МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
Декан факультету комп'ютерних інформаційних технологій
_____ Ігор ЯКИМЕНКО
«30» 08 2024 р.

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної роботи
_____ Віктор ОСТРОВЕРХОВ
«30» 08 2024 р.

РОБОЧА ПРОГРАМА

з дисципліни «Нормативно-правове забезпечення кібербезпеки»
ступінь вищої освіти – бакалавр
галузь знань – 12 Інформаційні технології
спеціальність – 125 Кібербезпека
освітньо-професійна програма – Кібербезпека

Кафедра кібербезпеки

Форма навчання	Курс	Семестр	Лекції (год.)	Лабор. роботи (год.)	ІРС (год.)	Тренінг (год.)	СРС (год.)	Разом (год.)	Залік / екзамен (семестр)
Денна	3	5	30	30	4	8	78	150	Екзамен (5)

30.08.2024

Тернопіль – 2024

Робоча програма складена на основі освітньо-професійної програми підготовки бакалавра галузі знань 12 Інформаційні технології спеціальності 125 Кібербезпека, затвердженої Вченою радою ЗУНУ (протокол №9 від 15.06.2022 р.).

Робочу програму склали: завідувач кафедри кібербезпеки, д.т.н., професор Василь ЯЦКІВ та старший викладач кафедри кібербезпеки, доктор філософії (спеціальність 125 - Кібербезпека та захист інформації) Сергій КУЛИНА.

Робоча програма затверджена на засіданні кафедри кібербезпеки, протокол № 1 від 26.08.2024 р.

Завідувач кафедри Василь ЯЦКІВ

Розглянуто та схвалено групою забезпечення спеціальності Кібербезпека та захист інформації, протокол №1 від 30 серпня 2024 р.

Керівник групи
забезпечення спеціальності _____ Василь ЯЦКІВ

Гарант освітньо-професійної
програми _____ Михайло КАСЯНЧУК

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Опис дисципліни «Нормативно-правове забезпечення кібербезпеки”

<table>
<tr><td>Дисципліна – «Нормативно-правове забезпечення кібербезпеки»</td><td>Галузь знань, спеціальність, СВО</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td>Кількість кредитів – 5.</td><td>Галузь знань – 12 «Інформаційні технології»</td><td>Статус дисципліни – обов’язкова.
Мова навчання – українська.</td></tr>
<tr><td>Кількість залікових модулів – 5.</td><td>Спеціальність – 125 «Кібербезпека»</td><td>Рік підготовки:
Денна – 3.

Семестр:
Денна – 5.</td></tr>
<tr><td>Кількість змістових модулів – 2.</td><td rowspan="3">Ступінь вищої освіти – бакалавр</td><td>Лекції (год):
Денна – 30.

Лабораторні заняття (год):
Денна – 30.</td></tr>
<tr><td>Загальна кількість годин – 150.</td><td>Самостійна робота (год): 78.
Тренінг (год): 8.
Індивідуальна робота (год): 4.</td></tr>
<tr><td>Тижневих годин – 10,
з них аудиторних – 4.</td><td>Вид підсумкового контролю – екзамен.</td></tr>
</table>

2. Мета і завдання дисципліни “Нормативно-правове забезпечення кібербезпеки”

2.1. Мета вивчення дисципліни

Мета дисципліни “Нормативно-правове забезпечення кібербезпеки” полягає у формуванні в майбутніх спеціалістів умінь та компетенцій для визначення місця і ролі кібербезпеки у загальній системі національної безпеки, стану та принципів забезпечення інформаційної безпеки особистості, суспільства та держави, необхідних для подальшої роботи та оволодіння навичками застосування методів та засобів ефективного та безпекового поводження з інформацією незалежно від її походження та виду в умовах широкого використання сучасних інформаційних технологій.

2.2. Завдання вивчення дисципліни

В результаті вивчення курсу «Нормативно-правове забезпечення кібербезпеки» студенти повинні:

– засвоїти основні фундаментальні поняття і закони нормативно-правового забезпечення кібербезпеки для їх використання в сучасних системах;

– розуміти взаємозв’язок інформаційної безпеки з інформаційним суверенітетом, національною безпекою та правами людини;

– знати основи державної та міжнародної політики у сфері забезпечення інформаційної безпеки та зміст основних положень нормативно-правових актів у сфері інформаційної безпеки;

– знати основні закони, принципи та правила поводження з інформацією;

– виявляти реальні та потенційні загрози у сфері інформаційної безпеки та законодавчі шляхи їх запобігання;

– знати основні методи маніпулювання свідомістю людини, впливу на суспільну думку з використанням сучасних інформаційно-комунікаційних технологій;

– знати основні положення юридичної відповідальності за правопорушення в інформаційній сфері та зміст основних міжнародних договорів з питань інформаційної безпеки;

– розуміти основні проблеми правового забезпечення інформаційної безпеки.

