Київський університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

«ЗАТВЕРДЖУЮ»
Проректор з науково-методичної
та навчальної роботи
_____ Олексій ЖИЛЬЦОВ
«05» 09 2022 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

для студентів

освітнього рівня — першого (бакалаврського)
освітньої програми — 000 Каталог вибіркових дисциплін

КИЇВСЬКИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА
Ідентифікаційний код 02136554
Начальник відділу
моніторингу якості освіти
Протокол № 05/58/22
(підпис) (прізвище, ініціали)
«___» _____ 20 22 р.

2022 – 2023 навчальний рік

Розробник:

Мазур Наталія Петрівна, кандидат педагогічних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Викладач:

Мазур Наталія Петрівна, кандидат педагогічних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Робочу програму розглянуто і затверджено на засіданні кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка

Протокол від 01.09.2022 р. № 12

Завідувач кафедри _____ Павло СКЛАДАННИЙ

(підпис)

Робочу програму перевірено

___.___. 2022 р.

Заступник декана _____ Євген ІВАНІЧЕНКО

(підпис)

Пролонговано:

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___

(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___

(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___

(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___

(підпис) (ПІБ)

1. Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання	
	денна	заочна
Вид дисципліни	вибіркова	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	4 / 120	
Курс	2	
Семестр	4	
Кількість змістових модулів з розподілом:	4	
Обсяг кредитів	4	
Обсяг годин, в тому числі:	120	
Аудиторні	56	
Модульний контроль	8	
Семестровий контроль	-	
Самостійна робота	56	
Форма семестрового контролю	залік	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Основи інформаційної безпеки» є нормативним документом Київського університету імені Бориса Грінченка, який розроблено кафедрою інформаційної та кібернетичної безпеки на основі освітньо-професійної програми підготовки здобувачів першого (бакалаврського) рівня відповідно до навчального плану 000 Каталог вибіркових дисциплін.

Робочу навчальну програму укладено згідно з вимогами Європейської кредитної трансферно-накопичувальної системи (ЄКТС) організації навчання.

Програма визначає обсяги знань, якими повинен опанувати здобувач першого (бакалаврського) рівня відповідно до вимог освітньо-кваліфікаційної характеристики, алгоритму вивчення навчального матеріалу дисципліни «Основи інформаційної безпеки» та необхідне методичне забезпечення, складові і технологію

Навчальна дисципліна «Основи інформаційної безпеки» складається з чотирьох змістовних модулів. Обсяг дисципліни – 120 год. (4 кредити).

Метою викладання навчальної дисципліни «Основи інформаційної безпеки» є:

- вивчення основних підходів до забезпечення інформаційної безпеки в організаціях різної форми власності;
- ґрунтовне ознайомлення студентів із основними нормативними документами в галузі інформаційної безпеки та особливостями їх застосування на практиці;
- ознайомлення студентів із основними типами технологічних рішень направленими на забезпечення інформаційної безпеки;
- формування у студентів знань, вмінь і навичок щодо впровадження та застосування теоретичних знань щодо забезпечення інформаційної безпеки в майбутній професійної діяльності.

Завдання полягає у:

- наданні студентам базових теоретичних знань у галузі інформаційної безпеки;
- наданні студентам базових знань щодо процесу створення безпечних інформаційних систем та процесів підтвердження їх відповідності;
- набутті студентами практичних навичок застосування сучасних технологій забезпечення інформаційної безпеки;
- вивченні основних принципів забезпечення інформаційної безпеки.

