

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ  
імені адмірала Макарова

Навчально-науковий інститут автоматики та електротехніки  
Кафедра комп'ютерних технологій та інформаційної безпеки

Код за ОПП  
ОК36

ЗТВЕРДЖУЮ  
Проректор з науково-педагогічної  
роботи, к.т.н., доцент  
С.О. Слободян  
«\_\_\_» \_\_\_\_\_ 2022 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ  
*Program of the Discipline*

БЕЗПЕКА ІНФОРМАЦІЙНИХ ТА КОМУНІКАЦІЙНИХ  
СИСТЕМ

**Information and communication systems security**

Рівень вищої освіти \_\_\_\_\_ перший (бакалаврський)

Тип дисципліни \_\_\_\_\_ обов'язкова

Мова викладання \_\_\_\_\_ українська

Миколаїв 2022 рік

Робоча програма навчальної дисципліни «Безпека інформаційних та комунікаційних систем» є однією із складових комплексної підготовки фахівців галузі знань 15 «Автоматизація та приладобудування», спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології», освітня програма «Комп'ютерно-інтегровані технології та системи автоматизації»  
«\_\_\_» \_\_\_\_\_ 2022 р. – 25 с.

Розробник: Турти М.В., доцент кафедри Комп'ютерних технологій та інформаційної безпеки, канд. техн. наук, доцент

Проект робочої програми навчальної дисципліни «Безпека інформаційних та комунікаційних систем» узгоджено з гарантом освітньої програми  
Гарант освітньої програми «Комп'ютерно-інтегровані технології та системи автоматизації» Вінниченко І.Л., доцент кафедри комп'ютеризованих систем управління, канд. техн. наук, доцент

Проект робочої програми навчальної дисципліни «Безпека інформаційних та комунікаційних систем» розглянуто на засіданні кафедри КСУ.

Протокол від «26» 09 2022 р. № 2.

Завідувач кафедри КСУ, д.т.н., доцент \_\_\_\_\_ О.О. Черно

Проект робочої програми навчальної дисципліни «Безпека інформаційних та комунікаційних систем» розглянуто на засіданні кафедри КТІБ.

Протокол від «29» 08 2022 р. № 1.

Завідувач кафедри КТІБ, к.т.н., доцент \_\_\_\_\_ С.М. Нужний

Проект робочої програми навчальної дисципліни «Безпека інформаційних та комунікаційних систем» розглянуто методичною радою Навчально-наукового інституту автоматики та електротехніки.

Протокол від «20» 10 2022 р. № 3.

Голова \_\_\_\_\_

Проект робочої програми навчальної дисципліни «Безпека інформаційних та комунікаційних систем» погоджено з навчальним відділом.

Начальник навчального відділу, к.т.н., доцент \_\_\_\_\_ А.В. Лабарткава

Робочу програму навчальної дисципліни «Безпека інформаційних та комунікаційних систем» затверджено Навчально-методичною радою НУК ім. адм. Макарова.

Протокол від «26» 10 2022 р. № 8.

Голова Навчально-методичної ради НУК ім. адм. Макарова,

д.т.н., професор \_\_\_\_\_ Є.І. Трушляков

## ЗМІСТ

|                                                                                                 |    |
|-------------------------------------------------------------------------------------------------|----|
| Вступ.....                                                                                      | 4  |
| 1. Опис навчальної дисципліни .....                                                             | 5  |
| 2. Мета вивчення навчальної дисципліни .....                                                    | 6  |
| 3. Передумови для вивчення навчальної дисципліни .....                                          | 6  |
| 4. Очікувані результати навчання .....                                                          | 7  |
| 5. Програма навчальної дисципліни .....                                                         | 7  |
| 6. Методи навчання, засоби діагностики результатів навчання та методи їх<br>демонстрування..... | 12 |
| 7. Форми поточного та підсумкового контролю .....                                               | 14 |
| 8. Критерії оцінювання результатів навчання.....                                                | 15 |
| 9. Засоби навчання .....                                                                        | 19 |
| 10. Рекомендовані джерела інформації.....                                                       | 20 |
| Додаток А. Перелік питань, що виносяться на вивчення.....                                       | 22 |

## ВСТУП

### Анотація

Навчальна дисципліна «Безпека інформаційних та комунікаційних систем» є дисципліною професійної підготовки бакалаврів зі спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології». Дана дисципліна є обов'язковим компонентом освітньої програми, який забезпечує здобуття студентами теоретичних відомостей про принципи побудови і формування практичних умінь створення захищених інформаційних та комунікаційних систем. Отримані слухачами курсу теоретичні знання та практичні навички є базовим програмним результатом навчання та формують фахову компетентність.

**Ключові слова:** інформаційно-комунікаційні системи, типові вразливості, віддалена атака, захист на рівні операційних систем, захист розподілених мереж

### Abstract

The educational discipline " Information and communication systems security " is a discipline of professional training of bachelors in the specialty 151 "Automation and computer-integrated technologies". This discipline is a mandatory component of the educational program, which ensures that students acquire theoretical information about the principles of construction and formation of practical skills for creating protected information and communication systems. The theoretical knowledge and practical skills acquired by the course participants are the basic program learning outcome and form professional competence.

