

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

Икономическа дейност	49.10 Пътнически железопътен транспорт
Длъжност	13245019 Началник служба метрополитен
Име на програмата	Специфични дигитални умения и компетентности за Началник служба метрополитен
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 служба метрополитен. Програмата отразява придобиването на необходимите познания за дейностите по планиране и управление на документооборота и информацията, създаване и редакция на документи в електронната система на компанията, касаещи персонала, техническата съоръженост и търговската дейност на службата. Разглеждат се възможностите за осигуряване на защита при проблеми със сигурността на компютърните мрежи и системи, прилагане на подходи за създаване на умения за справяне с най-често срещаните заплахи и създаване на надеждни защитни механизми, идентифициране на основни проблеми възникнали при осъществяване на връзка между всички отдели и служби в метрополитен.</p>	
Цели на обучението	
<p>Обучението цели да се придобият специализирани знания за работа с данни, набавяне, контрол, създаване и коригиране на информация. Извършване на мониторинг и комуникация с всички служби, осигуряващи сигурността на превозите. Обучаваните ще могат да прилагат съвременни технологии за защита и контрол, решаване на технически проблеми и идентифициране на потребности за намиране на технологични решения за подобряване надеждността и качеството на дигиталните инструменти.</p>	
Наименование на темите	
Тема 1	<p><b>Анализ и оценяване на данни, информация и дигитално съдържание</b></p> <p><b>Знания</b></p> <p>Притежава познания относно методите и принципите за работа със специализираните информационни системи използвани в метрополитен. Познава функциите на наличния фирмен/личен софтуер и различни методи и средства за обобщаването на информация за изготвянето на дигитални документи и отчети. Притежава знания за работа с документно информационни системи и с Microsoft Office пакет. Знае да използва дигитални технологии за управление на цифрова идентичност.</p> <p><b>Умения</b></p>

	<p>Анализира, обработва и оценява достоверността и надеждността на източниците на данни, информация и дигитално съдържание. Използва наличния фирмен/личен софтуер и прилага придобитите дигитални знания и умения при съставяне на справки, отчети и документи, като осигурява управление на цифровата идентичност. Съгласува електронно документи. Извлича и анализира точно информация от база данни съгласно зададени критерии. Адаптира данни от устройствата за телеуправление и телеконтрол към различни справки и отчети, както и дигитално съдържание съгласно нуждите.</p> <p><b>Компетентности</b></p> <p>Определя и организира дейностите на службата (отдела), като използва информацията в дигитална среда. Адекватно използва интегрирани управленчески системи за оперативен мениджмънт. Планира и координира организацията по изпълнението на специфичните задачи на службата с помощта на специализирани информационни управляващи системи, като използва цифрова идентификация. Създава справки, документи, графици за работа на персонала и актуализира документите съгласно системата "Управление на документираната информация". Периодично изготвя инструкции за персонала и експлоатационните звена на базата на промяната на оперативната информация.</p>
Тема 2	<p><b>Защита на устройствата и дигиталното съдържание</b></p> <p><b>Знания</b></p> <p>Познава вътрешна нормативната база за осигуряване на безопасност и сигурност на цифрови устройства и информацията в тях при осигуряване на движението на влаковете. Притежава знания за работа на съоръженията, осигуряващи защита на околната среда, както и тяхното използване за съхраняване на здравето на персонала и пътниците. Осъществява видеонаблюдение и контрол за спазване на изискванията за безопасност.</p> <p><b>Умения</b></p> <p>Умения да прилага изискванията за осигуряване на безопасност и сигурност на цифрови устройства. Да използва ефективно получаваната информация за състоянието на околната среда, да оценява нейната адекватност и да предприема дейности за осигуряване на здравословни и безопасни условия на труд и превоз на пътниците.</p> <p><b>Компетентности</b></p> <p>Работи със софтуерната система, използвана в метрото в рамките на определения му достъп. Ефективно и отговорно използва дигиталните инструменти и технологии при осъществяване на контрол на транспортния процес, както и съвместно използване на информационните канали за направляване на работата на</p>

	<p>служителите и координирането на действията им с другите сектори и отдели.</p> <p>Спазва инструкциите за защита на личните данни, да контролира правилната експлоатация на съоръженията и устройствата (компютри, монитори, комуникационни устройства). Разпознава рисковете и заплахите в дигитална среда и участва при изграждане на политики и стратегии за информационна сигурност. Да спазва общия регламент за защита на данни (GDPR) при работа с лични и чувствителни данни. Да осъществява контрол по спазване на инструкциите за правилната експлоатация на съоръженията и устройствата.</p>
Тема 3	<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 метрополитен - Диспечерска система за контрол и управление движението на влаковете, системата за "Управление на средствата за измерване" и система за управление на качеството. Знае как да направи оценка на потребностите и да идентифицира, оценява и избира дигитални инструменти и възможни технологични решения. Знае как да променя настройките и опциите на операционната система или специализирания софтуер при решаване на проблеми. Идентифицира дигитални инструменти и технологии за създаване на знания и решения, както и неоткрити досега организационни нужди. Запознат е с изискванията за определяне на нивото и пропуските в познанията на персонала и необходимостта от повишаване на квалификацията.</p> <p><b>Умения</b></p> <p>За работа със специализираните системи в метростанцията, в рамките на определения му достъп. Да спазва специфичните мерки за безопасност и сигурността на дигиталните устройства. Оценява съществуващите начини за настройване и персонализиране на дигиталната среда и избира най-подходящите, които да използва в работа си. Осигурява надеждност и поверителност при осъществяване на дейностите в метрополитена. Самостоятелно може да оценява техническите проблеми и да подбере дигитални инструменти и възможни технологични решения за решаването на възникналите казуси.</p> <p><b>Компетентности</b></p> <p>За самостоятелно идентифициране на основни мрежови промени/комуникационни проблеми и работа с цифрова идентификация в използваните системи. Оценява съществуващите начини за настройване и персонализиране на дигиталната среда и избира най-подходящите, които да използва в работа си. Осигурява достъп на служителите до специализиран софтуер и</p>

