МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ

"ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ   
ЛУЦЬКОГО НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ"

Циклова комісія комп’ютерних систем та інформаційних технологій

|  |  |
| --- | --- |
| **погождую**  Голова групи забезпечення  ОПП спеціальності  \_\_\_\_\_\_\_\_\_\_\_\_\_ П. ВОВК  \_\_\_\_\_\_\_\_\_\_\_\_\_ 2022 року | **ЗАТВЕРДЖУЮ**  Заступник директора  з навчальної роботи  \_\_\_\_\_\_\_\_\_\_\_С. БУСНЮК  “26” серпня 2022 року |

## РОБОЧА ПРОГРАМА

## навчальної дисципліни

**ЗАХИСТ ІНФОМАЦІЇ**

Розробник Завіша В.В.

Галузь знань 12 Інформаційні технології

Код та назва спеціальності 126 Інформаційні системи та технології

Освітньо-професійна програма Інформаційні системи та технології

Статус навчальної дисципліни нормативна

Мова навчання українська

2022 рік

Робоча програма навчальної дисципліни «Захист інформації» для здобувачів фахової передвищої освіти IV курсу денної форми навчання складена на основі ОПП «Інформаційні системи та технології»

“25” серпня 2022 року - 14 с.

Розробник:Завіша В.В.

Робоча програма розглянута і обговорена на засіданні циклової комісії комп’ютерних систем та інформаційних технологій

Протокол від. “ 25 ” серпня 2022 року № 1

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

Схвалено Педагогічною радою ТФК ЛНТУ

Протокол від “26 ” серпня 2022 року №1

**1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

|  |  |  |
| --- | --- | --- |
| Найменування показників | Галузь знань, спеціальність, освітньо-професійний ступінь | Характеристика навчальної дисципліни |
| Тем – 5 | Галузь знань:  12 Інформаційні технології | Форма навчання |
| денна |
| Спеціальність:  126 Інформаційні системи та технології |
| Рік підготовки |
| ІV |
| Семестр |
| Загальна кількість годин – 90 | VII |
| Для денної форми навчання:  аудиторних – 48 год;  самостійної роботи – 42 год. | Освітньо-професійний ступінь:  фаховий молодший бакалавр | Лекції |
| 24 год. |
| Практичні |
| 24 год. |
| Лабораторні |
| - |
| Самостійна робота |
| 42 год. |
| Курсова робота |
| - |
| Вид контролю: |
| екзамен |

|  |  |
| --- | --- |
| **2. Мета дисципліни, передумови її вивчення та заплановані результати навчання** | |
| Місце дисципліни в освітній програмі: | Метою викладання дисципліни “Захист інформації” є навчання студентів принципам побудови комплексних систем захисту інформації на основі синтезу організаційних і технічних заходів щодо забезпечення захисту інформації з обмеженим доступом, основ ведення електронного документообігу в умовах сучасних кіберзагроз та витоку технічними каналами, забезпечення захисту інформації від несанкціонованого доступу на основі вимог міжнародних стандартів з інформаційної безпеки, державних нормативних документів з технології захисту інформації..  Основними завданнями дисципліниє формування у студентів знань та вмінь з теорії та практики захисту інформації; ознайомлення із сучасними підходами, методиками, засобами та пристроями для захисту інформаційно-комп’ютерних систем і персональної інформації користувача; освоєння заходів, які сприяють захисту сучасних інформаційних систем у професійній діяльності, пов’язаній із отриманням, обробкою, накопиченням і захистом особистої інформації. |
| Компетентності загальні або фахові: | СК3. Здатність застосовувати фундаментальні та міждисциплінарні знання для успішного розв’язання завдань у галузі інформаційних систем та технологій.  СК7. Здатність використовувати методи і засоби забезпечення інформаційної та функціональної безпеки в області інформаційних систем та технологій. |
| Програмні результати навчання: | РН2. Накопичувати, систематизувати та узагальнювати інформацію про підходи й методики роботи в області інформаційних систем та технологій.  РН4. Знати способи ідентифікації, формулювання та класифікації вимог до інформаційних систем та технологій і застосовувати їх при прийнятті бізнес-рішень та в процесі аналізу отриманого технічного завдання.  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.  РН10. Розробляти та супроводжувати окремі компоненти інформаційних систем  РН16. Знати та розуміти предметну область, застосовувати знання у професійній діяльності.  РН17. Аналізувати та узагальнювати необхідну інформацію з різних джерел та ресурсів для вирішення професійних задач з урахуванням сучасних досягнень науки і техніки. |
| **Передумови для вивчення дисципліни:** | |
| Для вивчення навчальної дисципліни ««Захист інформації» необхідними є компетентності здобувачів фахової освіти з навчальних дисциплін «Інформатика», «Вища математика», «Алгоритми та структури даних», «Основи програмування», «Комп’ютерні мережі». Навчальна дисципліна забезпечує міжпредметні зв’язки з навчальними дисциплінами «Мобільні інформаційні технології». | |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **3. Обсяг та структура програми навчальної дисципліни** | | | | | | | | | | |
| **форма навчання** | | Кредити ЄКТС | **денна (очна)** | | | | | | | |
| **ФОРМА Контролю** | | **Підсумкові оцінки (екзамен)** | | | | | | | |
| № 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. | Тема 1. Основи безпеки інформації. |  | 14 | 8 | 6 | 4 |  | 2 |  |  |
| 2. | Тема 2. Основи та механізм захисту даних від несанкціонованого доступу. |  | 18 | 8 | 10 | 4 |  | 6 |  |  |
| 3. | Тема 3. Методи і засоби захисту інформації |  | 18 | 8 | 10 | 6 |  | 4 |  |  |
| 4. | Тема 4. Криптографічні методи захисту інформації |  | 22 | 12 | 14 | 4 |  | 10 |  |  |
| 5. | Тема 5Організаційно-правове забезпечення захисту інформації |  | 14 | 6 | 8 | 6 |  | 2 |  |  |
| **Разом з дисципліни:** | | **3** | **90** | **42** | **48** | **24** |  | **24** |  |  |