Фахові компетентності навчальної дисципліни:

КФ-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.
КФ-2	Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки.
КФ-3	Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
КФ-4	Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.
КФ-5	Здатність визначати міжнародну інформаційну безпеку, міжнародний інформаційний простір, міжнародну інформаційну інфраструктуру, основні принципи міжнародної інформаційної безпеки. Знання сучасних спеціальних технологій індивідуального та масового програмування, зомбування, застосування маніпулятивних технологій в політиці, бізнесі, діяльності організацій на національному та міжнародному рівнях. Здатність працювати в групах і здійснювати аналітичну роботу, готуючи аналітичні матеріали та довідки, спрямовані на прогнозування та запобігання інформаційним загрозам

3. Результати навчання за дисципліною

При вивченні курсу «Основи інформаційної безпеки» студенти повинні

знати:

- основні вітчизняні нормативні документи в галузі захисту інформації та міжнародні стандарти з інформаційної безпеки, процеси які висуваються ними при побудові захищених систем, особливості підтвердження відповідності побудованого захисту;
- принципи побудови систем забезпечення інформаційної безпеки;
- основні типи, призначення та характеристики технологічних рішень, направлених на забезпечення інформаційної безпеки.

вміти:

- використовувати на практиці нормативні документи в галузі захисту інформації та міжнародні стандарти з інформаційної безпеки, розуміти відмінності побудованих відповідно до їх вимог систем;
- реалізовувати організаційні та технічні завдання, які виникають в процесі побудови систем інформаційної безпеки.

та досягти наступних ***програмних результатів навчання***:

ПРз-1	- готувати пропозиції до нормативних актів і документів з метою забезпечення встановленої політики інформаційної та/або кібербезпеки; - розробляти проектну документацію, щодо програмних та програмно-апаратних комплексів захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем; - виконувати аналіз реалізації прийнятої політики інформаційної та/або кібербезпеки;
ПРз-2	- обирати основні методи та засоби захисту інформації відповідно до вимог сучасних стандартів інформаційної і кібербезпеки, та критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії захисту інформації; - - вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації, користувачів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах

	- проектувати та реалізувати комплексні системи захисту інформації в АС 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; - використовувати інструментальні засоби оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах.
ПРз-3	Демонструвати знання та розуміння принципів використання теоретичних знань з міжнародних відносин, зовнішньої політики, міжнародної безпеки та конфліктів при вирішенні практичних завдань. Оцінювати події міжнародного життя, процеси в сфері міжнародного співробітництва та міжнародної безпеки, стан взаємодії та конфлікту в міжнародних системах. Визначати політичні, дипломатичні, безпекові, суспільні, юридичні, економічні й інші ризики для України у сфері міжнародних відносин на глобальному та регіональному рівнях. Уміти використовувати засоби та методи протидії інформаційним загрозам, міжнародні інформаційні системи реагування на загрози, міжнародну інформаційну діяльність спрямовану на протидію загрозам суверенітету держави, застосовувати загальні принципи правового регулювання інформаційної безпеки.

4. Структура навчальної дисципліни

Тематичний план для денної форми навчання

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
Змістовий модуль 1. Загальні поняття про інформацію, інформаційні ресурси, інформаційний та кіберпростори							
Тема 1. Загальні поняття про інформацію, інформаційний та кіберпростори	14	4	4				6
Тема 2. Соціальне, психологічне та культурне середовище кіберпростору	14	4	4				6
Тема 3. Економічна діяльність у кіберпросторі	8	2	2				4
Модульний контроль	2						
Разом	38	10	10				16
Змістовий модуль 2. Загальні поняття про безпеку, події та інциденти безпеки							
Тема 4. Роль і місце кібербезпеки у системі національної безпеки держави	8	2	2				4

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
Тема 5. Основи безпеки інформаційного та кіберпросторів	10	2	2				6
Тема 6. Протиборство в інформаційній сфері та кіберпросторі	14	4	4				6
Модульний контроль	2						
Разом	34	8	8				16
Змістовий модуль 3. Загальні поняття про організацію захисту від деструктивного впливу кібератак							
Тема 7. Основні методи забезпечення кібербезпеки організації	10	2	2				6
Тема 8. Реалізація основних методів забезпечення кібербезпеки організації	10	2	2				6
Модульний контроль	2						
Разом	22	4	4				12
Змістовий модуль 4. Правове регулювання питання інформаційної безпеки та захисту інформації в Україні							
Тема 9. Правове та організаційне забезпечення захисту інформації. Правове регулювання інформації з обмеженим доступом	14	4	4				6
Тема 10. Правове регулювання суспільних відносин у сферах технічного, криптографічного захисту інформації та при застосуванні хмарних технологій в Україні	10	2	2				6
Модульний контроль	2						
Разом	26	6	6				12
Усього	**120**	**28**	**28**				**56**

