ПОНЕДЕЛНИК 20.04.2015 г.

Регистрация на участниците и попълване на въпросник за предварителна самооценка Откриване на семинара. Представяне на участниците и целите на обучението.

Информационна и мрежова сигурност в публичния сектор – как да се пазим от хакове и вируси. SPAM и системи за защита от SPAM
Лекция 10:00 - 11:30

Кафе - пауза 11:30–11:45

Основни заплахи и уязвими места на компютърните мрежи и системи
Лекция 11:45–13:15

Обяд 13:15 - 14:00

Методи и средства за защита на информацията в компютърните мрежи и системи
Лекция 14:00 – 15:30

Кафе - пауза 15:30 – 15:45

Инфраструктура на публичния ключ
Лекция 15:45 – 17:15

Обобщение на работата от деня 17:15 - 17:30

ВТОРНИК 21.04.2015 г.

Защитни стени (Firewalls) и системи за откриване на пробиви (англ. Intrusion Detection Systems)
Лекция 10:00 - 11:30

Кафе - пауза 11:30–11:45

Планиране на политиката за мрежова сигурност
Лекция 11:45–13:15

Обяд 13:15 – 14:00

Защита на класифицираната информация в автоматизираните информационни системи и мрежи с технически средства, осигурени срещу паразитни електромагнитни излъчвания
Лекция 14:00 – 15:30

Кафе - пауза 15:30 – 15:45

Защита на критичната инфраструктура (оборудване и съоръжения на АИС и мрежи) от въздействието на електромагнитни импулси
Лекция 15:45 – 17:15

Обобщение на работата от деня. Оценка и закриване на семинара 17:15 - 17:30

Центърът разполага с:

- единадесет съвременно оборудвани учебни зали;
- модерна конферентна зала с възможност за симултанен превод от няколко езика;
- библиотека с читателски места, копирни, компютърни услуги и интернет;
- хотелска част с три корпуса;
- ресторант със сто места и бар;
- тенис на корт;
- тенис на маса;
- билярд;
- дартс;
- баскетболна площадка;
- фитнес зала и сауна.

ЦЕНТЪР ЗА РАЗВИТИЕ НА ЧОВЕШКИТЕ РЕСУРСИ И РЕГИОНАЛНИ ИНИЦИАТИВИ

кв. Кремиковци 1849

телефони: 02/ 994 70 18, 02/ 994 70 38
0882 82 66 74, 0882 82 66 82, 0882 82 66 71

Обучението се осъществява в рамките на Споразумение между Международния обучителен център на МОТ и ЦРЧРРИ



AFS-FF-24-15

Информационна сигурност и системи за нейното управление

семинар, 20 - 21 април 2015 г.
форма на обучение: присъствена

ИНВЕСТИРАМЕ В ХОРАТА

МИНИСТЕРСТВО НА ТРУДА И СОЦИАЛНАТА ПОЛИТИКА
ЦЕНТЪР ЗА РАЗВИТИЕ НА ЧОВЕШКИТЕ РЕСУРСИ И РЕГИОНАЛНИ ИНИЦИАТИВИ

www.chrdri.net

ОБОСНОВКА

Комуникационните мрежи и информационни системи се превърнаха във важен фактор на икономическото и социално развитие на всяко общество. Тяхната сигурност и устойчивост представляват нарастваща грижа на съвременния човек. Наличието на сигурен интернет е важна предпоставка за създаването и на надеждна среда за работа, а от гледна точка на функциониране на съвременната администрация- и неоспорим фактор за нейните бързи и ефективни действия. За да се постигне необходимото ниво на защитеност на информацията, е нужно вниманието да се насочи към качествата на средата за изграждане на съответните знания и умения у специалистите, поддържащи мрежовата и информационна сигурност на различните административни структури. Предвид бързото развитие на технологиите тези знания и умения е необходимо и периодично да се допълват и доразвиват, за да се осигурява адекватен и безкомпромисен контрол на сигурността на информацията в интернет и киберпространството. В този аспект настоящото обучение има надграждащ характер предвид спецификацията на целевата група.

ЦЕЛИ НА ОБУЧЕНИЕТО

• Обогатяване на знанията относно основните заплахи и уязвимите места на компютърните мрежи и системи в публичния сектор;

• Придобиване на експертни знания и умения за защита на автоматизираните информационни системи и мрежи;

• Повишаване на компетентността по отношение на политиката за защита на класифицираната информация и автоматизираните информационни системи и мрежи.

ПРОФИЛ НА УЧАСТНИЦИТЕ

Обучението има надграждащ характер и е предназначено за служители на ръководни и експертни длъжности от МТСП и ВРБ към министъра на труда и социалната политика, работещи в областта на информационната сигурност и системите за нейното управление и които са участвали в обучение по тази тема през 2014 г.

СЪДЪРЖАНИЕ НА ОБУЧЕНИЕТО

В програмата са включени следните теми: Информационна и мрежова сигурност в публичния сектор – как да се пазим от хакове и вируси. SPAM и системи за защита от SPAM; Основни заплахи и уязвими места на компютърните мрежи и системи; Методи и средства за защита на информацията в компютърните мрежи и системи; Инфраструктура на публичния ключ; Защитни стени (Firewall) и системи за откриване на пробиви (Intrusion Detection Systems); Планиране на политиката за мрежова сигурност; Защита на класифицираната информация в автоматизираните информационни системи и мрежи с технически средства, осигурени срещу паразитни електромагнитни излъчвания; Защита на критичната инфраструктура (оборудване и съоръжения на АИС и мрежи) от въздействието на електромагнитни импулси.

МЕТОДИКА НА ПРЕПОДАВАНЕТО

Ще се използват интерактивни и групови методики, акцентиращи върху общуването и диалога в процеса на обучението. Провеждащият обучението ще използва презентации на преподавания материал под формата на експозета, обзори, прегледи на добри практики, процедури, анализи на ситуации, беседи и дискусии и други форми, които провокират интереса и участието на обучаваните в учебните занятия. За по-добро усвояване на теоретичния материал ще се прилага диалоговият режим на комуникация между преподавателя и обучаващите се с оглед адаптиране на теоретичните познания към спецификата на практическата реализация. Учебният материал ще се онагледява със съвременна презентационна техника. След завършване на учебната програма ще се извърши изпитна проверка на придобитите компетенции под различни форми – решаване на практически казуси, дискусия и др. форми съобразно характера на учебния материал и обучаемите.

ЛЕКТОРИ

Лектор на обучението ще бъде доц. д-р Марио Ангелов, хабилитирано лице в Института по отбрана „Проф. Цветан Лазаров”, с натрупан опит и специализация в информационната сигурност, криптографията и кодирането, комуникационните и информационните системи, дългогодишен преподавател във ВУЗ и ЦРЧРРИ.

ОЧАКВАНИ РЕЗУЛТАТИ

Надграждане на знанията и уменията по осигуряването на мрежовата и информационната сигурност, в съответствие с професионалните задължения на обучаемите. В края на обучението участниците ще могат:

• да дефинират основните заплахи и уязвимите места на компютърните мрежи и системи в публичния сектор;

• да планират и реализират адекватен модел на архитектурата за мрежовата и информационната сигурност и системите за нейното управление;

• да избират адекватни методи за защита срещу вредоносен софтуер и кибер атаки;

• да познават процедурите за сигурност на автоматизираните информационни системи и мрежи.

На успешно завършилите семинара ще бъде издаден сертификат.