НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

«ЗАТВЕРДЖУЮ»	«ПОГОДЖЕНО»
Ректор	Голова
Національного університету	Національного агентства України з
«Львівська політехніка»	Питань державної служби
_____Ю. Я. Бобало	_____ Н. О. Алюшина
«___» _____2022 р.	«___» _____2022 р.

ПРОГРАМА

короткострокових навчальних курсів підвищення кваліфікації державних службовців, посадових осіб місцевого самоврядування з питань **ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**

(Схвалено Вченою Радою
Інституту адміністрування та післядипломної освіти
Національного університету «Львівська політехніка»,
протокол № 8 від 17.05.2022р.)

Львів – 2022

ПРОФІЛЬ ПРОГРАМИ

1. Загальна інформація	
Назва програми	Інформаційна безпека
Шифр програми	ЗК-2/22
Тип програми за змістом	загальна короткострокова програма
Форма навчання	очна (денна) або дистанційна (в режимі реального часу)
Цільова група	державні службовці категорій «Б» та «В», посадові особи місцевого самоврядування IV-VII категорії посад, депутати місцевих рад
Передумови навчання за програмою	-
Найменування замовника освітніх послуг у сфері професійного навчання за програмою	Національне агентство з питань державної служби
Найменування партнера (партнерів)програми	-
Обсяг програми	1 кредит ЄКТС
Тривалість програми та організація навчання	3 робочих дні
Мова(и) викладання	Українська
Напрям(и) підвищення кваліфікації, який (які) охоплює програма	Кібербезпека Інформаційна безпека Цифрова грамотність
Перелік професійних компетенцій, на підвищення рівня яких спрямовано програму	- оцінка ризиків інформаційної безпеки; - володіння нормативно-правовою базою, чинними стандартами і технічними умовами з інформаційної безпеки; - ідентифікація, класифікація та опис роботи, пов'язаної з захистом інформації та інформаційною безпекою.
Укладач(і) програми	Гарасимчук Олег Ігорович, доцент кафедри захисту інформації Національного університету «Львівська політехніка», кандидат технічних наук, доцент, e-mail: oleh.i.harasymchuk@lpnu.ua
2. Загальна мета	
поглиблення базових та наведення нових теоретичних знань про сутність, прояви, наслідки та механізми інформаційної безпеки, розуміння сутності явища інформаційна безпека, опанування базовими знаннями про основні загрози інформаційній безпеці та вироблення уявлення про ефективність інструментів забезпечення інформаційної безпеки. Мета курсів також передбачає формування навиків щодо запобігання та усунення загроз в інформаційній сфері та набуття компетенцій для забезпечення ефективного захисту інформації, необхідних для подальшої роботи у органах державного управління та місцевого самоврядування. Основні цілі програми полягають у поглибленні знань та вмінь забезпечення інформаційної безпеки.	
3. Очікувані результати навчання	
За результатами навчання слухачі повинні демонструвати:	
знання:	- основної законодавчої, наукової та нормативно-методологічної бази у сфері забезпечення інформаційної безпеки; - реальних та потенційних загроз у сфері інформаційної безпеки та законодавчі шляхи їх запобігання; - основних моделей уразливостей та джерел загроз;

