**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ**

**"ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ЛУЦЬКОГО НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ"**

**Циклова комісія комп’ютерних систем та інформаційних технологій**

|  |  |
| --- | --- |
|  | **ЗАТВЕРДЖУЮ**Заступник директораз навчальної роботи\_\_\_\_\_\_\_\_\_\_\_С. БУСНЮК“29” серпня 2023 року |

## ПРОГРАМА

## навчальної дисципліни "ОСНОВИ КІБЕРБЕЗПЕКИ"

Розробник П. ВОВК

Галузь знань 12 Інформаційні технології

Код та назва спеціальності 123 Комп'ютерна інженерія, 126 Інформаційні системи та технології

Освітньо-професійна програма Комп'ютерна інженерія , Інформаційні системи та технології

Статус навчальної дисципліни вибіркова

Мова навчання українська

2023 рік

Програма навчальної дисципліни «Основи кібербезпеки» для здобувачів фахової передвищої освіти IV курсу освітньо-професійного ступеня фаховий молодший бакалавр спеціальностей 126 Інформаційні системи та технології та 123 Комп'ютерна інженерія денної форми навчання складена на основі ОПП Інформаційні системи та технології та ОПП Комп'ютерна інженерія.

“26” серпня 2023 року - 20 с.

Розробник:Вовк П.Б.

Програма обговорена та схвалена на засіданні циклової комісії комп’ютерних систем та інформаційних технологій

Протокол від “ 28 ” серпня 2023 року № 1

Голова циклової комісії комп’ютерних систем та інформаційних технологій \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ П. ВОВК

Схвалено Педагогічною радою ТФК ЛНТУ

Протокол від “29” серпня 2023 року №1

Програма обговорена та схвалена на засіданні циклової комісії комп’ютерних систем та інформаційних технологій

Протокол від “ ” серпня 202\_\_ року № \_\_\_\_

Голова циклової комісії комп’ютерних систем та інформаційних технологій \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_

Схвалено Педагогічною радою ТФК ЛНТУ

Протокол від “ ” серпня 202 року №\_\_\_

Ппрограма обговорена та схвалена на засіданні циклової комісії комп’ютерних систем та інформаційних технологій

Протокол від “ ” серпня 202\_\_ року № \_\_\_\_

Голова циклової комісії комп’ютерних систем та інформаційних технологій \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_

Схвалено Педагогічною радою ТФК ЛНТУ

Протокол від “ ” серпня 202 року №\_\_\_

**1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

|  |  |  |
| --- | --- | --- |
| **Найменування показників**  | **Галузь знань, спеціальність, освітньо-професійний ступінь** | **Характеристика навчальної дисципліни** |
| Тем – 2 | **Галузь знань:**12 Інформаційні технології | **Форма навчання** |
| денна  |
| **Спеціальність:**126 Інформаційні системи та технології123 Комп’ютерна інженерія |
| **Рік підготовки** |
| ІV |
| **Семестр** |
| Загальна кількість годин – 150  | VІІ |
| Для денної форми навчання:аудиторних – 60;самостійної роботи студента – 90. | **Освітньо-професійний ступінь:**фаховий молодший бакалавр | **Лекції** |
| 30 год |
| **Практичні** |
| 30 год |
| **Самостійна робота** |
| 90 год |
| **Вид контролю:** |
| диф. залік |