**Keywords:** information and communication systems, typical vulnerabilities, remote attack, protection at the level of operating systems, protection of distributed networks

## 1 Опис навчальної дисципліни

| Найменування показників                                                                                 | Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень                                                                                                   | Характеристика навчальної дисципліни     |                       |
|---------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|-----------------------|
|                                                                                                         |                                                                                                                                                                    | денна форма навчання                     | заочна форма навчання |
| Кількість кредитів – 3                                                                                  | <p><b>Галузь знань</b></p> <p>15 Автоматизація та приладобудування</p> <p><b>Спеціальність:</b></p> <p>151 Автоматизація та комп'ютерно-інтегровані технології</p> | Обов'язкова                              |                       |
| Модулів – 1                                                                                             | <p><b>Освітня програма</b></p> <p>«Комп'ютерно-інтегровані технології та системи автоматизації»</p>                                                                | <b>Рік підготовки</b>                    |                       |
| Змістових модулів – 2                                                                                   |                                                                                                                                                                    | 2-й                                      | 2-й                   |
|                                                                                                         |                                                                                                                                                                    | <b>Семестр</b>                           |                       |
| Загальна кількість годин – 90                                                                           |                                                                                                                                                                    | 4-й                                      | 4-й                   |
| <p>Тижневих годин для денної форми навчання:</p> <p>Аудиторних – 2;</p> <p>Самостійної роботи: – 4.</p> | <p>Рівень вищої освіти:</p> <p><b>перший</b></p> <p><b>(бакалаврський)</b></p>                                                                                     | <b>Лекції, год</b>                       |                       |
|                                                                                                         |                                                                                                                                                                    | 15 год.                                  | 4 год.                |
|                                                                                                         |                                                                                                                                                                    | <b>Лабораторні роботи, год</b>           |                       |
|                                                                                                         |                                                                                                                                                                    | 15 год.                                  | 4 год.                |
|                                                                                                         |                                                                                                                                                                    | <b>Практичні роботи, год</b>             |                       |
|                                                                                                         |                                                                                                                                                                    | -                                        | -                     |
|                                                                                                         |                                                                                                                                                                    | <b>Самостійна робота, год</b>            |                       |
|                                                                                                         |                                                                                                                                                                    | 60                                       | 82                    |
|                                                                                                         |                                                                                                                                                                    | <b>Вид контролю:</b><br>Екзамен          |                       |
|                                                                                                         |                                                                                                                                                                    | <b>Форма контролю:</b><br>усна, письмова |                       |

## **2. Мета та завдання навчальної дисципліни**

**Метою** вивчення навчальної дисципліни «Безпека інформаційних та комунікаційних систем» є ознайомлення студентів із теоретичними методами побудови захищених інформаційних і комунікаційних систем та здобуття практичних навичок налагодження ефективних систем захисту з врахуванням особливостей їх апаратної та програмної реалізації.

**Завданнями дисципліни** є теоретична та практична підготовка студентів для вирішення конкретних фахових питань, зокрема: обґрунтування прийняття проектних рішень в галузі захисту інформації в телекомунікаційних мережах і системах на основі аналізу загроз і моделі порушника; здобуття практичних навичок застосування спеціалізованого програмного і апаратного забезпечення для захисту інформації в телекомунікаційних мережах і системах для формування наступних компетентностей.

- (ЗК4) - Навички використання інформаційних і комунікаційних технологій;
- (ФК9) - Здатність вільно користуватись сучасними комп'ютерними та інформаційними технологіями для вирішення професійних завдань, програмувати та використовувати прикладні та спеціалізовані комп'ютерно-інтегровані середовища для вирішення задач автоматизації.

## **3. Передумови для вивчення навчальної дисципліни**

Для ефективного вивчення дисципліни «Безпека інформаційних та комунікаційних систем», студенти повинні засвоїти матеріал з дисциплін:

- Інформаційні технології систем управління та захисту інформації;
- Вища математика;
- Системи і мережі передачі даних.

## 4. Очікувані результати навчання

Основними (програмними) результатами навчання з дисципліни «Безпека інформаційних та комунікаційних систем» є:

– (ПРНЗ) – Вміти застосовувати сучасні інформаційні технології та мати навички розробляти алгоритми та комп'ютерні програми з використанням мов високого рівня та технологій об'єктно-орієнтованого програмування, створювати бази даних та використовувати інтернет-ресурси.

## 5. Програма навчальної дисципліни

### Модуль 1

**Змістовий модуль 1.** Основні принципи побудови захищених інформаційно-телекомунікаційних систем.

**Тема 1.** Базові поняття в галузі захисту інформаційно-телекомунікаційних систем. [1] – с.12-21; [3] – с.7-16, 57-61, 64-70, 74-80; [4] – с.18-26, 32-34, 62-75, 142-187, 316-332; [5] – с.26-31; [6-10]; [15]; [17] – с.71-84.

**Тема 2.** Вразливості і загрози інформаційно-комунікаційних систем [1] – с.27-30; [3] – с.24-29; [4] – с.27-30, 31-32, 78-97, 329-339; [5] – с.18-26; [17] - с.64-71; [30].

**Тема 3.** Типові віддалені атаки [1] – с.648-667; [3] – с.44-53; [4] – с.30-31; [16].

**Тема 4.** Шкідливі програмні засоби [1] – с.667-670; [3] – с.53, 80-84, 112-136; [4] – с.99-135; [5] – с.112-121.

**Змістовий модуль 2.** Базові засоби захисту інформації в інформаційно-телекомунікаційних системах

**Тема 5.** Організація захисту інформації в інформаційно-комунікаційних системах [1] – с.671-677; [2] – с.20-37; [3] – с.35-42, [4] – с.37-49, 333-340; [5] – с.7-17; [6-14]; [17] – с.38-54; [18]; [19].

