**Форма № Н - 3.04**

**Національний університет біоресурсів і природокористування України**

Кафедра комп’ютерних систем і мереж

“**ЗАТВЕРДЖУЮ**”

Декан факультету інформаційних технологій

\_\_\_\_\_\_\_\_\_\_\_\_ О.Г. Глазунова

“\_\_\_\_\_\_”\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2020 р.

## РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

“Захист інформації в комп'ютерних системах і кібербезпека (Частина 2)”

зі спеціальності 123 – «Комп’ютерна інженерія»

(шифр і назва напряму підготовки)

факультет інформаційних технологій

(назва факультету)

Київ – 2020 р.

Робоча програма з дисципліни «Захист інформації в комп'ютерних системах і кібербезпека (Частина 2)» для студентів ОС Магістр зі спеціальності 123 – «Комп’ютерна інженерія».

„10” червня 2020 р. − 13 с.

Розробники:Лахно Валерій Анатолійович, доктор технічних наук, професор

Робоча програма затверджена на засіданні кафедри комп’ютерних систем і мереж

Протокол від “10” червня 2020 р. № 10

Завідувач кафедри комп’ютерних систем і мереж

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Лахно В.А.)

(підпис)

Схвалено вченою радою факультету інформаційних технологій

Протокол від. “\_\_\_\_”\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2020 р. № \_\_\_

“\_\_\_\_\_”\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2020 р. Голова \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Глазунова О.Г.)

(підпис) (прізвище та ініціали)

© НУБіП України, Лахно В.А., 2020 р.

# **Опис навчальної дисципліни**

\_\_\_\_\_\_\_\_\_\_ Захист інформації в комп'ютерних системах і кібербезпека (Частина 2)\_\_\_\_\_\_\_\_\_\_\_

(назва)

|  |  |  |
| --- | --- | --- |
| **Галузь знань, напрям підготовки, спеціальність, освітньо-кваліфікаційний рівень** | | |
| Галузь знань | Інформаційні технології | |
| Спеціальність | 123 – «Комп’ютерна інженерія» | |
| другий (магістерський) рівень | Магістр | |
| **Характеристика навчальної дисципліни** | | |
| Вид | Нормативна | |
| Загальна кількість годин | 120 | |
| Кількість кредитів ECTS | 4 | |
| Кількість змістових модулів | 2 | |
| Курсовий проект (робота)  (якщо є в робочому навчальному плані) | - | |
| Форма контролю | Іспит | |
| **Показники навчальної дисципліни для денної та заочної форм навчання** | | |
|  | денна форма навчання | заочна форма навчання |
| Рік підготовки | 2020-2021 | 2020-2021 |
| Семестр | 2 | 2 |
| Лекційні заняття | 30 год. | 6 год. |
| Практичні, семінарські заняття |  |  |
| Лабораторні заняття | 30 год. | 6 год. |
| Самостійна робота | 60 год. | 108 год. |
| Індивідуальні завдання |  |  |
| Кількість тижневих годин  для денної форми навчання:  аудиторних | 4 год. | 6 год. |

1. **Мета та завдання навчальної дисципліни**

**Мета** - є формування у майбутніх фахівців умінь та компетенцій для забезпечення ефективного захисту інформації, необхідних для подальшої роботи за фахом комп’ютерна інженерія та навчити їх застосуванню методів та засобів захисту інформації в умовах широкого використання сучасних інформаційних технологій на зростання кількості та складності деструктивних впливів на інформаційні ресурси установ та підприємств.

**Завдання** навчальної дисципліни «Захист інформації в комп'ютерних системах і кібербезпека (Частина 2)» - є теоретичне та практичне засвоєння необхідного рівня умінь та компетенцій, необхідних для подальшої роботи в умовах зростаючої інформатизації суспільства та підвищення рівня загроз інформаційній та кібербезпеці безпеці.

