011

**КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**
**ІМЕНІ ТАРАСА ШЕВЧЕНКА**

**Факультет радіофізики, електроніки та комп'ютерних систем**

**Кафедра радіотехніки та радіоелектронних систем**

**«ЗАТВЕРДЖУЮ»**
Заступник декана
з навчальної роботи
_____ О. Нечипорук
«___» _____2021 року

# РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

# КОМПЛЕКСНІ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

**для студентів**

| | |
|---|---|
| галузь знань | **17 Електроніка та телекомунікації** |
| спеціальність | **172 Телекомунікації та радіотехніка** |
| освітній рівень | **другий (магістр)** |
| освітня програма | **Інформаційна безпека телекомунікаційних систем і мереж** |
| вид дисципліни | **Обов'язковий компонент ОП** |

| | |
|---|---|
| Форма навчання | **денна** |
| Навчальний рік | **2021/2022** |
| Семестр | **2** |
| Кількість кредитів ECTS | **6** |
| Мова викладання, навчання та оцінювання | **українська** |
| Форма заключного контролю | **іспит** |

**Викладач**:
Сергій Довбня,
канд. військ. наук, доцент кафедри радіотехніки та радіоелектронних систем

Пролонговано: на 20__/20__ н.р. _____ (_____) «___» _____ 20__ р.
на 20__/20__ н.р. _____ (_____) «___» _____ 20__ р.

**КИЇВ 2021**

011

**Розробник:**

**Сергій Довбня,**

канд. військ. наук, доцент кафедри радіотехніки та радіоелектронних систем

**ЗАТВЕРДЖЕНО**

Завідувач кафедри радіотехніки та радіоелектронних систем

_____ І. Анісімов

Протокол № 12 від «07» 12 2021 р.

Схвалено науково-методичною комісією факультету радіофізики, електроніки та комп'ютерних систем

Протокол № 10 від «14» 12 2021 р.

Голова науково-методичної комісії _____ С. Радченко

«___» _____ 2021 року.

**1. Мета дисципліни** – дати студентам знання та практичні навички з питань організації технічного захисту інформації з обмеженим доступом (далі – ІзОД) від витоку технічними каналами та через несанкціонований доступ на об'єктах інформаційної діяльності (далі – ОІД) та в інформаційно-телекомунікаційних система (далі – ІТС) установи (організації).

Набуття теоретичних знань:

- основні положення Законів України щодо інформаційної безпеки;
- основні напрямки державної політики в галузі технічного захисту інформації;
- законодавчі та нормативні акти з питань інформаційної безпеки;
- основи технічного інформаційної безпеки на ОІД та в ІТС;
- можливі технічні канали витоку інформації;
- основні технічні засоби та програмні методи інформаційної безпеки;
- вимоги до організації роботи з технічного інформаційної безпеки, напрямки її удосконалення;
- правила розроблення документів з інформаційної безпеки.

**2. Попередні вимоги до опанування або вибору навчальної дисципліни:**

Навчальна дисципліна "Комплексні системи інформаційної безпеки" є обов'язковою компонентою освітньої програми і використовує результати вивчення обов'язкових дисциплін "Теорія передавання інформації", "Наноелектроніка", "Наноструктурні елементи радіоелектронних засобів", "Адаптивні системи обробки сигналів", "Супутникові інформаційні системи" цієї ОП. Навчальна дисципліна "Комплексні системи інформаційної безпеки" є основою для дисциплін вільного вибору ВБ х.03, ВБ х.04 та обов'язкових компонент "Науково-виробнича практика" і "Дипломна робота магістра" іцеї ОП. Попередні вимоги:

1. Вміти запускати прикладні програмні засоби та керувати ними на основі графічного інтерфейсу користувача, знаходити інформацію в Інтернеті.
2. Знати основи побудови радіоелектронних засобів та інформаційно-телекомунікаційних систем.

**3. Анотація навчальної дисципліни:**

Вивчення дисципліни "Комплексні системи інформаційної безпеки" дозволяє зрозуміти сутність процесу створення комплексних систем інформаційної безпеки в інформаційно-телекомунікаційних системах. Розглядаються загальні принципи обробки та інформаційної безпеки в ІТС; організації та проведення державної експертизи технічних засобів захисту та КСЗІ в ІТС. Особливу увагу приділяється системному підходу до створення КСЗІ в ІТС. Вивчається застосування технічних, криптографічних засобів інформаційної безпеки в КСЗІ ІТС; застосування методів моделювання систем під час оцінки середовищ функціонування ІТС, розробки моделі загроз, порушника, оцінки рисків, проектуванні системи інформаційної безпеки.