	- основних компонентів автоматизованих систем управління доступом та вимог до їх функціональних характеристик; - основних методів, способів та засобів ідентифікації осіб; - етапів побудови комплексної системи санкціонованого доступу та засобів комплексного захисту об'єктів від несанкціонованого доступу;
уміння:	- враховувати чинну нормативно-правову базу при проектуванні систем захисту інформації або ж систем санкціонованого доступу до об'єктів; - виконувати аналіз ризиків та джерел загроз, розробляти модель загроз, розробляти модель порушника; - правильно оцінити потенційні загрози інформаційній безпеці об'єкта; - володіти типовими підходами та методологіями до проектування та модернізації захищених об'єктів інформаційної діяльності відповідно до нормативних вимог чинних стандартів і технічних умов; - планувати та організовувати свою роботу та роботу підрозділу з урахуванням вимог до захисту інформації з обмеженим доступом; - здійснювати ефективний контроль робіт із захисту інформації; - дотримуватися правил роботи з інформацією з обмеженим доступом та суворо виконувати вимоги до захисту інформації; - використовувати спеціальні технічні засоби захисту інформації; використовувати програмні та апаратні засоби розмежування доступу до інформації у автоматизованих системах
навички:	- побудови ефективної системи захисту інформації в організаціях згідно нормативних вимог чинних стандартів та законодавства України; - організації роботи з інформацією з обмеженим доступом; - навички вибору найбільш ефективних методів та засобів при реалізації системи санкціонованого доступу в організації.
4. Викладання та навчання (методи навчання, форми проведення навчальних занять)	
Навчання здійснюється у формі тренінгів, які включають проведення лекцій з використанням інтерактивних презентацій, консультативних форумів, тематичних дискусій й практичних робіт. Курс навчання передбачає самостійну роботу слухачів.	
5. Ресурсне забезпечення дистанційного навчання	
Назви вебплатформи, вебсайту, електронної	*програмний додаток для відеоконференцій

навчальної системи із зазначенням посилання (вебадреси), на основі яких забезпечуються процеси проведення дистанційного навчання	Zoom - https://zoom.us/ru-ru/meetings.html
Назва дистанційного етапу/модуля	Тема 1. Загальні положення інформаційної безпеки. Законодавча, наукова та нормативно-методологічна база у сфері забезпечення інформаційної безпеки. Тема 2. Основи побудови системи захисту інформації та основні етапи створення системи захисту інформації. Тема 3. Аналіз можливих загроз безпеці інформації. Тема 4. Автоматизовані системи управління доступом, їх основні компоненти та процедури. Тема 5. Методи та засоби ідентифікації осіб. Тема 6. Апаратна ідентифікація. Тема 7. Біометрична ідентифікація Тема 8. Електронний цифровий підпис.
6. Оцінювання і форми поточного, підсумкового контролю	
Критерії оцінювання та їх питома вага у підсумковій оцінці (%)	проходження дистанційного навчання (відвідування занять) - 40%; самостійна робота – 20 %; підсумковий контроль – 40%. Документ про підвищення кваліфікації видається слухачам, які в процесі вивчення короткострокової програми отримали не менше ніж 60 % за системою оцінювання ЄКТС, обчислених за питомою вагою наведених критеріїв оцінювання (підсумковий контроль обов'язковий)
Форма підсумкового контролю	Письмове тестування

.

СТРУКТУРА ПРОГРАМИ

Назви теми	Кількість годин/кредитів ЄКТС		
	загальна кількість годин	у тому числі:	
		аудиторні заняття	самостійна робота
Тема 1. Загальні положення інформаційної безпеки. Законодавча, наукова та нормативно-методологічна база у сфері забезпечення інформаційної безпеки.	3/0,1	2/0,07	1/0,03
Тема 2. Основи побудови системи захисту інформації та основні етапи створення системи захисту інформації.	5/0,17	4/0,14	1/0,03
Тема 3. Аналіз можливих загроз безпеці інформації.	3/0,1	2/0,07	1/0,03
Тема 4. Автоматизовані системи управління доступом, їх основні компоненти та процедури.	3/0,1	2/0,07	1/0,03
Тема 5. Методи та засоби ідентифікації осіб.	5/0,17	4/0,14	1/0,03

Тема 6. Апаратна ідентифікація.	3/0,1	2/0,07	1/0,03
Тема 7. Біометрична ідентифікація.	3/0,1	2/0,07	1/0,03
Тема 8. Електронний цифровий підпис.	3/0,1	2/0,07	1/0,03
Підсумковий контроль результатів навчання	2/0,07	2/0,07	-
РАЗОМ	30/1	22/0,73	8/0,27

ЗМІСТ ПРОГРАМИ

Тема 1. Загальні положення інформаційної безпеки. Законодавча, наукова та нормативно-методологічна база у сфері забезпечення інформаційної безпеки.

Основи розвитку інформаційного суспільства. Проблематика захисту інформації. Інформаційна безпека підприємства. Питання організації доступу до інформації. Мета комплексної інформаційної безпеки. Законодавчі заходи щодо захисту інформації. Основні закони, які регламентують діяльність у сфері захисту інформації. Нормативно-правові акти Президента України та адміністрації Держспецзв'язку.