Мета проведення лекцій полягає у тому, щоб ознайомити студентів із головними питаннями курсу «Нормативно-правове забезпечення кібербезпеки». Завдання проведення лекцій полягає у: викладенні студентам у відповідності з програмою та робочим планом основних питань курсу «Нормативно-правове забезпечення кібербезпеки» та формуванні у студентів цілісної системи теоретичних знань з курсу «Нормативно-правове забезпечення кібербезпеки».

Мета проведення практичних занять полягає у тому, щоб виробити у студентів практичні навички використання теоретичного матеріалу. Завдання проведення практичних занять полягає у глибшому засвоєнні та закріпленні теоретичних знань, одержаних на лекціях.

2.3. Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни

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.

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

Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

2.4. Передумови для вивчення дисципліни

Вивчення курсу «Нормативно-правове забезпечення кібербезпеки» передбачає наявність систематичних та ґрунтовних знань із суміжних курсів («Теорія інформації та кодування», «Основи кібербезпеки», «Архітектура комп'ютерів та систем»), а також цілеспрямованої роботи на лекційних та практичних заняттях, самостійної роботи студентів.

2.5. Результати навчання

Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.

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

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

Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно правових документів.

3. Програма навчальної дисципліни: «Нормативно-правове забезпечення кібербезпеки»

Змістовий модуль 1. Нормативно-правові акти України

Тема 1. Учасники кіберпростору, кібербезпека, загальні питання управління безпекою

Основні терміни кібербезпеки. Взаємозв'язки у кіберпросторі. Класифікація учасників кіберпростору. Взаємодія учасників кіберпростору. Концепції ведення кіберборотьби. Фактори впливу на кібербезпеку. Модель управління інформаційною та кібербезпекою.

Тема 2. Нормативно-правові акти, які закріплюють концептуальні положення кібербезпеки в Україні

Ієрархії нормативних актів. Конституція України. Закон України «Про національну безпеку». Визначення термінів. Стратегія національної безпеки України. Закони України «Про інформацію», «Про доступ до публічної інформації», «Про захист персональних даних», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про радіочастотний ресурс», «Про телекомунікації», «Про захист суспільної моралі», «Про оборону України», «Про Збройні Сили України», «Про Службу безпеки України», «Про Державну службу спеціального зв'язку та захисту інформації».

Тема 3. Нормативно-правові акти, які закріплюють визначальні положення щодо забезпечення кібербезпеки в Україні

Указ Президента «Про Стратегію кібербезпеки України». Закон України «Про Основні засади розвитку інформаційного суспільства в Україні». Стратегія розвитку інформаційного суспільства в Україні. Закон України «Про Національну програму інформатизації». Закон України «Про Концепцію Національної програми інформатизації». Концепція формування системи національних електронних інформаційних ресурсів. Положення про Національний реєстр електронних інформаційних ресурсів. Закон України «Про захист персональних даних».

Тема 4. Нормативно-правові акти, які визначають порядок охорони державної таємниці в Україні

Закон України «Про державну таємницю». Визначення термінів. Законодавство України про державну таємницю. Державна політика щодо державної таємниці. Компетенція державних органів, органів місцевого самоврядування та їх посадових осіб у сфері охорони державної таємниці. Реалізація прав на секретну інформацію та її матеріальні носії. Інформація, що може бути віднесена до державної таємниці. Строк дії рішення про віднесення інформації до державної таємниці.

Тема 5. Нормативно-правові акти з інформаційної безпеки телекомунікаційних систем

Закони України щодо інформаційної безпеки в Україні. Постанови Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 р. №373 та «Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію» від 19 жовтня 2016 р. № 736. Нормативні документи в галузі технічного захисту інформації.

Змістовий модуль 2. Закони та державні стандарти України у сфері забезпечення технічного захисту інформації

Тема 6. Закони України про електронний документообіг та електронний цифровий підпис

Визначення термінів. Законодавство про електронні документи та електронний документообіг. Державне регулювання електронного документообігу. Електронний документ. Електронний підпис. Правовий статус електронного документа та його копії. Електронний документообіг. Перевірка цілісності електронного документа.