**Тема 6.** Захист інформації в операційних системах [4] – с.189-312; [5] – с.73-82, 206-210.

**Тема 7.** Міжмережевий екран [1] – с.694-711; [2] – с.63-66; [4] – с.465-474; [5] - с.62-95; [20].

**Тема 8.** Безпека мережевих Інтернет-протоколів [4] – с.343-408, 500-508; [5] – с.170-174, 178-206.

### Тематичний план навчальної дисципліни

| Назви змістових модулів і тем                                                                   | Кількість годин |              |     |      |              |              |     |      |
|-------------------------------------------------------------------------------------------------|-----------------|--------------|-----|------|--------------|--------------|-----|------|
|                                                                                                 | денна форма     |              |     |      | заочна форма |              |     |      |
|                                                                                                 | усього          | у тому числі |     |      | усього       | у тому числі |     |      |
|                                                                                                 |                 | л            | лаб | с.р. |              | л            | лаб | с.р. |
| Модуль 1 (М1)                                                                                   |                 |              |     |      |              |              |     |      |
| Змістовий модуль 1. Основні принципи побудови захищених інформаційно-телекомунікаційних систем  |                 |              |     |      |              |              |     |      |
| Тема 1. Базові поняття в галузі захисту інформаційно-телекомунікаційних систем                  | 10              | 2            | 2   | 6    | 10           | 2            | -   | 8    |
| Тема 2. Вразливості і загрози інформаційно-комунікаційних систем                                | 6               | 2            | -   | 4    | 6            |              | -   | 6    |
| Тема 3. Типові віддалені атаки                                                                  | 6               | 2            | -   | 4    | 6            |              | -   | 6    |
| Тема 4. Шкідливі програмні засоби                                                               | 8               | 2            | 1   | 5    | 8            |              | 1   | 7    |
| Разом за змістовим модулем 1                                                                    | 30              | 8            | 3   | 19   | 30           | 2            | 1   | 27   |
| Змістовий модуль 2. Базові засоби захисту інформації в інформаційно-телекомунікаційних системах |                 |              |     |      |              |              |     |      |
| Тема 5. Організація захисту інформації в інформаційно-комунікаційних системах                   | 6               | 2            | -   | 4    | 6            | 2            | -   | 4    |
| Тема 6. Захист інформації в операційних системах                                                | 36              | 2            | 10  | 24   | 36           |              | 2   | 34   |
| Тема 7. Міжмережевий екран                                                                      | 12              | 2            | 2   | 8    | 12           |              | 1   | 11   |
| Тема 8. Безпека мережевих Інтернет-протоколів                                                   | 6               | 1            | -   | 5    | 6            |              | -   | 6    |
| Разом за змістовим модулем 2                                                                    | 60              | 7            | 12  | 41   | 60           | 2            | 3   | 55   |
| Разом                                                                                           | 90              | 15           | 15  | 60   | 90           | 4            | 4   | 82   |

Для студентів заочної форми навчання читаються оглядові лекції за темами змістових модулів в обсягах відповідно до вищенаведеної таблиці.

### Теми практичних занять

Практичні роботи програмою не передбачені

### Теми лабораторних занять

| № з/П                           | Назва теми                                                            | Кількість годин |          |
|---------------------------------|-----------------------------------------------------------------------|-----------------|----------|
|                                 |                                                                       | ДФН             | ЗФН      |
| 1                               | Захист інформації засобами BIOS                                       | 2               | -        |
| 2                               | Захист від вірусних загроз                                            | 1               | 1        |
| 3                               | Налаштування доступу користувачів до інформаційних ресурсів в Windows | 2               | 1        |
| 4                               | Захист файлових ресурсів                                              | 2               | -        |
| 5                               | Налаштування локальної політики безпеки в Windows                     | 2               | 1        |
| 6                               | Захищене резервне копіювання та відновлення                           | 2               | -        |
| 7                               | Система аудиту доступу до ресурсів у Windows                          | 2               | -        |
| 8                               | Робота брандмауера в Windows                                          | 2               | 1        |
| <i>Усього годин за модуль 1</i> |                                                                       |                 |          |
| <b>Разом за курсом</b>          |                                                                       | <b>15</b>       | <b>4</b> |

Студенти заочної форми виконують роботи № 2, 3, 5, 8 із розрахунку 1 год./ 1 лаб. роботу.

### Самостійна робота

Самостійна робота здобувача вищої освіти є однією з форм організації навчання, основною формою оволодіння навчального матеріалу в час, вільний від обов'язкових навчальних занять.

Метою самостійної роботи є повторення й осмислення студентом основних питань кожної теми, висвітлених на лекційних і лабораторних заняттях. Самостійна робота проводиться в лабораторіях НУК, читальних залах, на об'єктах майбутньої діяльності і/або вдома. Результати цієї роботи фіксуються студентом в індивідуальному робочому зошиті (конспекті).

Навчальний матеріал дисципліни, передбачений для засвоєння здобувачем вищої освіти в процесі самостійної роботи, виноситься на підсумковий контроль поряд з навчальним матеріалом, який опрацьовувався при проведенні навчальних занять.

*Розподіл годин самостійної роботи для денної форми навчання:*

- підготовка до лекційних занять – 0,5 год. / 1 заняття (на 1 лекцію);

- самостійне опрацювання окремих тем навчальної дисципліни (які не викладаються на лекціях) – 1-3 год. / 1 заняття;
- підготовка до лабораторних занять – 1 год. / 1 заняття;
- підготовка до модульних контрольних робіт 2-15 год на 1 роботу
- підготовка до екзамену – 15 год. на 1 захід.