|  |
| --- |
| **2. Мета дисципліни, передумови її вивчення та заплановані результати навчання** |
| Місце дисципліни в освітній програмі: | Під кібербезпекою (інформаційною безпекою) розуміють сукупність засобів, методів і процесів (процедур), які забезпечують захист інформаційних активів і гарантують збереження ефективності та практичної корисності як технічної інфраструктури інформаційних систем, так і відомостей, які в таких системах зберігаються і обробляються.Метою викладання навчальної дисципліни «Основи кібербезпеки» є формування у здобувачів освіти теоретичної та практичної бази знань з безпечної поведінки в мережі; умінь і навичок ефективно та безпечно налаштовувати свої облікові записи; розуміння принципів передачі даних через мережу та існуючих методів захисту.Висококваліфікований фахівець з кібербезпеки повинен мати достатній рівень знань, умінь та компетентностей у галузі забезпечення інформаційної безпеки і/або кібербезпеки; мати здатності до застосовування отриманих знань у практичних ситуаціях; знати та розуміти предметну область, розуміти професію; вміти виявляти, ставити та вирішувати проблеми у галузі кібербезпеки. |
| Компетентності загальні або фахові: | ЗК5. Знання та розуміння предметної області і професійної діяльності.ЗК7. Здатність застосовувати знання у практичних ситуаціях.СК3. Здатність застосовувати фундаментальні та міждисциплінарні знання для успішного розв’язання завдань у галузі інформаційних систем та технологій.СК6. Здатність дотримуватися стандартів в області інформаційних систем та технологій.СК7. Здатність використовувати методи і засоби забезпечення інформаційної та функціональної безпеки в області інформаційних систем та технологій.СК14. Здатність вибору хмарних платформ та розгортання на них, інтегрування, адміністрування і супроводу інформаційних систем та сервісів. |
| Програмні результати навчання: | РН2. Накопичувати, систематизувати та узагальнювати інформацію про підходи й методики роботи в області інформаційних систем та технологій.РН5. Обирати оптимальний спосіб вирішення завдань, налаштовувати та користуватись відповідними інструментальними засобами.РН6. Знати основні стандарти в галузі інформаційних систем та технологій і дотримуватись їх.РН7. Знати основні види кіберзагроз, основні методи і засоби забезпечення інформаційної та функціональної безпеки і застосовувати їх на практиці під час впровадження та супроводу інформаційних систем.РН19. Здійснювати розгортання, інтегрування, адміністрування й технічну підтримку хмарних систем та сервісів. |
| **Передумови для вивчення дисципліни:** |
| Для вивчення навчальної дисципліни «Основи кібербезпеки» необхідними є компетентності здобувачів освіти з навчальних дисциплін «Інформатика», «Вступ до спеціальності», «Основи програмування». Навчальна дисципліна забезпечує міжпредметні зв’язки з навчальними дисциплінами «Захист інформації», «Комп'ютерні системи обробки та аналізу даних», «Адміністрування комп'ютерних систем і мереж», «Хмарні технології».  |

|  |
| --- |
| **3. Обсяг та структура програми навчальної дисципліни**  |
| **форма навчання** | Кредити ЄКТС | **денна (очна)** |
| **ФОРМА Контролю** | **Підсумкові оцінки (диф. залік)** |
| № теми | Назва теми | Кількість годин: |
| Разом | Самостійна робота | Навчальні заняття: |
| Всього | з них: |
| Лекційні заняття | Семінарські заняття | Практичні заняття | Лабораторні заняття | Індивідуальні заняття |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** |
| 1. | Законодавча та нормативно-правова база в галузі інформаційної та /або кібербезпеки | 0,8 | 24 | 16 | 8 | 4 |  | 4 |  |  |
| 2. | Інструментальні та прикладні застосунки в інформаційній та/або кібербезпеці | 0,4 | 12 | 6 | 6 | 4 |  | 2 |  |  |
| 3. | Моделі безпеки в інформаційній та/або кібербезпеці | 1,7 | 50 | 28 | 22 | 12 |  | 10 |  |  |
| 4. | Управління інформаційною та/або кібербезпекою. | 1,3 | 38 | 22 | 16 | 8 |  | 8 |  |  |
| 5. | Технічний захист інформації. | 0,8 | 26 | 18 | 8 | 2 |  | 6 |  |  |
| **Разом з дисципліни:** | **5** | **150** | **90** | **60** | **30** |  | **30** |  |  |

**4. ІНФОРМАЦІЙНИЙ ОБСЯГ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

**4.1 Теми лекцій**

|  |  |  |  |
| --- | --- | --- | --- |
| **№****з/п** | **Назва теми** | **Кількість****годин** | **Рекомендована література** |
|  | Основні поняття інформаційної безпеки | 2 | [8], с. 12-34 |
|  | Законодавча та нормативно-правова база України в галузі інформаційної та/або кібербезпеки | 2 | [8], с.34-40 |
|  | Діяльність міжнародних організацій у сфері інформаційної безпеки | 2 | [7], с. 56-58 |
|  | Стандартизація в сфері інформаційної безпеки | 2 | [7], с. 63-73 |
|  | Спеціалізовані міжнародні організації та об’єднання в галузі інформаційної безпеки | 2 | [6], с. 45-47 |
|  | Міжнародні стандарти в галузі інформаційної та /або кібербезпеки | 2 | [7], с.82-102 |
|  | Інструментальні та прикладні застосунки в інформаційній та/або кібербезпеці | 2 | [7], с.107-117 |
|  | Методи і засоби обробки інформації | 2 | [7], с. 79-87 |
|  | Захисні механізми операційних систем | 2 | [8], с. 222-235 |
|  | Моделі безпеки в інформаційній та/або кібербезпеці | 2 | [8], с. 236-252 |
|  | Захист інформації, що обробляється та зберігається в інформаційно-телекомунікаційних системах (ІКС) | 2 | [7], с. 105-107 |
|  | Програмні та програмно-апаратні комплекси засобів захисту інформації (ЗЗІ) | 2 | [7], с. 117-123 |
|  | Відновлення функціонування інформаційно- комунікаційних систем (ІКС) після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження | 2 | [9], с. 87-95; |
|  | Моніторинг процесів функціонування інформаційно - комунікаційних систем (ІКС) | 2 | [9], с. 96-109; |
|  | Механізми безпеки комп'ютерних мереж | 2 | [9], с. 146-154 |
|  | **Всього** | 30 |  |