5. Програма навчальної дисципліни

Змістовий модуль 1. Загальні поняття про інформацію, інформаційні ресурси, інформаційний та кіберпростори

Тема 1. Загальні поняття про інформацію, інформаційний та кіберпростори

Вступ. Базові поняття у галузі інформаційної безпеки. Складові інформаційної безпеки. Характеристика інформації як предмета захисту. Інформаційний простір. Основні положення інформаційного простору. Інформаційні ресурси. Інформаційна інфраструктура. Визначення кіберпростору. Загальна структура. Створення та розвиток Інтернету як основної складової інфраструктури кіберпростору. Основні напрями розвитку теорії кіберпростору.

Тема 2. Соціальне, психологічне та культурне середовище кіберпростору

Основи спілкування у кіберпросторі. Психологія сприйняття у кіберпросторі. Особливості побудови та функціонування соціальних мереж. Соціально-культурологічні аспекти кіберпростору. Образи особистостей у кіберпросторі.

Тема 3. Економічна діяльність у кіберпросторі

Особливості кіберекономіки. Надання мережних ресурсів. Організація роботи в

кіберпросторі. Реклама у кіберпросторі.

Змістовий модуль 2. Загальні поняття про безпеку, події та інциденти безпеки

Тема 4. Роль і місце кібербезпеки у системі національної безпеки держави

Основи національної безпеки держави. Роль і місце кібербезпеки у системі національної безпеки держави. Стратегії кібербезпеки країн світу. Основні засади забезпечення кібербезпеки України.

Тема 5. Основи безпеки інформаційного та кіберпросторів

Загрози інформаційній безпеці. Класифікація та методи реалізації. Критерії класифікації загроз ІБ та функціональних послуг. Інциденти інформаційної і кібербезпеки. Еволюція та особливості реалізації атак в ІКС. Основні напрями захисту інформації в інформаційному і кіберпросторах. Заходи протидії деструктивному впливу кібератак

Тема 6. Протиборство в інформаційній сфері та кіберпросторі

Інформаційна боротьба: основні цілі та методи їх досягнення. Основні складові протиборства в інформаційному та кіберпросторі. Інформаційні війни.

Змістовий модуль 3. Загальні поняття про організацію захисту від деструктивного впливу кібератак

Тема 7. Основні методи забезпечення кібербезпеки організації

Заходи кібербезпеки на різних рівнях.

Тема 8. Реалізація основних методів забезпечення кібербезпеки організації

Визначення середовища кібербезпеки організації. Методи, засоби та технології кіберзахисту організації. Вибір технологічних механізмів забезпечення кібербезпеки організації.

Змістовий модуль 4. Правове регулювання питання інформаційної безпеки та захисту інформації в Україні

Тема 9. Правове та організаційне забезпечення захисту інформації. Правове регулювання інформації з обмеженим доступом

Види інформації. Поняття та правовий режим інформаційних ресурсів. Правове та організаційне забезпечення захисту інформації. Поняття «банківська таємниця» та її правовий режим. Поняття «комерційна таємниця» та її правовий режим. Поняття «службова інформація» та її правовий режим. Поняття «державна таємниця» та її правовий режим. Правове та організаційне забезпечення охорони державної таємниці. Поняття «персональні дані» та їх правовий режим. Правове та організаційне забезпечення захисту персональних даних.

