Форма № Н - 3.04

Національний університет біоресурсів і природокористування України
Кафедра комп'ютерних систем, мереж та кібербезпеки

"ЗАТВЕРДЖУЮ"
Декан факультету інформаційних технологій
_____ проф. О.Г. Глазунова
"__" _____ 2023 р.

СХВАЛЕНО
на засіданні кафедри
комп'ютерних систем, мереж та кібербезпеки
Протокол № 10 від "17" травня 2023 р.
Завідувач кафедри
(доц. Касаткін Д.Ю.)

РОЗГЛЯНУТО
Гарант ОП
«Кібербезпека»
_____
Гарант ОП
_____ (проф. Лахно В.А.)

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

"Інформаційна безпека держави"
зі спеціальності 125 – «Кібербезпека»
(шифр і назва напряму підготовки)
Освітня програма «Кібербезпека»

факультет інформаційних технологій
(назва факультету)

Київ – 2023 рік

1. Опис навчальної дисципліни

Інформаційна безпека держави

(назва)

Галузь знань, напрям підготовки, спеціальність, освітньо-кваліфікаційний рівень		
Галузь знань	Інформаційні технології	
Спеціальність	125 – «Кібербезпека»	
другий (магістерський) рівень	Бакалавр	
Характеристика навчальної дисципліни		
Вид	Обов’язкова	
Загальна кількість годин	120	
Кількість кредитів ECTS	4	
Кількість змістових модулів	4	
Курсовий проект (робота) (якщо є в робочому навчальному плані)	-	
Форма контролю	Залік	
Показники навчальної дисципліни для денної та заочної форм навчання		
	денна форма навчання	заочна форма навчання
Рік підготовки	2022-2023	
Семестр	2	
Лекційні заняття	30 год.	
Практичні, семінарські заняття		
Лабораторні заняття	45 год.	
Самостійна робота	45 год.	
Індивідуальні завдання		
Кількість тижневих годин для денної форми навчання: аудиторних	4 год.	

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.

Завдання навчальної дисципліни «Інформаційна безпека держави» - є теоретична та практична підготовка здобувачів з метою орієнтування у питаннях захисту інформації та безпеки у різних державних установах та на підприємствах, зокрема АПК.

Місце і роль дисципліни в системі підготовки фахівців відповідно до навчального плану. Дана навчальна дисципліна є теоретичною основою сукупності знань та вмінь, що формують профіль фахівця в галузі з питань

інформаційної безпеки держави, а також сприяє здачі єдиного державного кваліфікаційного іспиту зі спеціальності 125 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти.

Вимоги щодо знань і вмінь, набутих внаслідок вивчення дисципліни

Внаслідок вивчення 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.

Набуття компетентностей:

Відповідно до освітньої програми підготовки фахівців за спеціальністю 125 «Кібербезпека» навчальна дисципліна забезпечує формування загальних і фахових компетентностей:

***Загальні компетентності**:*

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

КЗ 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

КЗ 7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.

***Спеціальні (фахові) компетентності**:*

СК 1. 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.

В результаті вивчення навчальної дисципліни студент набуде певні програмні результати, а саме:

ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.

ПРН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.

ПРН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.

В контексті зазначених вище компетентностей та програмних результатів навчання задачі викладання дисципліни визначають необхідний комплекс знань і вмінь, що отримують студенти під час вивчення дисципліни.

Навчальна програма розрахована на здобувачів вищої освіти, які навчаються за освітньою програмою підготовки бакалаврів за спеціальністю 125 «Кібербезпека».

Робоча програма побудована за вимогами кредитно-модульної системи організації навчального процесу у закладах вищої освіти і використанням академічної системи оцінювання досягнень студентів та шкали оцінок Європейської кредитно-трансферної системи (ECTS).

Навчальна програма з курсу «Інформаційна безпека держави» є основним документом, що охоплює всі види навчальної роботи при вивченні курсу студентами та відбиває основні методичні настанови кафедри.

Навчальна програма дисципліни «Інформаційна безпека держави» розроблена на підставі наступних документів:

-освітньо-професійна програма підготовки фахівців за спеціальністю «Кібербезпека»;

-навчальний план підготовки бакалаврів за спеціальністю «Кібербезпека».

