**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**

**ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ**

спеціальність 125 «Кібербезпека»

**Київ – 2020 рік**

Робоча навчальна програма дисципліни «Кібербезпека» для студентів спеціальності 125 «Управління інформаційною безпекою», денної форми навчання. – НУБіП України, 2020. – 17 с.

Розробник:

Лахно В.А., доктор технічних наук, професор,

Касаткін Д.Ю., кандидат педагогічних 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 – 8 | галузь знань 12 Інформаційні технології  | Нормативна |
| 125 «Кібербезпека»  |
| Спеціальність  | **Рік підготовки:** |
| 1-й, 2-й |  |
| Індивідуальне науково-дослідне завдання: - | **Семестр** |
| Загальна кількістьгодин – 240 | 2,3-й |  |
| **Лекції** |
| Тижневих годин для денної форми навчання:аудиторних – 4самостійної роботи студента – 4 | Освітній ступінь«Бакалавр» | 30+30 год. |  |
| **Практичні, семінарські** |
| 0 год. |  |
| **Лабораторні** |
| 30+30 год. |  |
| **Самостійна робота** |
| 30+ 90 год. |  |
| **Індивідуальне завдання:** - |
| Вид підсумкового контролю: 2 семестр – **залік;** 3 семестр – **екзамен.**  |

**2. МЕТА ТА ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

**Мета:** *метою* викладання дисципліни є оволодіння поняттями забезпечення інформаційної безпеки, як однієї з найважливіших сфер діяльності в умовах входження держави в інформаційне суспільство, опанування основними термінами та категоріями інформаційної безпеки на рівні їх тлумачення та відтворення для практичного застосування та втілення у процесі діяльності майбутнього спеціаліста з інформаційної безпеки.

**Після вивчення даної дисципліни студенти повинні**

##### знати:

* поняття інформаційна безпека держави, суспільства та особи;
* стан інформаційного простору та інформаційної безпеки держави;
* джерела загроз інформаційній безпеці;
* проблеми інформаційної безпеки держави;
* небезпеки для інформаційної безпеки держави, особи та суспільства;
* методи запобігання та ліквідації загроз інформаційній безпеці;
* основні об’єкти та суб’єкти забезпечення інформаційної безпеки;
* різновиди інформаційної безпеки особи, суспільства і держави;
* проблеми у сфері інформаційних відносин;
* основи системного підходу до забезпечення інформаційної безпеки суспільства і держави;
* нормативно-правову базу, що регулює і забезпечує інформаційну безпеку держави;

***вміти:***

* визначати та враховувати у практичній діяльності основні тенденції розвитку сучасних інформаційних технологій та оцінювати їх можливий вплив на національну безпеку;
* визначати вплив факторів, загроз на забезпечення інформаційної безпеки держави;
* використовувати методи запобігання та ліквідації загроз інформаційній безпеці;
* визначати методи та засоби захисту життєва важливих інтересів особистості, суспільства, держави в інформаційній сфері;
* виявляти, давати оцінку джерел загроз інформаційній безпеці;
* давати оцінку загроз та засобів впливу на інформаційну безпеку;
* розрізняти основні напрями і можливості вдосконалення системи забезпечення інформаційної безпеки на національному і міжнародному рівнях, її проблемні аспекти;
* виявляти причини інформаційних воєн;
* оволодіти навичками прогнозування розвитку соціально-політичних процесів в контексті інформаційних операцій та воєн.
* формувати стратегічні рішення у сфері забезпечення інформаційної безпеки за результатами моніторингу і аналізу в інформаційній сфері;
* захищати права та інтереси суб’єктів інформаційної діяльності;
* творчо застосовувати у практичній діяльності вимоги нормативно-правових актів, що забезпечують інформаційний суверенітет та інформаційну безпеку держави.

##### Отримати такі компетенції:

* 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 визначати вимоги політики безпеки та формувати профіль захисту відповідно до забезпечення інформаційної безпеки в інформаційній сфері;
* здатність визначати та враховувати у практичній діяльності основні тенденції розвитку сучасних ІТ та оцінювати їх можливий вплив на національну безпеку;
* здатність визначати вплив факторів, загроз на забезпечення інформаційної безпеки держави;
* здатність використовувати методи та моделі запобігання та ліквідації загроз інформаційній безпеці;
* здатність виявляти, давати оцінку джерел загроз інформаційній безпеці держави;
* здатність формувати стратегічні рішення у сфері забезпечення інформаційної безпеки держави за результатами моніторингу і аналізу в інформаційній сфері;
* здатність захищати права та інтереси суб’єктів інформаційної діяльності.