Тема 10. Правове регулювання суспільних відносин у сферах технічного, криптографічного захисту інформації та при застосуванні хмарних технологій в Україні

Загальні положення про технічний захист інформації. Організаційні та правові засади технічного захисту інформації в Україні. Базові поняття криптографії. Порядок здійснення криптографічного захисту інформації в Україні. Правовий статус та порядок використання електронного цифрового підпису. Електронні документи та електронний документообіг. Основні поняття і принципи функціонування Інтернет, визначені національним законодавством. Суб'єкти і об'єкти правовідносин у функціонуванні Інтернет.

6. Контроль навчальних досягнень

Навчальні досягнення студентів з дисципліни оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип пооперaційної звітності, обов'язковості модульного контролю, накопичувальної системи оцінювання рівня знань, умінь та навичок, розширення кількості підсумкових балів до 100.

Оцінка за кожний змістовий модуль включає бали за поточну роботу студента на практичних та лабораторних заняттях, за виконання індивідуальних завдань, за модульну контрольну роботу. Виконання модульних контрольних робіт здійснюється в електронному

вигляді. Модульний контроль знань студентів здійснюється після завершення вивчення навчального матеріалу змістового модуля.

У процесі оцінювання навчальних досягнень студентів застосовуються такі методи:

- *Методи усного контролю*: індивідуальне опитування, фронтальне опитування, співбесіда, екзамен.
- *Комп'ютерного контролю:* тестові програми.
- *Методи самоконтролю:* уміння самостійно оцінювати свої знання, самоаналіз.

Кількість балів за роботу з теоретичним матеріалом, на практичних заняттях, під час виконання самостійної роботи залежить від дотримання таких вимог:

- систематичність відвідування занять;
- своєчасність виконання навчальних і індивідуальних завдань;
- повний обсяг їх виконання;
- якість виконання навчальних і індивідуальних завдань;
- самостійність виконання;
- творчий підхід у виконанні завдань;
- ініціативність у навчальній діяльності;
- виконання тестових завдань.

Контроль успішності студентів з урахуванням поточного і підсумкового оцінювання здійснюється відповідно до навчально-методичної карти дисципліни, де зазначено види контролю і кількість балів за видами. Систему рейтингових балів для різних видів контролю та порядок їх переведення європейську (ECTS) шкалу подано нижче у таблиці.

Розрахунок рейтингових балів за видами поточного (модульного) контролю

Вид діяльності студента	Максимальна к-сть балів за одиницю	Модуль 1		Модуль 2		Модуль 3		Модуль 4	
		кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	5	5	4	4	2	2	3	3
Відвідування семінарських занять	1	5	5	4	4	2	2	3	3
Відвідування практичних занять	1								
Відвідування лабораторних занять	1								
Робота на семінарському занятті	10	5	50	4	40	2	20	3	30
Робота на практичному занятті	10								
Лабораторна робота (в тому числі допуск, виконання, захист)	10								
Виконання завдань для самостійної роботи	5	1	5	1	5	1	5	1	5
Виконання модульної роботи	25	1	25	1	25	1	25	1	25
Виконання ІНДЗ	30								
Разом		-	90	-	78	-	54	-	66
Максимальна кількість балів: 288									
Розрахунок коефіцієнта: 288/100=2,88									

Завдання для самостійної роботи та критерії її оцінювання

Самостійна робота є видом поза аудиторної індивідуальної діяльності студента, результати якої використовуються у процесі вивчення програмового матеріалу навчальної дисципліни та містить результати дослідницького пошуку, відображає певний рівень його навчальної

компетентності.