**4.1 Теми лекцій**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Назва тем курсу, лекційних занять та їх зміст** | **Кількість**  **годин** |
| 1 | **Тема 1. Основи захисту інформації** | **4** |
| 1.1 | ***Лекція 1.*** Поняття інтелектуальної власності. Важливість захисту інформації в сучасних умовах. Канали проникнення та принципи побудови систем захисту. Основи фізичного захисту об'єктів. | 2 |
| 1.2 | ***Лекція 2***. Причини існування комп'ютерних злодіїв. Методи проникнення до інформації у комп'ютері. | 2 |
| 2 | **Тема 2. Основи та механізм захисту даних від несанкціонованого доступу** | **4** |
| 2.1 | ***Лекція 3.*** Поняття про ідентифікацію користувача та її особливості. Основні принципи та методи аутентифікації. | 2 |
| 2.2 | ***Лекція 4.***Основні принципи захисту інформації від НСД Технічні можливості зловмисника і засоби знімання інформації. Технічні засоби захисту інформації від їх витоку. | 2 |
| 3 | **Тема 3. Методи і засоби захисту інформації** | **6** |
| 3.1 | ***Лекція 5.*** Технічні методи і засоби захисту інформації. | 2 |
| 3.2 | ***Лекція 6.*** Захист інформації в розподілених інформаційних системах | 2 |
| 3.4 | ***Лекція 7.*** Шкідливі програми. Засоби захисту від комп’ютерних вірусів та їх особливості. | 2 |
| 4 | **Тема 4. Криптографічні методи захисту інформації** | **4** |
| 4.1 | ***Лекція 8.*** Основні терміни та поняття криптографії. Історія та законодавча база криптографії. | 2 |
| 4.2 | ***Лекція 9.*** Сучасні криптосистеми та їх особливості. Класичні техніки шифрування. Симетричні та асиметричні алгоритми шифрування інформації. Цифрові підписи. Адміністрування ключами. | 2 |
| 5 | **Тема 5. Організаційно-правове забезпечення захисту інформації** | **6** |
| 5.1 | ***Лекція 10.*** Організаційно-правове забезпечення захисту інформації | 2 |
| 5.2 | ***Лекція 11.*** Міжнародні стандарти криптографічних методів захисту інформації | 2 |
| 5.3 | ***Лекція 12.*** Світові стандарти із захисту даних в комп’ютерних системах. Державний стандарт України із захисту інформації. | 2 |
| **Разом** | | **24** |

**4.2 Теми практичних занять**

|  |  |  |
| --- | --- | --- |
| **№**  **з/п** | **Назва теми** | **Кількість**  **годин** |
| 1. | Класичні техніки шифрування. | 2 |
| 2. | Дослідження шифру Цезаря. | 2 |
| 3. | Вивчення афінної системи шифрування Цезаря. | 2 |
| 4. | Шифрувальна система на основі шифру гаммування. | 2 |
| 5. | Виявлення вірусів в комп'ютерній системі. | 2 |
| 6. | Організаційні заходи щодо захисту інформації. | 2 |
| 7. | Система блочного шифрування S-DES. | 2 |
| 8. | Дослідження асиметричних криптосистем | 4 |
| 9. | Система шифрування RSA | 2 |
| 10 | Вивчення та оцінка використання цифрового підпису | 2 |
| 11. | Основні нормативно-правові документи з питань захисту інформації. | 2 |
| **Разом** | | **24** |