Тема 2. Основи побудови системи захисту інформації та основні етапи створення системи захисту інформації.

Основні терміни та визначення. Вимоги до системи безпеки підприємства та основні принципи її побудови. Основні задачі, що ставляться перед фахівцями, які реалізують систему захисту інформації на об’єкті. Основні етапи побудови комплексної системи безпеки та результати дій на цих етапах.

Тема 3. Аналіз можливих загроз безпеці інформації.

Загальні положення. Механізми формування атаки. Аналіз можливих збитків від дій зловмисників. Можливі джерела загроз. Антропогенні, техногенні та стихійні джерела загроз.

Тема 4. Автоматизовані системи управління доступом, їх основні компоненти та процедури.

Визначення автоматизованих систем управління доступом. Управління первинним проходом на територію та управління переміщенням по території. Ідентифікатор. Типовий об’єкт. Об’єкти та суб’єкти контролю. Принципи функціонування АСУД. Класифікація точок доступу. Класифікація засобів АСУД. Виконавчі механізми АСУД. Об’єкти АСУД. Процедури АСУД. Основні завдання, які повинна забезпечувати АСУД. Категоріювання об’єктів доступу. Контроль збереження режиму доступу.

Тема 5. Методи та засоби ідентифікації осіб.

Загальні положення. Поняття ідентифікації та автентифікації, об’єкта та суб’єкта доступу, рівень неправильного дозволу на доступ та неправильної відмови в доступу. Класифікація ідентифікаторів.

Тема 6. Апаратна ідентифікація.

Ідентифікація за картками доступу. Магнітні картки. RFID-картки. Картки доступу, що використовують магнітну смугу. Штрих-кодові картки. Безконтактні Smart-картки. Картки Віганда. Електронні ідентифікатори контактної пам’яті. Токени.

Тема 7. Біометрична ідентифікація.

Розпізнавання за відбитками пальців. Ідентифікація за зображенням кисті руки.

Ідентифікація за венами долоні. Ідентифікація за веселковою оболонкою та сітківкою ока. Розпізнавання за формою обличчя. Розпізнавання за термограмою обличчя. Динамічні методи ідентифікації.

Тема 8. Електронний цифровий підпис.

Електронний підпис. Електронний цифровий підпис. Сертифікат відкритого ключа. Особистий ключ. Відкритий ключ. Акредитація. Використання та захищеність електронного цифрового підпису. Інфраструктура відкритого ключа. Сертифікат відкритого ключа.

РЕКОМЕДОВАНА ЛІТЕРАТУРА

1. Закон України “Про інформацію” від 02.10.92 р. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text.
2. Закон України “Про державну таємницю” від 21.01.94 р. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/3855-12#Text.
3. Закон України “Про науково-технічну інформацію” від 25.06.93 р. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/3322-12#Text.
4. Про внесення змін до Закону України "Про захист інформації в автоматизованих системах". [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2594-15#Text.
5. Закон України “Про захист персональних даних” від 01.06.10 р. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text.
6. Закон України “Про основні засади забезпечення кібербезпеки України” від 05.10.2017. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
7. Закон України “Про національну безпеку України” від 21.06.2018 р. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2469-19#Text.
8. Закон України “Про захист персональних даних” від 20.11.2012. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text.
9. Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 No373.
10. Постанова Кабінету Міністрів України “Про затвердження Концепції технічного захисту інформації в Україні” від 08.10.1997 р.
11. Постанова Кабінету Міністрів України “Про затвердження Положення про технічний захист інформації в Україні” від 09.09.1994 р.
12. Постанова Кабінету міністрів України “Про затвердження Концепції технічного захисту інформації в Україні” No 1126 від 08.11.1997 р.
13. Стратегія кібербезпеки України: Указ Президента України від 15.03.2016 р. No 96/2016// Офіційний вісник України. – 2016. – No 23. – С. 69. – Ст. 899.
14. Стратегія національної безпеки України : Указ Президента України від 06.05.2015 р. No 287/2015// Офіційний вісник України. – 2015. – No 43. – С. 14. – Ст. 1353
15. Доктрина інформаційної безпеки України : Указ Президента України від 25.02.2017 р. No 47/2017 // Офіційний вісник Президента України. – 2017. – No 5. – С. 15. – Ст. 102.
16. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).
17. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT).
18. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.
19. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Проведення робіт.
20. Антонюк А.О. Основи захисту інформації в автоматизованих системах.

