**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**Національний університет біоресурсів і природокористування України**

**Факультет інформаційних технологій**

**Кафедра комп’ютерних систем і мереж**

«ЗАТВЕРДЖУЮ»

декан факультету

інформаційних технологій

\_\_\_\_\_\_\_\_\_\_\_\_О.Г. Глазунова

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2020 р.

**РОБОЧА НАВЧАЛЬНА ПРОГРАМА**

**З ДИСЦИПЛІНИ**

**КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ**

спеціальність 125 «Кібербезпека»

**Київ – 2020 рік**

Робоча навчальна програма дисципліни «Комплексні системи захисту інформації» для студентів спеціальності 125 - Кібербезпека, освітня програма – Кібербезпека, денної форми навчання. – НУБіП України, 2020. – 15 с.

Розробник:

Сагун А.В., кандидат технічних наук, доцент.

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

Протокол № 9 від 15 червня 2020 року.

Завідувач кафедри комп’ютерних систем і мереж

 \_\_\_\_\_\_\_\_\_\_ В.А. Лахно,

доктор технічних наук, професор

Схвалено навчально-методичною радою факультету інформаційних технологій

Протокол № 9 від «22» червня 2020 року.

Голова навчально-методичної ради \_\_\_\_\_\_\_\_\_\_\_\_\_

# **1. Опис навчальної дисципліни**

|  |  |  |
| --- | --- | --- |
| Найменування показників  | Галузь знань, напрям підготовки, освітній ступінь | Характеристика навчальної дисципліни |
| **денна форма навчання** | **заочна форма навчання** |
| Кількість кредитів – 4 | галузь знань 12 Інформаційні технології  | Нормативна |
| 125 - Кібербезпека |
| Освітня програмаКібербезпека | **Рік підготовки:** |
| 2-й |  |
| Індивідуальне науково-дослідне завдання: - | **Семестр** |
| Загальна кількістьгодин – 120 | 4-й |  |
| **Лекції** |
| Тижневих годин для денної форми навчання:аудиторних – 4самостійної роботи студента – 4 | Освітній ступінь«Бакалавр» | 30 год. |  |
| **Практичні, семінарські** |
| 0 год. |  |
| **Лабораторні** |
| 30 год. |  |
| **Самостійна робота** |
| 60 год. |  |
| **Індивідуальне завдання:** - |
| Вид підсумкового контролю: 4 семестр – **іспит** |

**2. МЕТА ТА ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

**Мета:** є формування у студентів знань з організації комплексних систем захисту інформації (КСЗІ) на підприємстві.

**Завдання дисципліни:** вивчення сутності та завдань комплексної системи захисту інформації (КСЗІ); вивчення принципів організації та етапів розробки КСЗІ, факторів, що впливають на організацію КСЗІ; визначення та нормативне закріплення складу інформації, яка підлягає захисту; визначення об'єктів захисту; аналіз і оцінка загроз безпеці інформації: виявлення та оцінка джерел, способів і результатів дестабілізуючого впливу на інформацію; визначення потенційних каналів і методів несанкціонованого доступу до інформації, визначення можливостей несанкціонованого доступу до інформації, яка підлягає захисту; визначення компонентів і умов функціонування КСЗІ, розробка моделі, технологічного та організаційної побудови КСЗІ; кадрове, матеріально-технічне та нормативно-методичне забезпечення функціонування КСЗІ; призначення, структура і зміст управління КСЗІ, вивчення принципів і методів планування, сутності і змісту контролю функціонування КСЗІ; вивчення особливостей управління КСЗІ в умовах надзвичайних ситуацій; вивчення складу методів і моделей оцінки ефективності КСЗІ.

**Після вивчення даної дисципліни студенти повинні**

##### знати:

* основні поняття та принципи побудови комплексної системи захисту інформації;
* нормативно – правові базу, що регулює етапи побудови, аудиту та впровадження КСЗІ;
* методики визначення об’єктів КСЗІ, їх класифікації та оцінки джерел дестабілізуючого впливу;
* принципи класифікації інформації, що підлягає захисту в КСЗІ підприємств та організацій різної форми власності;
* механізми та методи забезпечення організаційної, криптографічної, інженерно-технічної складових КСЗІ;
* методологію розробки та складанні моделей порушника та моделі загроз з врахуванням особливостей протікання бізнес-процесів на підприємстві чи організації;
* етапи проектування, розробки та підтримки КСЗІ та принципи сертифікації створюваних систем захисті інформації;
* принципи розробки політики безпека підприємства або організації різних форм власності.

