**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**

**МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ**

спеціальність 125 «Кібербезпека»

**Київ – 2020 рік**

Робоча навчальна програма дисципліни « Методи та засоби захисту інофрмації» для студентів спеціальності 125 - Кібербезпека, освітня програма – Кібербезпека, денної форми навчання. – НУБіП України, 2020. – 16 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 – 5 | галузь знань  12 Інформаційні технології | Нормативна | |
| 125 - Кібербезпека |
| Освітня програма  Кібербезпека | **Рік підготовки:** | |
| 2-й |  |
| Індивідуальне науково-дослідне завдання: - | **Семестр** | |
| Загальна кількість  годин – 150 | 3-й |  |
| **Лекції** | |
| Тижневих годин для денної форми навчання:  аудиторних – 5  самостійної роботи студента – 5 | Освітній ступінь  «Бакалавр» | 30 год. |  |
| **Практичні, семінарські** | |
| 0 год. |  |
| **Лабораторні** | |
| 45 год. |  |
| **Самостійна робота** | |
| 75 год. |  |
| **Індивідуальне завдання:** - | |
| Вид підсумкового контролю:  3 семестр – **іспит** | |

**2. МЕТА ТА ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

**Мета:** ознайомлення з основними фізичними принципами, методами та засобами захисту інформації та пошуку розвідувальної апаратури, надання студентам знань з основ захисту інформації, принципів, методів та засобів несанкціонованого одержання інформації, а також створення протидії захисту інформації по каналах, на яких можливі її втрати. Вивчаються наступні питання: засоби несанкціонованого одержання інформації; методи протидії та захисту інформації від її несанкціонованого одержання; канали несанкціонованого одержання інформації; принципи та методи захисту інформації; механізми захисту інформації; методи захисту програмного забезпечення.

**Завдання дисципліни:**

**Після вивчення даної дисципліни студенти повинні**

##### знати:

* алгоритми створення проектів інформаційно-телекомунікаційних систем, базуючись на стандартизованих технологіях та протоколах передачі даних;
* принципи застосування теорії та методів захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;
* основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;
* принципи застосування різних класів політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;
* основи теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;
* принципи забезпечення введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту;
* алгоритми виявлення небезпечних сигналів технічних засобів.

***вміти:***

* вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
* вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.
* забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).
* реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
* вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).
* аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.

##### Отримати такі компетенції:

* здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.
* здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
* здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.
* здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.
* здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

**3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

**Змістовий модуль 1**

#### Методи та засоби захисту інформації. Формальні та неформальні методи та захисту

**Тема 1.1.** Методи та засоби захисту інформації, їх класифікація.Фізичні, апаратні, організаційні, програмні, законодавчі та психологічні засоби захисту.

**Тема 1.2.** Апаратні засоби захисту інформації.Реалізація криптографічних методів захисту (хешування та шифрування) в апаратних засобах ІКС.

**Тема 1.3.** Захист властивостей інформації при передавання в комп’ютерних мережах. Захист цілісності з використанням алгоритмів підрахунку контрольних сум Ethernet-пакетів.

**Тема 1.4.** Психологічні засоби захисту інформації. Соціальна інженерія та методи боротьби з психологічними методами атаки на властивості інформації.

**Змістовний модуль 2**

**Програмні та організаційні засоби захисту інформації на рівні елементів операційних систем. Автентифікації та її реалізація в ОС типу Linux**

**Тема 2.1.** Будова та принцип захисту інформації в середовищах ОС типу Linux (клієнтських та серверних). Механізми захисту файлових ресурсів та логіка розмежування доступу до файлових ресурсів в ОС Windows.

**Тема 2.2.** Автентифікація в ОС. Алгоритм та механізми автентифікації користувачів в ОС Linux.

**Тема 2.3**. Багатофакторна автентифікація та її реалізації в ОС типу Linux.

**Тема 2.4.** Програмно – організаційні засоби захисту інформації в ОС. Реалізація парольних політик захисту інформації в ОС Linux.

