ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАГАЛЬНА КОРОТКОСТРОКОВА ПРОГРАМА ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ

Кібербезпека
(назва програми)

Шифр програми ЗК/2026/008

Рік запровадження програми 2026 р.

Програму затверджено Вченою радою Поліського національного університету 25.06.2025 р., протокол № 11

Програму погоджено: наказ НАДС від 08 вересня 2026 року № 119-26

Профіль програми

1. Загальна інформація	
Назва програми	Кібербезпека
Шифр програми	ЗК/2026/008
Тип програми за змістом	Загальна короткострокова програма
Відомості про акредитацію для загальної професійної (сертифікатної) програми	
Форма(и) навчання	Дистанційна, Очна (денна)
Цільова група	Категорії посад державної служби: Б, В Категорії посад в органах місцевого самоврядування: I, II, III, IV, V, VI, VII
Найменування замовника освітніх послуг у сфері професійного навчання за програмою	
Найменування партнера (партнерів) програми	
Обсяг програми	1.0
Тривалість програми та організація навчання	5 днів протягом 1 тижня
Мова(и) викладання	українська
Напрям(и) підвищення кваліфікації, який (які) охоплює програма	Кібербезпека (кібербезпека та кіберзахист)
Перелік професійних компетентностей, на підвищення рівня яких спрямовано програму	Знання законодавства у сфері забезпечення кібербезпеки, захисту інформації та персональних даних, у тому числі Закону України «Про основні засади забезпечення кібербезпеки України», Закону України «Про захист інформації в інформаційно-комунікаційних системах», Закону України «Про захист персональних даних»; Професійні знання щодо організації базових заходів кіберзахисту, запобігання кіберзагрозам та реагування на кіберінциденти; Робота з інформацією, Цифрова грамотність
Укладач(і) програми (для типових загальних програм - найменування розробника(ів) програми)	Якобчук Валентина Павлівна, кандидат економічних наук, професор, завідувач кафедри економічної теорії, інтелектуальної власності та публічного управління Поліського національного університету, e-mail valentyna.iakobchuk@gmail.com Іванюк Ольга Володимирівна, кандидат економічних наук, доцент, доцент кафедри економічної теорії, інтелектуальної власності та публічного управління Поліського національного університету, e-mail olha.ivanuk@gmail.com

2. Загальна мета	
Розвиток професійних компетентностей державних службовців та посадових осіб місцевого самоврядування щодо застосування законодавства України у сфері забезпечення кібербезпеки та захисту інформації, формування практичних навичок безпечного використання інформаційно-комунікаційних систем, електронних комунікацій, державних інформаційних ресурсів, захисту персональних даних, а також здійснення першочергових дій під час виявлення кіберінцидентів відповідно до вимог законодавства України.	
3. Очікувані результати навчання	
За результатами навчання слухачі повинні демонструвати:	
Знання	- законодавства України у сфері забезпечення кібербезпеки, захисту інформації та персональних даних; - основних понять у сфері кібербезпеки, кіберзахисту, кіберзагроз та кіберінцидентів; - типових способів здійснення кібератак (фішинг, шкідливе програмне забезпечення, соціальна інженерія, атаки на облікові записи тощо); - базових заходів кіберзахисту інформаційно-комунікаційних систем; - порядку реагування працівниківна кіберінциденти відповідно до вимог законодавства та внутрішніх документів установи; - вимог щодо захисту персональних даних під час виконання службових повноважень.
Уміння	- визначати ознаки потенційних кіберзагроз та кіберінцидентів; - розпізнавати фішингові повідомлення, підроблені вебресурси, спроби соціальної інженерії та інші поширені способи компрометації інформації; - безпечно використовувати електронну пошту, вебресурси, мобільні пристрої та засоби дистанційної роботи; - застосовувати базові заходи кіберзахисту під час роботи з інформаційними ресурсами установи; - діяти відповідно до визначених процедур у разі виявлення кіберінциденту або ознак порушення інформаційної безпеки.
Навички	- створення та використання надійних паролів і багатофакторної автентифікації; - безпечного використання службових облікових записів; - роботи з інформацією з дотриманням вимог конфіденційності, цілісності та доступності; - повідомлення відповідальних осіб про кіберінциденти відповідно до встановлених процедур; - застосування базових заходів кіберзахисту на робочому місці.