**3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

**Змістовий модуль 1**

**Основні поняття та визначення інформаційної безпеки держави**

#### Тема 1. Аналіз стану інформаційного простору та інформаційної безпеки держави

Інформаційна сфера, інформаційна безпека, національна безпека, кібернетична безпека. Інформаційне суспільство. Підходи до дослідження інформаційної безпеки. Статичний, діяльнісний, комплексний підходи. Система забезпечення інформаційної безпеки. Національний інтерес, класифікація національних інтересів, національний інтерес в інформаційній сфері.

Аналіз стану інформаційного простору та інформаційної безпеки держави. Базові терміни та визначення. Проблеми інформаційної безпеки держави. Поняття «інформаційна безпека» (ІБ): проблема визначення, об’єкт, напрямки державної політики щодо забезпечення ІБ. Поняття «інформаційне право» та загальні недоліки українського інформаційного законодавства. Інформаційний суверенітет: визначення, дискусії. Проблема доступу до інформації, що не становить державної таємниці. Інформаційна відкритість влади: стан, проблеми та перспективи.

**Тема 2. Джерела загроз інформаційній безпеці**

Джерела загроз інформаційній безпеці. Класифікація загроз інформаційній безпеці держави. Засоби впливу загроз на інформаційну безпеку. Методи боротьби в інформаційному просторі. Фактори збільшення ефективності інформаційної операції. Фактор еквівалентності. Фактор соціального середовища (повідомлення масової комунікації, обговорення повідомлення, прийняття індивідуального рішення). Фактор візуального домінування. Фактор тематичного домінування. Фактор домінування форми. Фактор невідповідності власної та чужої комунікації. Фактор неоднорідності аудиторії. Фактор переведення в дію. Фактор спростування можливих контраргументів. Фактор деталізації контексту. Фактор розбіжності візуальних та вербальних повідомлень. Фактор створення відповідного очікування події.

**Тема 3. Сутність інформаційної безпеки держави, суспільства та особи**

Сутність інформаційної безпеки держави, суспільства та особи. Різновиди інформаційної безпеки особи, суспільства та держави. Поняття: спеціальні інформаційні операції, акти зовнішньої інформаційної агресії, інформаційний тероризм, інформаційні війни. Об’єкти інформаційного впливу. Інформаційно-психологічна протидія, контроль каналів передачі інформації, система моніторингу та прогнозування негативних інформаційно-психологічних впливів. Принципи інформаційної війни. Логіка інформаційної війни. Моделі інформаційної війни. Різновиди інформаційних воєн. Засоби, методи і технології інформаційних воєн.

#### Тема 4. Основи інформаційного протиборства

Поняття і різновиди загроз інформаційній безпеці. Інформаційне протиборство, інформаційна експансія, інформаційна війна, інформаційний тероризм. Інформаційна акція, інформаційна атака, інформаційна операція, інформаційна кампанія. Механізми реагування на загрози інформаційній безпеці. Інтернет-ресурси як об’єкти загроз інформаційній безпеці держави. Система моніторингу Інтернет-ресурсів. Актори соціальних Інтернет-сервісів. Контент і дані акторів соціальних Інтернет-сервісів. Методики оцінювання загроз інформаційній безпеці у соціальних Інтернет-сервісах.

Сучасні інформаційні війни. Вплив на інфраструктуру систем життєзабезпечення – телекомунікації, транспортні мережі, електростанції тощо. Промисловий шпіонаж. Хакінг. Кібервійна. Мережева війна. Електронна війна. Психологічна війна. Радіоелектронна боротьба.

**Змістовий модуль 2**

**Загрози національній безпеці держави та боротьба з ними в інформаційній сфері**

#### Тема 5. Основні загрози національній безпеці держави в інформаційній сфері

Загрози національній безпеці України в інформаційній сфері. Інформаційний тероризм. Комп’ютерна злочинність. Розголошення інформації з обмеженим доступом. Розвідувально-підривна діяльність іноземних спецслужб. Конкурентоспроможність вітчизняної продукції, що обслуговує інформаційну сферу. Шляхи забезпечення інформаційної безпеки України.

