20261392032

МИНИСТЕРСТВО ЗА ДИГИТАЛНА ТРАНСФОРМАЦИЈА

Врз основа на член 39 став (9) од Законот за безбедност на мрежни и информациски системи (*) („Службен весник на Република Северна Македонија“ бр. 135/25), министерот за дигитална трансформација донесе

ПРОГРАМА ЗА СПЕЦИЈАЛИЗИРАНА ОБУКА НА ОФИЦЕРИ ЗА САЈБЕР БЕЗБЕДНОСТ

I. Обуката е дизајнирана да обезбеди офицерите за сајбер безбедност да стекнат потребни знаења и вештини за ефективно извршување на своите задолжителни задачи, кои опфаќаат разбирање на националните и меѓународните правни рамки, управување со ризик од сајбер безбедноста, спроведување технички операции и обезбедување навремено пријавување на инциденти.

Вкупното проценето времетраење на обуката е: 140 часа.

1. Целна публика

Оваа програма за обука е за сите административни службеници назначени како офицери за сајбер безбедност во институции од јавниот сектор.

2. Модули за обука и наставна програма

Програмата за обука е структурирана во основни и напредни модули, кои ги одразуваат општите и специјалните компетенции потребни за офицер за сајбер безбедност. Секој модул ќе комбинира теоретско знаење со практична примена.

Модул 1: Правна и регулаторна рамка (GRC Foundation)

Времетраење: 15 часа.

Теми:

- Законот за безбедност на мрежни и информатички системи и подзаконските акти кои произлегуваат од овој закон.
- Законот за заштита на лични податоци и Закон за класифицирани информации.
- Вовед во директивите на ЕУ за сајбер безбедност: Директива NIS2 (корпоративна одговорност, управување со ризик, обврски за известување, континуитет на бизнисот).
- Етички и правни предуслови за офицери за сајбер безбедност (доверливост, интегритет, правни забрани).

Резултати од учењето: Разбирање на правниот систем што ја регулира сајбер безбедноста во Република Северна Македонија и релевантните меѓународни акти.

Модул 2: Управување со сајбер безбедност, ризик и усогласеност

Времетраење: 25 часа.

Теми:

- Политики за сајбер безбедност: подготовка и имплементација на политики, процедури и мерки.
- Методологии за проценка на ризик (на пр., ISO 27005, NIST SP 800-30) и дефинирање на ризични сценарија.
- Пропорционалност на безбедносните мерки врз основа на изложеност на ризик и потенцијално влијание.
- Мониторинг на усогласеност, безбедносни ревизии и регулаторни проценки.
- Внатрешни контроли и спроведување на политики.
- Безбедноста на ланецот на снабдување, вклучувајќи проценка на директни добавувачи и даватели на услуги.

Резултати од учењето: Развој, имплементација и управување со сеопфатна рамка на политики за сајбер безбедност, спроведување на ефективни проценки на ризик и обезбедување на усогласеност на работата на институциите со законската рамка.

Модул 3: Технички операции за сајбер безбедност

Времетраење: 30 часа.

Теми:

- Мерки за безбедност на мрежи и информациски системи (физички, технички, организациски мерки).
- Животен циклус на управување со ранливости: идентификација, проценка и отстранување.
- Управување со закрпи и конфигурации.
- Безбедност на податоци и криптографија: политики и процедури за енкрипција.
- Политики за контрола на пристап, вклучувајќи мултифакторска автентикација (МФА) и решенија за континуирана автентикација.
- Принципи на безбеден животен циклус на развој на софтвер.

Резултати од учењето: Примена на основни технички безбедносни мерки, управување со ранливости и имплементирање на безбедни конфигурации во институциите.

Модул 4: Детекција, анализа и одговор на инциденти

Времетраење: 25 часа.