	<p>открива пропуски в тяхната дигиталната компетентност. Контролира спазването на правилата и инструкциите. Демонстрира умения, свързани с настройване и персонализиране на дигиталната среда в зависимост от ситуацията</p> <p>Преценява нуждите на службата и избира най-подходящите дигитални инструменти и възможни технологични решения за изпълнението на възложените им дейности, както и в случаите на аварийни ситуации. При идентифициране на проблем, свързан със сигурността, своевременно уведомява техническите и охранителните служби и отговорно прилага процедурите за осигуряване на сигурността на устройствата.</p> <p>Самостоятелно предоставя готови решения при възникнали проблеми при работа с нови технологии в метрополитен.</p>
<b>Очакваните резултати от обучението</b>	
<p>След завършване на курса обучаемите следва да могат:</p> <ul style="list-style-type: none"><li>- да търсят данни и информация, да организират, съхраняват, извличат и анализират данни, информация и съдържание в дигитална среда; да създават, редактират и извличат документи и справки;</li><li>- да идентифицират проблеми със сигурността и да разрешават проблеми в областта на киберсигурността, да идентифицират рискове и заплахи при информационните системи и технологии, да се справят с компютърни заплахи и да бъдат компетентни при изграждането на защитни механизми и информационни политики;</li><li>- да следят техническото състояние на поверената им техника, да идентифицират основни проблеми, възникнали при функционирането на информационните системи и да намират пътища за тяхното решение;</li><li>- при възникване на събития, злополуки, инциденти даспазват стриктно заповедите и нормативната уредба и да намират решения за преодоляването им.</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 мултимедиян 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 и 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>Анализ на данни, информация и дигитално съдържание</b></p> <p>Специализирани документно информационни системи. Същност и основни начини за събиране, анализ, обработка и визуализация на данни. Начини за генериране на справки, извличане на информация, създаване на документи и комуникация. Запознаване с използването на дигитални технологии за управление на цифрова идентичност. Технологични средства за колаборация.</p>	2
2.	<p><b>Защита на устройствата и дигиталното съдържание.</b></p> <p>Рискове и предизвикателства за сигурността на информационните системи. Подходи/практики за идентифициране на основни проблеми, свързани с комплексната защита на информационните ресурси. Технологични решения (процедури и специализиран хардуер) свързани с осигуряване защитата на информацията. Проблеми и повреди, начин на действие при възникването им. Контрол и регламентиране на достъпа до данните, защита на информацията. Стъпки при провеждане на консултации с техническите служби и охранителните звена,</p>	2

	предприемане на действия съответни със ситуацията.	
3.	<b>Идентифициране на нуждите и технологични решения</b> Основни принципи на функциониране и използване на информационните системи, свързани с коригирането и подобряването на нейните възможности.. Запознаване с прилагането на общите политики и механизми за осигуряване на безопасност и сигурност. Настройка и персонализиране на дигиталната среда за лични нужди. Подходи/практики за идентифициране на основни проблеми, свързани с комплексната защита на информационните ресурси. Възможности и средства за комуникация при установяване на технологични проблеми.	2
<b>ОБЩО ЧАСОВЕ:</b>		<b>6</b>

№	II. ТЕМАТИЧЕН ПЛАН НА УПРАЖНЕНИЯ	ЧАСОВЕ
1.	Създаване на цифрово съдържание в различни формати. Оформяне на документи, таблици, диаграми, изображения и презентации. Форматиране на текст. Представяне на обработените данни. Особеностите на документно информационни системи. Начини за генериране и редактиране на справки, извличане на информация. Осигуряване управлението на цифровата идентичност. Същност и използване на електронна комуникация. Технологични средства за колаборация и съвместна работа онлайн.	4
2.	Подбор на дигитални инструменти и технологични решения свързани с подобряване функционирането на информационните системи. Работи със специализиран софтуерен пакет, създаване на документи в дигитална среда, начини на действие при ситуации, свързани с безопасността и загуба на информация. Използване на защитни стени и антивирусна защита, защита на уеб трафик, защита от хардуерни и софтуерни грешки, защита от грешки на персонала. Защита на мобилни и облачни приложения.	3
3.	Подходи и инструменти за идентифициране на основни проблеми свързани с дигиталните инструменти. Следене и контролиране чрез дигитални средства на експлоатационната обстановка. Начини за идентифициране на основни мрежови промени/комуникационни проблеми. Възможности за използване на дигитални инструменти и подбор на възможни технологични решения за решаването на възникналите казуси.	3
<b>ОБЩО ЧАСОВЕ:</b>		<b>10</b>