Робоча навчальна програма з курсу «Інформаційна безпека держави» є основним документом, що охоплює всі види навчальної роботи при вивченні курсу студентами та відбиває основні методичні настанови кафедри.

Навчальна програма характеризує шляхи перетворення інформації, що одержується студентом впродовж вивчання курсу, і відбиває зміст курсу, розподілення його на розділи та їх обсяги, дані про форми вивчення та контролю знань.

Курс «Інформаційна безпека держави» є базовим для вивчення наступних дисциплін: «Методи та засоби захисту інформації», «Організаційне забезпечення захисту інформації» та «Комплексні системи захист інформації».

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 інформаційного простору та інформаційної безпеки держави.	5	2		1	-	2						
Тема 2. Джерела загроз інформаційній безпеці.	5	1		2	-	2						
Тема 3. Сутність інформаційної безпеки держави, суспільства та особи.	5	2		1	-	2						
Тема 4. Основи інформаційного протиборства.	6	2		2	-	2						
	21	**7**		**6**		**8**						
Змістовий модуль 2. Загрози національній безпеці держави та боротьба з ними в інформаційній сфері												
Тема 5. Основні загрози нац. безпеці держави в інформа-ційній сфері**.**	7	2		3	-	2						
Тема 6. Стратегічні цілі та завдання інформаційної боротьби.	7	2		3	-	2						
Тема 7. Державне управління інформаційною безпекою.	7	2		3	-	2						
Тема 8. Національний інформаційний простір.	7	2		3	-	2						
Тема 9. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності.	6	1		3	-	2						
	34	**9**		**15**	**-**	**10**						
Змістовий модуль 3. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності												
Тема 10.	8	2		3	-	3						

Свобода слова та інформаційна безпека.												
Тема 11. Основи державної політики інформаційної безпеки України.	8	2		3	-	3						
Тема 12. Досвід забезпечення інформаційної безпеки в державах ЄС, США.	8	2		3	-	3						
Тема 13. Модель представлення системи інформаційної безпеки.	7	2		2	-	3						
Тема 14. Види та властивості інформації як предмета захисту.	8	2		3	-	3						
	39	**10**		**14**		**15**						
Змістовий модуль 4. Державна політика у сфері телекомунікацій												
Тема 15. Інформаційно-комунікаційні технології та проблеми їхньої безпеки.	7	1		3	-	3						
Тема 16. Критерії безпеки інформаційних технологій	6	1		2	-	3						
Тема 17. Державна політика у сфері телекомунікацій. Проблеми розвитку захищених телекомунікацій в Україні та основні шляхи їх розв'язання.	7	1		3	-	3						
Тема 18. Інформаційна безпека в умовах сучасного стану та перспектив розвитку державності.	6	1		2	-	3						
	26	**4**		**10**	**-**	**12**						
Загальне (4 модулі)												
Всього годин	**120**	**30**		**45**	**-**	**45**						

5. Теми семінарських занять

Семінарські заняття не передбачені програмою навчальної дисципліни.

6. Теми практичних занять

Практичні заняття не передбачені програмою навчальної дисципліни.

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1.	Дослідження організаційної та інформаційної структури підприємства	1
2.	Забезпечення інформаційної безпеки в провідних зарубіжних країнах	2
3.	Урядове реагування на комп'ютерні надзвичайні події України	1
4.	Національна система кібербезпеки	2
5.	Порядок пошуку роботи в галузі кібербезпеки	3
6.	Вивчення загроз мережевої безпеки	3
7.	Структура кібербезпеки в Smart City	3
8.	Дослідження політики облікових записів ОС WINDOWS	3
9.	Знайомство Освітньо-професійна програма 123-"Кібербезпека"	3
10.	Пошук особистої інформації у відкритих джерелах	3
11.	Огляд складових інформаційної безпеки	3
12.	Забезпечення надійного захисту онлайн-активності користувача	3
13	Основи інформаційного протиборства.	2
14	Основні загрози національній безпеці держави в інформаційній сфері.	3
15	Свобода слова та інформаційна безпека.	3
16	Критерії безпеки інформаційних технологій	2
17.	Досвід забезпечення інформаційної безпеки в державах ЄС, США.	3
18.	Інформаційна безпека в умовах сучасного стану та перспектив розвитку державності.	2
	Разом за семестр	**45**
	Разом	**45**