***вміти:***

* вирішувати задачі супроводу та впровадження комплексних систем захисту інформації, а також протидії несанкціонованому доступу до ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
* здійснювати оцінку рівня захищеності інформації що обробляється в інформаційно-телекомунікаційних системах використовувати інструментальні засоби оцінювання;
* готувати пропозиції до нормативних актів і документів з метою забезпечення встановленої політики інформаційної безпеки і \або кібербезпеки; - розробляти проектну документацію, щодо програмних та програмно-апаратних комплексів захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем; - виконувати аналіз реалізації прийнятої політики інформаційної і /або кібербезпеки;
* проектувати та реалізувати комплексні системи захисту інформації в автоматизованих системах організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації;
* вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;
* визначати рівень захищеності інформаційних ресурсів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;

##### Отримати такі компетенції:

- здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів

- здатність застосовувати законодавчу та нормативно - правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки

- здатність забезпечувати захист інформації, що обробляється в інформаційно - телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

- здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.

**3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

**Змістовий модуль 1**

#### Нормативно-правове забезпечення процесу створення та впровадження КСЗІ та підприємстві

**Тема 1.1.** Комплексні системи захисту інформації.Стандарти та нормативні акти систем захисту інформації. Методика аналізу інформаційної та організаційної інфраструктури підприємства. Стандарти серії ISO 27000. Нормативні документи оцінки КСЗІ.

**Тема 1.2.** Нормативні документи технічного захисту інформації (НД ТЗІ) автоматизованих систем. Принципи формування функціонального профілю захищеності інформації. Етапи побудови КСЗІ. Формулювання заявки на КСЗІ та визначення механізмів та технологій захисту.

**Тема 1.3.** Алгоритм оцінки та вибору об’єктів комплексного захисту в інформаційній системі підприємства. Основний принцип та умови побудови КСЗІ підприємства.

**Тема 1.4.** Інформаційні активи (ІА). Принципи класифікації ІА та нормативно – правове обґрунтування класифікації ІА. Інформація з обмеженим доступом, державна таємниця, відкрита інформація та інформація, що є власністю держави.

**Тема 1.5.** Сертифікація КСЗІ. Порядок отримання та підтвердження сертифікату. Види сертифікатів КСЗІ. Методологія вибору компонентів КСЗІ з використанням вимог, щодо відомостей про засоби технічного захисту інформації, встановлені розпорядженнями регуляторних органів (НБУ, Держспецзв’язку України, Наказами та розпорядженнями КМУ тощо).

**Змістовний модуль 2**

**Організаційно-методичне забезпечення КСЗІ**

**Тема 2.1.** Технології забезпечення конфіденційності, цілісності та доступності інформації в складі КСЗІ. Інструментальні засоби проектування**.** Джерела вразливостей та засоби реалізації НСД і інформаційно – комунікаційних системах.Передумови появи НСД, методи виявлення.

**Тема 2.2.** Впливи на роботу ІС. Модель порушника та типи порушників ІБ стосовно захищуваної інформації.

 **Тема 2.3.** Моделі загроз. Політики та правила доступу до ІА. Політики безпеки. Формування правил та матриць доступу до ІА на підприємствах.

**Тема 2.4.** Організаційні заходи забезпечення та супроводу КСЗІ. Складання та супроводження інструктажів, графіків підвищення кваліфікації.

 **Тема 2.5.** Складання планів та графіків аудиту заходів та систем безпеки. Опитувальник. Складання опитувальника відповідно рекомендації стандартів серії ISO/IEC 27000. Календарні плани та графіки аудиту КСЗІ. Автоматизовані засоби аудиту КСЗІ.

**Змістовий модуль 3**

**Інженерно – технічні засоби захисту інформації в КСЗІ**

**Тема 3.1.** Технології та методи захисту конфіденційності, цілісності та доступності інформації з використання інженерно – технічних методів КСЗІ. **З**абезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом.

**Тема 3.2.** Планування досліджень витоків інформації в приміщенні фізичними каналами (звукові, візуальні, радіо та електронні). Методи детектування та попередження витоків інформації через технічні канали зв’язку.

**Тема 3.3.** Захист кабельних мереж та каналів. Канали витоків інформації. Телевідеонагляд та системи охоронно-пожежної сигналізації.