Перелік тем та оцінювання самостійної роботи студента

№ з/п	Назва теми	Кількість годин	Бали
Змістовий модуль 1. Загальні поняття про інформацію, інформаційні ресурси, інформаційний та кіберпростори		**16**	**5**
1	Загальні поняття про інформацію, інформаційний та кіберпростори	6	2
2	Соціальне, психологічне та культурне середовище кіберпростору	6	2
3	Економічна діяльність у кіберпросторі	4	1
Змістовий модуль 2. Загальні поняття про безпеку, події та інциденти безпеки		**16**	**5**
43	Роль і місце кібербезпеки у системі національної безпеки держави	4	1
5	Основи безпеки інформаційного та кіберпросторів	6	2
6	Протиборство в інформаційній сфері та кіберпросторі	6	2
Змістовий модуль 3. Загальні поняття про організацію захисту від деструктивного впливу кібератак		**12**	**5**
7	Основні методи забезпечення кібербезпеки організації	6	2
8	Реалізація основних методів забезпечення кібербезпеки організації	6	3
Змістовий модуль 4. Правове регулювання питання інформаційної безпеки та захисту інформації в Україні		**12**	**5**
9	Правове та організаційне забезпечення захисту інформації. Правове регулювання інформації з обмеженим доступом	6	3
10	Правове регулювання суспільних відносин у сферах технічного, криптографічного захисту інформації та при застосуванні хмарних технологій в Україні	6	2
	Разом	**56**	**20**

Критерії оцінювання самостійної роботи студента

№ п/п	Критерії оцінювання роботи	Максимальна кількість балів за кожним критерієм
1	Критичний аналіз суті та змісту першоджерел. Виклад фактів, ідей, результатів досліджень в логічній послідовності. Аналіз сучасного стану дослідження проблеми, розгляд тенденцій подальшого розвитку даного питання.	2 бали
2	Доказовість висновків, обгрунтованість власної позиції, пропозиції щодо розв’язання проблеми, визначення перспектив дослідження	2 бали
3	Дотримання вимог щодо технічного оформлення	1 бал
	Разом	5 балів

Форми проведення модульного контролю та критерії оцінювання

Модульний контроль здійснюється відповідно до навчально-методичної карти дисципліни та перевіряє рівень досягнення результатів навчання студентів. Форма проведення – комп’ютерний тест, що складається запитань закритої та відкритої форм. Модульна контрольна робота оцінюється у 25 балів.

Форми проведення семестрового контролю та критерії оцінювання

Семестрове (підсумкове) оцінювання здійснюється у формі заліку, умовою отримання якого є отриманням студентом 60 балів (з врахуванням коефіцієнту) за результатами поточного контролю.

Орієнтовний перелік питань для самоконтролю

1. Надайте визначення наступним поняттям: «кібернетичний простір», «Інтернет», «Всесвітня павутина», «веб-браузер».

2. Опишіть основні складові кіберпростору.
3. Виділіть три рівні кібернетичного простору.
4. Що виконує служба доменних імен?
5. Назвіть основні функції веб-браузерів.
6. Перерахуйте та опишіть основні компоненти веб-браузера.
7. Назвіть три рівні адресації в комп'ютерних мережах, та наведіть приклади адрес до кожного з рівнів.
8. Поясніть, що таке MAC-адреса, та опишіть її структуру.
9. Опишіть структуру IP-адреси та поясніть що таке маска підмережі і для чого вона використовується?
10. Назвіть основні критерії віднесення IP-адреси до певного класу мережі.
11. Назвіть та опишіть IP-адреси спеціального призначення.
12. Поясніть, що таке служба DNS?
13. Поясніть, що таке протокол DHCP?
14. Для чого призначена утиліта ipconfig?
15. Назвіть основне призначення утиліти ping та опишіть алгоритм її роботи.
16. Пакетами якого мережевого протоколу є ехо-пакети команди ping?
17. Назвіть основну відмінність утиліт ping та traceroute.
18. Поясніть, що таке сервіс Whois?
19. Що таке гіпертекст у сучасному розумінні та назвіть основні його елементи?
20. Надайте визначення наступним поняттям: «сайт» та «web-сторінка».
21. Що таке копірайтинг та які основні цілі переслідуються при формуванні інформаційного наповнення сайту?
22. Опишіть структуру інтернет-ресурсу.
23. Назвіть основні шаблони поведінки користувача в кіберпросторі.

