УКРАЇНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
імені МИХАЙЛА ДРАГОМАНОВА

ЗАГАЛЬНА КОРОТКОСТРОКОВА ПРОГРАМА ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ «ІНФОРМАЦІЙНА БЕЗПЕКА»

Шифр програми: ЗК/2025/004
Рік запровадження програми: 2025
Програму затверджено: засідання Вченої ради УДУ імені Михайла Драгоманова, протокол № від
Програму погоджено: Наказ НАДС№

ПРОФІЛЬ ПРОГРАМИ

1. Загальна інформація	
Назва програми	Інформаційна безпека
Шифр програми	ЗК/2025/004
Тип програми за змістом	загальна короткострокова програма підвищення кваліфікації
Форма (и) навчання	дистанційна (в асинхронному та синхронному режимах)
Цільова група	державні службовці категорії посад «Б» і «В» і посадові особи місцевого самоврядування, посади яких віднесені до першої-четвертої категорії посад
Передумови навчання за програмою	– базові знання з інформатики; – навички роботи за комп'ютером, зокрема обізнаність з операційними системами та мережевими технологіями
Найменування замовника освітніх послуг у сфері професійного навчання за програмою	Національне агентство України з питань державної служби
Найменування партнера (партнерів) програми	-
Обсяг програми	1 кредити ЄКТС (30 год.)
Тривалість програми та організація навчання	загальна тривалість програми – 10 робочих днів. організація (режим) навчання – вечірній час, після завершення робочого дня
Мова (и) викладання	українська мова
Напрям (и) підвищення кваліфікації, який (які) охоплює програма	Інформаційна безпека
Перелік професійних компетентностей, на підвищення рівня яких спрямовано програму	– здатність аналізувати інформаційні потоки, виявляти загрози та оцінювати ризики; – навички оцінювання безпеки IT-систем, виявлення вразливостей та прийняття оптимальних рішень; – ефективна взаємодія з фахівцями у сфері інформаційних технологій та безпеки; – здатність до навчання новим технологіям та методам кіберзахисту. – виявлення, аналіз і мінімізація загроз інформаційній безпеці; – організація та підтримка заходів з інформаційної безпеки; – розроблення та впровадження політик безпеки для організацій;

	– використання методів шифрування, цифрового підпису, управління ключами; – конфігурація та управління міжмережевими екранами, VPN, IDS/IPS; – аналіз мережевого трафіку, виявлення вторгнень та аномалій; – розуміння правових аспектів захисту даних та відповідальності за порушення кібербезпеки.
Укладач (і) програми	Франчук Наталія Петрівна – кандидат педагогічних наук, доцент, доцент кафедри інформаційних технологій і програмування Українського державного університету імені Михайла Драгоманова; – старший дослідник, старший науковий співробітник відділу відкритих освітньо-наукових інформаційних систем Інституту цифровізації освіти Національної академії педагогічних наук України. n.p.franchuk@udu.edu.ua
2. Загальна мета	
Програма спрямована на формування, розвиток та вдосконалення професійних компетентностей у сфері інформаційної безпеки відповідно до вимог державного управління, забезпечення кіберзахисту та дотримання правових норм у цифровому середовищі. *Навчальна мета* – забезпечити слухачів фундаментальними знаннями та практичними навичками щодо організації інформаційної безпеки, управління ризиками, захисту державних інформаційних ресурсів, реагування на кіберінциденти та впровадження сучасних засобів захисту. *Виховна мета* – формувати відповідальне ставлення до дотримання норм інформаційної безпеки, кіберетики, конфіденційності та правових аспектів роботи з даними, розвивати культуру інформаційної гігієни та цифрової відповідальності. *Розвивальна мета* – сприяти розвитку критичного мислення, навичок аналізу кіберзагроз, оперативного прийняття рішень у сфері інформаційної безпеки, здатності до адаптації в умовах цифрової трансформації державного управління. Програма забезпечує підготовку державних службовців до ефективного виконання функцій із забезпечення інформаційної безпеки в органах влади та місцевого самоврядування, що сприяє зміцненню національної кібербезпеки та захисту державних даних.	
3. Очікувані результати навчання	
За результатами навчання слухачі повинні демонструвати:	
знання	– описувати ключові поняття, принципи, стандарти та нормативно-правові акти у сфері інформаційної безпеки; – розуміти основи управління інформаційними ризиками, загрозами та вразливостями;

