

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

Икономическа дейност	52 (Складиране на товари и спомагателни дейности в транспорта)
Длъжност	13247006 Началник, летище
Име на програмата	Киберсигурност
Брой часове	15
Общо представяне на програмата за обучение за всички идентифицирани дигитални умения	
<p>Програмата за неформално обучение ” Киберсигурност“ разглежда защита и проблеми на сигурността на компютърните мрежи и системи, както и стандартните начини за подход и разрешаване на тези проблеми, като включва съответните реални примери. Практическите занятия позволят на обучаваните да прилагат теорията в реална среда. Целта на практическата част е създаване на умения за справяне с най-често срещаните заплахи и създаване на надеждни защитни механизми.</p>	
Цели на обучението	
<p>Обучаваните ще придобият специализирани знания за решаване на проблеми на изследването, нововъведенията и приложението на комуникационните и информационните системи и технологии, развиване на способности и усъвършенстване на необходими навици и умения в отговор на повишените изисквания към киберсигурността и определяне на средства за киберзащита. Обучаваните ще получат знания за методите за защита на компютърните мрежи, видовете атаки и адекватно противодействие.</p> <p>Обучението цели да се придобият 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>Рискове и предизвикателства за сигурността на ИТ системите. Компютърни заплахи. Социално инженерство.</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 и други атаки срещу електронна поща, спам, уеб-базирани атаки и др.;</li> <li>• Компетентности – за изграждане на политики и стратегии за информационна сигурност в организациите</li> </ul>
Тема 2	Противодействие и защита. Защита при облачни технологии. Електронна идентификация, цифрови подписи и сертификати.

	<p>Криптиране на данни.</p> <ul style="list-style-type: none"> <li>• Знания - за неоторизиран достъп; изтичане на информация; загуба на информация; уязвимост към кибератаки; разкриване на поверителна информация; Insider атака. DDoS атаки.</li> <li>• Умения – 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.</li> <li>• Компетентности – за надеждно и сигурно използване на компютърните технологии за поддържане на киберхигиена в организациите</li> </ul>
Тема 3	<p>Критична инфраструктура. SCADA системи. Биометрична сигурност. Биометрични 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) и режими на работа на биометрични системи – идентификация и верификация.</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>
Очакваните резултати от обучението	
<p>След завършването на обучението служителите ще могат успешно да разрешават проблеми в областта на киберсигурността, 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 за сигурност в летищата.</p>	
Методи на обучение	
<p>Чрез различни методи на обучение (лекции, практически занятия, защита на курсови проекти и дискусии) у обучаемите ще се формират умения за разбиране на проблемите в сферата на компютърната сигурност.</p> <p>Методите за обучение се базират на запознаване на служителите 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 основите на компютърните заплахи и начините за справяне с тях. 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 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 идентифициране на видовете атаки и методите за противодействие. 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 представяне на възникнал проблем и методи за справяне.

Критерии за оценяване на проекта:

Функционална и логическа завършеност

Сложност на проблема/атаката

Адекватно решение

### Средства за оценяване

Използва се точкова система за оценяване:

Функционална и логическа завършеност (пълнота): - 20 точки

Сложност на проблема/атаката - 20 точки

Адекватно решение - 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 бази данни, контролни системи и електронно оборудване.

## Учебно съдържание

№	I. ТЕМАТИЧЕН ПЛАН НА ЛЕКЦИИ	ЧАСОВЕ
1.	<p>Рискове и предизвикателства за сигурността на ИТ системите. Компютърни заплахи. Социално инженерство:</p> <p>Подтеми:</p> <p>Мрежови скенери, скенери за слаби страни, разбивачи на пароли, мрежови анализатори (sniffers), подмяна на обекти, модификация на данни или информация. Възможност за промяна на чужд мрежов трафик (MITM man in the middle). Неоторизиран достъп чрез пароли и вредни програми. Spyware, Adware, Malware, Trojan, Backdoor, Phishing и др. Ботнет мрежи. Крипто вируси.</p>	3
2.	<p>Противодействие и защита. Защита при облачни технологии. Електронна идентификация, цифрови подписи и сертификати. Криптиране на данни.</p> <p>Подтеми:</p> <p>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. Излагане на информация пред неоторизиран достъп; изтичане на информация; загуба на информация; уязвимост към кибератаки; разкриване на поверителна информация; Insider атака. DDoS атаки. Криптографска защита на данните.</p>	4
3.	<p>Критична инфраструктура. SCADA системи. Биометрична сигурност. Биометрични системи.</p> <p>Подтеми:</p> <p>Сигурност при SCADA системите. Уязвимост на HMI. Zero day експлойти. PLC уязвимости. Социално инженерство. Препоръки за защита на SCADA системи.</p> <p>Биометрични системи. Биометрични модалности. Проекти – Soli, CIR, Auth0, EarEcho и др.</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.	Използване на защитни стени и антивирусна защита, защита на уеб трафик	2
2.	Защита на мобилни и облачни приложения	2
3.	Използване на мултифакторна идентификация	1
<b>ОБЩО ЧАСОВЕ:</b>		<b>5</b>