**Змістовий модуль 3**

**Методи, алгоритми та протоколи захисту інформації в сегментах та вузлах комп’ютерних систем**

**Тема 3.1.** Криптографічні методи та засоби захисту інформації в комп’ютерних мережах. Засоби симетричної та асиметричної криптографії. Симетричне шифрування. Організація захищеної передачі даних з використанням мережевого протоколу ssh.

**Тема 3.2.** Асиметричні криптоалгоритми RSA та DSA. Та їх реалізація в системах автентифікації.

**Тема 3.3.** Дослідження та аналіз захищеності передавання даних в комп’ютерних мережах на різних рівнях мережевої моделі OSI. Мережеві сканери. Використання мережевих сканерів для фіксації втручань в роботу ІКС. Технологія збирання доказів кібервтручань.

**Тема 3.4.** Статистично-сигнатурні методи та засоби захисту інформації в ІКС. Антивірусні системи.Налаштування систем блокування та попередження вторгнень (IDS та IPS системи). Міжмережеві екрани.

**Змістовий модуль 4**

**Методи та засоби захисту інформації в системах електронного документообігу**

**Тема 4.1.** Система електронного документообігу з точки зору кібербезпеки. Вид та форми електронного документу та властивості ЕД, які підлягають захисту. Роль та функції ЕЦП в захисті документаційної інформації.

**Тема 4.2.** Захист конфіденційності та доступності електронного документу та електронного ресурсу в хмарній системі ЕДО. Налаштування авторизації та механізмів доступу до хмарних сховищ електронних документів. Спеціалізовані засоби захисту конфіденційності.

**Тема 4.3.** Створення та налаштуваннямеханізмів розмежування доступу в системі ЕДО google docs та контроль доступу до електронного документу.

**Змістовий модуль 5**

**Способи та засоби захисту інформації в ОС типу Linux. Засоби відновлення даних та елементів ІС на базі ОС Windows**

**Тема 5.1.** Особливості зберігання та захисту користувацьких даних та організації системи розмежування доступу до них в ОС сімейства Windows. Криптографічні засоби захисту авторизаційних та користувацьких даних.

**Тема 5.2.** Політики безпеки. Засоби створення, редагування та імпортування локальних політик безпеки та механізмів аудиту безпеки в ОС Windows.

**Тема 5.3.** Засоби відновлення працездатності ОС Windows після збоїв. Інструментальні засоби та пакети для проведення криптоаналізу авторизаційних даних при аудиті безпеки Windows.

**Тема 5.4.** Системний реєстр ОС та принцип його роботи в ОС Windows. Створення резервних копій та технологія відновлення працездатності ОС Windows при збоях із застосування утиліт роботи з системним реєстром.