**Тема 3.4.** Проектування та комп’ютерна реалізація систем розмежування доступу до інформації на основі матриць доступу. Інструментальні засоби реалізації політики доступу до інформації.

**Тема 3.5.** Механізми та технології захисту Web-ресурсів. Захист інформаційного контенту web-сторінки відповідно до вимог НД ТЗІ 2.5-010-03. Методики сканування web-ресурсів на вразливості.

**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**Нормативно-правове забезпечення процесу створення та впровадження КСЗІ та підприємстві |
| **Тема 1.1.** Комплексні системи захисту інформації.Стандарти та нормативні акти систем захисту інформації. Методика аналізу інформаційної та організаційної інфраструктури підприємства. Стандарти серії ISO 27000. Нормативні документи оцінки КСЗІ. | 8 | 2 | - | 2 | - | 4 |  |  |  |  |  |  |
| **Тема 1.2.** Нормативні документи технічного захисту інформації (НД ТЗІ) автоматизованих систем. Принципи формування функціонального профілю захищеності інформації. Етапи побудови КСЗІ. Формулювання заявки на КСЗІ та визначення механізмів та технологій захисту. | 10 | 2 | - | 4 | - | 4 |  |  |  |  |  |  |
| **Тема 1.3.** Алгоритм оцінки та вибору об’єктів комплексного захисту в інформаційній системі підприємства. Основний принцип та умови побудови КСЗІ підприємства. | 6 | 2 | - | - | - | 4 |  |  |  |  |  |  |
| **Тема 1.4.** Інформаційні активи (ІА). Принципи класифікації ІА та нормативно – правове обґрунтування класифікації ІА. Інформація з обмеженим доступом, державна таємниця, відкрита інформація та інформація, що є власністю держави. | 8 | 2 | - | 2 | - | 4 |  |  |  |  |  |  |
| **Тема 1.5.** Сертифікація КСЗІ. Порядок отримання та підтвердження сертифікату. Види сертифікатів КСЗІ. Методологія вибору компонентів КСЗІ з використанням вимог, щодо відомостей про засоби технічного захисту інформації, встановлені розпорядженнями регуляторних органів (НБУ, Держспецзв’язку України, Наказами та розпорядженнями КМУ тощо). | 8 | 2 | - | 2 |  | 4 |  |  |  |  |  |  |
| **Всього годин на 1 модуль** | 40 | 10 | - | 10 | - | 20 |  |  |  |  |  |  |
| **Змістовний модуль 2****Організаційно-методичне забезпечення КСЗІ**  |
| **Тема 2.1.** Технології забезпечення конфіденційності, цілісності та доступності інформації в складі КСЗІ. Інструментальні засоби проектування**.** Джерела вразливостей та засоби реалізації НСД і інформаційно – комунікаційних системах.Передумови появи НСД, методи виявлення. | 6 | 2 | - | - | - | 4 |  |  |  |  |  |  |
| **Тема 2.2.** Впливи на роботу ІС. Модель порушника та типи порушників ІБ стосовно захищуваної інформації.  | 8 | 2 |  | 4 | - | 4 |  |  |  |  |  |  |
| **Тема 2.3.** Моделі загроз. Політики та правила доступу до ІА. Політики безпеки. Формування правил та матриць доступу до ІА на підприємствах. | 10 | 2 |  | 4 | - | 4 |  |  |  |  |  |  |
| **Тема 2.4.** Організаційні заходи забезпечення та супроводу КСЗІ. Складання та супроводження інструктажів, графіків підвищення кваліфікації.  | 6 | 2 |  | - | - | 4 |  |  |  |  |  |  |
| **Тема 2.5.** Складання планів та графіків аудиту заходів та систем безпеки. Опитувальник. Складання опитувальника відповідно рекомендації стандартів серії ISO/IEC 27000. Календарні плани та графіки аудиту КСЗІ. Автоматизовані засоби аудиту КСЗІ. | 10 | 2 |  | 2 | - | 4 |  |  |  |  |  |  |
| **Всього годин на 2 модуль** | 40 | 10 |  | 10 |  | 20 |  |  |  |  |  |  |
| **Змістовий модуль 3****Інженерно – технічні засоби захисту інформації в КСЗІ** |
| Тема 3.1. Технології та методи захисту конфіденційності, цілісності та доступності інформації з використання інженерно – технічних методів КСЗІ. Забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом. | 6 | 2 | - | - | - | 4 |  |  |  |  |  |  |
| Тема 3.2. Планування досліджень витоків інформації в приміщенні фізичними каналами (звукові, візуальні, радіо та електронні). Методи детектування та попередження витоків інформації через технічні канали зв’язку. | 6 | 2 | - | - | - | 4 |  |  |  |  |  |  |
| Тема 3.3. Захист кабельних мереж та каналів. Канали витоків інформації. Телевідеонагляд та системи охоронно-пожежної сигналізації. | 8 | 2 | - | 2 | - | 4 |  |  |  |  |  |  |
| Тема 3.4. Проектування та комп’ютерна реалізація систем розмежування доступу до інформації на основі матриць доступу. Інструментальні засоби реалізації політики доступу до інформації. | 10 | 2 | - | 4 | - | 4 |  |  |  |  |  |  |
| **Тема 3.5.** Механізми та технології захисту Web-ресурсів. Захист інформаційного контенту web-сторінки відповідно до вимог НД ТЗІ 2.5-010-03. Методики сканування web-ресурсів на вразливості. | 10 | 2 | - | 4 | - | 4 |  |  |  |  |  |  |
| **Всього годин на 3 модуль** | 40 |  |  | 10 |  | 20 |  |  |  |  |  |  |
| **Всього годин на курс** | **120** | **30** |  | **30** | **-** | **60** |  |  |  |  |  |  |