Тема 7. Підзаконні нормативні акти щодо електронного документообігу та електронного цифрового підпису

Закон України «Про концепцію Національної програми інформатизації». Указ Президента України «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні». Указ Президента України «Про додаткові заходи щодо забезпечення відкритості у діяльності

органів державної влади». Постанова Кабінету Міністрів України «Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади».

Тема 8. Нормативно-правові акти, які визначають порядок технічного захисту інформації в Україні

Концепція технічного захисту інформації в Україні. Положення про технічний захист інформації в Україні. Закон «Про стандартизацію». Положення про порядок розроблення, прийняття, перегляду та скасування міжвідомчих нормативних документів системи технічного захисту інформації.

Тема 9. Нормативно-правові акти у сфері захисту державних електронних інформаційних ресурсів України

Закон України «Про Державну службу спеціального зв'язку та захисту інформації України». Закон України «Про захист інформації в інформаційно-комунікаційних системах». Закон України «Про електронну комерцію». Типова інструкція з документування управлінської інформації в електронній формі та організації роботи з електронними документами в діловодстві, електронного міжвідомчого обміну.

Тема 10. Державні стандарти України в сфері забезпечення технічного захисту інформації

ДСТУ 3396.0-96 «Захист інформації Технічний захист інформації. Основні положення». ДСТУ 3396.1-96 «Захист інформації Технічний захист інформації. Порядок проведення робіт». ДСТУ 3396.2-97 «Захист інформації Технічний захист інформації. Терміни та визначення».

4. Структура залікового кредиту дисципліни «Нормативно-правове забезпечення кібербезпеки»

<table>
<tr><td></td><td colspan="6">Кількість годин</td></tr>
<tr><td></td><td>Лекції</td><td>Лаб. заняття</td><td>Інд. робота</td><td>Тренінг, КПІЗ</td><td>Самост. робота</td><td>Контрольні заходи</td></tr>
<tr><td colspan="7">Змістовий модуль 1. Нормативно-правові акти України</td></tr>
<tr><td>Тема 1. Учасники кіберпростору, кібербезпека, загальні питання управління безпекою.</td><td>4</td><td rowspan="5">4</td><td rowspan="5">2</td><td rowspan="5">4</td><td>8</td><td rowspan="5">Поточне опитування</td></tr>
<tr><td>Тема 2. Нормативно-правові акти, які закріплюють концептуальні положення кібербезпеки в Україні</td><td>2</td><td>8</td></tr>
<tr><td>Тема 3. Нормативно-правові акти, які закріплюють визначальні положення щодо забезпечення кібербезпеки в Україні</td><td>2</td><td>8</td></tr>
<tr><td>Тема 4. Нормативно-правові акти, які визначають порядок охорони державної таємниці в Україні</td><td>2</td><td>6</td></tr>
<tr><td>Тема 5. Нормативно-правові акти з інформаційної безпеки телекомунікаційних систем</td><td>4</td><td>4</td><td>8</td></tr>
<tr><td colspan="7">Змістовий модуль 2. Закони та державні стандарти України у сфері забезпечення технічного захисту інформації</td></tr>
</table>

Тема 6. Закони України про електронний документообіг та електронний цифровий підпис	4	4	2	4	8	Поточне опитування
Тема 7. Підзаконні нормативні акти щодо електронного документообігу та електронного цифрового підпису	2				8	
Тема 8. Нормативно-правові акти, які визначають порядок технічного захисту інформації в Україні	2	4			8	
Тема 9. Нормативно-правові акти у сфері захисту державних електронних інформаційних ресурсів України	4	4			8	
Тема 10. Державні стандарти України в сфері забезпечення технічного захисту інформації	4	4			8	
Разом	30	30	4	8	78	

5. Тематика лабораторних занять

Лабораторна робота №1

Тема: Реалізація політики менеджменту інформаційної безпеки між різними організаціями.

Мета: розглянути запропонований кейс та розробити конкретні пропозиції по реалізації політики менеджменту інформаційної безпеки стосовно запропонованих у кейсі аспектів.

Лабораторна робота №2

Тема: Реалізація політики менеджменту внутрішньої інформаційної безпеки.

Мета: розглянути запропонований кейс та розробити конкретні пропозиції по реалізації політики менеджменту інформаційної безпеки стосовно запропонованих у кейсі аспектів.

Лабораторна робота №3

Тема: Забезпечення фізичної безпеки в рамках менеджменту інформаційної безпеки.