**4.2 Теми практичних занять**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№****з/п** | **Назва теми, план.** | **Кількість****годин** | **Форма та засоби контролю** | **Рекомендована література** |
|  | Вступ до кібербезпеки. Правові та етичні проблеми кібербезпеки. Персональні дані. Корпоративні дані. Зловмисники та експерти з кібербезпеки. Кібервійни. | 2 | виконання завдань, індивідуальне оцінювання | [7], с. 28 - 31[8], с. 230-270 |
|  | Загрози кібербезпеці, вразливості та атаки | 2 | виконання завдань, індивідуальне оцінювання | [7], с. 33-50[8], с. 510-588 |
|  | Захист мереж. Атака на фонд | 2 | виконання завдань, індивідуальне оцінювання | [7], с. 56-58[8], с. 55-70 |
|  | Бездротовий мережевий зв’язок | 2 | виконання завдань, індивідуальне оцінювання | [7], с. 135-143[8], с. 60-66 |
|  | Захист і безпека інфраструктури мережі | 2 | виконання завдань, індивідуальне оцінювання | [7], с. 63-77[8], с. 32-36 |
|  | Захист в операційній системі Windows | 2 | виконання завдань, індивідуальне оцінювання | [7], с. 63-77[8], с. 32-36 |
|  | Захист в операційній системі Linux | 2 | виконання завдань, індивідуальне оцінювання | [3], с. 183 - 256 |
|  | Захист системи та кінцевої точки | 2 | виконання завдань, індивідуальне оцінювання | [3], с. 258 - 330 |
|  | Принципи, практики та процеси кібербезпеки | 2 | виконання завдань, індивідуальне оцінювання | [3], с. 334 - 415 |
|  | Контроль доступу | 2 | виконання завдань, індивідуальне оцінювання | [3], с. 559 - 636 |
|  | Технології брандмауера | 2 | виконання завдань, індивідуальне оцінювання | [3], с. 559 - 636 |
|  | Хмарна безпека | 2 | виконання завдань, індивідуальне оцінювання | [3], с. 417 - 487 |
|  | Криптографія | 2 | виконання завдань, індивідуальне оцінювання | [3], с. 488 - 530 |
|  | Управління ризиками та засоби контролю безпеки | 2 | виконання завдань, індивідуальне оцінювання | [3], с. 642 -684 |
|  | Цифрова криміналістика та аналіз і реагування на інциденти | 2 | виконання завдань, індивідуальне оцінювання | [3], с. 642 -684 |
| **Разом** | **30** |  |  |

**4.3 Самостійна робота**

|  |  |  |  |
| --- | --- | --- | --- |
| **№****з/п** | **Назва теми** | **Кількість****годин** | **Рекомендована література** |
| 1. | Загрози кібербезпеці, вразливості та атаки | 6 | [3], с.147 - 179 |
| 2. | Захист мереж | 8 | [3], с. 37 -69 |
| 3. | Бездротовий мережевий зв’язок | 8 | [3], c. 72 -92 |
| 4. | Інфраструктура безпеки мережі | 6 | [3], с. 256 - 278 |
| 5. | Захист системи та кінцевої точки | 8 | [3], с. 278 - 298 |
| 6. | Принципи, практики та процеси кібербезпеки | 8 | [3], с. 559 - 636 |
| 7. | Захист системи та мережі | 6 | [3], с. 112-122 |
| 8. | Контроль доступу. Списки контролю доступу | 6 | [3], с. 124-133 |
| 9. | Технології брандмауера. Брандмауери зональної політики | 6 | [3], с. 134 - 143 |
| 10. | Хмарна безпека | 6 | [3], с. 185-198 |
| 11. | Криптографія | 6 | [3], с. 304-318 |
| 12. | Оцінка вразливості та управління ризиками | 8 | [3], с. 741 - 763 |
| 13. | Цифрова криміналістика та аналіз і реагування на інциденти | 8 | [3], с. 417 - 556 |
| **Разом** | **90** |  |