**Місце і роль дисципліни** в системі підготовки фахівців відповідно до навчального плану.

Курс “Захист інформації в комп'ютерних системах і кібербезпека” входить до складу магістерської програми. Дана навчальна дисципліна є теоретичною основою сукупності знань та вмінь, що формують профіль фахівця в області захисту інформації та кібербезпеки управляючих систем в різних галузях.

**Вимоги щодо знань і вмінь, набутих внаслідок вивчення дисципліни**

Внаслідок вивчення дисципліни студенти повинні:

**знати:** правову та організаційну основи забезпечення інформаційної безпеки України; основні види загроз інформаційній безпеці та технічних каналів витоку інформації, методи їх виявлення та блокування; основні види та можливості технічних засобів і систем захисту інформації; основні методи та засоби криптографічного та стеганографічного захисту інформації, що циркулює у автоматизованих системах та передаються телекомунікаційними каналами та мережами;

**вміти**: планувати та організовувати свою роботу та роботу підрозділу з урахуванням вимог до захисту інформації, зокрема, з обмеженим доступом; планувати й організовувати роботи щодо створення та розвитку системи інформаційної безпеки підприємств; організовувати роботи щодо виявлення і блокування технічних каналів витоку інформації; здійснювати ефективний контроль робіт із захисту інформації; здійснювати ефективний вибір комп’ютерних систем захисту; використовувати технічні засоби захисту інформації; використовувати програмні та апаратні засоби розмежування доступу до інформації у автоматизованих системах та антивірусні засоби захисту інформації у персональних комп’ютерах; використовувати комп’ютерні криптографічні, стеганографічні системи захисту інформації.

1. **Програма навчальної дисципліни**

**Змістовий модуль 1. Захист у технічних каналах витоку інформації**

**Тема лекційного заняття 1. Концептуальні засади забезпечення інформаційної безпеки України.**

Завдання курсу. Нормативно-правові основи захисту інформації в Україні. Концепція національної безпеки України, концепція інформаційної безпеки України.

**Тема лекційного заняття 2. Доктрина інформаційної безпеки України.**

Доктрина інформаційної безпеки України. Доктрини інформаційної безпеки США, країн ЄС. Основні поняття, терміни та визначення.

**Тема лекційного заняття 3. Технічні канали витоку інформації.**

Місце технічного захисту інформації у системі інформаційної безпеки. Сутність та завдання технічного захисту інформації. Основні поняття, терміни та визначення технічного захисту інформації. Види інформації, яка може стати об’єктом злочинних посягань.

**Тема лекційного заняття 4. Способи несанкціонованого зняття інформації.**

Поняття технічних каналів витоку інформації та механізм їх утворення. Види та класифікація технічних каналів витоку інформації та способів несанкціонованого зняття інформації. Визначення можливих джерел витоку акустичної та електромагнітної інформації у приміщенні. Визначення можливих джерел витоку інформації з радіоканалу.

**Тема лекційного заняття 5. Методи та засоби блокування технічних каналів витоку інформації.**

Складові ТЗІ. Методи пасивного та активного захисту інформації. Методи та засоби захисту акустичної інформації.

**Тема лекційного заняття 6. Методи та засіб захисту електромагнітної інформації.**

Методи та засіб захисту електромагнітної інформації. Методи захисту від ВЧ-нав’язування. Методики і засоби пошуку радіозакладних пристроїв.

**Тема лекційного заняття 7. Методи захисту інформації у автоматизованих системах (Частина 1).**

Захист інформації з обмеженим доступом у захищеній комп’ютерній мережі. Розмежування доступу до інформації в залежності від повноважень користувача. Використання паролів. Шифрування інформації у комп’ютерах при її зберіганні.

**Тема лекційного заняття 8. Методи захисту інформації у автоматизованих системах (Частина 2).**

Програмні засоби захисту інформації. Вибір програм розмежування доступу до інформації. Вибір та застосування антивірусних програм. Вибір програм автоматичного шифрування інформації при її збереженні на дисках та відпрацювання практичних навичок їх застосування.

