МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ЗАГАЛЬНА КОРОТКОСТРОКОВА ПРОГРАМА ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ

«ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ»

Шифр програми ЗК/2023/003

Рік запровадження програми 2023

Програму затверджено:
рішення Вченої ради
Маріупольського державного університету МОН України (м. Київ)
протокол № 8 від 28.04.2023р.

Програму погоджено:
наказ Національного агентства України з питань державної служби від 20.07.2023 № 100-23

ПРОФІЛЬ ПРОГРАМИ

1. Загальна інформація	
Назва програми	Захист інформації в комп'ютерних системах
Шифр програми	ЗК/2023/003
Тип програми за змістом	загальна
Форма навчання	дистанційна
Цільова група	державні службовці категорії «Б»,«В»
Передумови навчання за програмою	
Обсяг програми	1 кредит за ЄКТС
Тривалість програми та організація навчання	тривалість програми становить 1 тиждень. Навчання відбувається п'ять днів з урахуванням запланованих годин для дистанційних занять з доступом до всіх
Мова(и) викладання	державна
Напрям(и) підвищення кваліфікації, який (які) охоплює програма	кібербезпека
Перелік професійних компетентностей, на підвищення рівня яких спрямовано програму	Професійні знання стандартів Європейського Союзу у сфері кібербезпеки та захисту інформації. Професійні знання засад і принципів державної політики у сфері інформаційної безпеки. Вміння використовувати комп'ютерне обладнання та програмне забезпечення, використовувати офісну техніку
Укладач(і) програми	Мартинюк Ганна Вадимівна, доцент, кандидат технічних наук, доцент кафедри системного аналізу та інформаційних технологій МДУ g.martyniuk@mdu.in.ua Політова Анна Сергіївна, доцент, кандидат юридичних наук, доцент кафедри права МДУ a.politova@mdu.in.ua
2. Загальна мета	
формування у слухачів сукупності знань, навичок та вмінь стосовно типових підходів, методів та технологій захисту інформації в комп'ютерних системах під час виконання професійної діяльності	
3. Очікувані результати навчання	
За результатами навчання слухачі повинні демонструвати:	
знання	основних нормативно-правових документів із захисту від несанкціонованого доступу в комп'ютерних системах, моделей загроз та механізмів захисту; принципів кібербезпеки і приватності; методів, принципів і концепцій комунікацій, які підтримують інфраструктуру мережі; управління мережевим доступом, ідентифікацією, та доступом

уміння	застосовувати принципи кібербезпеки і приватності при формуванні вимог організації (стосовно конфіденційності, цілісності, доступності, автентифікації і неспростовності); налаштовувати і використовувати програмні засоби захисту комп'ютерів (наприклад, програмні фільтри, антивірусна програма й антишпигунське ПЗ)
навички	виявлення проблем в захищеності інформації в комп'ютерних системах, в порядку експлуатації, управління та супроводження систем документообігу
4. Викладання та навчання (методи навчання, форми проведення навчальних	
методи навчання: оволодіння знаннями, формування умінь і навичок, застосування здобутих знань, умінь і навичок; пояснювально-ілюстративний, проблемного викладу, частково-пошуковий, виконавський тощо. форми проведення навчальних занять: лекція, семінар, розв'язання ситуаційних та тестових завдань	
5. Ресурсне забезпечення дистанційного навчання	
Назви вебплатформи, вебсайту, електронної системи навчання, через які здійснюватиметься дистанційне навчання із зазначенням посилання (вебадреси)	http://moodle.mdu.in.ua/ _____
Назва дистанційного етапу/модуля	
6. Оцінювання і форми поточного, підсумкового контролю	
Критерії оцінювання та їх питома вага у підсумковій оцінці (%)	Відвідування занять (очно та/або дистанційно в синхронному режимі) -30 % Проходження дистанційного навчання (в асинхронному режимі, у тому числі онлайн-курс) -10 % Опрацювання обов'язкової літератури, інформаційних та інших матеріалів – 5% Поточний контроль – 15% Підсумковий контроль- 40% документ про підвищення кваліфікації видається за умови набрання учасником професійного навчання не менше ніж 75 %, обрахованих з урахуванням
Форма підсумкового контролю	Онлайн тестування

СТРУКТУРА ПРОГРАМИ

Назва теми	Кількість годин				
	загальна кількість годин/ кредитів ЄКТС	у тому числі:			
		аудиторні заняття	дистанційні заняття	навчальні візити	самостійна робота слухачів
1	2	3	4	5	6
Тема 1. Нормативно-правове забезпечення інформаційної безпеки	5 /0,167	-	5	-	0
Тема 2. Основи кібербезпеки державних установ	4 /0,13	-	3	-	1
Тема 3. Захист операційних систем та баз даних	5 /0,17	-	4	-	1
Тема 4. Моделі та механізми захисту інформації	5 /0,17	-	4	-	1
Тема 5. Криптографічні засоби захисту інформації в комп'ютерних системах	10/0,33	-	8	-	2
Підсумковий контроль результатів навчання	1 /0,03	-	-	-	1
РАЗОМ	**30 /1**	-	**24**	-	**6**

ЗМІСТ ПРОГРАМИ

Тема 1. Нормативно-правове забезпечення інформаційної безпеки

Перелік питань для вивчення

- загальна нормативно правова база інформаційної безпеки. Основні поняття та положення;
- спеціалізована нормативно-правова база інформаційної безпеки;
- забезпечення функціонування Національної системи конфіденційного зв'язку;
- міжнародні норми та положення щодо сфери інформатизації і захисту інформатизації.