	– оцінювати рівень безпеки інформаційних систем органів державної влади та місцевого самоврядування; – методи криптографічного захисту даних, зокрема шифрування, цифровий підпис та управління ключами; – принципів цифрового розвитку державної політики; – політики інформаційної безпеки та вимоги до захисту даних в державному секторі.
уміння	– оцінювати рівень інформаційної безпеки в державних установах та виявляти потенційні загрози; – використовувати сучасні засоби кіберзахисту (антивірусні програми, системи моніторингу трафіку, міжмережеві екрани, VPN); – реагувати на кіберінциденти, проводити базовий аналіз атак і розробляти заходи щодо їх нейтралізації; – розробляти та впроваджувати політики безпеки в органах державної влади та місцевого самоврядування; – проводити навчання співробітників щодо правил інформаційної безпеки та цифрової гігієни.
навички	– використання методів багатофакторної автентифікації та управління доступом; – налаштування та адміністрування безпечного середовища IT-інфраструктури; – виявлення вразливостей у комп’ютерних мережах та оцінка їх впливу; – аналіз цифрових слідів та розслідування кіберінцидентів; – дотримання правових та етичних норм у сфері кібербезпеки.
4. Викладання та навчання (методи навчання, форми проведення навчальних занять)	
Навчальний процес організовується у дистанційній формі з використанням *синхронного* (онлайн-зустрічі в реальному часі) та *асинхронного* (самостійне навчання) режимів. ***1. Методи навчання:*** – інформаційно-репродуктивний метод – подання навчального матеріалу через відеолекції, електронні підручники, презентації; – проблемно-орієнтоване навчання – аналіз реальних кейсів із кібербезпеки, розв’язування практичних задач;	

– проєктний метод – виконання групових або індивідуальних проєктів (розроблення політики безпеки, аналіз кіберзагроз тощо);
– метод моделювання – використання спеціалізованих програм для моделювання кіберзагроз, аналізу мережевого трафіку;
– методи інтерактивного навчання – робота в групах, дискусії, рольові ігри;
– гейміфікація – використання тестів, симуляцій, змагальних завдань у вигляді кібер-квестів.

2. Форми проведення навчальних занять

Синхронні форми (режим реального часу)

– Відеолекції та вебінари – інтерактивні заняття в Zoom, Google Meet, Microsoft Teams із можливістю ставити запитання та обговорювати теми.
– Практичні заняття – онлайн-демонстрації використання інструментів кібербезпеки, аналізу атак, тестування систем.
– Дискусії та круглі столи – обговорення реальних кейсів кібербезпеки в державному секторі.
– Консультації з викладачем – індивідуальні або групові зустрічі для відповідей на запитання та роз'яснень складних тем.

Асинхронні форми (самостійне навчання)

– Відеолекції та навчальні матеріали – записані лекції, підручники, презентації, які слухачі можуть переглядати у зручний час.
– Онлайн-курси та тренажери – курси на платформах Coursera, Cisco Networking Academy, Udemy.
– Тестування та самоперевірка – проходження онлайн-тестів для закріплення знань.
– Форуми та обговорення – асинхронні дискусії у Google Classroom, Moodle, корпоративних чатах.
– Індивідуальні та групові завдання – виконання практичних робіт із розроблення політик безпеки, аналізу атак тощо.

Гнучке поєднання синхронних та асинхронних методів дозволяє адаптувати навчання під потреби слухачів, підвищуючи ефективність засвоєння матеріалу та практичну спрямованість програми.