**Тема лекційного заняття 9. Методи захисту інформації у телекомунікаційних мережах та відкритих мережах зв’язку.**

Захист мовленнєвої інформації, що передається у відкритих каналах зв’язку. Стеганографічні методи захисту письмової інформації, що передається у відкритих каналах зв’язку. Типи шифрів. Поняття алгоритму шифрування та секретного ключа. Поняття незламного шифру. Разовий шифроблокнот та його застосування. Використання спеціальних технічних засобів, в умовах забезпечення режиму секретності на підприємствах, установах, організаціях з різними формами власності. Виявлення ознак можливого несанкціонованого доступу до інформації, зокрема у ЗІКС та КМ.

**Змістовий модуль № 2. Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем.**

**Тема лекційного заняття 10. Загальні принципи побудови захищених інформаційно-комунікаційних систем (ЗІКС) та КМ.**

Призначення та класифікація ІКМ та КМ. Логічна та фізична структури ІКМ та КМ. Телекомунікаційна система КМ та характеристика її елементів. Завдання адміністрування та експлуатація захищених інформаційно-комунікаційних систем. Часове впорядкування виконуваних робіт у ЗІКС та КМ.

Аналіз діяльності КМ підприємства, установи, організації, органу державної влади або його структурного підрозділу та причин виникнення проблем з ІБ і можливих способів їхнього вирішення, відповідно до своєї компетенції приймати управлінське рішення, використовуючи форми і методи добору й аналізу відповідної інформації щодо розв’язання ситуаційних проблем, які виникають у сфері забезпечення ІБ.

Атестацію захищених інформаційних та комунікаційних систем в умовах додержання режиму секретності із зафіксуванням результатів у відповідних документах.

**Тема лекційного заняття 11. Основні принципи організації взаємодії в ЗІКС та КМ.**

Логічна модель взаємодії ЗІКС та КМ. Функціональні рівні взаємодії та їх ієрархія. Особливості еталонної моделі взаємодії відкритих систем (ВВС) для локальних комп’ютерних мереж (ЛКМ).

**Тема лекційного заняття 12. Програмне забезпечення для адміністрування ЗІКС та КМ*.***

Структура, призначення, склад і загальна характеристика основних елементів. Мережеві операційні системи та їх характеристика. Аналізатори протоколів. Особливості функціонування ОС різних типів. Основи мережевої безпеки. Адміністрування у ОС NetWare фірми Novell. Засоби управління локальними ресурсами ЗІКС та КМ.

**Тема лекційного заняття 13. Якісний та кількісний аналіз ризику для ІБ та КБ об’єкту інформатизації.**

Сутність якісного та кількісного аналізу ризиків для ІБ та кібербезпеки підприємства, фірми. Принципи аналізу ризиків для ІБ. Напрямки аналізу підприємницьких ризиків для ІБ. Збитки, які виникають в процесі підприємницької діяльності. Методи аналізу ступеня ризику для ІБ. Характеристика області абсолютної стійкості, нормальної стійкості, області нестійкого стану, критичного стану, кризового стану підприємства на основі аналізу ризику для ІБ.

**Тема лекційного заняття 14. Методи кількісної оцінки ступеня ризику: аналітичний метод; метод використання аналогів. Комплексна оцінка ризиків для ІБ.**

Визначення ключового параметру, вибір чинників впливу, програмування величини ключового параметру для оцінки ризиків ІБ та КБ. Визначення імовірності досліджуваного проекту на основі оцінок імовірності проектів-аналогів для побудови СЗІ на ОБІ. Прогноз очікуваних характеристик досліджуваного проекту захисту ОБІ. Принципи управління ризиками ІБ. Система управління ризиками ІБ. Основи профілактики ризиків: диверсифікація та лімітування. Ризики, пов'язані з вкладенням капіталу у засоби ЗІ. Комплексне управління довгостроковими інвестиціями у політику ІБ ОБІ.