**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** Методи та засоби захисту інформації. Формальні та неформальні методи та захисту | | | | | | | | | | | | |
| **Тема 1.1.** Методи та засоби захисту інформації, їх класифікація. Фізичні, апаратні, організаційні, програмні, законодавчі та психологічні засоби захисту. | 6 | 2 | - |  | - | 4 |  |  |  |  |  |  |
| **Тема 1.2.** Апаратні засоби захисту інформації. Реалізація криптографічних методів захисту (хешування та шифрування) в апаратних засобах ІКС. | 8 | 2 | - | 2 | - | 4 |  |  |  |  |  |  |
| **Тема 1.3.** Захист властивостей інформації при передавання в комп’ютерних мережах. Захист цілісності з використанням алгоритмів підрахунку контрольних сум Ethernet-пакетів. | 8 | 2 | - | 4 | - | 2 |  |  |  |  |  |  |
| **Тема 1.4.** Психологічні засоби захисту інформації. Соціальна інженерія та методи боротьби з психологічними методами атаки на властивості інформації. | 6 | 2 |  | - |  | 4 |  |  |  |  |  |  |
| **Всього годин на 1 модуль** | 28 | 8 | - | 6 | - | 14 |  |  |  |  |  |  |
| **Змістовний модуль 2**  **Програмні та організаційні засоби захисту інформації на рівні елементів операційних систем. Автентифікації та її реалізація в ОС типу Linux** | | | | | | | | | | | | |
| **Тема 2.1.** Будова та принцип захисту інформації в середовищах ОС типу Linux (клієнтських та серверних). Механізми захисту файлових ресурсів та логіка розмежування доступу до файлових ресурсів в ОС Windows. | 12 | 2 | - | 4 | - | 6 |  |  |  |  |  |  |
| **Тема 2.2.** Автентифікація в ОС. Алгоритм та механізми автентифікації користувачів в ОС Linux. Багатофакторна автентифікація та її реалізації в ОС типу Linux. | 12 | 2 | - | 4 | - | 6 |  |  |  |  |  |  |
| **Тема 2.3.** Програмно – організаційні засоби захисту інформації в ОС. Реалізація парольних політик захисту інформації в ОС Linux. | 8 | 2 | - | 2 | - | 4 |  |  |  |  |  |  |
| **Всього годин на 2 модуль** | 32 | 6 | - | 10 | - | 16 |  |  |  |  |  |  |
| **Змістовий модуль 3**  **Методи, алгоритми та протоколи захисту інформації в сегментах та вузлах комп’ютерних систем** | | | | | | | | | | | | |
|  | 10 | 2 | - | 4 | - | 4 |  |  |  |  |  |  |
| Тема 3.2. Дослідження та аналіз захищеності передавання даних в комп’ютерних мережах на різних рівнях мережевої моделі OSI. Мережеві сканери. Використання мережевих сканерів для фіксації втручань в роботу ІКС. Технологія збирання доказів кібервтручань. | 10 | 2 | - | 4 | - | 4 |  |  |  |  |  |  |
| Тема 3.3. Статистично-сигнатурні методи та засоби захисту інформації в ІКС. Антивірусні системи. Налаштування систем блокування та попередження вторгнень (IDS та IPS системи). Міжмережеві екрани. | 12 | 2 | - | 4 | - | 6 |  |  |  |  |  |  |
| **Всього годин на 3 модуль** | 32 | 6 | - | 12 | - | 14 |  |  |  |  |  |  |
| **Змістовний модуль 4**  **Методи та засоби захисту інформації в системах електронного документообігу** | | | | | | | | | | | | |
| **Тема 4.1.** Система електронного документообігу з точки зору кібербезпеки. Вид та форми електронного документу та властивості ЕД, які підлягають захисту. Роль та функції ЕЦП в захисті документаційної інформації. | 10 | 2 | - | 2 | - | 6 |  |  |  |  |  |  |
| **Тема 4.2.** Захист конфіденційності та доступності електронного документу та електронного ресурсу в хмарній системі ЕДО. Налаштування авторизації та механізмів доступу до хмарних сховищ електронних документів. Спеціалізовані засоби захисту конфіденційності. | 10 | 2 | - | 4 | - | 4 |  |  |  |  |  |  |
| **Тема 4.3.** Створення та налаштування механізмів розмежування доступу в системі ЕДО google docs та контроль доступу до електронного документу. | 12 | 2 | - | 4 | - | 6 |  |  |  |  |  |  |
| **Всього годин на 4 модуль** | 32 | 6 | - | 10 | - | 16 |  |  |  |  |  |  |
| **Змістовний модуль 5**  **Способи та засоби захисту інформації в ОС типу Linux. Засоби відновлення даних та елементів ІС на базі ОС Windows** | | | | | | | | | | | | |
| **Тема 5.1.** Особливості зберігання та захисту користувацьких даних та організації системи розмежування доступу до них в ОС сімейства Windows. Криптографічні засоби захисту авторизаційних та користувацьких даних. | 8 | 2 | - | - | - | 6 |  |  |  |  |  |  |
| **Тема 5.2.** Політики безпеки. Засоби створення, редагування та імпортування локальних політик безпеки та механізмів аудиту безпеки в ОС Windows. | 9 | 1 | - | 4 | - | 4 |  |  |  |  |  |  |
| **Тема 5.3.** Засоби відновлення працездатності ОС Windows після збоїв. Інструментальні засоби та пакети для проведення криптоаналізу авторизаційних даних при аудиті безпеки Windows. Створення резервних копій та технологія відновлення працездатності ОС Windows при збоях із застосування утиліт роботи з системним реєстром. | 9 | 1 | - | 3 | - | 5 |  |  |  |  |  |  |
| **Всього годин на 5 модуль** | 26 | 4 | - | 7 | - | 15 |  |  |  |  |  |  |
| **Всього годин на курс** | **150** | **30** |  | **45** | **-** | **75** |  |  |  |  |  |  |