5. Ресурсне забезпечення дистанційного навчання	
Назви вебплатформи, вебсайту, електронної системи навчання, через які здійснюватиметься дистанційне навчання із зазначенням посилання (веб-адреси)	Google Classroom Google Meet
Назва дистанційного етапу/модуля	Усі теми

6. Оцінювання і форми поточного, підсумкового контролю	
Критерії оцінювання та їх питома вага у підсумковій оцінці (%)	Проходження дистанційного навчання – 40 % Самостійна робота, що містить опрацювання обов'язкової літератури, інформаційних та інших матеріалів – 10 % Поточний контроль – 20 % Підсумковий контроль – 30 % Документ про підвищення кваліфікації видається за умови, якщо слухач набрав не менше 75 % та за умови успішного проходження підсумкового контролю.
Форма підсумкового контролю	Комп'ютерне 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. Основи інформаційної безпеки	3	-	2	-	1
Тема 2. Загрози та вразливості інформаційних систем	3		2		1
Тема 3. Захист персональних та конфіденційної даних	3	-	2	-	1
Тема 4. Криптографічні методи захисту даних	3	-	2	-	2
Тема 5. Управління доступом та автентифікація	3	-	2	-	1
Тема 6. Захист інформаційних систем та мереж	3	-	2	-	1
Тема 7. Кібергігієна та цифрова грамотність державних службовців	3	-	2	-	1
Тема 8. Політики інформаційної безпеки в державних установах	3	-	2	-	1
Тема 9. Реагування на кіберінциденти та кризовий менеджмент	3	-	2	-	1
Підсумковий контроль результатів навчання	2	-	2	-	-
РАЗОМ	30/1	-	20	-	10

ЗМІСТ ПРОГРАМИ

Тема 1. Основи інформаційної безпеки

Визначення інформаційної безпеки, її принципи та роль у державному управлінні.

Законодавче та нормативне регулювання у сфері кібербезпеки.

Перелік питань, які виносяться на самостійну роботу учасників професійного навчання:

1. Що таке інформаційна безпека? Які її основні цілі?
2. Які існують основні загрози інформаційній безпеці?
3. Які міжнародні стандарти та нормативні документи регулюють інформаційну безпеку?

Тема 2. Загрози та вразливості інформаційних систем

Загрози інформаційній безпеці держави та їх класифікація.

Основні елементи системи державного управління цифровим розвитком.

Види кіберзагроз (шкідливе ПЗ, фішинг, DDoS-атаки, соціальна інженерія).

Методи виявлення та нейтралізації загроз.

Перелік питань, які виносяться на самостійну роботу учасників професійного навчання:

1. Які основні види кіберзагроз сьогодні?
2. Що таке соціальна інженерія? Які методи вибірки зловмисників?
3. Які основні вразливості можуть бути в програмному забезпеченні?

Тема 3. Захист персональних та конфіденційної даних

Основні принципи захисту персональних даних. Закон України «Про захист персональних даних».

Технічні та організаційні заходи захисту даних.

Перелік питань, які виносяться на самостійну роботу учасників професійного навчання:

1. Які основні положення Закону України «Про захист персональних даних»?
2. Які методи використовують для захисту конфіденційних даних?
3. Які вимоги до зберігання та опрацювання персональних даних у державних установах?

Тема 4. Криптографічні методи захисту даних

Основи шифрування, електронний цифровий підпис, управління ключами.

Практичне використання криптографічних технологій.

Перелік питань, які виносяться на самостійну роботу учасників професійного навчання:

1. Які основні методи шифрування даних?
2. У чому відмінність між симетричними та асиметричними шифруванням?
3. Що таке цифровий підпис і як він працює?

Тема 5. Управління доступом та автентифікація

Методи автентифікації (двофакторна, біометрична, рольова модель доступу).

Адміністрування доступу до інформаційних систем у державних органах.

Електронні послуги.

Електронний документообіг.

Електронна ідентифікація.

Електронна демократія.

Портал державних послуг Дія.

Мобільний за стосунок Дія.

Перелік питань, які виносяться на самостійну роботу учасників професійного навчання:

1. Які основні моделі управління доступом до комп’ютера?
2. Що таке двофакторна автентифікація? Які її переваги?
3. Як працює рольова модель доступу?