*Розподіл годин самостійної роботи для заочної форми навчання:*

- підготовка до лекційних занять – 0,5 - 2 год. / 1 заняття (на 1 лекцію);
- самостійне опрацювання окремих тем навчальної дисципліни (які не викладаються на лекціях) – 1-3 год. / 1 заняття;
- підготовка до лабораторних занять – 2-3 год. / 1 заняття;
- підготовка до модульних контрольних робіт 8-15 год на 1 роботу
- підготовка до екзамену – 15-30 год. на 1 захід.

**Розподіл годин самостійного опрацювання окремих тем навчальної дисципліни**

| №<br>з/п                 | Назва теми                                                                                            | Кількість<br>годин |        |
|--------------------------|-------------------------------------------------------------------------------------------------------|--------------------|--------|
|                          |                                                                                                       | Д.Ф.Н              | З.Ф.Н. |
| М1                       |                                                                                                       |                    |        |
| 1                        | До теми 1. Захист інформації засобами BIOS                                                            | 0,25               | 0,5    |
| 2                        | До теми 2. Нормативно-правове забезпечення захисту інформації в телекомунікаційних системах і мережах | 0,5                | 0,5    |
| 3                        | До теми 3. Статистика віддалених атак на розподілені обчислювальні системи                            | 0,25               | 0,5    |
| 4                        | До теми 4. Сучасні антивірусні програми                                                               | 0,25               | 0,5    |
| 5                        | До теми 5. Сучасні апаратні засоби побудови захищених телекомунікаційних систем і мереж               | 0,5                | 0,5    |
| 6                        | До теми 6. Сучасні програмні засоби побудови захищених телекомунікаційних систем і мереж              | 0,5                | 1      |
| 7                        | До теми 7. Сучасні засоби інспекції потоків даних                                                     | 0,5                | 1      |
| 8                        | До теми 8. Мультиагентні системи захисту інформації                                                   | 0,25               | 0,5    |
| Усього годин за модуль 1 |                                                                                                       | 3                  | 5      |
| Разом за курсом          |                                                                                                       | 3                  | 5      |

### Розподіл годин підготовки самостійної роботи

| №                        | Вид роботи                                               | Кількість годин |     |
|--------------------------|----------------------------------------------------------|-----------------|-----|
|                          |                                                          | ДФН             | ЗФН |
| М1                       |                                                          |                 |     |
| 1                        | Підготовка до лекцій                                     | 4               | 1   |
| 2                        | Підготовка до лабораторних робіт                         | 8               | 10  |
| 3                        | Підготовка до модульних контрольних робіт                | 30              | 30  |
| 4                        | Самостійне опрацювання окремих тем навчальної дисципліни | 3               | 5   |
| 5                        | Підготовка до екзамену                                   | 15              | 30  |
| Усього годин за модуль 1 |                                                          | 60              | 76  |
| Разом за курсом          |                                                          | 240             | 317 |

### Індивідуальне науково-дослідне завдання

Програмою не передбачено виконання навчально-дослідного завдання.

### 6. Методи навчання, засоби діагностики результатів навчання та методи їх демонстрування

Здобувач зобов'язаний вивчити теоретичний матеріал та здобути практичні навички у відповідності до тематичного плану навчальної дисципліни.

*Методами навчання є:*

- пояснення, демонстрування;
- лекція; відеометод;
- робота з літературою;
- лабораторна робота;
- інструктаж (інструктаж з техніки безпеки та пожежної безпеки проводиться одноразово на першому занятті в лабораторії);
- репродуктивний метод;
- проблемного викладу.

При вивченні дисципліни використовуються 3 групи методів навчання:

I група методів - методи організації та здійснення навчально-пізнавальної діяльності:

- словесні: розповідь-пояснення, лекція;
- наочні: ілюстрація, презентація, демонстрація;

- практичні: лабораторні роботи;
- індуктивні методи: узагальнення, пов'язані із проведенням експериментів;
- дедуктивні методи: розвиток абстрактного мислення для засвоєння навчального матеріалу на основі узагальнень;
- репродуктивні методи: робота за готовими прикладами;
- творчі, проблемно-пошукові методи: самостійна, творча пізнавальна діяльність;
- навчальна робота студентів під керівництвом НПП;
- самостійна робота студентів.

II група методів - методи стимулювання й мотивації навчально-пізнавальної діяльності:

- методи стимулювання інтересу до навчання: створення ситуації інтересу при викладанні матеріалу; аналіз життєвих ситуацій;
- методи стимулювання обов'язку й відповідальності: роз'яснення мети навчального предмета; вимоги до вивчення предмета; заохочення та покарання в навчанні;

III група методів - методи контролю (самоконтролю, взаємоконтролю), корекції (самокорекції, взаємокорекції) за ефективністю навчально-пізнавальної діяльності:

*Засобами* оцінювання результатів навчання є:

- модульні контрольні роботи;
- звіти з лабораторних робіт;
- командні проекти; індивідуальні та групові завдання;
- завдання на лабораторному обладнанні;
- екзаменаційна робота;
- комплексна контрольна робота (за необхідністю).

*Методами* демонстрування результатів навчання є:

- усні відповіді;
- письмові відповіді;
- виконання завдань із застосуванням комп'ютерної техніки;
- оформлення звітів з лабораторних робіт;
- презентації результатів виконаних завдань та досліджень.

Допускається застосування дистанційних технологій для діагностики результатів навчання.

## 7. Форми поточного та підсумкового контролю

Досягнення здобувача вищої освіти оцінюються за 100-бальною системою Університету.