Шкала відповідності оцінок

Рейтингова оцінка	**Сума балів за всі види навчальної діяльності**	**Значення оцінки**
A	90-100	Відмінно — відмінний рівень знань (умінь) в межах обов'язкового матеріалу з, можливими, незначними недоліками
B	82-89	Дуже добре - достатньо високий рівень знань (умінь) в межах обов'язкового матеріалу без суттєвих (грубих) помилок
C	75-81	Добре - в цілому добрий рівень знань (умінь) з незначною кількістю помилок
D	69-74	Задовільно - посередній рівень знань (умінь) із значною кількістю недоліків, достатній для подальшого навчання або професійної діяльності
E	60-68	Достатньо - мінімально можливий допустимий рівень знань (умінь)
FX	35-59	Незадовільно з можливістю повторного складання - незадовільний рівень знань, з можливістю повторного перескладання за умови належного самостійного доопрацювання
F	1-34	Незадовільно з обов'язковим повторним вивченням курсу - досить низький рівень знань (умінь), що вимагає повторного вивчення дисципліни

7. Навчально-методична картка дисципліни

Разом: 120 год., лекції – 28 год., семінарські заняття – 28 год., модульний контроль – 8 год., самостійна робота – 56 год.

Модулі (назви, бали)	**Змістовий модуль 1. Загальні поняття про інформацію, інформаційні ресурси, інформаційний та кіберпростори** (90 балів)				**Змістовий модуль 2. Загальні поняття про безпеку, події та інциденти безпеки** (78 бали)				**Змістовий модуль 3. Загальні поняття про організацію захисту від деструктивного впливу кібератак** (54 балів)		**Змістовий модуль 4. Правове регулювання питання інформаційної безпеки та захисту інформації в Україні** (66 балів)		
Лекції (теми, бали)	Загальні поняття про інформацію, інформаційний та кіберпростори (2 бали)		Соціальне, психологічне та культурне середовище кіберпростору (2али)	Економічна діяльність у кіберпросторі (1 бал)	Роль і місце кібербезпеки у системі національної безпеки держави (1 бал)	Основи безпеки інформаційного та кіберпросторів (1 бал)	Протиборство в інформаційній сфері та кіберпросторі (2 бали)		Основні методи забезпечення кібербезпеки організації (1 бал)	Реалізація основних методів забезпечення кібербезпеки організації (1 бал)	Правове та організаційне забезпечення захисту інформації. Правове регулювання інформації з обмеженим доступом. (2 бали)		Правове регулювання суспільних відносин у сферах технічного, криптографічного захисту інформації та при застосуванні хмарних технологій в Україні (1 бал)
Семінарські заняття (теми, бали)	Інформаційний та кіберпростори. Поява Інтернет (11 балів)	Інтернет. Найпопулярніші сервіси та небезпеки їх використання (11 балів)	Інтернет. Соціальні сервіси та небезпеки пов’язані з їх використанням (11 балів)	Соціальне та культурне середовище Інтернет (11 балів)	Економічна діяльність у кіберпросторі (11 балів)	Стратегії кібербезпеки України та країн світу (11 балів)	Основи безпеки інформаційного та кіберпросторів (11 балів)	Інформаційна боротьба (11 балів)	Інформаційні війни (11 балів)	Заходи кібербезпеки на різних рівнях (11 балів)	Методи, засоби та технології кіберзахисту організації (11 балів)	Таємна інформація (11 балів)	Конфіденційна та службова інформація (11 балів)	Технічні аспекти захисту інформації у нормативних документах (11 балів)
Самостійна робота	Самостійна робота (5 балів)				Самостійна робота (5 балів)				Самостійна робота (5 балів)		Самостійна робота (5 балів)		
Поточний контроль (вид, бали)	Модульна контрольна робота 1 (25 балів)				Модульна контрольна робота 2 (25 балів)				Модульна контрольна робота 3 (25 балів)		Модульна контрольна робота 4 (25 балів)		
Підсумковий контроль (вид, бали)	Залік												