**4. Структура навчальної дисципліни**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Назви змістових модулів і тем | Кількість годин | | | | | | | | | | | |
| денна форма | | | | | | Заочна форма | | | | | |
| усього | у тому числі | | | | | усього | у тому числі | | | | |
| л | п | лаб | інд | с.р. | л | п | лаб | інд | с.р. |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| **Змістовий модуль 1. Захист у технічних каналах витоку інформації.** | | | | | | | | | | | | |
| Тема 1. Концептуальні засади забезпечення інформаційної безпеки (ІБ) України. | 4 | 1 |  | 1 |  | 2 | 6 |  |  |  |  | 6 |
| Тема 2. Доктрина ІБ України. | 8 | 2 |  | 2 |  | 4 | 8 | 1 |  | 1 |  | 6 |
| Тема 3. Технічні канали витоку інформації. | 6 | 2 |  | 2 |  | 2 | 6 |  |  |  |  | 6 |
| Тема 4. Способи несанкціонованого зняття інформації. | 8 | 2 |  | 2 |  | 4 | 8 | 1 |  | 1 |  | 6 |
| Тема 5. Методи та засоби блокування технічних каналів витоку інформації. | 8 | 2 |  | 2 |  | 4 | 8 | 1 |  | 1 |  | 6 |
| Тема 6. Методи та засіб захисту електромагнітної інформації. | 8 | 2 |  | 2 |  | 4 | 6 |  |  |  |  | 6 |
| Тема 7. Методи захисту інформації у автоматизованих системах (АС) (Частина 1). | 6 | 1 |  | 1 |  | 4 | 6 |  |  |  |  | 6 |
| Тема 8. Методи захисту інформації у АС (Частина 2). | 6 | 2 |  | 2 |  | 2 | 6 |  |  |  |  | 6 |
| Тема 9. Методи захисту інформації у телекомунікаційних мережах та відкритих мережах зв’язку. | 8 | 2 |  | 2 |  | 4 | 6 |  |  |  |  | 6 |
| **Разом за змістовим модулем 1** | **62** | **16** |  | **16** |  | **30** | **60** | **3** |  | **3** |  | **54** |
| **Змістовий модуль 2. Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем.** | | | | | | | | | | | | |
| Тема 10. Загальні принципи побудови захищених інформаційно-комунікаційних систем (ЗІКС) та КМ. | 10 | 2 |  | 2 |  | 6 | 12 |  |  |  |  | 12 |
| Тема 11. Основні принципи організації взаємодії в ЗІКС та КМ. | 10 | 2 |  | 2 |  | 6 | 12 | 1 |  | 1 |  | 10 |
| Тема 12. Програмне забезпечення для адміністрування ЗІКС та КМ. | 10 | 2 |  | 2 |  | 6 | 14 | 1 |  | 1 |  | 12 |
| Тема 13. Якісний та кількісний аналіз ризику для ІБ та КБ об’єкту інформатизації. | 14 | 4 |  | 4 |  | 6 | 12 | 1 |  | 1 |  | 10 |
| Тема 14. Методи кількісної оцінки ступеня ризику: аналітичний метод; метод використання аналогів. Комплексна оцінка ризиків для ІБ. | 14 | 4 |  | 4 |  | 6 | 10 |  |  |  |  | 10 |
| **Разом за змістовим модулем 2** | **58** | **14** |  | **14** |  | **30** | **60** | **3** |  | **3** |  | **54** |
| Усього годин за курс | **120** | **30** |  | **30** |  | **60** | **120** | **6** |  | **6** |  | **108** |

**7. Теми лабораторних занять**

|  |  |  |
| --- | --- | --- |
| №  з/п | Назва теми | Кількість  годин |
| 1 | Аналіз технічних каналів витоку інформації та механізм їх утворення. | 2 |
| 2 | Аналіз методів та засобів захисту електромагнітної інформації. | 2 |
| 3 | Аналіз методів захисту інформації у автоматизованих системах. | 2 |
| 4 | Адміністрування та експлуатація захищених інформаційно-комунікаційних систем. | 2 |
| 5 | Програмне забезпечення для адміністрування ЗІКС та КМ. | 2 |
| 6 | Адміністрування у ОС NetWare фірми Novell. | 4 |
| 7 | Засоби управління локальними ресурсами ЗІКС та КМ. | 4 |
| 8 | Якісний та кількісний аналіз ризику для ІБ та КБ об’єкту інформатизації (ОБІ). | 4 |
| 9 | Аналізу ступеня ризику для ІБ ОБІ. | 4 |
| 10 | Кількісна оцінка ступеня ризику для ІБ. | 4 |
|  | **Разом за семестр** | **30** |
|  | **Разом** | **30** |