**5. ТЕМИ СЕМІНАРСЬКИХ ЗАНЯТЬ**

Семінарські заняття не передбачені програмою навчальної дисципліни.

**6. ТЕМИ ЛАБОРАТОРНИХ ЗАНЯТЬ**

|  |  |  |
| --- | --- | --- |
| №з/п | Назва теми | Кількістьгодинденна/заочна |
| 1 | Визначення інформаційної структури підприємства | 2 |
| 2 | Формування функціонального профілю захищеності інформації АС | 4 |
| 3 | Класифікація інформаційних активів підприємства | 2 |
| 4 | Етапи реалізації КСЗІ на підприємстві. Формування заявки на створення КСЗІ. | 2 |
| 5 | Створення моделі порушника інформаційної безпеки | 4 |
| 6 | Розробка політики інформаційної безпеки підприємств та організацій | 2 |
| 7 | Розробка процедури аудиту стану ІБ для підприємства | 4 |
| 8 | Організація системи телевідеонагляду. | 2 |
| 9 | Реалізація систем розмежування доступу до інформації на основі матриць доступу для терміналу на базі ОС Windows | 4 |
| 10 | Механізми та технології захисту Web-ресурсів (НД ТЗІ 2.5-010-03). Сканування web-ресурсів на вразливість. | 4 |
|  | Всього, годин | 30 |

**7. ТЕМИ ПРАКТИНИХ ЗАНЯТЬ**

Практичні заняття не передбачені програмою навчальної дисципліни.

**8. САМОСТІЙНА РОБОТА**

|  |  |  |
| --- | --- | --- |
| №з/п | Назва теми | Кількістьгодинденна/заочна |
| 1 | Законодавче регулювання захисту інформації. Стандарт «помаранчева» книга. Британський стандарт BS 7799. | 4 |
| 2 | Проектний та процесний підхід щодо впровадження та супроводу систем захисту інформації | 4 |
| 3 | Методи оцінки вартості інформації. Експертний метод, метод  | 4 |
| 4 | Грифування інформації та особливості захисту, обороту та знищення інформації, яка містить гриф. | 4 |
| 5 | Особливості захисту інформації в банківських установах. Елементи систем банківської безпеки. | 4 |
| 6 | Серії стандартів управління інформаційної безпекою та особливості їх імплементації на підприємствах і організаціях різної форми власності. | 4 |
| 7 | Апаратні методи захисту інформації. | 4 |
| 8 | Елемент систем телевідеонагляду | 4 |
| 9 | Поняття аудиту стану захищеності. Алгоритми проведення аудиту захищеності інформації на підприємствах та організаціях. | 4 |
| 10 | Методи соціальної інженерії та їх вплив на стан захищеності та побудову КСЗІ. | 4 |
| 11 | Акустичні та візуальні методи здійснення спроб НСД стосовно конфіденційної інформації. | 4 |
| 12 | Сканери вразливостей комп’ютерних систем та мереж. | 4 |
| 13 | Криптографічні методи захисту інформації в ІКС. | 4 |
| 14 | Типові вразливості Web-ресурсів. Вразливостей типу SQL-injection, XSS. | 4 |
| 15 | Вразливості захисту популярних CMS та Web-платформ. | 4 |
| Всього годин | **60** |

**9. ІНДИВІДУАЛЬНЕ ЗАВДАННЯ**

Самостійна робота виконується у протягом семестру.