*Поточний контроль* проводиться в межах навчальних занять і передбачає оцінювання теоретичної підготовки здобувачів вищої освіти із зазначених тем (у тому числі, самостійно опрацьованого матеріалу) та практичних навичок, набутих під час виконання лабораторних робіт.

Поточний контроль здійснюється протягом семестру в наступних формах:

- перевірка екзаменаційних робіт;
- перевірка та захист звітів з лабораторних робіт;
- проведення та перевірка модульних контрольних робіт;
- контрольна робота на заочній формі навчання;
- семестрова атестація;
- перевірка конспекту лекцій;
- контроль відвідування занять.

Перевірка звіту з лабораторної роботи включає оцінювання правильності та повноти виконання завдання, правильності та повноти висновків, правильності оформлення звіту.

Процедура захисту звіту з лабораторної роботи включає один або декілька елементів:

- письмове викладення відповідей на запитання за тематикою роботи;
- усне опитування за тематикою роботи;
- виконання завдань із застосуванням комп'ютерної техніки.

При виконанні модульних контрольних робіт здобувач вищої освіти відтворює засвоєні знання шляхом надання письмових відповідей на поставлені запитання. На теоретичні запитання необхідно давати розгорнуті відповіді, супроводжуючи їх прикладами та ілюстраціями. Повнота відповідей оцінюється згідно з теоретичним матеріалом, наведеним у джерелах інформації для кожної теми. На тестові запитання потрібно вказати номер правильної відповіді та її формулювання.

Контрольна робота на заочній формі навчання за змістом є об'єднаним представленням модульних контрольних робіт, які проводяться для здобувачів

денної форми навчання, і має відповідати тим самим вимогам. Контрольна робота на заочній формі навчання виконується протягом семестру і здається до проведення підсумкового контролю.

Поточний модульний контроль проводиться з урахуванням даних поточного контролю за відповідний змістовний модуль і має на меті оцінку результатів знань студента після вивчення матеріалу з логічно завершеної частини дисципліни – змістового модуля.

Семестрова атестація дає змогу здійснити проміжну оцінку досягнень здобувача вищої освіти. В період семестрової атестації викладач оцінює результати поточного контролю та атестує чи не атестує здобувача вищої освіти.

За рішенням кафедри студентам, які брали участь у науково-дослідній роботі – роботі конференцій, студентських наукових гуртків, підготовці публікацій, а також були учасниками олімпіад, конкурсів, тощо можуть присуджуватися додаткові бали. Додаткові бали також можуть присуджуватися за результатами перевірки конспекту лекцій, контролю відвідування занять та за активність на лекціях і лабораторних заняттях.

За всі поточні контрольні заходи протягом семестру, з урахуванням додаткових балів, студент сумарно може отримати від 0 до 100 балів.

Умовою допуску студента до семестрового підсумкового контролю є мінімальна сума у 60 балів, яку студент повинен набрати у разі виконання всіх елементів модулів.

Семестровий підсумковий контроль з дисципліни проводиться відповідно до навчального плану у вигляді *екзамену* в терміни, встановлені графіком навчального процесу, та в обсязі навчального матеріалу, визначеному робочою програмою навчальної дисципліни.

Студент, який набрав за всі поточні контрольні заходи менше 60 балів або хоче отримати додаткові бали, пише семестрову екзаменаційну роботу (проводиться у письмовій формі), до якої він допускається, якщо має за виконання всіх передбачених елементів модулів не менше 35 балів.

Максимальна кількість балів за семестрову підсумкову екзаменаційну роботу (екзамен) становить 40 балів. Студенти заочної форми навчання пишуть підсумкову екзаменаційну роботу обов'язково.

Підсумкова оцінка з дисципліни від 60 до 100 балів визначається як сума балів за змістовими модулями та семестрової екзаменаційної роботи (у разі її написання).

Зарахування кредитів навчального курсу можливе тільки після досягнення результатів, запланованих РПНД, що виражається в одній з позитивних оцінок, передбачених чинним законодавством.

## **8. Критерії оцінювання результатів навчання**

### **8.1 Критерії оцінювання лабораторних робіт**

При оцінюванні лабораторних робіт враховуються наступні критерії:

- виконання роботи та правильність виконання;
- наявність звіту, вчасність подачі та якість звіту;
- захист звіту.

Максимальна оцінка за кожну лабораторну роботу для ДФН – 5 балів, для ЗФН – 6 балів.

Максимальна сумарна кількість балів за лабораторні роботи становить:

- для студентів ДФН:  $8 \times 5 = 40$  балів;
- для студентів ЗФН:  $4 \times 6 = 24$  бали.

### Критерії оцінювання лабораторних робіт

| Кількість балів<br>(в дужках для ЗФН) | Критерії оцінювання                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>М1</b>                             |                                                                                                                                                                                                                                                                                                                                                                     |
| 5 (6)                                 | Роботу виконано самостійно, завдання виконано правильно. Звіт здано у встановлений термін, оформлення звіту повністю відповідає вимогам, у висновках проведено коректну інтерпретацію результатів. Студент надав правильні відповіді на всі питання захисту.                                                                                                        |
| 4 (5)                                 | Робота виконана правильно з консультаціями викладача. Звіт здано у встановлений термін, можливі несуттєві помилки в оформленні звіту та незначні некоректності у висновках. Студент надав принципово правильні відповіді на питання захисту (без суттєвих помилок).                                                                                                 |
| 3 (4)                                 | Роботу виконано із підказками викладача та незначними помилками. Звіт містить неточності у висновках та окремі помилки. Студент відповів на питання захисту частково чи з принциповими помилками.                                                                                                                                                                   |
| 2 (3)                                 | Завдання виконано у повному об'ємі але з помилками. Звіт містить неточності у висновках та окремі помилки. Студент не відповів на питання захисту.                                                                                                                                                                                                                  |
| 1 (1)                                 | Завдання виконано не у повному об'ємі (не менше 70%). Надано звіт, що містить неточності і помилки. Студент не відповів на питання захисту.                                                                                                                                                                                                                         |
| 0 (0)                                 | Робота не виконана.                                                                                                                                                                                                                                                                                                                                                 |
|                                       | <i>Максимальна сумарна оцінка студента за даний компонент програми для ДФН – 40 балів (8 робіт по 5 балів). Максимальна сумарна оцінка студента за даний компонент програми для ЗФН – 30 балів (5 робіт по 6 балів). При незначних відхиленнях від вказаних критеріїв оцінка може доповнюватись знаками «-» або «+», що при підсумовуванні відповідає 0,5 бала.</i> |