**8. Самостійна робота**

|  |  |  |
| --- | --- | --- |
| №  з/п | Назва теми | Кількість  годин |
| 1 | Технічні канали витоку інформації та механізм їх утворення. | 6 |
| 2 | Методи та засоби захисту електромагнітної інформації. | 4 |
| 3 | Методи захисту інформації у автоматизованих системах. | 4 |
| 4 | Адміністрування та експлуатація захищених інформаційно-комунікаційних систем. | 6 |
| 5 | Програмне забезпечення для адміністрування ЗІКС та КМ. | 6 |
| 6 | Адміністрування у ОС NetWare фірми Novell. | 6 |
| 7 | Засоби управління локальними ресурсами ЗІКС та КМ. | 6 |
| 8 | Якісний та кількісний аналіз ризику для ІБ та КБ об’єкту інформатизації (ОБІ). | 4 |
| 9 | Визначення ступеня ризику для ІБ ОБІ. | 6 |
| 10 | Кількісна оцінка ступеня ризику для ІБ. | 4 |
| 11 | Система управління ризиками ІБ. | 4 |
| 12 | Комплексне управління довгостроковими інвестиціями у політику ІБ ОБІ. | 4 |
|  | **Разом** | **60** |

**9. Індивідуальні завдання**

1. Концептуальні засади забезпечення інформаційної безпеки України.
2. Нормативно-правові основи захисту інформації в Україні.
3. Концепція національної безпеки України, концепція інформаційної безпеки України.
4. Доктрина інформаційної безпеки України.
5. Доктрини інформаційної безпеки країн ЄС.
6. Доктрини інформаційної безпеки США.
7. Місце технічного захисту інформації у системі інформаційної безпеки.
8. Сутність та завдання технічного захисту інформації.
9. Способи несанкціонованого зняття інформації.
10. Визначення можливих джерел витоку акустичної та електромагнітної інформації у приміщенні.
11. Визначення можливих джерел витоку інформації з радіоканалу.
12. Складові ТЗІ.
13. Методи пасивного та активного захисту інформації.
14. Методи та засоби захисту акустичної інформації.
15. Методи та засіб захисту електромагнітної інформації.
16. Методи захисту від ВЧ-нав’язування.
17. Методики і засоби пошуку радіозакладних пристроїв.
18. Методи захисту інформації у автоматизованих системах.
19. Програмні засоби захисту інформації.
20. Вибір програм розмежування доступу до інформації.
21. Вибір та застосування антивірусних програм.
22. Вибір програм автоматичного шифрування інформації при її збереженні на дисках та відпрацювання практичних навичок їх застосування.
23. Методи захисту інформації у телекомунікаційних мережах та відкритих мережах зв’язку.
24. Захист мовленнєвої інформації, що передається у відкритих каналах зв’язку.
25. Загальні принципи побудови захищених інформаційно-комунікаційних систем (ЗІКС) та КМ.
26. Призначення та класифікація ІКМ та КМ.
27. Логічна та фізична структури ІКМ та КМ.
28. Телекомунікаційна система КМ та характеристика її елементів.
29. Завдання адміністрування та експлуатація захищених інформаційно-комунікаційних систем.
30. Атестацію захищених інформаційних та комунікаційних систем в умовах додержання режиму секретності із зафіксуванням результатів у відповідних документах.
31. Основні принципи організації взаємодії в ЗІКС та КМ.
32. Логічна модель взаємодії ЗІКС та КМ.
33. Функціональні рівні взаємодії та їх ієрархія.
34. Особливості еталонної моделі взаємодії відкритих систем (ВВС) для локальних комп’ютерних мереж (ЛКМ).
35. Програмне забезпечення для адміністрування ЗІКС та КМ.
36. Структура, призначення, склад і загальна характеристика основних елементів.
37. Мережеві операційні системи та їх характеристика.
38. Аналізатори протоколів.
39. Особливості функціонування ОС різних типів.
40. Основи мережевої безпеки.
41. Адміністрування у ОС NetWare фірми Novell.
42. Засоби управління локальними ресурсами ЗІКС та КМ.
43. Якісний та кількісний аналіз ризику для ІБ та КБ об’єкту інформатизації.
44. Сутність якісного та кількісного аналізу ризиків для ІБ та кібербезпеки підприємства, фірми.
45. Принципи аналізу ризиків для ІБ.
46. Напрямки аналізу підприємницьких ризиків для ІБ.
47. Збитки, які виникають в процесі підприємницької діяльності.
48. Методи аналізу ступеня ризику для ІБ.
49. Характеристика області абсолютної стійкості, нормальної стійкості, області нестійкого стану, критичного стану, кризового стану підприємства на основі аналізу ризику для ІБ.
50. Методи кількісної оцінки ступеня ризику: аналітичний метод; метод використання аналогів. Комплексна оцінка ризиків для ІБ.
51. Визначення ключового параметру, вибір чинників впливу, програмування величини ключового параметру для оцінки ризиків ІБ та КБ.
52. Визначення імовірності досліджуваного проекту на основі оцінок імовірності проектів-аналогів для побудови СЗІ на ОБІ.
53. Прогноз очікуваних характеристик досліджуваного проекту захисту ОБІ.
54. Принципи управління ризиками ІБ.
55. Система управління ризиками ІБ.
56. Основи профілактики ризиків: диверсифікація та лімітування.
57. Ризики, пов'язані з вкладенням капіталу у засоби ЗІ.
58. Комплексне управління довгостроковими інвестиціями у політику ІБ ОБІ.