**Мета, завдання і зміст самостійної роботи**

мета роботи полягає в: оволодіння навичками проектування комплексних системи захисту інформації, методами розробки окремих підсистем та механізмів таких систем, опанування основними означеннями та поняттями в КСЗІ на рівні їх тлумачення та відтворення для практичного застосування та втілення у процесі діяльності бакалавра з кібербезпеки.

**Завдання роботи:** розробляти базові нормативні та альтернативні складники КСЗІ, враховуючи вплив дестабілізуючих фа­кторів та інформаційних загроз на безпеку підприємств та організацій.

Мати аналітичний погляд на композицію та декомпозиціє КСЗІ, та ї її окремих складників та вміти оцінити та запропонувати оптимальну концепцію КСЗІ для конкретних умов та мети.

**10. МЕТОДИ НАВЧАННЯ**

Пояснювально-ілюстративний метод – застосовується в ході лекцій та у процесі самостійної роботи студентів для передачі великих масивів навчальної інформації в опрацьованому вигляді.

Репродуктивний метод – застосовується в ході практичних занять і процесі самостійної роботи, передбачає набуття студентами навичок використання визначених алгоритмів вирішення навчальних та професійних завдань.

Метод проблематизації та евристичний метод – застосовуються в ході лекційних, практичних занять, самостійної та індивідуальної роботи.

**11. МЕТОДИ КОНТРОЛЮ**

Поточний контроль – усне опитування в ході лекцій та практичних занять, перевірка конспектів (у тому числі самостійної роботи), оцінювання правильності вирішення тестових та практичних завдань на практичних заняттях.

Підсумковий контроль – 2 семестр – **іспит.**

**12. РОЗПОДІЛ БАЛІВ ТА КРИТЕРІЇ ОЦІНЮВАННЯ**

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

**Розподіл балів, які отримують студенти (аудиторна робота)**

|  |  |
| --- | --- |
| Поточне тестування та самостійна робота | Сума |
| **Змістовний модуль 1** | **Змістовний модуль 2** | **Змістовний модуль 3** |
| Т1.1 | Т1.2 | Т1.3 | Т1.4 | Т1.5 | Т2.1 | Т2.2 | Т2.3 | Т2.4 | Т2.5 | Т3.1 | Т3.2 | Т3.3 | Т3.4 | Т3.5 | 60 |
| 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |  |

Т1.1, Т1.2 ... Т3.5 – теми змістових модулів

**Розподіл балів, які отримують студенти (для екзамену)**

|  |  |  |
| --- | --- | --- |
| Поточне тестування та самостійна робота | Підсумковий тест (екзамен) | Сума |
| № змістовного модуля | 40 | 100 |
| **1** | **2** | **3** |
| 20 | 20 | 20 |

**Оцінювання знань студента здійснюється за 100-бальною шкалою (для екзаменів і заліків).**

**12.2. Нарахування балів під час поточного контролю**

|  |  |
| --- | --- |
| **Форма поточного контролю** | **Максимальна сума балів за одну тему** |
| Активність та виконання завдань на практичному занятті | 1,5 |
| Виконання самостійної роботи | 1,5 |
| Виконання наукової роботи | 12 |

**Нарахування балів за наукову роботу**

|  |  |  |
| --- | --- | --- |
| **Зміст роботи** | **Бали за зміст** | **Максимальна кількість балів** |
| Підготовка доповіді за обраною темою, виступ з доповіддю за темою дисципліни на конференції | 1-12 | 12 |
| Підготовка за темою дисципліни статті, роботи на конкурс | 12 | 12 |

Оцінювання студента відбувається згідно положення «Про екзамени та заліки у НУБіП України» від 27.02.2019 р. протокол №7.

|  |  |
| --- | --- |
| **національна**  | **Рейтинг здобувача вищої освіти, бали**  |
| **Відмінно**  | **90-100**  |
| **Добре**  | **74-89**  |
| **Задовільно**  | **60-73**  |
| **Незадовільно**  | **0-59**  |