Форми проведення навчальних занять та методи навчання: лекція, тренінг, практична робота, тематична дискусія, вебінар, аналіз ситуацій та розв'язання ситуаційних завдань.

Тема 2. Основи кібербезпеки державних установ

Перелік питань для вивчення

- поняття конфіденційності, цілісності та доступності;
- співвідношення понять інформаційна безпека та кібербезпека;
- протидія загрозам безпеки з боку персоналу;
- особливості застосування систем та технологій захищеного документообігу.

Форми проведення навчальних занять та методи навчання: лекція, тренінг, практична робота, тематична дискусія, вебінар, аналіз ситуацій та розв'язання ситуаційних завдань.

Самостійна робота учасників професійного навчання:

- розробка організаційного плану реагування на інцидент;

- чек лист для спеціалістів, що займаються подоланням інциденту.

Тема 3. Захист операційних систем та баз даних

Перелік питань для вивчення:

- безпека клієнтських операційних систем;
- безпека серверних операційних систем;
- апаратні та програмні засоби захисту баз даних.

Форми проведення навчальних занять та методи навчання: лекція, тренінг, практична робота, тематична дискусія, вебінар, аналіз ситуацій та розв'язання ситуаційних завдань.

Самостійна робота учасників професійного навчання:

- кібербезпека операційних технологій;
- ключові аспекти захисту для критичної інфраструктури.

Тема 4. Моделі та механізми захисту інформації

Перелік питань для вивчення:

- термінологія та зміст основних понять моделювання кібербезпеки;
- методи структурної ідентифікації об'єктів і процесів, поточного стану кібербезпеки;
- моделювання можливих сценаріїв кібератак на підприємство.

Форми проведення навчальних занять та методи навчання: лекція, тренінг, практична робота, тематична дискусія, вебінар, аналіз ситуацій та розв'язання ситуаційних завдань.

Самостійна робота учасників професійного навчання:

- розробка наступальної програми з кібербезпеки для завчасного виявлення та усунення вразливих місць у системі захисту.

Тема 5. Криптографічні засоби захисту інформації в комп'ютерних системах

Перелік питань для вивчення:

- симетричні криптосистеми;
- асиметричні криптосистеми;
- криптоаналіз алгоритмів шифрування;
- криптографічне гешування;
- проблема ідентифікації та аутентифікації;
- принципи генерації, розподілу та збереження ключів;
- сучасні криптографічні механізми та протоколи.

Форми проведення навчальних занять та методи навчання: лекція, тренінг, практична робота, тематична дискусія, вебінар, аналіз ситуацій та розв'язання ситуаційних завдань.

Самостійна робота учасників професійного навчання:

- можливості квантової криптографії;
- постквантова криптографія.

ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Оцінювання результатів навчання здійснюється шляхом поточного та підсумкового контролю.

Поточний контроль здійснюється у формі тестування, розв'язання ситуаційного завдання, письмових відповідей на запитання. Підсумковий контроль здійснюється у формі підсумкового тестування.

ЛІТЕРАТУРА, ІНФОРМАЦІЙНІ РЕСУРСИ, ОБОВ'ЯЗКОВІ ДЛЯ ОПРАЦЮВАННЯ. ПЕРЕЛІК НОРМАТИВНО-ПРАВОВИХ АКТІВ

Література та інші інформаційні ресурси

1. Гапак О.М. Захист інформації в комп'ютерних системах: підручник / О.М. Гапак, С.І. Балога. – Ужгород: ДВНЗ «УжНУ», 2021. – 184 с.
2. Остапов С.Е., Євсеєв С.П. , Король О.Г. Кібербезпека: сучасні технології захисту. – Х.: «Новий світ-2000», 2020. – 678 с.
3. Вишня В. Б. Основи інформаційної безпеки : навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. – 128 с.

Інформаційні ресурси

4. https://cert.gov.ua/ - Новини про кіберінциденти та їх усунення.
5. https://tzi.com.ua/normatbazaukr.html - Нормативна база України в сфері технічного захисту інформації
6. https://tzi.com.ua/downloads/1.1-002-99.pdf - НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

Перелік нормативно-правових актів

1. Закон України "Про інформацію".
2. Закон України "Про державну таємницю".
3. Закон України "Про захист персональних даних".
4. Закон України "Про основні засади забезпечення кібербезпеки України".
5. Закон України "Про захист інформації в інформаційно-комунікаційних системах".