**ПЕРЕЛІК ПИТАНЬ ДЛЯ САМОСТІЙНОЇ РОБОТИ**

**10. Методи навчання**

Проведення лекцій з використанням технічних засобів навчання. Проведення лабораторних робіт та самостійної роботи засобами інформаційно-комунікаційних технологій в освіті. Використовується електронний навчальний курс на платформі Moodle «Захист інформації в комп'ютерних системах і кібербезпека (Частина 2)».

**11. Форми контролю**

Наприкінці кожного змістовного модуля проводиться контрольна робота у вигляді тесту, що створений у комп’ютерному навчальному середовищі. Підсумкова атестація: іспит.

**12. Розподіл балів, які отримують студенти**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Поточний контроль | | | Рейтинг з навчальної роботи  R НР | Рейтинг з додаткової роботи R ДР | Рейтинг штрафний R ШТР | Підсумкова атестація  (екзамен  чи залік) | Загальна кількість балів |
| Змістовий модуль 1 | Змістовий модуль 2 | Змістовий модуль 3 |
| 0-100 | 0-100 | 0-100 | 0-70 | 0-20 | 0-5 | 0-30 | 0-100 |

Оцінка виконання та захисту лабораторних робіт за кожний модуль здійснюється у наступній відповідності:

|  |  |  |
| --- | --- | --- |
| **№ лабораторної роботи** | **Кількість балів** | **Загальна кількість балів** |
| **1 модуль** | | |
| Лабораторна робота № 1 | 10 | 70 |
| Лабораторна робота № 2 | 10 |
| Лабораторна робота № 3 | 10 |
| Лабораторна робота № 4 | 10 |
| Лабораторна робота № 5 | 10 |
| Самостійна робота | 20 |
| Модульна контрольна |  | 30 |
| **2 модуль** | | |
| Лабораторна робота № 6 | 14 | 70 |
| Лабораторна робота № 7 | 14 |
| Лабораторна робота № 8 | 7 |
| Лабораторна робота № 9 | 7 |
| Лабораторна робота № 10 | 14 |
| Самостійна робота | 14 |
| Модульна контрольна |  | 30 |