**4.3 Самостійна робота**

|  |  |  |
| --- | --- | --- |
| **№**  **з/п** | **Назва теми** | **Кількість**  **годин** |
| 1. | Сучасні заходи по забезпеченню безпеки програмних продуктів. | 4 |
| 2. | Основні сучасні програмно-технічні заходи забезпечення безпеки інформації. | 4 |
| 3. | Сучасні охоронні системи: види, особливості використання, переваги та недоліки. | 4 |
| 4. | Заходи щодо забезпечення безпеки інформації при роботі в мережі Internet. | 4 |
| 5. | Антивірусні програми: типи, властивості, особливості застосування. | 4 |
| 6. | Методи захисту від вірусів: види, переваги та недоліки | 4 |
| 7. | Сучасні системи кодування та стиску інформації: види, особливості побудови та застосування. | 4 |
| 8. | Криптографічні методи захисту інформації: технологія, особливості застосування. | 4 |
| 9. | Цифрові підписи як перспективна технологія захисту інформації. | 4 |
| 10 | Основні стандарти із захисту інформації в Україні: типи, їх характеристика. | 6 |
| **Разом** | | **42** |

**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 освіти з навчальною та довідковою літературою, самостійне виконання завдань, консультації. Використовуються демонстраційні вузли та компоненти комп’ютера, інструктивні картки для практичних робіт, картки з індивідуальними завданнями для практичних робіт. Використовується доступ до мережі інтернет.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **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 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 компетент-ності | | оцінка: | | |
| 4-бальна | | 2-бальна |  |
| **1** | | **2** | | **3** | **4** |
| Високий  (творчий) | | 5  (відмінно) | | зараховано | Здобувач освіти вiльно володiє програмовим матерiалом, виявляє здiбностi, вмiє самостiйно поставити мету дослiдження, вказує шляхи її реалiзацiї, робить аналiз та висновки.  Здобувач передвищої освіти вільно володієіеекекен 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  (конструкттивно-варіативний) | | 4  (добре) | | зараховано | 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 на комп’ютері, виправляти допущені неточностi, виявляє знання i розуміння програмного забезпечення на комп’ютері |
| Середній  (репродуктивний) | | 3  (задовіль-но) | | зараховано | Здобувач освіти може зi сторонньою допомогою пояснювати явища, виправляти допущені неточностi (власнi, iнших уч­нiв), виявляє елементарнi знання основних по­ложень функціонування комп’ютера (законiв, понять, формул).  Здобувач освіти описує явища, відтворює значну частину навчального матеріалу, знає складові комп’ютера, їх характеристики, записує основнi формули, рівняння i закони.  Здобувач освіти за допомогою викладача описує явища, без пояснень наводить приклади, що ґрунтуються на його власних спостереженнях чи матерiалi пiдручника, розповідях викладача тощо. |
| Початковий  (рецептивно-продуктивний) | 2  (незадо-вільно) | | Незарахо-вано | Здобувач освіти за допомогою викладача описує комп’ютер 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 на комп’ютері, 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. Швачич Г.Г., Толстой В.В., Петречук Л.М. Сучасні інформаційно-комунікаційні технології : навч. посіб. Дніпро : НМетАУ, 2017. 230 с.
      2. Захист інформації в комп’ютерних системах та мережах : навч. посіб. / С.Г. Семенов, А.О. Подорожняк, О.І. Баленко, С.Ю. Гавриленко Х.: НТУ «ХПІ», 2014. 251 с.
      3. Програмні технології захисту інформації: конспект лекцій для студентів за напрямом підготовки 6.050103 «Програмна інженерія» факультету інформаційних технологій УжНУ / Розробник: к.т.н. Поліщук В.В. Ужгород: 2018. 80 с.
      4. Технології захисту інформації [Електронний ресурс] : підручник для студ. спеціальності 122 «Комп’ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в інформаційних системах» / Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського. Київ : КПІ ім. Ігоря Сікорського, 2018. 162 с.
      5. Організація захисту інформації з обмеженим доступом: навч. посіб. /А.М.Гуз, І.П.Касперський, С.О.Князєв та ін. К.: Нац. акад., СБУ, 2018. 252 с.