**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

$$R\_{нр}=\frac{0,7∙\left(R\_{зм}^{\left(1\right)}∙К\_{зм}^{\left(1\right)}+R\_{зм}^{\left(2\right)}∙К\_{зм}^{\left(2\right)}+R\_{зм}^{\left(3\right)}∙К\_{зм}^{\left(3\right)}\right)}{К\_{дис}}+ R\_{др}+ R\_{штр} ,$$

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

$$R\_{нр}=\frac{0,7∙\left(R\_{зм}^{\left(1\right)}∙0,6+R\_{зм}^{\left(2\right)}∙1,5+R\_{зм}^{\left(3\right)}∙0,4\right)}{2,5}+ R\_{др}+ R\_{штр} ,$$

***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.

**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, перелік питань для самостійної роботи студента тощо.

**14. РЕКОМЕНДОВАНА ЛІТЕРАТУРА**

**Основна література**

1. Закон «Про інформацію»: Прийнятий 2 жовтня 1992 р. №2657-ХІІ // Відомості Верховної Ради України, 1992. – № 48. – С. 650.

2. Закон України «Про захист інформації в автоматизованих системах» // Відомості Верховної Ради України, 1994. - № 31. – С. 286.

3. Закон України «Про державну таємницю» // Відомості ВРУ, 1999. - № 49. – С. 428.

4. Богуш В.М., Юдін О.К. Інформаційна безпека держави: навчальний посібник/ В.М. Богуш, О.К. Юдін. – К.: Мк-Пресс, 2005. – 432 с.

5. Данільян О.Г., Дзьобань О.П., Панов М.І. Національна безпека України: структура та напрямки реалізації: навчальний посібник/ О.Г. Данільян, О.П. Дзьобань, М.І. Панов. – Харків: Фоліо, 2002. – 285 с.

7. Інформаційна безпека держави у контексті протидії інформаційним війнам: Навч. Посіб. // ред.. В.Б. Толубка, - К.: НАО, 2004.

8. Баранов О. А. Інформаційне право України: стан, проблеми, перспективи / О. А. Баранов. – К.: Видавничий дім "СофтПрес", 2005. – 316 с.

9. Кузнецов О.О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х.: Вид. ХНЕУ, 2011. – 510 с.

11. 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.

12. Кормич Б.А. Інформаційна безпека: організаційно-правові основи. / Б.А. Кормич. − К., Принт. 2004. -169 с.

**Додаткова література**

1. Юдін О.К., Корченко О.Г., Конахович В.Г. Захист інформації в мережах передачі даних. – К.: Вид-во ТОВ «НВП»ІНТЕРСЕРВІС», 2009. – 716 с.
2. Юдін О.К., Богуш В.М. Інформаційна безпека держави. – К.: «МК- Прес», 2005. – 432 с.
3. Домарєв В.В., Швець В.А., Шестакова В.В. Організаційне забезпечення захисту інформації з обмеженим доступом. Навчальний посібник. – К.: НАУ, 2006. – 108 с.
4. Мельников В.П. Информационная безопасность и защита информации. – М.: «Академия», 2008. – 336 с.
5. Дудатьєв А.В. Інформаційна безпека. Навчальний посібник. – Вінниця: УНІВАР-Сум-Вінниця, 2009. – 240 с.
6. Домарєв В.В., Скворцов С.О. Організація захисту інформації на об’єктах державної та підприємницької діяльності. Навчальний посібник. – К.: Вид-во Європ. Ун-ту, 2006. – 102 с.
7. Качинський А.Б. Безпека, загрози і ризик: наукові концепції та математичні методи / Інститут проблем національної безпеки; Національна академія Служби безпеки України. – К.: 2004. – 472 с.
8. Девянин П.Н. Модели безопасности компьютерных систем: Учеб. пособие. – М.: «Академия», 2005. – 114 с.
9. Завгородний В.И. Комплексная защита информации в компьютерных системах – М.: Логос; 2001. – 264 с.

**15. ІНФОРМАЦІЙНІ РЕСУРСИ**

1. Офіційний сайт ПВНЗ «Європейський університет» <http://www.e-u.in.ua>

2. Офіційний сайт Національної бібліотеки України імені В.І. Вернадського <https://www.google.com.ua>

3. Онлайн-бібліотека навчальної літератури <http://libfree.com>

4. Онлайн-бібліотека навчальної літератури <http://subject.com.ua>

5. Онлайн-бібліотека навчальної літератури <http://www.vuzllib.su>