8. Рекомендовані джерела

Базова

1. Андрєєв В.І., Хорошко В.О., Чередніченко В.С., Шелест М.Є. Основи інформаційної безпеки. Підручник. – К.: вид. ДУІКТ, 2009. –292 с.
2. Богуш В.М., Богуш В.В., Бровко В.Д., Настрадін В.П. Основи кіберпростору, кібербезпеки та кіберзахисту. – К.: Ліра-К, 2021. – 554 с.
3. Богуш В.М., Юдін О.К. Інформаційна безпека держави. –К.: «МК-Прес», 2005. – 432с.
4. Господарський кодекс України: Коментар. – Х.: "Одіссей", 2004. – 848 с.
5. Гулак Г.М., Гринь А.К., Мельник С.В. Методологія захисту інформації: навчально-методичний посібник. – К.: Видавництво НА СБ України, 2015. – 251 с.
6. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).
7. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT)
8. Закон України "Про захист інформації в автоматизованих системах" // Відомості Верховної Ради України, 1994. - № 31. – С. 286.
9. Закон України “Про державну таємницю” від 21.01.1994 // Відомості Верховної Ради України. – 1994. – № 16. – с. 93.
10. Закон України “Про доступ до публічної інформації ”від 13.01.2011 № 2939-VI// Відомості Верховної Ради України. – 2011. – № 16. – с. 93.
11. Закон України “Про інформацію” // Відомості Верховної Ради, 1992, № 48, с. 650 – 651.
12. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа]; за заг. ред. д-ра техн. наук, професора В.Б. Толубка.— К.: ДУТ, 2015.— 288 с.
13. Кобозева А.А., Мачалін І.О., Хорошко В.О., Аналіз захищеності інформаційних систем. Підручник. – К.: вид. ДУІКТ, 2010. - 316 с.
14. НД ТЗІ 1.1-003-99, «Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу», - 30с.
15. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.
16. НД ТЗІ 3.7-003-2005. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
17. Постанова Верховної Ради України від 16 січня 1997 року N 3/97-ВР “Про затвердження Концепції національної безпеки України”
18. Постанова Кабінету Міністрів України “Про затвердження Концепції технічного захисту інформації в Україні” від 08.10.1997 р.
19. Постанова Кабінету Міністрів України від 18.05.2011 року №517 Про затвердження переліку послуг у галузі технічного захисту інформації, господарська діяльність щодо надання яких підлягає ліцензуванню.
20. Постанова Кабінету Міністрів України від 25.05.2011 року №543 Про затвердження переліків послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та криптосистем і засобів криптографічного захисту інформації, господарська діяльність щодо яких підлягає ліцензуванню.
21. Цимбалюк В.С. Інформаційне право (теорія і практика). Монографія. – К.: 2009. - 364 с.

Допоміжна

1. Богуш В.М., Довидьков О.А., Кривуца В.Г. Теоретичні основи захищених інформаційних технологій. Навч. посібник. – К.: ДУІКТ, 2010. – 454 с.
2. 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.

3. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. /В.Л. Бурячок, С.В. Толюпа, А.О. Аносов, В.А. Козачок, Н.В. Лукова-Чуйко/ –К.:ДУТ, 2015. – 345 с.
4. Єрмошин В.В., Невойт Я.В. Аналіз і оцінка ризиків інформаційної безпеки. /Невойт Я.В., Єрмошин В.В.// Монографія. – К: ДУТ, 2015. – 124 с.

9. Інформаційні ресурси

1. Верховна Рада України. Законодавство України [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/
2. Державна служба спеціального зв’язку та захисту інформації [Електронний ресурс]. – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/index.
3. CERT-UA [Електронний ресурс]. – Режим доступу: http://cert.gov.ua/.