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	13243016 Началник експлоатационно звено
Име на програмата	Киберсигурност и електронно управление
Брой часове	15

Общо представяне на програмата за обучение за всички идентифицирани дигитални умения
Програмата за неформално обучение” Киберсигурност и електронно управление“ разглежда защитата и проблеми на сигурността на компютърните мрежи и системи при процесите на доставка, транспорт, складиране и диструбуция, както и стандартните начини за подход и разрешаване на тези проблеми, като включва съответните реални примери. Акцент в курса са механизмите на електронното управление като платформа за цифрова трансформация, за повишаване на качеството на услугите, за преминаването към рационални електронни процеси на функциониране и управление и за достъп по електронен път на информацията, с която разполагат институциите. Практическите занятия позволят на обучаваните да прилагат теорията в реална среда. Чрез практическо обучение ще се създадат умения за ползване на електронни услуги и създаване на надеждни защитни механизми.
Цели на обучението
Обучаваните служители ще придобият специализирани знания за решаване на проблеми на изследването, нововъведенията и приложението на комуникационните и информационните системи и технологии в транспорта, развиване на способности и усъвършенстване на необходими навици и умения в отговор на повишените изисквания към киберсигурността и определяне на средства за киберзащита. Служителите ще получат знания за методите за защита на компютърните мрежи, видовете атаки и адекватното им противодействие. Обучението цели придобиването на специализирани знания за процесите в електронното управление за да се реализира основната му цел – освобождаване на ценни ресурси, като време, хора и финанси. Обучаваните ще получат знания за информационните и комуникационни технологии, правната рамка, взаимодействието между участниците в е-управлението и обществените отношения.
Наименование на темите

Тема 1	Компютърни заплахи. Видове кибер атаки. Защита. Технологични и юридически мерки за обезпечаване на киберсигурността. • Знания – за видовете компютърни заплахи: фишинг, мрежови скенери, разбивачи на пароли, мрежови анализатори, подмяна на обекти, промени в данните; неоторизиран достъп; изтичане на информация; загуба на информация; уязвимост към кибератаки; разкриване на поверителна информация. • Умения - за справяне с модификация на данни, крипто

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

	вируси; Spyware, Adware, Malware, Phishing и други атаки срещу електронна поща, спам, уеб-базирани атаки и др.; за контрол и регламентиране на достъпа до данните; защита от разрушаване: антивирусна защита, контрол за автентичност на данните и програмите, защита от хардуерни и софтуерни грешки, защита от грешки на персонала, криптографска защита на данните. • Компетентности – за изграждане на политики и стратегии за информационна сигурност и за надеждно и сигурно използване на компютърните технологии за поддържане на киберхигиена в организациите.
Тема 2	Критична инфраструктура. SCADA системи. Биометрична сигурност. Биометрични системи. • Знания – за същността на критичната инфраструктура и SCADA системите; уязвимостите на HMI, Zero day експлойти, PLC уязвимости и биометрични модалности. • Умения – за работа със SCADA, стратегии за използване на "демилитаризирани зони" (DMZ) и режими на работа на биометрични системи – идентификация и верификация. • Компетентности – за оценка на системи от речни и пристанищни съоръжения, чието спиране, неизправно функциониране или разрушаване би имало сериозно негативно въздействие върху населението и околната среда.
Тема 3	Електронна идентификация, цифрови подписи и сертификати. Национална схема за електронна идентификация. Трансгранична електронна идентификация. Оперативна съвместимост. Сигурност и защита при електронното управление. Заплахи при електронното управление. Протоколи SSL и SET. • Знания – за основните стъпки за гарантиране на сигурността при електронното управление: мрежова сигурност, защита срещу вируси, VPN, защитни стени, пароли, архивиране на жизненоважни данни, създаване и ползване на дигитална лична карта. • Умения – за контрол и регламентиране на достъпа до данните при електронните услуги; защита от разрушаване: антивирусна защита, контрол за автентичност на данните и програмите, криптографска защита на данните. • Компетентности – за създаване на стратегии за приложение на принципите на електронното управление и за надеждно и сигурно използване на електронните услуги.
Очакваните резултати от обучението	
След завършването на обучението служителите ще могат успешно да разрешават проблеми в областта на киберсигурността при процесите на доставка, транспорт, складиране и	

диструбуция, ще идентифицират рискове и уязвимости при информационните системи и технологии, ще се справят с компютърни заплахи и ще бъдат компетентни при изграждането на защитни механизми и информационни политики. Обучените служители ще могат да прилагат успешно електронни услуги, ще идентифицират рискове и уязвимости при процесите на електронното управление, ще се справят с компютърни заплахи и ще бъдат компетентни при изграждането на защитни механизми и информационни политики за сигурност в организациите.
Методи на обучение
Чрез различни методи на обучение (лекции, практически занятия, защита на курсови проекти и дискусии) в обучаемите ще се формират умения за разбиране на проблемите в сферата на компютърната сигурност и електронното управление. 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 като специалисти по кибер сигурност в транспортния сектор.
Условия за провеждане
Лекциите са от съществена важност за разбиране на същността и приложението на дигиталните близнаци и 3D принтирането при процесите в логистичния сектор. 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 дигиталните технологии. 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
Защита на курсов проект. Проектът е на тема по избор от областта на киберсигурността и електронното управление 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 точк
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 бази данни, контролни системи и електронно оборудване

Учебно съдържание

№	I. ТЕМАТИЧЕН ПЛАН НА ЛЕКЦИИ	ЧАСОВЕ
1.	Компютърни заплахи. Видове кибер атаки. Защита. Технологични и юридически мерки за обезпечаване на киберсигурността. Подтеми: Фишинг. Видове фишинг. Мрежови скенери. Разбивачи на пароли. Мрежови анализатори, подмяна на обекти. Неоторизиран достъп. Изтичане на информация. Загуба на информация. Уязвимост към кибератаки. Разкриване на поверителна информация. Модификация на данни. Крипто вируси. Spyware, Adware, Malware. Антивирусна защита, контрол за автентичност на данните и програмите. Криптографска защита на данните.	3
2.	Критична инфраструктура. SCADA системи. Биометрична сигурност. Биометрични системи. Подтеми: Сигурност при SCADA системите. Уязвимост на HMI. Zero day експлойти. PLC уязвимости. Социално инженерство. Препоръки за защита на SCADA системи. Биометрични системи. Биометрични модалности. Проекти – Soli, CIR, Auth0, EarEcho и др.	4
3.	Електронна идентификация, цифрови подписи и сертификати. Национална схема за електронна идентификация. Трансгранична електронна идентификация. Оперативна съвместимост. Сигурност и защита при електронното управление. Заплахи при електронното управление. Протоколи SSL и SET. Подтеми: Основни стъпки за гарантиране на сигурността при електронното управление: мрежова сигурност, защита срещу вируси, VPN, защитни стени, пароли, архивиране на жизненоважни данни. Контрол и	3

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

	регламентиране на достъпа до данните при електронните услуги; защита от разрушаване: антивирусна защита, контрол за автентичност на данните и програмите, криптографска защита на данните.	
	ОБЩО ЧАСОВЕ:	**10**

№	II. ТЕМАТИЧЕН ПЛАН НА УПРАЖНЕНИЯ	ЧАСОВЕ
1.	Използване на защитни стени и антивирусна защита, защита на уеб трафик	2
2.	Правила за защита от кибератаки. Работа с генератор на пароли.	2
3.	Издаване и приложение на цифрови подписи и цифрови сертификати.	1
	ОБЩО ЧАСОВЕ:	**5**