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	13247007 Началник, морска гара
Име на програмата	Киберсигурност
Брой часове	15

Общо представяне на програмата за обучение за всички идентифицирани дигитални умения
Програмата за неформално обучение ” Киберсигурност“ разглежда защита и проблеми на сигурността на компютърните мрежи и системи в морския транспорт, 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.

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 морския транспорт, 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. 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.

Наименование на темите	
Тема 1	Компютърни заплахи в морската индустрия. Кибер атаки срещу корабни навигационни системи и атаки върху компютърните мрежи на кораби. • Знания – за видовете компютърни заплахи, като промени в данните на кораба, вкл. неговото местоположение, курс, информация за товара, скорост и име; създаване на „кораби-призраци“, разпознати от други кораби като истински, на всяко място в света; изпращане на невярна метеорологична информация до конкретни кораби, за да променят курса и да избегнат несъществуваща буря; активиране на фалшиви предупреждения за сблъсък за автоматична корекция на курса на плавателния съд; превръщане на съществуващ кораб в „невидим“. • Умения - за справяне с фалшифицирането на EPIRB

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

	(Emergency Position Indicating Radio Beacon) сигнали за активиране на аларми на близките кораби; DoS (Denial of Service) атака чрез увеличаване на честотата на предаване на AIS (Automatic Identification System) съобщения. • Компетентности – за изграждане на политики и стратегии за информационна сигурност на морските гари и пристанища.
Тема 2	Защита от кибератаки срещу корабни и пристанищни системи. Технологични и юридически мерки за обезпечаване на киберсигурността. Резолюция MSC.428 (98) Maritime Cyber Risk Management In Safety Management Systems. Препоръки MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management. Система за Управление на Безопасността на Корабите (СУБК). Guidelines on Cyber Security Onboard Ships. • Знания - за неоторизиран достъп; изтичане на информация; загуба на информация; уязвимост към кибератаки; разкриване на поверителна информация; • 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. • Компетентности – за надеждно и сигурно използване на компютърните технологии за поддържане на киберхигиена в в морските гари и пристанища.
Тема 3	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 морски и пристанищни съоръжения, чието спиране, неизправно функциониране или разрушаване би имало сериозно негативно въздействие върху населението и околната среда.
Очакваните резултати от обучението	
След завършването на обучението служителите ще могат успешно да разрешават проблеми в областта на киберсигурността в морската индустрия, 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 морския сектор.	

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

Методи на обучение
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. 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 в морския транспортен сектор.
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 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 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 тръководството 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 проект. Работа със специализиран софтуер за управление и поддържане на бази данни, контролни системи и електронно оборудване

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

Учебно съдържание

№	I. ТЕМАТИЧЕН ПЛАН НА ЛЕКЦИИ	ЧАСОВЕ
1.	Компютърни заплахи в морската индустрия. Кибер атаки срещу корабни навигационни системи и атаки върху компютърните мрежи на кораби. Подтеми: Видовете компютърни заплахи: промени в данните на кораба, вкл. неговото местоположение, курс, информация за товара, скорост и име; създаване на „кораби-призраци“, разпознати от други кораби като истински, на всяко място в света; изпращане на невярна метеорологична информация до конкретни кораби, за да променят курса и да избегнат несъществуваща буря; активиране на фалшиви предупреждения за сблъсък за автоматична корекция на курса на плавателния съд; превръщане на съществуващ кораб в „невидим“; фалшифициране на EPIRB (Emergency Position Indicating Radio Beacon) сигнали за активиране на аларми на близките кораби; DoS (Denial of Service) атака чрез увеличаване на честотата на предаване на AIS (Automatic Identification System) съобщения.	3
2.	Защита от кибератаки срещу корабни и пристанищни системи. Технологични и юридически мерки за обезпечаване на киберсигурността. Резолюция MSC.428 (98) Maritime Cyber Risk Management In Safety Management Systems. Препоръки MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management. Система за Управление на Безопасността на Корабите (СУБК). Guidelines on Cyber Security Onboard Ships. Подтеми: 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. Криптографска защита на данните.	4
3.	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.	3

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

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

	Биометрични системи. Биометрични модалности. Проекти – Soli, CIR, Auth0, EarEcho и др.	
	ОБЩО ЧАСОВЕ:	**10**

№	II. ТЕМАТИЧЕН ПЛАН НА УПРАЖНЕНИЯ	ЧАСОВЕ
1.	Използване на защитни стени и антивирусна защита, защита на уеб трафик	2
2.	Резолюция MSC.428 (98) Maritime Cyber Risk Management In Safety Management Systems. Препоръки MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management	2
3.	Система за Управление на Безопасността на Корабите (СУБК). Guidelines on Cyber Security Onboard Ships.	1
	ОБЩО ЧАСОВЕ:	**5**