**4. Завдання (навчальні цілі):**

1. Надати основні відомості курсу "Комплексні системи інформаційної безпеки", які складають важливу частину загально-технічної та інженерної підготовки студента-магістра за спеціальністю "Телекомунікації та радіотехніка".
2. Узагальнити та розширити відомі поняття курсів "Теорія передавання інформації", "Наноелектроніка", "Наноструктурні елементи радіоелектронних засобів", "Оптимізація проектування радіоелектронних засобів", "Адаптивні системи обробки сигналів", "Супутникові інформаційні системи", простежити взаємозв'язок об'єктів досліджень системи інформаційної безпеки з іншими компонентами підготовки; продемонструвати застосування теоретичних відомостей до розв'язання практичних та експериментальних задач;
3. Навчити застосовувати знання, уміння, навички і комунікації у професійній діяльності, розвивати логічне та аналітичне мислення студентів.
4. Прищепити вміння розв'язувати прикладні задачі методами системного підходу (декомпозиція складної системи, аналіз складових процесів та підсистем, визначення вимог з інформаційної безпеки, синтез системи захисту, оцінка захищеності інформації).

**Забезпечити досягнення компетентностей:**

ЗК 3. Знання та розуміння предметної області та розуміння професійної діяльності.
ЗК 4. Навички використання інформаційних і комунікаційних технологій.
ФК 1. Здатність обирати і застосовувати методи комп'ютерного моделювання та обробки інформації при дослідженні для потреб розробки нових телекомунікаційних та радіотехнічних виробів і систем.
ФК 2. Здатність забезпечувати інформаційну безпеку під час виконання дослідження для потреб розробки телекомунікаційних та радіотехнічних виробів і систем.
ФК 5. Здатність вибирати основні й допоміжні матеріали при виконанні досліджень для потреб розробки телекомунікаційних та радіотехнічних виробів і систем.

**5. Результати навчання за дисципліною**:

| Результат навчання (1, знати; 2, вміти; 3, комунікація; 4, автономність та відповідальність) | | Форми (та/або методи і технології) викладання і навчання | Методи оцінювання та пороговий критерій оцінювання (за необхідності) | Відсоток у підсумковій оцінці з дисципліни |
|---|---|---|---|---|
| Код | Результат навчання | | | |
| **1** | студент повинен **знати**: | лекційні заняття, заняття з використанням математичних пакетів | письмові модульні контрольні роботи, оцінювання виконання завдань для самостійної роботи | до 45 |
| 1.1 | вимоги щодо інформаційної безпеки в ІТС | –//– | –//– | до 2 |
| 1.2 | організацію та порядок створення КСЗІ в інформаційно-телекомунікаційних системах | –//– | –//– | до 3 |
| 1.3 | організацію створення комплексу ТЗІ на ОІД | –//– | –//– | до 5 |
| 1.4 | захист інформації від витоку за рахунок несанкціонованого використання закладних пристроїв | –//– | –//– | до 5 |
| 1.5 | захист інформації від витоку акустичними та віброакустичними каналами | –//– | –//– | до 5 |
| 1.6 | захист ІзОД від витоку каналами ПЕМВН на ОІД та в ІТС | –//– | –//– | до 5 |
| 1.7 | захист інформації на ОІД та в ІТС від спеціальних впливів | –//– | –//– | до 5 |
| 1.8 | захист інформації в інформаційно-телекомунікаційних системах від несанкціонованого доступу | –//– | –//– | до 5 |
| 1.9 | використання засобів ТЗІ, КЗІ при створенні КСЗІ в ІТС | –//– | –//– | до 5 |
| 1.10 | оцінку захищеності інформації, проведення державної експертизи засобів ТЗІ та КСЗІ в ІТС | –//– | –//– | до 5 |
| **2** | студент повинен **вміти**: | лекційні заняття, заняття з використанням математичних пакетів | письмові модульні контрольні роботи, оцінювання виконання завдань для самостійної роботи | до 45 |
| 2.1 | розраховувати параметри загроз до інформації в ІТС | –//– | –//– | до 15 |
| 2.2 | визначити значення вагових | –//– | –//– | до 15 |

| | | | | |
|---|---|---|---|---|
| | коефіцієнтів при оцінці рисків до інформації | | | |
| 2.3 | оволодіти програмними засобами обстеження середовищ функціонування ІТС та проектування системи захисту | –//– | –//– | до 15 |
| **3** | **комунікація** | лекційні заняття, заняття з використанням математичних пакетів | | до 5 |
| 3.1 | здатність грамотно будувати комунікацію, виходячи з мети і ситуації спілкування | | | до 3 |
| 3.2 | здатність бути відповідальним за внесок в роботу команди при вирішенні проблеми | лекційні заняття з використанням роботи у підгрупах | оцінювання виконання завдань для самостійної | до 2 |
| 4 | **автономність та відповідальність** | лекційні заняття, заняття з використанням математичних пакетів | письмові модульні контрольні роботи, оцінювання виконання завдань для самостійної роботи | до 5 |
| 4.1 | самостійність у навчанні та/або професійній діяльності | | | до 5 |