4. Викладання та навчання (методи навчання, форми проведення навчальних занять)	
Навчання здійснюється у формі лекцій, лекцій-презентацій, практичних і лабораторних занять, тренінгів, семінарів, дискусій, моделювання кіберінцидентів, виконання практичних робіт із використанням спеціалізованого програмного забезпечення та самостійної роботи. Освітній процес передбачає виконання індивідуальних і групових практичних завдань, аналіз кейсів у сфері кібербезпеки, опрацювання нормативно-правових актів, міжнародних стандартів і рекомендацій з інформаційної та кібербезпеки, використання сучасних цифрових інструментів, віртуальних лабораторій, засобів моніторингу, аналізу мережевого трафіку, виявлення та реагування на кіберзагрози.	
5. Ресурсне забезпечення дистанційного навчання	
Назви вебплатформи, вебсайту, електронної системи навчання, через які здійснюватиметься таке навчання, посилання (вебадреса)	В ході навчання використовуються такі веб платформи: Цифрові інструменти Google (Google Classroom, Google Форми); Moodlle (http://moodle.znau.edu.ua), Платформа для організації відеоконференцій Zoom. Доступ до вебкабінету відеоконференції надається учасникам професійного навчання після реєстрації.
Назва дистанційного курсу (модуля)	Кібербезпека
6. Оцінювання і форми поточного, підсумкового контролю	
Складові оцінювання та їх питома вага у підсумковій оцінці (%)	Відвідування занять очно та / або дистанційно в синхронному режимі з вчасним виконанням всіх завдань передбачених програмою оцінюється у 70 балів (питома вага у підсумковій оцінці 70 %). Відвідування занять очно та / або дистанційно в асинхронному режимі з виконанням всіх завдань з порушенням термінів виконання, але в часових межах програми оцінюється у 45 балів (питома вага у підсумковій оцінці 45 %). Підсумковий контроль у формі письмового онлайн тестування оцінюється у 30 балів (питома вага у підсумковій оцінці 30 %). Документ про підвищення кваліфікації видається за умови набрання учасником професійного навчання не менше ніж 75 балів (за максимально можливих 100 балів), або 75 %, обрахованих з урахуванням питомої ваги кожного із критеріїв оцінювання та за умови успішного проходження підсумкового контролю.
Форма та періодичність поточного контролю	
Форма підсумкового контролю	Комп'ютерне тестування у онлайн форматі, що передбачає понад 50 % правильних відповідей

СТРУКТУРА ПРОГРАМИ
(Дистанційна)

Назва теми	Кількість годин				
		у тому числі:			
	загальна кількість годин / кредитів ЄКТС за модулем	аудиторні заняття	дистанційні заняття	навчальні візити	самостійна робота
1	2	3	4	5	6
Тема 1. Типові кіберзагрози, кібератаки та кіберінциденти	2		2		
Тема 2. Захист інформаційно-комунікаційних систем та державних інформаційних ресурсів	3		2		1
Тема 3. Безпечне використання електронної пошти та мережі Інтернет	3		2		1
Тема 4. Безпечне використання мобільних пристроїв та засобів дистанційної роботи	2		2		
Тема 5. Дії державного службовця щодо забезпечення кібербезпеки	5		4		1
Тема 6. Захист персональних даних та службової інформації	2		2		
Тема 7. Автентифікація, управління доступом та парольна безпека	3		2		1
Тема 8. Реагування на кіберінциденти	3		2		1
Тема 9. Організація базових заходів кіберзахисту в державних органах	2		2		
Тема 10. Законодавчі та організаційні засади забезпечення кібербезпеки	3		2		1
Підсумковий контроль результатів навчання	**2**		**2**		**0**
РАЗОМ	**30 / 1,00**		**24**		**6**

