практическите тренинг-сесии лекторът прави демонстрация, а обучаемите работят по конкретни задачи. В рамките на обучението се решават примерни (предварително подготвени) казуси с конкретни хардуерни и софтуерни средства.</p>	
<b>Условия за провеждане</b>	
<p>Учебната зала за лекционните занятия трябва да бъде оборудвана с мултимедийен 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.</p> <p>Практическите занятия се провеждат в компютърна зала с осигурен специализиран (необходим) софтуер. Занятията са под формата на решаване на казуси под ръководството и насоките на преподавателя, който да им помага да се справят с възникнали в процеса на работа трудности, неясноти или допуснати грешки.</p>	
<b>Критерии за оценяване</b>	
Текущ контрол на теоретичните знания и практическите умения. За заключителната част на приключване на обучението се предлага тест за решаване на казус.	

<b>Средства за оценяване</b>
Използва се точкова система за оценяване, като за теоретичната част максимумът е 50 точки и за казус – 50 точки.
<b>Условия за провеждане на оценяването</b>
Компютърна зала с персонален компютър за всеки обучаем, както и достъп до специализиран софтуер. За успешно преминал курс се счита получаване на мин. 60 точки.

### Учебно съдържание

№	I. ТЕМАТИЧЕН ПЛАН НА ЛЕКЦИИ	ЧАСОВЕ
1.	<p><b>Сътрудничество чрез дигитални технологии.</b></p> <p>Дигитални документи и регистри. Специализиран софтуер за търговската експлоатация и работа с клиенти. Запознаване с използването на дигитални технологии за управление на цифрова идентичност. Онлайн услуги с използване на цифрова идентификация.</p> <p>Специализирани документно информационни системи. Същност и особености на приложението им в транспорта. Начини за генериране на справки, извличане на информация и комуникация.</p>	1
2.	<p><b>Сътрудничество чрез дигитални технологии.</b></p> <p>Запознаване с различни специализирани бази от данни. Приложение на информационните технологии за представяне и търсене на информация в Интернет. Подходи за прецизиране на информация и решаване на конкретни проблеми.</p> <p>Същност и използване на електронна комуникация. Механизми за комуникация и основни комуникационни канали. Способи за колаборация и съвместна работа онлайн. Взаимодействие в реално време чрез социалните мрежи.</p>	2
3.	<p><b>Защита на данни и поверителност в дигитална среда.</b></p> <p>Рискове и предизвикателства за сигурността на информационните системи. Видове компютърни заплахи. Запознаване с прилагането на общите политики и механизми за осигуряване на безопасност и сигурност.</p> <p>Използване на облачни технологии позволяващи съхранение на данни. Защита при облачни технологии. Познаване на общ регламент за защита на данни (GDPR) при работа с лични и чувствителни данни. Проблеми на сигурност при IoT.</p>	2



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

4.	<p><b>Идентифициране на нуждите и технологични решения</b></p> <p>Основни принципи на функциониране и съпровождане на информационните системи, свързани с коригирането и подобряването на нейните възможности. Работа с техническа документация и инструкции. Настройва и персонализира дигиталната среда за лични нужди.</p> <p>Как да се идентифицира проблема дали е свързан със софтуера или с хардуера чрез достъп до компютъра през „Безопасен режим“. Запознаване с най-често срещаните възникващи грешки при хардуера и начин на действие. Начини за безпроблемно управление на софтуер. Проблеми и грешки при работа със специализираните документно информационни системи и системата за търговска експлоатация.</p>	2
<b>ОБЩО ЧАСОВЕ:</b>		<b>7</b>

№	II. ТЕМАТИЧЕН ПЛАН НА УПРАЖНЕНИЯ	ЧАСОВЕ
1.	Особеностите на различни специализирани бази от данни. Търсене на информация в Интернет. Осигуряване управлението на цифровата идентичност.	1
2.	Анализ на информация от използваните системи за търговската експлоатация. Намиране и обобщаване на информация за натоварването на персонала. Същност и използване на електронна комуникация. Технологични средства за колаборация и съвместна работа онлайн.	2
3.	Подходи и инструменти за идентифициране на основни проблеми свързани с вируси (видове), подмяна на обекти, модификация на данни и неоторизиран достъп, изтичане и загуба на информация, уязвимост към кибератаки и др. Изпълняване на процедури осигуряващи предотвратяването на загуба на данни.	3
4.	Стартиране на „Безопасен режим“ на работа на компютъра. Изпълняване на процедури за отстраняване на най-често срещаните хардуерни грешки. Проблеми възникващи при работа със специализираните системи и системата за търговската експлоатация. Подбор на дигитални инструменти и технологични решения свързани с подобряване функционирането на информационните системи	3
<b>ОБЩО ЧАСОВЕ:</b>		<b>9</b>