**Тема 6. Стратегічні цілі та завдання інформаційної боротьби**

Суть та основні завдання інформаційної безпеки як складової національної безпеки України. Інформаційна безпека суспільства та держави. Стратегічні цілі та завдання інформаційної боротьби.

Особливості захоплення і захисту інформаційного простору. Інформаційно-комунікативні процеси в сучасних суспільствах. Державне управління в умовах інформаційного суспільства. Стратегічні, інформаційні і віртуальні потоки. Стратегічні і тактичні, інформаційні та віртуальні потоки. Інформаційне протиборство і національна безпека. Інформаційне протиборство та операції національної безпеки. Пропаганда та комунікативні складники інформаційно-психологічної боротьби. Інформаційні та віртуальні потоки в соціосистемах. Підготовка спеціалістів у сфері інформаційного протиборства на пострадянському просторі. Інформаційне протиборство: сучасність. Росія і Україна у співставленні їх комунікативних пропагандистських можливостей. Особливості пропагандистських механізмів з двох боків російсько-українського конфлікту.

#### Тема 7. Державне управління інформаційноЮ безпекОЮ

Державне управління забезпеченням інформаційної безпеки. Актуальність проблеми. Складові національної безпеки України. Комплексний характер проблем в інформаційній сфері. Методи дослідження системи забезпечення системи інформаційної безпеки. Зміст та логіка зв’язку основних категорій (понять) теорії інформаційної безпеки.

**Тема 8. Національний інформаційний простір**

Національний інформаційний простір. Внутрішні та зовнішні джерела інформаційної безпеки України. Класифікація інформації за режимом доступу. Класифікація інформаційних ресурсів відповідно до вимог міжнародних критеріїв. Інформаційні ризики від застосування інформаційних технологій. Основні об’єкти забезпечення інформаційної безпеки.

**Тема 9. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності**

#### Стан розбудови інформаційного суспільства в Україні порівняно зі світовими тенденціями. Види загроз інформаційній безпеці України. Загрози конституційним правам і свободам людини і громадянина у сфері духовного життя, інформаційної діяльності. Стан ЗМІ на внутрішньому інформаційному ринку. Інформаційна безпека держави як комплекс правових, організаційних та інженерно-технічних заходів при формуванні та використанні інформаційних технологій, інфраструктури та інформаційних ресурсів.

**Змістовий модуль 3**

**Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності**

#### Тема 10. Свобода слова та інформаційна безпека

Свобода слова в Україні та інформаційна безпека держави. Інформаційний простір України. Проблеми утвердження свободи слова в Україні. Незалежність засобів масової інформації. Права людини в інформаційному суспільстві: міжнародні правові акти, що стосуються інформаційних прав особи. Принцип верховенства права в інформаційній політиці держави. Конституція України про інформаційні права громадян та інформаційну безпеку. Основні положення Закону України «Про інформацію». Закон України Про національну безпеку України {Із змінами, внесеними згідно із Законом № 522-IX від 04.03.2020}.

#### Тема 11. основи державної політики В СФЕРІ інформаційної безпеки

Основні принципи забезпечення інформаційної безпеки України. Національні інтереси України в інформаційній сфері. Система забезпечення інформаційної безпеки України. Основні напрями та першочергові заходи державної політики забезпечення інформаційної безпеки України.

Правові засади організації системи інформаційної безпеки в Україні. Державна політика забезпечення інформаційної безпеки України. Інститути забезпечення інформаційної безпеки України. Механізми реагування на загрози інформаційній безпеці України. ЗМІ як інструмент інформаційної безпеки України. Громадські організації в контексті інформаційної безпеки України.

#### Тема 12. Досвід забезпечення інформаційної безпеки в державах ЄС, США

Характеристика основних загроз інформаційній безпеці в світі. Проблеми забезпечення інформаційної безпеки в ЄС, США. Глобальні виклики інформаційній безпеці. Сучасний стан інформаційного простору в постіндустріальних країнах. Основні пріоритети інформаційної безпеки в світі.