**5. ТЕМИ СЕМІНАРСЬКИХ ЗАНЯТЬ**

Семінарські заняття не передбачені програмою навчальної дисципліни.

**6. ТЕМИ ЛАБОРАТОРНИХ ЗАНЯТЬ**

|  |  |  |
| --- | --- | --- |
| №  з/п | Назва теми | Кількість  годин  денна/заочна |
| 1 | Дослідження технологій захисту цілісності та конфіденційності інформації (хешування). ЕЦП та її використання для захисту документаційної інформації. | 2 |
| 2 | Дослідження технологій захисту цілісності інформації. Механізм контрольних сум. Алгоритму типу CRC та їх використання в мережевих протоколах Ethernet. | 4 |
| 3 | Налаштування елементів політик доступу до файлових ресурсів в середовищі ОС Linux. | 4 |
| 4 | Засоби криптоаналізу шифрованих даних користувача. Багатофакторна автентифікація та її реалізації в ОС типу Linux. | 4 |
| 5 | Реалізація парольних політик захисту інформації в ОС Linux. | 2 |
| 6 | Організація захищеного з’єднання протоколом ssh з віддаленим web-ресурсом. | 4 |
| 7 | Мережеві сканери. Використання мережевих сканерів для фіксації втручань в роботу ІКС. Технологія збирання доказів кібервтручань. | 4 |
| 8 | Налаштування систем блокування та попередження вторгнень. Міжмережеві екрани. | 4 |
| 9 | Реалізація та супровід складних систем розмежування доступу для систем електронного документообігу (google docs). | 2 |
| 10 | Налаштування системи авторизації для системи ЕДО google docs. Спеціалізовані плагіни. | 4 |
| 11 | Проектування систем розмежування доступу в системі ЕДО google docs та контроль доступу до електронного документу. | 4 |
| 12 | Налаштування елементів локальних політик безпеки та механізмів аудиту безпеки в ОС Windows. Інструментальні засоби імпортування локальних політики безпеки в ОС Windows. | 4 |
| 13 | Засоби відновлення працездатності ОС Windows після збоїв. Робота з системним реєстром ОС Windows. | 3 |
|  | Всього, годин | 45 |

**7. ТЕМИ ПРАКТИНИХ ЗАНЯТЬ**

Практичні заняття не передбачені програмою навчальної дисципліни.