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
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.	2
5.	Основні загрози національній безпеці держави в інформаційній сфері.	2
6.	Стратегічні цілі та завдання інформаційної боротьби.	2
7.	Державне управління інформаційною безпекою.	2
8.	Національний інформаційний простір.	2
9.	Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності.	2
10.	Свобода слова та інформаційна безпека.	3
11.	Основи державної політики в сфері інформаційної безпеки України.	3
12.	Досвід забезпечення інформаційної безпеки в державах ЄС, США.	3

13.	Модель представлення системи інформаційної безпеки.	3
14.	Види та властивості інформації як предмета захисту.	3
15.	Інформаційні технології та проблеми їхньої безпеки.	3
16.	Критерії безпеки інформаційних технологій	3
17.	Державна політика у сфері телекомунікацій.	3
18.	Інформаційна безпека в умовах сучасного стану та перспектив розвитку державності.	3
	Разом	**45**

9. Індивідуальне завдання

Мета, завдання і зміст індивідуальної 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, лабораторних занять, самостійної та індивідуальної роботи.

11. Форми контролю

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

Підсумкова атестація – залік.

12. Розподіл балів, які отримують студенти

Оцінювання знань студента відбувається за 100-бальною шкалою і переводиться в національні оцінки згідно з табл.1 «Положення про екзамени та заліки у НУБіП України» (наказ про уведення в дію від 27.12.2019 р. № 1371):

Рейтинг здобувача вищої освіти, бали	**Оцінка національна за результати складання екзаменів заліків**	
	Екзамен	**Залік**
90-100	Відмінно	зараховано
74-89	Добре	
60-73	Задовільно	
0-59	незадовільно	не зараховано

Для визначення рейтингу студента із засвоєння дисципліни $R_{дис}$ (до 100 балів) одержаний рейтинг з атестації $R_{АТ}$ (до 30 балів) додається до рейтингу студента з навчальної роботи $R_{НР}$ (до 70 балів): $R_{дис}=R_{НР}+R_{АТ}$.

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

№ лабораторної роботи	**Кількість балів**	**Загальна кількість балів**
	1-2 модуль	**100**
Лабораторна робота № 1	6	70
Лабораторна робота № 2	7	
Лабораторна робота № 3	7	
Лабораторна робота № 4	7	
Лабораторна робота № 5	6	
Лабораторна робота № 6	7	
Лабораторна робота № 7	7	
Лабораторна робота № 8	7	
Лабораторна робота № 9	6	
Самостійна робота	10	
Модульна контрольна		30
	3-4 модуль	**100**
Лабораторна робота № 10	6	70
Лабораторна робота № 11	7	
Лабораторна робота № 12	7	
Лабораторна робота № 13	7	
Лабораторна робота № 14	6	
Лабораторна робота № 15	7	
Лабораторна робота № 16	7	
Лабораторна робота № 17	7	
Лабораторна робота № 18	6	
Самостійна робота	10	
Модульна контрольна		30

13. Методичне забезпечення

1. Електронний навчальний курс на платформі Elearn вміщує повне методичне забезпечення включаючи: лекції, презентації до лекцій, методичні вказівки до виконання лабораторних робіт, глосарій термінів тощо. https://elearn.nubip.edu.ua/course/view.php?id=2097

2. Касаткін Д.Ю. «Інформаційна безпека держави» методичні рекомендації до виконання лабораторних робіт / Д.Ю.Касаткін // – К.: НУБіП України, ВЦ Компрінт, 2019 р., - 48 с.