СТРУКТУРА ПРОГРАМИ

(Очна (денна))

Назва теми	Кількість годин				
		у тому числі:			
	загальна кількість годин / кредитів ЄКТС за модулем	аудиторні заняття	дистанційні заняття	навчальні візити	самостійна робота
1	2	3	4	5	6
Тема 1. Типові кіберзагрози, кібератаки та кіберінциденти	2	2			
Тема 2. Захист інформаційно-комунікаційних систем та державних інформаційних ресурсів	3	2			1
Тема 3. Безпечне використання електронної пошти та мережі Інтернет	3	2			1
Тема 4. Безпечне використання мобільних пристроїв та засобів дистанційної роботи	2	2			
Тема 5. Дії державного службовця щодо забезпечення кібербезпеки	5	4			1
Тема 6. Захист персональних даних та службової інформації	2	2			
Тема 7. Автентифікація, управління доступом та парольна безпека	3	2			1
Тема 8. Реагування на кіберінциденти	3	2			1
Тема 9. Організація базових заходів кіберзахисту в державних органах	2	2			
Тема 10. Законодавчі та організаційні засади забезпечення кібербезпеки	3	2			1
Підсумковий контроль результатів навчання	**2**	**2**			
РАЗОМ	**30 / 1,00**	24			6

ЗМІСТ ПРОГРАМИ

Тема 1. Типові кіберзагрози, кібератаки та кіберінциденти

Основні види кіберзагроз для державних органів. Соціальна інженерія, фішинг, шкідливе програмне забезпечення, компрометація облікових записів. Категорії кіберінцидентів відповідно до Методичних рекомендацій, затверджених наказом Адміністрації Держспецзв'язку № 570. Первинні дії користувача у разі виявлення ознак кіберінциденту.

Форма проведення навчальних занять та методи навчання, які дозволяють розкрити зміст теми: лекція, наочний метод (метод ілюстрацій і метод демонстрацій), практичний тренінг, дискусія, самостійна робота (частково-пошуковий; дослідницький).

Тема 2. Захист інформаційно-комунікаційних систем та державних інформаційних ресурсів

Основні вимоги до захисту інформації в інформаційно-комунікаційних системах. Базові принципи кіберзахисту державних інформаційних ресурсів. Контроль доступу та захист інформації від несанкціонованого доступу. Організація безпечної роботи з державними інформаційними ресурсами.

Форма проведення навчальних занять та методи навчання, які дозволяють розкрити зміст теми: лекція, наочний метод (метод ілюстрацій і метод демонстрацій), практичний тренінг, дискусія, самостійна робота (частково-пошуковий; дослідницький).

Перелік питань, які виносяться на самостійну роботу учасників професійного навчання: огляд сучасних засобів захисту інформації.

Тема 3. Безпечне використання електронної пошти та мережі Інтернет

Основні загрози під час використання електронної пошти. Ознаки фішингових повідомлень. Безпечне використання вебресурсів. Правила роботи з електронними вкладеннями та посиланнями.

Форма проведення навчальних занять та методи навчання, які дозволяють розкрити зміст теми: лекція, наочний метод (метод ілюстрацій і метод демонстрацій), практичний тренінг, дискусія, самостійна робота (частково-пошуковий; дослідницький)

Перелік питань, які виносяться на самостійну роботу учасників професійного навчання: аналіз прикладів фішингових повідомлень.

Тема 4. Безпечне використання мобільних пристроїв та засобів дистанційної роботи

Загрози під час використання мобільних пристроїв. Захист службової інформації під час дистанційної роботи. Безпечне використання месенджерів та

хмарних сервісів. Захист мобільних пристроїв від несанкціонованого доступу.