**6. Співвідношення результатів навчання дисципліни із програмними результатами навчання**

| **Результати навчання дисципліни (код)** / **Програмні результати навчання (назва)** | 1.1 | 1.2 | 1.3 | 1.4 | 1.5 | 1.6 | 1.7 | 1.8 | 1.9 | 1.10 | 2.1 | 2.2 | 2.3 | 3.1 | 3.2 | 4.1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ПРН 1. Знати фізичні та математичні теорії та моделі, перспективні для досліджень та інноваційної діяльності у сфері радіотехніки, електроніки та телекомунікацій. | + | + | + | + | + | + | + | + | + | + | + | + | + | | | |
| ПРН 4. Знати аналогові та цифрові, в тому числі адаптивні, методи обробки інформації. | | | | + | + | + | + | | | | | | + | | | |
| ПРН 6. Знати сучасні телекомунікаційні та мережеві технології, тенденції їх розвитку. | + | + | + | | | | | | | + | + | + | | | + | |
| ПРН 7. Знати теоретичні основи та принципи забезпечення інформаційної без-пеки. | | | + | + | + | + | + | | | | | | + | | | |
| ПРН 9. Знаходити і аналізувати потрібну для роботи наукову та інженерно-технічну інформацію. | + | + | + | | | | | | | + | | | | + | | + |

**7. Схема формування оцінки**

**7.1. Форми оцінювання студентів:** рівень досягнення всіх запланованих результатів навчання визначається за результатами написання письмової контрольної роботи, за результатами виступу на семінарі і за результатами виконання самостійних і лабораторних робіт. Вклад результатів навчання у підсумкову оцінку, за умови їх опанування на належному рівні і успішної здачі всіх лабораторних робіт наступний:

- результати навчання 1.1 – 1.10 [**знання**] до 45 %;
- результат навчання 2.1 – 2.3 [**вміння**] – до 45%;
- результат навчання 3.1 [**комунікація**] – до 5%;
- результат навчання 4.1 [**автономність та відповідальність**] – до 5%.

**Форми оцінювання студентів:**

- **семестрове оцінювання**: контроль здійснюється за таким принципом. Навчальний семестр має один змістовний модуль. Після завершення відповідних тем проводиться письмова модульна контрольна робота. Для визначення рівня досягнення результатів навчання завдання для модульної контрольної роботи перевіряють уміння розв'язувати конкретні задачі з теорії адаптивних систем. Обов'язковим для допуску до іспиту є написання модульної контрольної роботи з кількістю балів не менше 7 балів та виступ з доповіддю на семінарі. Іншими формами контролю є виконання студентами самостійних та лабораторних робіт.
- **підсумкове оцінювання (у формі іспиту):** форма іспиту – письмово-усна. Екзаменаційний білет складається із 2 питань, питання оцінюються по 20 балів. Всього на іспиті можна отримати від 0 до 40 балів. Умовою досягнення позитивної оцінки за дисципліну є отримання не менш ніж 60 балів, при цьому оцінка за результатами навчання 2 [вміння] і 3 [комунікативність та відповідальність] не може бути меншою ніж 50% від максимального рівня (23 і 5 балів відповідно), оцінка за іспит не може бути меншою **24 балів.**
- **умови допуску до підсумкового іспиту:** умовою допуску до іспиту є отримання студентом сумарно не менше, ніж *критично-розрахунковий мінімум 36 балів* за семестр. Студенти, які протягом семестру набрали сумарно меншу кількість балів, ніж критично-розрахунковий мінімум **36 балів**, для одержання допуску до іспиту обов'язково повинні написати, на необхідну порогову кількість балів, додаткову контрольну роботу за матеріалом модуля.

У випадку відсутності студента з поважних причин відпрацювання та перездачі модульних контрольних робіт здійснюються у відповідності до „Положення про порядок оцінювання знань студентів при кредитно-модульній системі організації навчального процесу" від 1 жовтня 2010 року.