**8. САМОСТІЙНА РОБОТА**

|  |  |  |
| --- | --- | --- |
| №  з/п | Назва теми | Кількість  годин  денна/заочна |
| 1 |  | 6 |
| 2 | Нормативно-правові передумови захисту інформації від атак типу «соціальна інженерія» | 4 |
| 3 | Морально-етичні методи та засоби захисту інформації | 6 |
| 4 | Засоби захисту інформації типу «примушення» та «маскування» | 4 |
| 5 | Механізми автентифікації в ОС Android | 6 |
| 6 | Утілити аудити захищеності інформації. Засоби для криптоаналізу користувацьких даних JohnTheRipper | 4 |
| 7 | Законодавче забезпечення технології збирання кіберзлочинів в сегментах локальних мереж. | 4 |
| 8 | Альтернативні засоби встановлення програм для ОС Linux та їх вразливості | 6 |
| 9 | Модулі PAM-автентифікації для біометричної автентифікації. Налаштування PAM-модулів | 4 |
| 10 | Системи електронного документообігу локального типу та технології їх захисту | 6 |
| 11 | Засоби для генерування ЕЦП типу PGP. | 6 |
| 12 | Законодавче регулювання обертання ЕЦП в Україні | 4 |
| 13 | Система електронного документообігу G-Suite. Особливості ліцензування та супровіду хмарних систем електронного документообігу | 4 |
| 14 | Технології імпорту локальних політик безпеки в ОС Windows | 4 |
| 15 | Альтернативні засоби для роботи з системним реєстром | 7 |
| Всього годин | | **75** |

**9. ІНДИВІДУАЛЬНЕ ЗАВДАННЯ**

Самостійна робота виконується у протягом семестру.

**Мета, завдання і зміст самостійної роботи**

мета роботи полягає в: оволодінні основними методами та засобами захисту інформації в комп’ютерних мережах та системах, операційних системах та їх компонентах. Вміти застосовувати методи та засоби захисту інформації в окремих підсистемах. Опанувати основні означеннями та поняттями в МЗЗІ на рівні їх тлумачення та відтворення для практичного застосування та втілення у процесі діяльності бакалавра з кібербезпеки.

**Завдання роботи:** розробляти базові нормативні та альтернативні системи захисту, що містять окремі оптимальні МЗЗІ, враховуючи вплив дестабілізуючих фа­кторів та інформаційних загроз на безпеку підприємств та організацій.

Мати аналітичний погляд на синтез КСЗІ та інших систем безпеки,, що містять нормативні та альтернативні методи та засоби захисту, вміти оцінити та запропонувати оптимальну концепцію систем та засобів захисту інформації для конкретних умов та мети захисту.

**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** | | | | |
| Т1.1 | Т1.2 | Т1.3 | | Т1.4 | 12 |
| 3 | 3 | 3 | | 3 |
| Т2.1 | Т2.2 | | Т2.3 | | 12 |
| 4 | 4 | | 4 | |
| Т3.1 | Т3.2 | | Т3.3 | | 12 |
| 4 | 4 | | 4 | |
| Т4.1 | Т4.2 | | Т4.3 | | 12 |
| 4 | 4 | | 4 | |
| Т5.1 | Т5.2 | | Т5.3 | | 12 |
| 4 | 4 | | 4 | |

Т1.1, Т1.2 ... Т. – 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** | **4** | **5** |
| 12 | 12 | 12 | 12 | 12 |

**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

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.

**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. Концепція технічного захисту інформації в Україні. Постанова КМУ №1126 від 08.10.1997.
2. ДСТУ 3396.0-96.Захист інформації. Технічний захист інформації. Основні положення. Затверджено наказом Держстандарту України від 11.10.96 р. № 423.
3. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. Затверджено наказом Держстандарту України від 19.12.96 р. № 511.
4. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. Затверджено наказом Держстандарту України від 11.04.97 р. №200.
5. НД ТЗІ 1.1-002-99.Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу.
6. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. 13. National Institute of Standards and Technology Special Publication 800-100, Information Security Handbook: A Guide for Managers. Recommendations of the National Institute of Standards and Technology, October 2006.

**Додаткова література**

1. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с. (Укр. мов.)
2. Виявлення та розслідування злочинів, що вичиняються у сфері інформаційних технологій: Наук.-практ.посіб./ За заг.ред.проф. Я.Ю.Кондратьєва. – К., 2004.
3. Ніколаюк С.І., Никифорчук Д.Й., Томма Р.П., Барко В.І. Протидія злочинам у сфері інтелектуальної власності. – К., 2006.

**15. ІНФОРМАЦІЙНІ РЕСУРСИ**

linuxpage.ru.

www.securityfocus.com.

www.sysinternals.com.

http://zakon1.rada.gov.ua