Навчальний посібник.-НУ «Києво-Могилянська академія», 2003 р., 242 с.

21. Богуш В.М. Інформаційна безпека держави / В.М. Богуш, О.К. Юдін – К. “МК-Прес”, 2005. – 432 с.

22. Бурячок В.Л. та ін. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л.Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа]; за заг. ред. д-ра техн. наук, професора В.Б. Толубка.— К.: ДУТ, 2015.— 288 с.

23. Гарасимчук О.І., Дудикевич В.Б., Ромака В.А., Комплексні системи санкціонованого доступу. Навчальний посібник. – Львів, НУЛП, 2010, 207 с.

24. Головань С.М. Нормативно-правове забезпечення інформаційної безпеки /С.М. Головань, С.Б. Гордієнко, О.С. Петров, В.О. Хорошко, Л.М. Щербак; під ред.В.О. Хорошко. – Луганськ: Ноулідж, 2012. – 480 с.

25. Домарєв В.В., Скворцов С.О. Організація захисту інформації на об’єктах державної та підприємницької діяльності. Навчальний посібник. – К.: Вид-во Європ. Ун-ту, 2006. – 102 с.

26. Домарєв В.В., Швець В.А., Шестакова В.В. Організаційне забезпечення захисту інформації з обмеженим доступом. Навчальний посібник. – К.: НАУ, 2006. – 108 с.

27. Дудатьєв А.В. Інформаційна безпека. Навчальний посібник. – Вінниця: УНІВАР-Сум-Вінниця, 2009. – 240 с.

28. Дудикевич, В. Б. Основи інформаційної безпеки : навч. пос. / Дудикевич В. Б., Хорошко В. О., Яремчук Ю. Є. – Вінниця : ВНТУ, 2018. – 316 с.

29. Інформаційна безпека держави : підручник / [В.М. Петрик, М.М. Присяжнюк, Д.С. Мельник та ін.] ; в 2 т. – Т.1. / за аг. ред.. В.В. Остроухова. – К. : ДНУ «Книжкова палата Україна», 2016. – 264 с.

30. Кавун С.В. (2008). Інформаційна безпека: навчальний посібник. Харків: Харківський національний економічний ун-т. 196.

31. Качинський А.Б. Безпека, загрози і ризик: наукові концепції та математичні методи / Інститут проблем національної безпеки; Національна академія Служби безпеки України. – К.: 2004. – 472 с.

32. Кравець Є.А. (1992). Інформаційна безпека держави. Київ: Укр. енцикл. 1235.

33. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навч. посіб. - К.: Кондор, 2004. - 384 с.

34. Лужецький В.А., Кожухівський А.Д., Войтович О.П. Основи інформаційної безпеки. Навч. посібник. – Вінниця: ВНТУ, 2009. – 268 с.

35. Лужецький В.А. Захист персональних даних. Навчальний посібник. – Вінниця: ВНТУ, 2009. – 487 с.

36. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання. – К.: ВД “Гельветика”, 2017. – 168 с.

37. Русин Б.П. Біометрична аутентифікація та криптографічний захист / Б.П. Русин, Я.Ю. Варецький. – Львів: «Коло», 2007. – 287 с.

38. Самохвалов Ю.А, Темніков В.О., Хорошко В.О. Організаційно-технічне забезпечення захисту інформації. Навчальний посібник. - К., НАУ, 2002, 207 с.

39. Термінологічний довідник з питань технічного захисту інформації / Коженевський С.Р., Кузнецов Г.В., Хорошко В.О., Чирков Д.В. / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2007. – 365 с.

40. Юдін О.К., Богуш В.М. Інформаційна безпека держави. – К.: «МК-Прес», 2005. – 432 с.