Інститути й інструменти забезпечення інформаційної безпеки Європейського Союзу. Нормативно-правові акти ЄС у сфері забезпечення інформаційної безпеки (програми, директиви тощо): «Про захист фізичних осіб у контексті обробки персональних даних і вільного обігу таких даних» (1995 р.), «Єдині критерії безпеки інформаційних технологій» (1996 р.), «Безпечніший Інтернет» (1999 р.), «Мережева та інформаційна безпека: європейський політичний підхід» (2001 р.), «На шляху до загальної політики в сфері боротьби з кіберзлочинністю» (2007 р.), «Захист Європи від широкомасштабних кібератак та руйнувань: посилення рівня підготовленості, безпеки та стійкості» (2009 р.). Основні засади політики інформаційної безпеки НАТО. Північноатлантична Рада з питань, що стосуються безпеки НАТО, Комітет внутрішньої безпеки НАТО, Комітет з планування використання цивільних систем зв’язку, Орган з управління кібернетичною безпекою НАТО, Комісія з управління діяльністю в галузі кіберзахисту.

#### Тема 13. модель представлення системи інформаційної безпеки

Моделювання процесів створення та оцінки ефективності системи захисту інформації. Наслідки атак на інформацію. Категорії інформаційної безпеки. Системний підхід у створенні механізмів захисту інформаційних систем. Постановка задачі моделювання процесів створення систем захисту інформації. модель представлення системи інформаційної безпеки, вимоги до моделі.

#### Тема 14. Види та властивості інформації як предмета захисту

Класифікація інформації. Види інформації як предмета захисту. Властивості інформації як предмета захисту - об'єктивність; достовірність; повнота; точність; актуальність; корисність; цінність; своєчасність; зрозумілість; доступність та ін. Інформаційні стосунки. Основні принципи. Суб'єкти і об'єкти. Інформація як об'єкт прав.

Режими доступу до інформації. Інформація як об'єкт права власності. Відповідальність за порушення законодавства про інформацію. Службова таємниця (СТ). Конфіденційна інформація, що є власністю держави (КІВД). Гриф ДСК (Для службового користування). Комерційна таємниця та її захист. Захист професійної таємниці. Захист персональних даних (інформації про особу) в Україні.

Поняття “державна таємниця“ (ДТ). Основні положення Закону України «Про державну таємницю». Зведення відомостей, що становлять державну таємницю. Правові наслідки розголошення державної таємниці. Політика держави щодо ДТ. Режимно-секретні органи.

**Змістовий модуль 4**

**Державна політика у сфері телекомунікацій**

#### Тема 15. Інформаційні технології та проблеми їхньої безпеки

Інформаційні технології та проблеми їхньої безпеки. Методи та види НСД. Методи реалізації НСД. Канали витоку інформації. Побудова моделі порушника. Потенційно можливі злочинні дії. Поняття про криптографічний захист інформації. Технічний захист інформації (ТЗІ): поняття, концепція, стан, напрямки державної політики із захисту інформації.

Правові аспекти захисту інформації в АС. Інтернет як об’єкт інформаційного права та ІБ. Основні положення Закону України «Про захист інформації в АС».

#### Тема 16. Критерії безпеки інформаційних технологій

## Критерії оцінки захищених комп'ютерних систем Міністерства оборони США. «Жовтогаряча книга. Європейські критерії безпеки інформаційних технологій. Федеральні критерії безпеки інформаційних технологій США. Нормативні документи технічного захисту інформації (НД ТЗІ) України по захисту інформації в комп'ютерних системах від несанкціонованого доступу. Загальні критерії безпеки інформаційних технологій. Міжнародний стандарт ISO 15408.

**Тема 17. Державна політика у сфері телекомунікацій. Проблеми розвитку захищених телекомунікацій в Україні та основні шляхи їх розв’язання**

Концепція розвитку телекомунікацій в Україні. Напрями розвитку захищених телекомунікаційних мереж. Розвиток телекомунікацій для потреб національної безпеки та оборони держави. Безпека телекомунікаційних мереж. Використання мережі Інтернет.

#### Тема 18. Інформаційна безпека в умовах сучасного стану та перспектив розвитку державності

Негативний зовнішній вплив на інформаційний простір України. Організаційно-правові засади у сфері інформаційної безпеки. Зовнішні та внутрішні чинники інформаційної безпеки.