**5. Засоби діагностики результатів навчання, інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна**

Засобами оцінювання та методами демонстрування результатів навчання є екзамен, практичні завдання на лабораторному обладнанні, реальних об’єктах (комп’ютер та його складові), аналітичні звіти, реферати, презентації результатів виконаних завдань та досліджень, письмове виконання ІНДЗ, виступи на наукових заходах, Використовуються відео лекції, практичні заняття з індивідуальними завданнями, самостійна робота здобувача фахової передвищої освіти з навчальною та довідковою літературою, самостійне виконання завдань, консультації. Використовуються демонстраційні вузли та компоненти комп’ютера, лабораторний навчальний комп’ютер, інструктивні картки для практичних робіт, картки з індивідуальними завданнями для практичних робіт. Використовується доступ до мережі інтернет.

Під час вивчення дисципліни «Основи кібербезпеки» студенту рекомендується пройти курси «Introduction to Cybersecurity» та «Cybersecurity Essentials» освітньої платформи CISCO NETWORKING ACADEMY https://www.netacad.com.

|  |
| --- |
| **6. Порядок та критерії оцінювання результатів навчання** |
| **6.1. Порядок оцінювання результатів навчання** |
| Форма контролю | Порядок проведення контролю |
| Поточний контроль | Усне опитування, домашні завдання, виступи на практичних заняттях, практичні та письмові роботи оцінюються за 4-бальною шкалою |
| Підсумковий контроль | Екзаменаційна оцінка визначається за рівнем компетентності розв’язання запропонованих завдань екзаменаційних білетів за 4 бальною шкалою. |
| **6.2. Критерії оцінювання результатів навчання** |
| Оцінювання за національною шкалою: | Критерії та визначення оцінювання |
| рівень компетентності | оцінка: |
| 4-бальна |  |
| **1** | **2** | **3** |
| Високий(творчий) | 5(відмінно) | Здобувач освіти вiльно володiє програмовим матерiалом, виявляє здiбностi, вмiє самостiйно поставити мету дослiдження, вказує шляхи її реалiзацiї, робить аналiз та висновки.Здобувач освіти вiльно володiє вивченим матерiалом, умiло послуговується науковою термiнологiєю, вмiє опрацьовувати наукову iнформацiю (знаходити новi фак­ти, явища, iдеї, самостiйно використовувати їх вiдповiдно до поставленої мети тощо).Здобувач освіти вiльно володiє вивченим матерiалом, умiло послуговується науковою термiнологiєю, вмiє опрацьовувати наукову iнформацiю (знаходити новi фак­ти, явища, iдеї, самостiйно використовувати їх вiдповiдно до поставленої мети тощо). |
| Достатній(конструктивно-варіативний) | 4(добре) | Здобувач освіти вiльно володiє вивченим матерiалом у стандартних ситуацiях, наводить приклади його практичного застосування та аргументи на пiдтвердження власних думок. Здобувач освіти умiє пояснювати явища, ана­лiзувати, узагальнювати знання, систематизувати їх, зi сторонньою допомогою (викладача, одногрупників тощо) ро­бити висновки. Здобувач освіти може пояснювати роботу комп’ютера, виправляти допущенi неточностi, виявляє знання i розумiння основних вузлів компютера (призначення, функціонування, характеристики, особливості застосування). |
| Середній(репродуктивний) | 3(задовільно) | Здобувач освіти може зi сторонньою допомогою пояснювати явища, виправляти допущенi неточності (власні, iнших уч­нiв), виявляє елементарнi знання основних по­ложень функціонування комп’ютера (законiв, понять, формул). Здобувач освіти описує явища, вiдтворює значну частину навчального матерiалу, знає складові комп’ютера, їх характеристики, записує основнi формули, рiвняння i закони. Здобувач освіти за допомогою викладача описує явища, без пояснень наводить приклади, що ґрунтуються на його власних спостереженнях чи матерiалi пiдручника, розповiдях викладача тощо. |
| Початковий(рецептивно-продуктивний) | 2(незадовільно) | Здобувач освіти за допомогою викладача описує компютер або його частини у зв’язаному вигляді без пояснень вiдповiдних причин, називає параметри та характеристики складових, розрiзняє призначення окремих складових комп’ютера. |
| Здобувач освіти описує роботу комп’ютера на ос­новi свого попереднього досвiду, за допомогою викладача вiдповiдає на запитання, що потребують однослiвної вiд­по­вiдi. |
| Здобувач освіти володiє навчальним мате­рiа­лом на рiвнi­ розпiзнавання складових комп’ютера, за допомогою викладача вiдповiдає на запитання, що потребують вiдповiдi “так” чи “нi”. |