Тема 6. Захист інформаційних систем та мереж

Використання антивірусного ПЗ, міжмережевих екранів, VPN, IDS/IPS.

Аналіз та моніторинг безпеки мережевого трафіку.

Обмеження доступу до даних з обмеженим доступом.

Перелік питань, які виносяться на самостійну роботу учасників професійного навчання:

1. Які основні заходи захисту інформаційних систем?
2. Як працювати міжмережеві екрани (Firewall)?
3. Що таке VPN і як він забезпечує безпеку даних?

Тема 7. Кібергігієна та цифрова грамотність державних службовців

Основи безпечної поведінки в цифровому середовищі.

Практичні поради щодо захисту особистих та робочих акаунтів.

Шкідливе програмне забезпечення (комп’ютерні віруси та програми-шпигуни).

Антивірусні програми.

Архівування та резервне копіювання даних.

Перелік питань, які виносяться на самостійну роботу учасників професійного навчання:

1. Які основні правила кібергігієни потрібно виконувати в державних установах?
2. Як захистити свої акаунти та паролі?
3. Які ознаки фішингових атак?

Тема 8. Політики інформаційної безпеки в державних установах

Розробка внутрішніх регламентів та процедур інформаційної безпеки.

Організація навчання співробітників із питань кібербезпеки.

Перелік питань, які виносяться на самостійну роботу учасників професійного навчання:

1. Які основні елементи політики інформаційної безпеки?
2. Як проводиться аудит інформаційної безпеки?
3. Які вимоги до навчання персоналу з питань кібербезпеки?

Тема 9. Реагування на кіберінциденти та кризовий менеджмент

Алгоритми дій у разі кібератаки.

Планування та реалізація заходів з відновлення після атак.

Перелік питань, які виносяться на самостійну роботу учасників професійного навчання:

1. Як діяти у випадку виявлення кібератаки?
2. Що таке план реагування на інциденти?
3. Які заходи слід вжити після усунення кіберзагрози?

ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

– теоретичні запитання щодо знання правових основ та законодавства України в галузі інформаційної безпеки – 40 %;

– самостійна робота, що містить опрацювання обов’язкової літератури, інформаційних та інших матеріалів – 10 %

– завдання до практичних робіт щодо дотримання вимог до захисту, здійснення опрацювання та управління інформацією в інформаційно-комунікаційних системах – 20 %;

– комплексний тестовий контроль оцінювання готовності здійснювати опрацювання, критичного аналізу та збереження цілісності даних у професійній діяльності – 30 %.

Форма підсумкового контролю: комп'ютерне тестування.

ЛІТЕРАТУРА, ІНФОРМАЦІЙНІ РЕСУРСИ, ОБОВ'ЯЗКОВІ ДЛЯ ОПРАЦЮВАННЯ

Закони, нормативно-правові акти та документи

1. Про інформацію: Закони України від 02.10.1992, № 2658-XII (2658-12). Дата оновлення: 23.06.2005 № 2707-IV (2707-15). URL: https://msu.edu.ua/library/wp-content/uploads/2017/05/4.-zakon-u.-pro-informaciju.pdf

2. Про державну таємницю: Закони України від 21.01.1994 № 3856-XII. Дата оновлення: 10.10.2024 № 4019-IX}. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text

3. Про захист інформації в автоматизованих системах: Закони України від 05.07.1994 року № 81/94-ВР. Дата оновлення: 05.06.2024 № 3783-IX. URL: http://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

4. Про науково-технічну інформацію: Закони України від 25.06.1993, № 3323-XII. Дата оновлення: 27.03.2014 № 1170-VII. URL: https://zakon.rada.gov.ua/laws/show/3322-12#Text

5. Про захист персональних даних: Закони України від 01.06.2010 № 2297-VI. Дата оновлення: від 19.12.2024 № 4170-IX. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

6. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=69172

7. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=69173

8. Нормативний документ системи технічного захисту інформації. Загальні положення захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 1.1.-002-99. ДСТСЗІ СБ України. Київ. 21 с. URL: https://tzi.com.ua/downloads/1.1-002-99.pdf