**Додаткова**:

* + - 1. Безпека інформаційних систем і технологій : навчальний посібник [для студентів вищих навчальних закладів, які навчаються за напрямами підготовки «Безпека інформаційних і комунікаційних систем»] / В.І. Єсін, О.О. Кузнецов, Л.С. Сорока. Х. : ХНУ імені В.Н. Каразіна, 2013. 632 с.
      2. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник / [ В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін. ]. К. : ДУТ-КНУ, 2016. 178 с.
      3. Класичні методи криптології: методичні рекомендації для здобувачів спеціальностей «Прикладна математика» та «Системний аналіз» / М.М. Повідайчик, І.Я. Шпонтак. Ужгород: Видавництво УжНУ «Говерла», 2020. 28  с.
      4. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. НД ТЗІ 2.2.-002 -98, ДСТСЗІ СБ України, Київ, 1998.
      5. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. - НД ТЗІ 2.2-001-98, ДСТСЗІ СБ України, Київ, 1998.

**Інформаційні ресурси:**

1. АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ’ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ – Режим доступу: <https://cip.gov.ua/ua>
2. Лекції\_КК [Електронний ресурс]. – Режим доступу: <http://dspace.wunu.edu.ua/jspui/bitstream/316497/24961/1/%D0%9B%D0%B5%D0%BA%D1%86%D1%96%D1%97_%D0%9A%D0%9A.pdf>
3. Курс «Основи криптології» [Електронний ресурс]. – Режим доступу: <https://moodle.znu.edu.ua/course/view.php?id=4199>

**Перелік питань до іспиту**

1. Категорії інформаційної безпеки з точки зору інформації та інформаційних систем.
2. Технічні засоби захисту інформації.
3. Програмно-апаратні засоби захисту інформації.
4. Адміністративні засоби захисту інформації.
5. Визначення об’єкта захисту та можливих загроз.
6. Принцип розімкнутого управління захистом інформації.
7. Принцип зворотного зв’язку при захисті інформації.
8. Ідентифікація й аутентифікація.
9. Класи безпеки.
10. Критерії інформаційної безпеки.
11. Канали витоку інформації.
12. Класифікація інформації за рівнем конфіденційності.
13. Класифікація криптоалгоритмів.
14. Тайнопис, криптографія з ключем.
15. Симетричні криптоалгоритми.
16. Асиметричні криптоалгоритми.
17. Скремблери.
18. Мережа Фейcтеля.
19. Переставні криптоалгоритми.
20. Підставні криптоалгоритми.
21. Поточні, блочні шифри. Одиниці кодування.
22. Системи шифрування дискових даних (системи прозорого та спеціального видів шифрування).
23. Системи шифрування даних, які передаються в мережах (канальне та абонементне шифрування).
24. Системи аутентифікації електронних даних: електронний підпис.
25. Засоби управління криптографічними ключами: генерація, зберігання і розподілення ключів.
26. Стратегія захисту інформації у фінансово-економічних інформаційних системах.
27. Комплекс технічних засобів захисту інформації.
28. Комплекс програмних засобів захисту інформації.
29. Сучасна ситуація у сфері інформаційної безпеки.
30. Рівні мережних атак (фізичний, канальний) згідно із моделлю OSI.
31. Рівні мережних атак (мережний, транспортний, сеансовий) згідно із моделлю OSI.
32. Типи атак.
33. Вимоги при роботі з конфіденційною інформацією.
34. Технології цифрових підписів.
35. Значення інформаційної безпеки для суб’єктів інформаційних відносин.
36. Загрози інформаційної безпеки в Україні.
37. Українське законодавство про захист персональних даних.
38. Основні принципи захисту інформації.
39. Класифікація джерел та загроз інформаційній безпеці.
40. Конфіденційність інформації в мережі Інтернет.
41. Проблеми захисту інформації на підприємстві.
42. Загрози комерційного шпигунства.
43. Технічні канали витоку інформації.
44. Державна служба спеціального зв’язку та захисту інформації.
45. Загрози мовного перехоплення інформації зловмисниками
46. Види моделей політики інформаційної безпеки.
47. Запобігання витоку, розкраданню, втраті, підробці інформації.
48. Причини втрати і пошкодження інформації.
49. Види інформації за ступенем доступу.
50. Технології антивірусного захисту інформації.
51. Електронний цифровий підпис як програмно-технічний та правовий засіб захисту інформації.
52. Конфіденційна інформація та державна таємниця.
53. Захист персональних даних.
54. Параметри приватності та умови безпечного користування інформаційними ресурсами мережі Інтернет.
55. Типи комп’ютерних вірусів та їх шкода безпеці інформації.
56. Адміністративна, дисциплінарна, кримінальна відповідальності за порушення інформаційної безпеки.
57. Найбільш популярні джерела зараження комп’ютера вірусами.
58. Заходи щодо забезпечення захисту конфіденційної інформації.
59. Правовий захист інформації та його основні завдання.
60. Світові стандарти по захисту інформації