**7. РЕКОМЕНДОВАНА ЛІТЕРАТУРА**

**Основна**

1. Доктрина інформаційної безпеки України : Указ Президента України від 25.02.2017 р. № 47/2017 // Офіційний вісник Президента України. – 2017. – № 5. – С. 15. – Ст. 102. <https://www.president.gov.ua/documents/472017-21374>
2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
3. Стратегія кібербезпеки України : Указ Президента України від р. № 96/2016// Офіційний вісник України. – 2016. – № 23. – С. 69. – Ст. 899. <https://zakon.rada.gov.ua/laws/show/96/2016#Text>
4. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Посібник]. / В. Л. Бурячок, С.В.Толюпа, В.В.Семко, Л.В.Бурячок, П.М.Складанний Н.В. Лукова-Чуйко – К. : ДУТ - КНУ, 2016. – 178 с.
5. Бурячок, В. Л. 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.
6. Кавун С. В. Інформаційна безпека. Навчальний посібник / С. В. Кавун, В. В. Носов, О. В. Манжай. — Харків: Вид. ХНЕУ, 2008. – 352 с.
7. Словник термінів з кібербезпеки / За загальною редакцією Копана О.В., Скулиша Є.Д. –К. : ВБ «Аванпост-Прим». – 2012. – 214 c.
8. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Книшук А.В. Вступ до кібербезпеки: навч. посіб. – Кропивницький: ЦНТУ, 2022. – 967 с.
9. 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.
10. Дудатьєв А. В.Захист комп’ютерних мереж. Теорія та практика. Навчальний посібник / Дудатьєв А. В., Войтович О. П., Каплун В. А. – Вінниця ВНТУ, 2010. – 219 с.
11. Гулак Г.М., Гринь А.К., Мельник С.В. Методологія захисту інформації: навчально-методичний посібник. – К.: Видавництво НА СБ України, 2015. – 251 с.

**Допоміжна**

1. Про кіберзлочинність : Конвенція Ради Європи від 23.11.01 р. № 994-575. https://zakon.rada.gov.ua/laws/show/994\_575#Text
2. Про інформацію : Закон України від 02.10.92 р. № 2657-XII //Відомості Верховної Ради України. – 1992. – № 48. – ст. 650. https://zakon.rada.gov.ua/laws/show/2657-12#Text
3. Закон України «Про захист інформації в інформаційно телекомунікаційних системах» <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>
4. Інформаційна безпека держави : підручник / [ В.М. Петрик, М.М.4 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.
5. Законодавчі основи забезпечення інформаційної безпеки України: наукова доповідь / Пилипчук В.Г., Корж І.Ф., Петришин О.В., Савінова Н.А., Фурашев В.М. (За заг. ред. Пилипчука В.Г.) – К: НДІІП НАПрН України, 2014. – 60 с.
6. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., ЛуковаЧуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. /В.Л. Бурячок, С.В. Толюпа, А.О. Аносов, В.А. Козачок, Н.В. Лукова-Чуйко/ –К.:ДУТ, 2015. – 345 с.
7. Богуш В.М., Довидьков О.А., Кривуца В.Г. Теоретичні основи захищених інформаційних технологій. Навч. посібник. – К.: ДУІКТ, 2010. – 454 с.
8. Хорошко В.О. Основи комп’ютерної стеганографії / В.О. Хорошко, О.Д. Азаров, М.Є. Шелест, Ю.Є. Яремчук. – Вінниця.: ВДТУ, 2003. – 142 с.
9. Русин Б.П. Біометрична аутентифікація та криптографічний захист / Б.П. Русин, Я.Ю. Варецький. – Львів: «Коло», 2007. – 287 с.

**8. ІНФОРМАЦІЙНІ РЕСУРСИ**

1. Системи онлайн-освіти: <https://prometheus.org.ua/>, <https://www.coursera.org>, <http://www.udacity.com>,
2. Портал безпека [Електронний ресурс]. – Режим доступу: <https://www.bezpeka.com/uk/golovna/>
3. Верховна Рада України. Законодавство України: [Електронний ресурс]. – Режим доступу: <http://zakon.rada.gov.ua/laws/>
4. Державна служба спеціального зв’язку та захисту інформації: [Електронний ресурс]. – Режим доступу: <https://cip.gov.ua/ua>
5. Команда реагування на комп'ютерні надзвичайні події України: [Електронний ресурс]. – Режим доступу: <https://cert.gov.ua/>