9. Нормативний документ системи технічного захисту інформації. Критерії оцінки захищеності інформації в комп`ютерних системах від несанкціонованого доступу. НД ТЗІ 2.5.-004-99. ДСТСЗІ СБ України. Київ. 60 с. URL: https://tzi.com.ua/downloads/2.5-004-99.pdf

10. Концепція інформаційної безпеки України. URL: https://www.osce.org/files/f/documents/0/2/175056.pdf

Література

1. Смалько О.А. Захист інформаційних ресурсів: Монографія. Кам'янець-Подільський: ПП Буйницький О А, 2011. 704 с.

2. Богуш В.М., Кудін А.М. Інформаційна безпека від А до Я. Київ: МОУ, 2012.

3. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем. Київ: Видавнича група BHV, 2009.

4. Конахович Г.Ф., Климчук В.П., Паук С.М., Потапов В.Г. Защитаинформации в телекоммуникационных системах. Київ: «МК-Пресс», 2005. – 288 с.

5. Франчук В.М. Захист інформаційних ресурсів. Київ: Редакції газет природничо-математичного циклу, 2012. 112 с. (Бібліотека "Шкільного світу").

6. Управління інформаційною безпекою. URL: https://www.scribd.com/document/650227679/6-Управління-інформаційною-безпекою

7. Новини комітетів - Створюйте ШІ-продукти з безпекою для людей, - Комітет з питань цифрової трансформації - Офіційний портал Верховної Ради України. URL: https://www.rada.gov.ua/news/news_kom/258663.html

Онлайн-курси, тренажери та безоплатні платформи для самоосвіти

1. Цифровізація державного сектору. URL: https://osvita.diia.gov.ua/courses/digitalisation-in-public-sector

2. Відкриті дані для державних службовців. URL: https://osvita.diia.gov.ua/courses/open-data

3. Доступ до публічної інформації. URL: https://osvita.diia.gov.ua/courses/access-to-public-information

4. Як діяти далі: Державним службовцям про сталий розвиток. URL: https://courses.prometheus.org.ua/courses/course-v1:Prometheus+SDG101+2020_T2/about

5. Європейська зовнішня політика: просто про складне. URL: https://courses.prometheus.org.ua/courses/course-v1:Prometheus+EUFP101+2019_T3/about

6. Основи державної політики. URL: https://courses.prometheus.org.ua/courses/Prometheus/GOV101/2015_T2/about

7. Взаємодія органів державної влади з громадськістю. URL: https://courses.prometheus.org.ua/courses/course-v1:Prometheus+IAP101+2019_T3/about

8. Децентралізація: від патерналізму до відповідального розвитку. URL: https://courses.prometheus.org.ua/courses/course-v1:Prometheus+DC101+2019_T3/about

9. Децентралізація в Україні – теорія та практика. URL: https://courses.prometheus.org.ua/courses/course-v1:Prometheus+DC101+2017_T4/about

10. Захист прав людей з інвалідністю. URL:

https://courses.prometheus.org.ua/courses/course-v1:FFR+PRPD101+2020_T1/about

11. Ефективний бюджетний процес в органах місцевого самоврядування. URL: https://courses.prometheus.org.ua/courses/course-v1:AMU+BP_101+2017_T1/about

12. Ґендерно орієнтоване бюджетування для розвитку громад. URL: https://courses.prometheus.org.ua/courses/course-v1:AMU+GOB101+2018_T3/about

13. Публічні закупівлі https://courses.prometheus.org.ua/courses/course-v1:Prometheus+PP101+2018_T3/about

14. Основи інформаційної безпеки. URL: https://courses.prometheus.org.ua/courses/KPI/IS101/2014_T1/about

15. Цифрові комунікації в глобальному просторі. URL: https://courses.prometheus.org.ua/courses/course-v1:Prometheus+ITArts101+2017_T1/about

16. Цифрова грамотність державних службовців 1.0. на базі інструментів Google. URL: https://osvita.diia.gov.ua/courses/civil-servants