Форма проведення навчальних занять та методи навчання, які дозволяють розкрити зміст теми: лекція, наочний метод (метод ілюстрацій і метод демонстрацій), практичний тренінг, дискусія, самостійна робота (частково-пошуковий; дослідницький)

Тема 5. Дії державного службовця щодо забезпечення кібербезпеки

Обов'язки працівників щодо дотримання вимог кібербезпеки. Базові заходи кіберзахисту на робочому місці. Взаємодія з відповідальними особами та підрозділами з питань кібербезпеки. Алгоритм дій працівника під час виникнення кіберінциденту.

Форма проведення навчальних занять та методи навчання, які дозволяють розкрити зміст теми: лекція, наочний метод (метод ілюстрацій і метод демонстрацій), практичний тренінг, дискусія, самостійна робота (частково-пошуковий; дослідницький)

Перелік питань, які виносяться на самостійну роботу учасників професійного навчання: ознайомлення з Методичними рекомендаціями, затвердженими наказом Адміністрації Держспецзв'язку № 570.

Тема 6. Захист персональних даних та службової інформації

Законодавство України про захист персональних даних. Обробка персональних даних під час виконання службових повноважень. Організаційні та технічні заходи захисту інформації. Типові порушення вимог щодо захисту персональних даних.

Форма проведення навчальних занять та методи навчання, які дозволяють розкрити зміст теми: лекція, наочний метод (метод ілюстрацій і метод демонстрацій), практичний тренінг, дискусія, самостійна робота (частково-пошуковий; дослідницький).

Тема 7. Автентифікація, управління доступом та парольна безпека

Політика автентифікації користувачів. Вимоги до створення та використання надійних паролів. Багатофакторна автентифікація. Управління правами доступу користувачів.

Форма проведення навчальних занять та методи навчання, які дозволяють розкрити зміст теми: лекція, наочний метод (метод ілюстрацій і метод демонстрацій), практичний тренінг, дискусія, самостійна робота (частково-пошуковий; дослідницький)

Перелік питань, які виносяться на самостійну роботу учасників професійного навчання: практичні інструменти безпечного управління паролями.

Тема 8. Реагування на кіберінциденти

Ознаки кіберінцидентів та порядок їх виявлення. Алгоритм повідомлення про кіберінцидент. Порядок взаємодії з відповідальними особами та компетентними органами. Практичне відпрацювання сценаріїв реагування на кіберінциденти.

Форма проведення навчальних занять та методи навчання, які дозволяють розкрити зміст теми: лекція, наочний метод (метод ілюстрацій і метод демонстрацій), практичний тренінг, дискусія, самостійна робота (частково-пошуковий; дослідницький)

Перелік питань, які виносяться на самостійну роботу учасників професійного навчання: аналіз практичних кейсів реагування на кіберінциденти.

Тема 9. Організація базових заходів кіберзахисту в державних органах

Базові заходи кіберзахисту відповідно до наказу Адміністрації Держспецзв'язку № 54. Організація внутрішніх процедур із забезпечення кібербезпеки. Контроль виконання вимог щодо кіберзахисту. Основні напрями підвищення рівня кіберстійкості установ.

Форма проведення навчальних занять та методи навчання, які дозволяють розкрити зміст теми: лекція, наочний метод (метод ілюстрацій і метод демонстрацій), практичний тренінг, дискусія, самостійна робота (частково-пошуковий; дослідницький)

Тема 10. Законодавчі та організаційні засади забезпечення кібербезпеки

Основні поняття у сфері забезпечення кібербезпеки: кібербезпека, кіберзахист, кіберпростір, кіберзагроза, кіберінцидент. Система забезпечення кібербезпеки України та повноваження її суб'єктів. Законодавче регулювання забезпечення кібербезпеки та захисту інформації в Україні.