**Примітки.** 1. Відповідно до «Положення про кредитно-модульну систему навчання в НУБіП України», затвердженого ректором університету 03.04.2011 р., рейтинг студента з навчальної роботи **R НР** стосовно вивчення певної дисципліни визначається за формулою

де **R(1)ЗМ, … R(3)ЗМ** − рейтингові оцінки змістових модулів за 100-бальною шкалою;

**К(1)ЗМ, … К(3)ЗМ**− кількість кредитів ЕСТS, передбачених робочим навчальним планом для відповідного змістового модуля;

**КДИС = К(1)ЗМ + К(2)ЗМ****+ К(2)ЗМ**− кількість кредитів ЕСТS, передбачених робочим навчальним планом для дисципліни у поточному семестрі (**КДИС=2,5)**;

**R ДР** − рейтинг з додаткової роботи;

**R ШТР** − рейтинг штрафний.

Наведену формулу можна спростити, якщо прийняти **К(1)ЗМ = 0,6кр, К(2)ЗМ =1,5кр, К(3)ЗМ=0,4кр.** Тоді вона буде мати вигляд

***Рейтинг з додаткової роботи* R ДР** додається до **R НР** і не може перевищувати 20 балів. Він визначається лектором і надається студентам рішенням кафедриза виконання робіт, які не передбачені навчальним планом, але сприяють підвищенню рівня знань студентів з дисципліни.

***Рейтинг штрафний* R ШТР** не перевищує 5 балів і віднімається від **R НР**. Він визначається лектором і вводиться рішенням кафедри для студентів, які матеріал змістового модуля засвоїли невчасно, не дотримувалися графіка роботи, пропускали заняття тощо.

2. Згідно із зазначеним Положенням ***підготовка і захист*** ***курсового проекту (роботи)*** оцінюється за 100 бальною шкалою і далі переводиться в оцінки за національною шкалою та шкалою ECTS.

**Шкала оцінювання: національна та ECTS**

|  |  |  |  |
| --- | --- | --- | --- |
| Сума балів за всі види навчальної діяльності | ОцінкаECTS | Оцінка за національною шкалою | |
| для екзамену, курсового проекту (роботи), практики | для заліку |
| 90 – 100 | **А** | відмінно | зараховано |
| 82-89 | **В** | добре |
| 74-81 | **С** |
| 64-73 | **D** | задовільно |
| 60-63 | **Е** |
| 35-59 | **FX** | незадовільно з можливістю повторного складання | не зараховано з можливістю повторного складання |
| 0-34 | **F** | незадовільно з обов’язковим повторним вивченням дисципліни | не зараховано з обов’язковим повторним вивченням дисципліни |

**13. Методичне забезпечення**

1. Електронний навчальний курс на платформі Moodle вміщує повне методичне забезпечення включаючи: лекції, презентації до лекцій, методичні вказівки до виконання лабораторних робіт, глосарій термінів тощо.