**7.2. Організація оцінювання:**

**Оцінювання за формами контролю:**

| | ***ЗМ*** | |
|---|---|---|
| | *Мін. – балів* | *Мах. – балів* |
| Модульна контрольна робота | 7 | 12 |
| Виступ на семінарі | 15 | 25 |
| Виконання студентами самостійних робіт | 5 | 8 |
| Виконання студентами лабораторних робіт | 9 | 15 |

**Орієнтовний графік оцінювання:**

| | *Орієнтовний період для здійснення відповідної форма оцінювання* |
|---|---|
| Модульна контрольна робота | січень-травень |
| Виступ на семінарі | січень-травень |
| Виконання студентами самостійних робіт | січень-травень |
| Виконання студентами лабораторних робіт | січень-травень |

| | |
|---|---|
| Добір балів/додаткова контрольна робота та/або доскладання домашніх завдань | квітень |
| Іспит | травень |

**Розрахунок балів, які студент отримує при успішній здачі іспиту:**

| | Змістовий модуль | Іспит | Підсумкова оцінка |
|---|---|---|---|
| *Мінімум* | *36* | *24* | *60* |
| **Максимум** | **60** | **40** | **100** |

**7.3. Шкала відповідності оцінок**

| Оцінка (за національною шкалою) / National grade | Рівень досягнень, % / Marks, % |
|---|---|
| **Відмінно** / Excellent | 90-100% |
| **Добре** / Good | 75-89% |
| **Задовільно** / Satisfactory | 60-74% |
| **Незадовільно** / Fail | 0-59% |

**8. Структура навчальної дисципліни. Тематичний план занять**

| № з/п | Назва теми | Кількість годин | | | |
|---|---|---|---|---|---|
| | | лекції | семінари | лаб. роботи | самост. робота |
| **Змістовий модуль 1. Базові принципи інформаційної безпеки** | | | | | |
| 1. | Вимоги щодо інформаційної безпеки в ІТС | 4 | 2 | | 10 |
| 2. | Організація та порядок створення КСЗІ в інформаційно-телекомунікаційних системах | 4 | 2 | 2 | 20 |
| 3. | Організація створення комплексу ТЗІ на ОІД | 4 | 2 | | 10 |
| 4. | Захист інформації від витоку за рахунок несанкціонованого використання закладних пристроїв | 2 | 2 | | 10 |
| 5. | Захист інформації від витоку акустичними та віброакустичними каналами | 4 | 2 | | 10 |
| 6. | Захист ІзОД від витоку каналами ПЕМВН на ОІД та в ІТС | 4 | 2 | | 10 |
| 7. | Захист інформації на ОІД та в ІТС від спеціальних впливів | 2 | 2 | | 10 |
| 8. | Захист інформації в інформаційно-телекомунікаційних системах від несанкціонованого доступу | 4 | 2 | | 20 |
| 9. | Використання засобів ТЗІ, КЗІ при створенні КСЗІ в ІТС | 2 | 2 | 4 | 10 |
| 10. | Оцінка захищеності інформації, проведення державної експертизи засобів ТЗІ та КСЗІ в ІТС | 4 | 2 | | 10 |
| ЗАГАЛОМ | | 34 | 20 | 6 | 120 |

Загальний обсяг **180** год., з них:
лекції **– 34** год.;
семінарські заняття – **20** год.;
лабораторні роботи – **6** год.;
самостійна робота **- 120** год.

**9. Рекомендовані джерела:**

**Основні:**


1. Г.Ф. Конахович та інші. Захист інформації в телекомунікаційних системах: Навчальний посібник. – К.: НАУ, 2009.-380 с.
2. Г.М. Гулак та інші. Основи криптографічного захисту інформації. -К.: ІММ НАНУ, 2011.-200 с.
3. Основи інформаційної безпеки. Лужецький В.А., Кожухівський А.Д., Войтович О.П. Навчальний посібник. – Вінниця: ВНТУ, 2009. – 268 с.


**Додаткові:**


1. Оцінка захищеності інформації, Створення та атестація комплексів технічного захисту інформації на об’єктах інформаційної діяльності Сил спеціальних операції України: Методичні рекомендації/ С.Я. Довбня. – К.: ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «ДЕПС СОЛЮШЕНЗ» 2020. – 120 с.
2. С.Я. Довбня. Методи (моделі) розробки комплексів технічного захисту інформації на об’єктах інформаційної діяльності та радіоелектронної техніки: Навчальний посібник. – К.: ДП «Український центр «Безпека», 2019. – 95 с.
3. С.Я. Довбня, П.П. Наталенко. Основи використання, адміністрування та забезпечення захисту інформації в автоматизованих системах: Навчальний посібник. – К.: ТОВ «Софтлайн ІТ», 2017. – 164 с.
4. С.Я. Довбня. Підготовка користувачів та адміністраторів ЗАТК "Персонал-Командування" з технічного захисту інформації: Навчальний посібник. – К.: ТОВ «Софтлайн ІТ», 2018. – 280 с.