### 8.2 Критерії оцінювання модульних контрольних робіт

Для поточного модульного контролю студентами виконуються дві модульні контрольні роботи за матеріалами змістовних модулів.

Критерієм оцінювання МКР є відсоток правильних відповідей на питання МКР.

Максимальна кількість балів за кожну МКР становить:

- для студентів ДФН: 10 балів;
- для студентів ЗФН: 18 балів.

Загальна сума балів за модульні контрольні роботи становить:

- для студентів ДФН:  $2 \times 10 = 20$  балів;
- для студентів ЗФН:  $2 \times 18 = 36$  балів;

### Критерії оцінювання задач та практичних завдань в МКР для ДФН

|                             |     |    |    |    |    |    |    |    |    |    |
|-----------------------------|-----|----|----|----|----|----|----|----|----|----|
| Правильних<br>відповідей, % | 100 | 90 | 80 | 70 | 60 | 50 | 40 | 30 | 20 | 10 |
| Бал                         | 10  | 9  | 8  | 7  | 6  | 5  | 4  | 3  | 2  | 1  |

### Критерії оцінювання задач та практичних завдань в МКР для ЗФН

|                             |     |      |      |      |      |     |     |     |     |     |
|-----------------------------|-----|------|------|------|------|-----|-----|-----|-----|-----|
| Правильних<br>відповідей, % | 100 | 90   | 80   | 70   | 60   | 50  | 40  | 30  | 20  | 10  |
| Бал                         | 18  | 16,2 | 14,4 | 12,6 | 10,8 | 9,0 | 7,2 | 5,4 | 3,6 | 1,8 |

### 8.3 Критерії оцінювання екзаменаційної роботи

Максимальна оцінка за екзаменаційну роботу – 40 балів.

|                             |     |    |    |    |    |    |    |    |    |    |
|-----------------------------|-----|----|----|----|----|----|----|----|----|----|
| Правильних<br>відповідей, % | 100 | 90 | 80 | 70 | 60 | 50 | 40 | 30 | 20 | 10 |
| Бал                         | 40  | 36 | 32 | 28 | 24 | 20 | 16 | 12 | 8  | 4  |

### Рівні підсумкової оцінки екзамену з дисципліни (перерахунковий коефіцієнт – 0,4)

| Оцінка за 100-бальною шкалою<br>університету /<br>Grade according to 100-points scale of<br>University | Оцінка за шкалою ЄКТС /<br>Grade according to ECTS scale                                                                        |
|--------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>90-100</b><br>(творчий рівень)/(creative level)                                                     | <b>A</b> (відмінно) / (excellent)                                                                                               |
| <b>82-89</b><br>(високий рівень)/(high level)                                                          | <b>B</b> (дуже добре) / (very good)                                                                                             |
| <b>74-81</b><br>(добрий рівень)/(good level)                                                           | <b>C</b> (добре) / (good)                                                                                                       |
| <b>64-73</b><br>(середній рівень)/(average level)                                                      | <b>D</b> (посередньо) / (average)                                                                                               |
| <b>60-63</b><br>(задовільний рівень)/(satisfactory level)                                              | <b>E</b> (достатньо) / (satisfactory)                                                                                           |
| <b>35-59</b><br>(низький рівень)/(low level)                                                           | <b>FX</b> (незадовільно з можливістю повторного<br>складання) / (unsatisfactory with the possibility<br>to repass the exam)     |
| <b>1-34</b><br>(незадовільний рівень)/(unsatisfactory level)                                           | <b>F</b> (незадовільно з обов'язковим повторним<br>вивченням) / (unsatisfactory with the<br>compulsory repeating of the course) |

## 8.4 Розподіл балів

### Розподіл оцінки за змістовними модулями та видами контролю

|                                  |      | Денна форма                      |                 | Заочна форма            |                 |
|----------------------------------|------|----------------------------------|-----------------|-------------------------|-----------------|
|                                  |      | Вид роботи                       | Кількість балів | Вид роботи              | Кількість балів |
| <b>М1</b>                        |      |                                  |                 |                         |                 |
| ЗМ1                              | T1   | Лабораторна робота 1             | 5               | -                       | --              |
|                                  | T2   | -                                | -               | -                       | -               |
|                                  | T3   | -                                | -               | -                       | -               |
|                                  | T4   | Лабораторна робота 2             | 5               | Лабораторна робота 2    | 6               |
|                                  | МКР1 | Тест                             | 10              | Тест                    | 18              |
| ЗМ2                              | T5   | -                                | -               | -                       | -               |
|                                  | T6   | Лабораторні роботи 3, 4, 5, 6, 7 | 25              | Лабораторні роботи 3, 5 | 12              |
|                                  | T7   | Лабораторна робота 8             | 5               | Лабораторна робота 8    | 6               |
|                                  | T8   | -                                | -               | -                       | -               |
|                                  | МКР2 | Тест                             | 10              | Тест                    | 18              |
| Підсумковий семестровий контроль |      | екзамен                          | 40              | екзамен                 | 40              |
| Всього                           |      |                                  | 100             | 100                     |                 |

## 9. Засоби навчання

Апаратне забезпечення, необхідне для вивчення навчальної дисципліни, включає персональний комп'ютер (настільний або ноутбук) та спеціалізовані лабораторні стенди із доступом до Інтернет.