Форма проведення навчальних занять та методи навчання, які дозволяють розкрити зміст теми: лекція, наочний метод (метод ілюстрацій і метод демонстрацій), практичний тренінг, дискусія, самостійна робота (частково-пошуковий; дослідницький).

Перелік питань, які виносяться на самостійну роботу учасників професійного навчання: Стратегія кібербезпеки України. Повноваження суб'єктів національної системи кібербезпеки.

ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Якісне завершення програми передбачає отримання учасником професійного навчання не менше ніж 75 балів, зі 100 максимально можливих, за такими складовими оцінювання: Відвідування занять дистанційно в синхронному режимі з вчасним виконанням всіх завдань передбачених програмою оцінюється у 70 балів (питома вага у підсумковій оцінці 70 %).

Відвідування занять очно та / або дистанційно в асинхронному режимі з виконанням всіх завдань з порушенням термінів виконання, але в часових межах програми оцінюється у 45 балів (питома вага у підсумковій оцінці 45 %).

Облік відвідування здійснюється на підставі реєстраційної форми учасників навчання.

Проходження підсумкового контролю у формі письмового онлайн тестування оцінюється у 30 балів (питома вага у підсумковій оцінці 30 %). Успішне тестування передбачає понад 50% правильних відповідей.

Документ про підвищення кваліфікації видається лише за умови якісного завершення програми.

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

1. Бурячок В. Л., Киричок Р. В., Складанний П. М. Основи інформаційної та кібернетичної безпеки : навч. посіб. К. 2018. 320 с. URL: https://elibrary.kubg.edu.ua/id/eprint/27370/1/V_Buriachok_Posibnik_2019_FITU.pdf.

2. Войнова Е. О. Електронна демократія як спосіб політичної комунікації та політичної партисипації у мережевому суспільстві : дис. докт. філос. в галузі галузі знань 05 «Соціальні та поведінкові науки» за спеціальністю 052 «Політологія». Одеса. 2023. 226 с. URL: http://dspace.pdpu.edu.ua/bitstream/123456789/16682/1/Voinova%20E.%20O..pdf.

3. Жовнірчик Я. Ф., Квасюк В. В. Електронне врядування та електронна демократія стосовно децентралізації в Україні: стратегії реалізації та розвитку. Інвестиції: практика та досвід. 2020. № 1. С. 105–113. DOI: 10.32702/2306-6814.2020.1.105

4. Мельничук Н. Ю. Електронне урядування: сучасний стан та перспективи застосування у бюджетній сфері. Збірник наукових праць Національного авіаційного університету «Проблеми системного підходу в економіці». Випуск 5(73). 2019. С. 97–105. URL: http://psae-jrnl.nau.in.ua/journal/5_73_2_2019_ukr/5_73_2_2019.pdf

5. Моніторинг впровадження інструментів електронного урядування в органах місцевого самоврядування [Електронний ресурс] ; наук. ред. Андрій Яскевич. Вінниця : ГО «Подільська агенція регіонального розвитку», 2015. 84 с. https://dialog.lviv.ua/wp-content/uploads/2016/01/Monitoryng_REZ_final_2015_ukr.pdf

ПЕРЕЛІК НОРМАТИВНО-ПРАВОВИХ АКТІВ

1. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text.

2. Про інформацію : Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

3. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text.

4. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text.

5. Про захист персональних даних : Закон України від 01.06.2010 №

2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

6. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 № 851-IV. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text.

7. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

8. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" : Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

9. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 19.06.2019 № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-п#Text.

10. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки та затвердження плану заходів щодо її реалізації : розпорядження Кабінету Міністрів України від 17.01.2018 № 67-р. URL: https://zakon.rada.gov.ua/laws/show/67-2018-р#Text.

11. Методичні рекомендації щодо реагування на кіберінциденти : наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 03.07.2023 № 570.12. Про затвердження Базових заходів з кіберзахисту : наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 30.01.2025 № 54.