**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 |
| **Модуль 1 (2 семестр)** |
| **Змістовий модуль 1****Основні поняття та визначення інформаційної безпеки держави** |
| **Тема 1.** Аналіз стану інформа-ційного простору та інформаційної безпеки держави. | 6 | 2 |  | 2 | - | 2 |  |  |  |  |  |  |
| **Тема 2.** Джерела загроз інформаційній безпеці. | 6 | 2 |  | 2 | - | 2 |  |  |  |  |  |  |
| **Тема 3.** Сутність інформацій-ної безпеки держави, суспільства та особи. | 6 | 2 |  | 2 | - | 2 |  |  |  |  |  |  |
| **Тема 4.** Основи інформацій-ного протиборства. | 12 | 4 |  | 4 | - | 4 |  |  |  |  |  |  |
| **Змістовий модуль 2****Загрози національній безпеці держави та боротьба з ними в інформаційній сфері**  |
| **Тема 5.**Основні загрози національній безпеці держави в інформа-ційній сфері.  | 12 | 4 |  | 4 | - | 4 |  |  |  |  |  |  |
| **Тема 6.** Стратегічні цілі та завдання інформа-ційної боротьби. | 12 | 4 |  | 4 | - | 4 |  |  |  |  |  |  |
| **Тема 7.** Державне управління інформаційною безпекою. | 12 | 4 |  | 4 | - | 4 |  |  |  |  |  |  |
| **Тема 8.** Національний інфор-маційний простір. | 12 | 4 |  | 4 | - | 4 |  |  |  |  |  |  |
| **Тема 9.** Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності. | 12 | 4 |  | 4 | - | 4 |  |  |  |  |  |  |
| **Всього годин****(5 семестр)** | **90** | **30** |  | **30** | **-** | **30** |  |  |  |  |  |  |
| **(3 семестр)** |
| **Змістовий модуль 3****Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності** |
| **Тема 10.** Свобода слова та інформаційна безпека. | 12 | 2 |  | 2 | - | 8 |  |  |  |  |  |  |
| **Тема 11.** Основи державної політики інформаційної безпеки України. | 12 | 2 |  | 2 | - | 8 |  |  |  |  |  |  |
| **Тема 12.** Досвід забезпечення інформаційної безпеки в державах ЄС, США. | 14 | 2 |  | 2 | - | 10 |  |  |  |  |  |  |
| **Тема 13.** модель представлення системи інформаційної безпеки. | 18 | 4 |  | 4 | - | 10 |  |  |  |  |  |  |
| **Тема 14.** Види та властивості інформації як пред-мета захисту. | 18 | 4 |  | 4 | - | 10 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Змістовий модуль 4****Державна політика у сфері телекомунікацій** |
| **Тема 15.** Інформаційно-комунікаційні техно-логії та проблеми їхньої безпеки. | 20 | 4 |  | 4 | - | 12 |  |  |  |  |  |  |
| **Тема 16.** Критерії безпеки інформаційних технологій | 20 | 4 |  | 4 | - | 12 |  |  |  |  |  |  |
| **Тема 17.** Державна політика у сфері телекомунікацій. Проблеми розвитку захищених телекому-нікацій в Україні та основні шляхи їх розв’язання. | 18 | 4 |  | 4 | - | 10 |  |  |  |  |  |  |
| **Тема 18.** Інформаційна безпека в умовах сучасного стану та перспектив розвитку державності. | 18 | 4 |  | 4 | - | 10 |  |  |  |  |  |  |
| **Всього годин****(3 семестр)** | **150** | **30** |  | **30** | **-** | **90** |  |  |  |  |  |  |
|  **(2+3 семестр)** |
| **Всього годин** | **240** | **60** |  | **60** | **-** | **120** |  |  |  |  |  |  |

**5. ТЕМИ СЕМІНАРСЬКИХ ЗАНЯТЬ**

Семінарські заняття не передбачені програмою навчальної дисципліни.

**6. ТЕМИ ЛАБОРАТОРНИХ ЗАНЯТЬ**

**7. ТЕМИ ПРАКТИНИХ ЗАНЯТЬ**

Практичні заняття не передбачені програмою навчальної дисципліни.