**14. Рекомендована література**

**Базова**

1. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. – Х.: Вид. ХНЕУ, 2010. – 316 с.
2. Браіловський М.М. Захист інформації у банківській діяльності / М.М. Браіловський, Г.П. Лазарєв, В.О. Хорошко. – К.: ТОВ “ПоліграфКонсалтинг”, 2010. – 216 с.
3. Поповский В.В. Защита информации в телекоммуникационных системах: Учебник в 2-х т. / В.В. Поповский, А.В. Персиков. – Харьков: ООО «Компания СМИТ», 2006. – 238 с. [1]. – 292 c.
4. Конахович Г.Ф. Защита информации в телекоммуникационных системах / Г.Ф. Конахович, В.П. Климчук, С.М. Паук, В.Г. Потапов. – К.: “МК–Пресс”, 2005. – 288 с.
5. Баранов О. А. Інформаційне право України: стан, проблеми, перспективи / О. А. Баранов. – К. : Видавничий дім "СофтПрес", 2005. – 316 с.
6. Венбо М. Современная криптография: теория и практика: пер. с англ. / М.Венбо – М.: Издательский дом "Вильямс", 2014. – 768 с.
7. Вербіцький О. В. Вступ до криптології / О.В. Вербіцький. – Львів: ВНТЛ, 1998. – 248 с.
8. Горбатов В. С. Основы технологии PKI / В. С. Горбатов, О. Ю. Полянская – М.: Горячая линия – Телеком, 2012. – 248 с.
9. Гребенчук В. Г. Цифровая стеганография / В.Г. Гребенчук, И. Н. Оков, И. В. Туринцев. – М.: СОЛОН-Пресс, 2012. – 272 с.
10. Грибунин В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. – М.: СОЛОН-Прес, 2008. – 272 с.
11. Зима В. М. Безопасность глобальных сетевых технологий / В. М. Зима, А. А. Молдовян, Н. А. Молдовян. – 2-е изд. – СПб.: БХВ- Петербург, 2009. – 368 с.
12. Кузнецов О.О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х.: Вид. ХНЕУ, 2011. – 510 с.
13. Ленков С. В. Методы и средства защиты информации. В 2-х томах / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко. Т.II. Информационная безопасность. – К.: Арий, 2008. – 344 с.

**Допоміжна**

1. Петров А. А. Компьютерная безопасность. Криптографические методы защиты / А. А. Петров – М.: ДМК, 2000. – 448 с.
2. Столлингс В. Криптография и защита сетей: принципы и практика. – 2-е изд. / В. Столлингс; пер. с англ. – М.: Издательский дом "Вильямс", 2001. – 672 с.
3. Хорошко В.А. Методы и средства зашиты информации / В. А. Хорошко, А. А. Чекатков – К.: Юниор, 2003. – 504 с.
4. Чмора А. Л. Современная прикладная криптография / А. Л. Чмора. – М.: Гелиос АРВ, 2001. – 256 с.
5. Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа / А. Ю. Щеглов. – СПб.: Наука и Техника, 2004. – 384 с.

**15. Інформаційні ресурси**

1. ЗАКОН УКРАЇНИ Про національну безпеку України (Відомості Верховної Ради (ВВР), 2019, № 31, ст.241) [Електронний ресурс] – Режим доступу: <http://zakon.rada.gov.ua/laws/show/2469-19>

2. ЗАКОН УКРАЇНИ про внесення змін до Закону України "Про захист інформації в автоматизованих системах" [Електронний ресурс] – Режим доступу: http://zakon.rada.gov.ua/laws/show/2594-15

3. АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ’ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ [Електронний ресурс] – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art\_id=81998&cat\_id=38835

**16. Нормативна література**

1. ДСТУ ГОСТ 28147: 2009 Система обробки інформації. Захист криптографічний. Алгоритм криптографічного перетворення (ГОСТ 28147-89) ДСТУ 2396-94 Системи оброблення інформації. Теорія інформації. Терміни та визначення
2. ДСТУ 4145-2002 “Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння”;
3. ДСТУ ISO/IEC 11770-3:2002 “Інформаційні технології. Методи захисту. Управління ключовими даними. Частина 3. Протоколи, що ґрунтуються на асиметричних криптографічних перетвореннях”;
4. ДСТУ ISO/IEC 15946-3:2002 “Інформаційні технології. Методи захисту. Криптографічні методи, що ґрунтуються на еліптичних кривих. Частина 3. Установлення ключів”;
5. ДСТУ ГОСТ 28147-2009 “Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования”;
6. ДСТУ ISO/IEC 10118-3:2005 “Інформаційні технології. Методи захисту. Геш-функції. Частина 3. Спеціалізовані геш-функції”.
7. ДСТУ 2481-94 Системи оброблення інформації. Інтелектуальні інформаційні технології. Терміни та визначення
8. ДСТУ 2505-94 Системи оброблення інформації. Організація даних. Терміни та визначення.