Програмне забезпечення, необхідне для вивчення навчальної дисципліни, включає операційні системи (Windows, Linux), спеціалізоване програмне забезпечення для захисту комп'ютерних мереж (брандмауери, антивірусні програми, засоби боротьби із спамом), спеціалізоване програмне забезпечення для інженерних розрахунків та моделювання технічних засобів, текстовий процесор та редактор растрових зображень (для підготовки звітів з практичних робіт); pdf-, djv-переглядач (для ознайомлення з джерелами інформації, представленими в електронному вигляді).

Використовуються апаратні та програмні можливості лабораторії №130, кафедри КТІБ ННІАЕ НУК.

## 10. Рекомендовані джерела інформації

### Основна література

#### Навчально-методична література

1. Бабак В.П., Ключников А.А. Теоретические основы защиты информации: учебник / В.П. Бабак, А.А. Ключников; НАН Украины, Ин-т проблем безопасности АЭС. - Чернобыль (Киев.обл.) : Ин-т проблем безопасности АЭС, 2012. - 776 с.
2. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.
3. Бурячок В. Л., Толубко В.Б., Хорошко В. О., Толюпа С.В. Інформаційна та кібербезпека: соціотехнічний аспект. [Підручник]. / В. Л. Бурячок, В.Б. Толубко, В. О. Хорошко, С.В. Толюпа. – Львів. : «Магнолія 2006», 2018. – 320 с.
4. Гайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BVH, 2009. – 608 с.
5. Жилін А. В. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.

#### Нормативно-правова база

##### Закони України:

6. 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>
7. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»/ URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>
8. Закон України “Про основні засади забезпечення кібербезпеки України». URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
9. Стратегія кібербезпеки України : Указ Президента України від 15.03.2016 р. № 96/2016// Офіційний вісник України. – 2016. – № 23. – С. 69. – Ст. 899. <https://zakon.rada.gov.ua/laws/show/96/2016#Text>

##### Нормативні документи системи ТЗІ:

10. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 28.04.99 № 22
11. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 28.04.99 № 22 (Зміна № 1 наказ від 28.12.2012 № 806)
12. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблювальної інформації від

несанкціонованого доступу, наказ ДСТСЗІ СБУ від 28.04.99 № 22 (Зміна № 1 наказ від 15.10.2008 № 172)

Постанови кабінету міністрів України

13. Порядок функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, затверджений постановою №1295 Кабінету міністрів України 23.12.2020. URL: <https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF>

14. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою Кабінету Міністрів України від 29.03.06 № 373

### Допоміжна література

Навчально-методична література

15. 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.

16. Васильцов І.В. Атаки спеціального виду на криптопристрої та методи боротьби з ними. – Кременець: Видавничий центр КОГПІ, 2009.- 294.с.

17. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник.– К.: Видавництво НА СБ України, 2020. – 256 с. URL: [http://www.immsp.kiev.ua/postgraduate/Biblioteka\\_trudy/Gulak\\_MetodolZahystuInfOsnKiberbezp\\_2020.pdf](http://www.immsp.kiev.ua/postgraduate/Biblioteka_trudy/Gulak_MetodolZahystuInfOsnKiberbezp_2020.pdf).

18. Команда реагування на комп'ютерні надзвичайні події України: URL: <https://cert.gov.ua/>

19. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах: Навчальний посібник / В. Д. Козюра, В. О. Хорошко, М. Є. Шелест, Ю. М. Ткач, Я.Ю. Усов. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2019. – 144 с.

20. Норткатт С. Защита сетевого периметра: Наиболее полное руководство по брандмауэрам, виртуальным частным сетям, маршрутизаторам и системам обнаружения вторжений. - М. : DiaSoft, 2004. - 672 с.

### Інформаційні ресурси в Інтернеті

1. Державна служба спеціального зв'язку та захисту інформації. URL: <https://cip.gov.ua/ua>

2. Команда реагування на комп'ютерні надзвичайні події України. URL: <https://cert.gov.ua/>

3. Портал безпека. URL: <https://www.bezpeka.com/uk/golovna/>

## Додаток А

### Перелік питань, що виносяться на вивчення

**Змістовий модуль 1.** Основні принципи побудови захищених інформаційно-телекомунікаційних систем.

**Тема 1.** Базові поняття в галузі захисту інформаційно-телекомунікаційних систем.

Кіберпростір, кібербезпека та кібертероризм: поняття і визначення.

Інформаційне протиборство, інформаційна війна, інформаційна зброя.

Способи та методи ведення розвідки ІТ-систем.

Системи, в яких здійснюється захист інформації.

Об'єкти захисту. Завдання захисту інформації.

Політика інформаційної безпеки.

Профіль захищеності автоматизованої системи.

Загрози і вразливості.

Захищена комп'ютерна система, комплекс засобів захисту, ідентифікація, автентифікація, авторизація, правила розмежування доступу.