**8. САМОСТІЙНА РОБОТА**

|  |  |  |
| --- | --- | --- |
| №з/п | Назва теми | Кількістьгодинденна/заочна |
| 1 | Аналіз стану інформаційного простору та інформаційної безпеки держави. | 2 |
| 2 | Аналіз джерела загроз інформаційній безпеці. | 2 |
| 3 | Сутність інформаційної безпеки держави, суспільства та особи. | 2 |
| 4 | Основи інформаційного протиборства. | 4 |
| 5 | Основні загрози національній безпеці держави в інформаційній сфері.  | 4 |
| 6 | Стратегічні цілі та завдання інформаційної боротьби. | 4 |
| 7 | Державне управління інформаційною безпекою. | 4 |
| 8 | Національний інформаційний простір. | 4 |
| 9 | Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності. | 4 |
| 10 | Свобода слова та інформаційна безпека. | 8 |
| 11 | Основи державної політики в сфері інформаційної безпеки України. | 8 |
| 12 | Досвід забезпечення інформаційної безпеки в державах ЄС, США. | 10 |
| 13 | модель представлення системи інформаційної безпеки. | 10 |
| 14 | Види та властивості інформації як предмета захисту. | 10 |
| 15 | Інформаційні технології та проблеми їхньої безпеки. | 12 |
| 16 | Критерії безпеки інформаційних технологій | 12 |
| 17 | Державна політика у сфері телекомунікацій.  | 10 |
| 18 | Інформаційна безпека в умовах сучасного стану та перспектив розвитку державності. | 10 |
| Всього годин | **120** |

**9. ІНДИВІДУАЛЬНЕ ЗАВДАННЯ**

Самостійна робота виконується у протягом семестрів.

**Мета, завдання і зміст самостійної роботи**

мета роботи: є оволодіння навичками забезпечення інформаційної безпеки ІБ, як однієї з найважливіших сфер діяльності в умовах входження держави в інформаційне суспільство, опанування основними термінами та категоріями ІБ держави на рівні їх тлумачення та відтворення для практичного застосування та втілення у процесі діяльності спеціаліста з інформаційної безпеки.

Завдання роботи: Описати місце інформаційної безпеки в загальній системі національної безпеки, вплив дестабілізуючих фа­кторів та інформаційних загроз на безпеку особистості, суспільства та держа­ви, методи інформаційного протиборства та інформаційної боротьби, зміст і форми психологічних операцій та інформаційно-психологічної безпеки, а та­кож загальні підходи до забезпечення безпеки інформаційних технологій. Де­тально розглянути основні положення інформаційної безпеки України, способи та форми її забезпечення.

**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 – **залік; 3** семестр – **екзамен.**

**12. РОЗПОДІЛ БАЛІВ ТА КРИТЕРІЇ ОЦІНЮВАННЯ**

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

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

|  |  |
| --- | --- |
| Поточне тестування та самостійна робота | Сума |
| **Змістовий модуль №1** |
| **Т1** | **Т2** | **Т3** | **Т4** | **Т5** | **Т6** | **Т7** | **Т8** | **Т9** | 100 |
| 12 | 10 | 12 | 10 | 12 | 10 | 12 | 12 | 10 |

Т1, Т2 ... Т9 – теми змістових модулів

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

|  |  |  |
| --- | --- | --- |
| Поточне тестування та самостійна робота | Підсумковий тест (екзамен) | Сума |
| Змістовий модуль 2 | 50 | 100 |
| **Т10** | **Т11** | **Т12** | **Т13** | **Т14** | **Т15** | **Т16** | **Т17** | **Т18** |
| 5 | 6 | 6 | 5 | 6 | 6 | 6 | 5 | 5 |

Т10, Т11 ... Т18 – теми змістових модулів

**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 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. Поповский В. В. Защита информации в телекоммуникационных системах: учебник: в 2 т. / В. В. Поповский, А. В. Персиков. – Х.: ООО "Компания СМИТ", 2006. – Т. 1. – 292 с.
2. Хорошко В.А. Методы и средства зашиты информации / В. А. Хорошко, А. А. Чекатков – К.: Юниор, 2003. – 504 с.
3. Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа / А. Ю. Щеглов. – СПб.: Наука и Техника, 2004. – 384 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>