Теми:

- Процедури за справување со инциденти: детекција, анализа, задржување, искоренување, опоравување.
- Анализа на разузнавачки информации и мониторинг на безбедноста (SIEM/SOC операции).
- Собирање и анализа на форензички податоци.
- Задолжителни барања и рокови за пријавување на инциденти.
- Принципи на управување со кризи и системи за итна комуникација.
- Координирани процеси за откривање ранливости.

Резултати од учењето: Ефикасно откривање, анализирање, реагирање и пријавување на сајбер-безбедносни инциденти во согласност со националните и меѓународните стандарди.

Модул 5: Комуникација, координација и свесност

Времетраење: 15 часа.

Теми:

- Внатрешна комуникација со засегнатите страни: известување до раководителите и другите претпоставени.
- Надворешна координација: комуникација со надлежните органи (Министерство за дигитална трансформација, АЕК) и тимовите за одговор на компјутерски инциденти (MKD-GOV-CSIRT, MKD-CIRT).
- Национален екосистем за сајбер безбедност и механизми за споделување информации.
- Развивање и спроведување обуки за свесност за сајбер безбедност за вработените и раководните структури (сајбер хигиена, фишинг, складирање на податоци).
- Прилагодена комуникација за кадар со технички познавања и кадар без технички познавања.

Резултати од учењето: Совладување на ефективни комуникациски стратегии со внатрешни и надворешни засегнати страни во сајбер безбедноста и промовирање на силна безбедносна култура.

Модул 6: Напредни вештини за сајбер безбедност

Времетраење: 30 часа.

Теми:

- Напредна анализа и откривање на сајбер закани: собирање, анализа и интерпретација на разузнавачки информации за сајбер закани и идентификување на изворите на заканите.
- Дигитална форензика и реконструкција на инциденти: Детална форензичка анализа, зачувување на докази и поддршка на кривични истраги.
- Архитектура и дизајн на безбедноста: Планирање и дизајнирање на безбедносни решенија по дизајн и интегрирање на безбедносни контроли од самиот почеток.
- Континуитет на бизнисот и обновување од катастрофи, преку развивање и тестирање на сеопфатни планови, управување со резервни копии и протоколи за управување со кризи.

- Безбедност во „Облак“ и нови технологии: безбедносни импликации, ризици и најдобри практики за работа во „Облак“ и управувани услуги.

- Безбедносна ревизија и тестирање на пенетрација, преку ревизии и пенетрациски тестови, толкување на резултатите и препорачување корективни мерки.

Резултати од учењето: Стекнување на специјализирани вештини за справување со сложени сајбер закани, дизајнирање безбедни системи и обезбедување на отпорност на институцијата.

Вкупно проценето времетраење на обуката: 140 часа.

3. Методологија на обука

Програмата за обука ќе користи комбиниран пристап на учење, комбинирајќи различни методи на настава за максимизирање на ефикасноста:

- Предавања и презентации, одржани од сертифицирани експерти за сајбер безбедност и право поврзано со сајбер безбедноста.

- Интерактивни работилници: Практични вежби, студии на случај и симулации базирани на сценарија за примена на теоретското знаење во практични ситуации.

- Групни дискусии: Олеснување на споделување знаење и решавање проблеми меѓу учесниците.

- Практични лаборатории: Користење виртуелни средини и специјализирани алатки за развој на технички вештини (на пр., скенирање на ранливости, симулации за одговор на инциденти).

- Гости -говорници: Поканување експерти од национални тимови за одговор на компјутерски инциденти, регулаторни тела и научната и стручната јавност, како и приватниот сектор за споделување на реални сознанија.

- Самостојно учење: Зајакнување на концепти и поттикнување континуирано учење.

- Комбинирано учење: Вклучување на онлајн модули и ресурси за флексибилно учење, слично на НАТО програмата за сајбер безбедност.

II. Оваа програма влегува во сила наредниот ден од денот на објавувањето во „Службен весник на Република Северна Македонија”.

Бр. 10-1442/1
23 јуни 2026 година
Скопје

Министер за дигитална
трансформација,
Стефан Андоновски с.р.