Моделі інформаційної безпеки: модель загроз, модель порушника, Cyber Kill Chain, , моделі доступу (дискреційна, мандатна, рольова, безпека потоків даних, ізольоване програмне середовище), моделі цілісності, теорія інформаційної безпеки.

Критерії оцінювання захищеності інформаційно-комунікаційних систем.

**Тема 2.** Вразливості і загрози інформаційно-комунікаційних систем

Класифікація загроз.

Типові загрози безпеці

Узагальнена схема загроз комп'ютерній системі

Методика класифікації загроз STRIDE.

Класифікація кібернетичних втручань і загроз за схемою, запропонованою Конвенцією Ради Європи (2001 р.)

Передумови виникнення вразливостей в комп'ютерних системах.

Класифікація джерел інцидентів, а також способів, об'єктів та результатів їхнього впливу. Класифікація мережових аномалій. Класифікація індикаторів компрометації. Класифікація вад захисту. Класифікація помилок програмної реалізації системи. Помилки переповнення буферу. Помилки обробки рядків тексту.

Загрози інформації в комп'ютерних мережах

Стеки протоколів відкритих систем.

Сервіси і механізми безпеки.

**Тема 3.** Типові віддалені атаки

Класифікація атак: віддалене проникнення, локальне проникнення, віддалена відмова в обслуговуванні, локальна відмова в обслуговуванні, сканування мережі, сканування вразливостей, злам паролів, пасивне прослуховування трафіку.

Загальна структура кібернетичної атаки.

Класифікація типових віддалених атак за базовими ознаками несанкціонованого доступу.

Класифікація кібернетичних атак П.Ноймана.

Особливості найбільш поширених атак (DoS: Flood, ICMP flood, Identification flood, TCP SYN flood, Ping of Death, Tribe Flood Network, Trinco, Stacheldrucht, Trinity; DDoS: TCP SYN flood, TCP flood, SYN flooding, UDP flood, ICMP flood; сніфер пакетів; IP-спуфінг; паролні атаки, логічні бомби; троянські коні; вірусні атаки; ін'єкції).

#### **Тема 4. Шкідливі програмні засоби**

Класифікація шкідливого програмного забезпечення.

Програми-шпигуни.

Класифікація вірусів за середовищем розповсюдження, способам маскуванню в середовищі, інфікованим об'єктам, способу інфікування об'єктів, способу розміщення в інфікованому об'єкті, руйнівним впливам, здатності до змін, стилю написання, типу кода.

Програмні закладки.

Хробак Морріса.

Класифікація троянських вірусів.

Соціальна інженерія.

Фшинг, бейтинг, вішинг, фармінг,

Методи боротьби з ШПЗ: методи виявлення ШПЗ, технології боротьби з ШПЗ, методи усунення наслідків зараження ШПЗ.

Захист від комп'ютерних вірусів: структура системи антивірусного захисту, сучасні антивірусні програми.

### **Змістовий модуль 2. Базові засоби захисту інформації в інформаційно-телекомунікаційних системах**

#### **Тема 5. Організація захисту інформації в інформаційно-комунікаційних системах**

Структура інформаційно-комунікаційних систем та їх рівні

Зонування мережевої безпеки.

Підходи до забезпечення захисту інформації в ІТС.

Моделі управління мережевими ресурсами.

Несанкціонований доступ на різних рівнях інформаційно-комунікаційних систем.

Функціональні сервіси безпеки і механізми, що їх реалізують.

Класифікація засобів захисту від НСД.

Базові вимоги до засобів захисту.

Класифікація засобів захисту програмного забезпечення

Структура комплексу засобів захисту.

Рекомендації американської ІТ-компанії SANS щодо заходів забезпечення кібербезпеки комп'ютерних систем і мереж.

Рекомендації CERT-UA щодо захисту інформації в інформаційно-комунікаційних системах.

#### **Тема 6. Захист інформації в операційних системах**

Апаратне забезпечення засобів захисту.

Функції захисту інформації в процесорах Intel.

Керування оперативною пам'яттю.

Керування задачами.

Загрози безпеці операційних систем

Побудова захищених операційних систем.

Засоби захисту в операційних системах Windows, Unix, Linux, Solaris, Фенікс. PGP.

## **Тема 7. Міжмережевий екран**

Архітектура захищених мереж.

Функції міжмережевих екранів.

Структура міжмережевих екранів.

Рівні реалізації міжмережевих екранів.

Схеми підключення міжмережевих екранів.

Особливості персональних брандмауерів.

Екрануючий шлюз прикладного рівня (пакетний фільтр). Екрануючий шлюз сеансового рівня

Недоліки міжмережевих екранів.

Політика міжмережевої взаємодії: політика доступу до мережевих сервісів, політика роботи міжмережевого екрану.

Налагодження параметрів міжмережевих екранів.

## **Тема 8. Безпека мережевих Інтернет-протоколів**

Ієрархія протоколів

Протоколи прикладного рівня: Telnet, FTP, мережні служби Unix.

Протоколи транспортного рівня: UDP, TCP.

Протоколи мережного рівня: IP.

Протокол маршрутизації BGP.

Протоколи керування мережею: ICMP, SNMP

Архітектура засобів захисту IPSec.

Протокол AH

Протокол ESP.

Робота AH і ESP в транспортному режимі і в режимі тунелювання.

Протокол IKE. Протокол ISAKMP.

Протоколи створення криптозахищених віртуальних каналів на канальному рівні.

Протокол PPP. Протокол PPTP. Протокол L2TP. Протокол SSL/TLS. Протокол SSH.

## **Зміни та доповнення**