14. Рекомендована література

Основна література

1. Кочубей Л.О. Інформаційна безпека держави: інструменти захисту українського інформаційного поля (на прикладі особливостей інформаційно-комунікаційних технологій у сучасному Донбасі). Наукові записки Інституту політичних і етнонаціональних досліджень імені І. Ф. Кураса. 2015, Вип. 3. С.220-237.
2. Богуш В. М., Кривуца В. Г., Кудін А. М. «Інформаційна безпека: Термінологічний навчальний довідник». - за ред. Кривуци В. Г. – Київ, 2004. - 508 с.
3. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Підручник]. / В. Л. Бурячок, Г.М.Гулак, В.Б. Толубко. – К. : ТОВ «СІК ГРУП УКРАЇНА», 2015. – 449 с.
4. Жарков Я.М., Дзюба М.Т., Замаруєва І.В., ін. Інформаційна безпека особистості, суспільства, держави: Підручник. – К.: Видавничо-поліграфічний центр “Київський університет”, 2008. – 274 с.
5. Забезпечення інформаційної безпеки держави: Навчальний посібник / В. Б. Дудикевич, І. Р. Опірський, П. І. Гаранюк, В. С. Зачепило, А. І. Партика. Львів : Видавництво Львівської політехніки, 2017. 204 с.
6. Іванченко Є.В., Іванченко І.С., Хорошко В.О., Хохлачова Ю.Є. Забезпечення інформаційної безпеки держави Є.В. Іванченко [та ін.] ; за ред. проф. В.О. Хорошка ; Вид-во Нац. авіац. ун-ту, 2016. 254 с.
7. Т.М. Мужанова. «Інформаційна безпека держави». - 2019.
8. Богуш В.М., Юдін О.К. Інформаційна безпека держави: навчальний посібник/ В.М. Богуш, О.К. Юдін. – К.: Мк-Пресс, 2005. – 432 с.

Допоміжна література

1. Остроухов В.В., Присяжнюк М.М., Фермагей О.І., Чеховська М.М. Інформаційна безпека. Підручник / В.В.Остроухов, М.М.Присяжнюк, О.І.Фермагей, М.М.Чеховська // - К.: Ліра-К, 2021, - 412с.
2. Бобала Ю.Я., Горбатий І. В. Інформаційна безпека. Навчальний посібник / за ред. Ю. Я. Бобала та І. В. Горбатого // - Л.: Видавництво Львівської політехніки, 2019 р., - 580 с.
3. Кузнецов О.О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король // – Х.: Вид. ХНЕУ, 2011. – 510 с.
4. 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.
5. Інформаційна безпека держави у контексті протидії інформаційним війнам: Навч. Посіб. // ред.. В.Б. Толубка. - К.: НАО, 2004.
6. Баранов О. А. Інформаційне право України: стан, проблеми, перспективи / О. А. Баранов. – К.: Видавничий дім "СофтПрес", 2005. – 316 с.
7. Кормич Б.А. Інформаційна безпека: організаційно-правові основи. / Б.А. Кормич. − К., Принт. 2004. -169 с.

15. Інформаційні ресурси

1. Офіційний сайт Національної бібліотеки України імені В.І. Вернадського http://www.nbuv.gov.ua/

2. Державна науково-технічна бібліотека України (ДНТБ України) https://dntb.gov.ua/

16. Нормативна література

1. Закон «Про інформацію»: Прийнятий 2 жовтня 1992 р. №2657-XII // Відомості Верховної Ради України, 1992. ({Із змінами, внесеними згідно із Законами № 317-VIII від 09.04.2015, ВВР, 2015, № 26, ст.219, № 1405-VIII від 02.06.2016, ВВР, 2016, № 28, ст.533, № 1774-VIII від 06.12.2016, ВВР, 2017, № 2, ст.25, № 2704-VIII від 25.04.2019, ВВР, 2019, № 21, ст.81, № 324-IX від 03.12.2019, ВВР, 2020, № 11, ст.63, № 720-IX від 17.06.2020, ВВР, 2020, № 47, ст.408, № 692-IX від 16.06.2020, ВВР, 2020, № 43, ст.371, № 1089-IX від 16.12.2020})– № 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. ДСТУ ISO/IEC 11770-3:2002 «Інформаційні технології. Методи захисту».