Мета: розглянути запропонований кейс та запропонувати конкретні механізми реалізації цієї політики на підприємстві, наприклад: визначення контрольованої зони, засоби контролю, розміщення обладнання, кабельної мережі, небезпечних речовин, технічне обслуговування обладнання тощо.

Лабораторна робота №4

Тема: Забезпечення апаратно-програмних комплексів безпеки менеджменту інформаційної безпеки.

Мета: розглянути запропонований кейс та надати рекомендації щодо організації апаратно-програмних комплексів безпеки менеджменту інформаційної безпеки та запропонувати конкретні механізми реалізації цієї політики на підприємстві, наприклад: захист від шкідливих програм, резервування інформації, мережева безпека, поводження з носіями інформації, моніторинг тощо.

Лабораторна робота №5

Тема: Зберігання відкритих даних.

Мета: розглянути запропонований кейс та розробити пропозиції с точки зору виконання законодавства про персональні дані до технічного завдання (ТЗ) на розробку модуля сайту з отримання зберігання та використання відкритих даних.

Лабораторна робота №6

Тема: Захист персональних даних.

Мета: розглянути запропонований кейс та розробити пропозиції с точки зору виконання законодавства про персональні дані до технічного завдання (ТЗ) на розробку модуля сайту з отримання зберігання та використання персональних даних клієнтів.

Лабораторна робота №7

Тема: Захист даних з обмеженим доступом.

Мета: розглянути запропонований кейс та розробити пропозиції с точки зору виконання законодавства про персональні дані до технічного завдання (ТЗ) на розробку модуля сайту факультету з автентифікацією та зберіганням даних студентів.

Лабораторна робота №8

Тема: Захист персональних даних пацієнтів.

Мета: розглянути запропонований кейс та розробити пропозиції с точки зору виконання законодавства про персональні дані до технічного завдання (ТЗ) на розробку модуля сайту з отримання зберігання та використання персональних даних пацієнтів приватного кабінету.

6. Самостійна робота

Самостійне завдання студента полягає у виконанні обраного та підтвердженого викладачем наскрізного завдання. Метою виконання самостійного завдання є дослідження та оволодіння навиками застосування відповідних нормативно-правових актів для конкретних задач кібербезпеки. Студенти повинні обрати одну із запропонованих тематик:

Тематика

1. Тотожності та відмінності об`єктів інформаційної небезпеки та інформаційної безпеки.
2. Об’єкти інформаційної діяльності.
3. Суб’єкти інформаційної діяльності.
4. Небезпечність інформаційної діяльності з точки зору національної безпеки.
5. Спрямованість розвитку інформаційної діяльності.
6. Загальне розуміння поняття «суверенітет».
7. Чинники які впливають на інформаційний суверенітет.
8. Оцінка стану національного інформаційного суверенітету в сучасних умовах.
9. Оцінка сучасного стану правового захисту кіберпростору.
10. Розуміння поняття «національна безпека» у сучасних умовах.
11. Розуміння ролі та місця інформаційної безпеки в системі національної безпеки.
12. Основні положення Доктрини інформаційної безпеки України, затвердженої Указом Президента України від 25.02.2017 р. № 47/2017.
13. Основні положення Стратегії кібербезпеки України, затвердженої Указом Президента України від 15.03.2016 р. № 96/2016.

14. Основні положення Стратегії національної безпеки України, затвердженої Указом Президента України від 06.05.2015 р. № 287/2015.
15. Основні положення Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 09.01.2007 р. № 537- V.
16. Структура нормативно-правової бази забезпечення захисту інформації.
17. Основні положення Закону України «Про телекомунікації» від 18.11.2003 р. № 1280- IV.
18. Основні положення Закону України «Про інформацію» від 02.10.92 р. № 2657-XII.
19. Розкриття поняття «інформаційно-комунікаційна технологія».
20. Розкриття понять «глобальна інформаційна система» та «глобальна мережа».
21. Природа тероризму.
22. Кібертероризм та шляхи захисту від нього.
23. Кіберзагрози та захист інформації від них.
24. Розкриття поняття «соціалізація».
25. Основні положення Конвенції Ради Європи « Про кіберзлочинність від 23.11.2001 р. № 994-575.
26. Кіберзахист в Україні та світі.
27. Основні положення розділу XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Кримінального кодексу України.
28. Захист об'єктів інформаційної діяльності.
29. Правовий захист свободи слова в Україні.
30. Захист інформаційних свобод в мережі інтернет.

7. Організація та проведення тренінгу з дисципліни «Нормативно-правове забезпечення кібербезпеки»

Тематика: Нормативно-правові інструменти та механізми протидії інформаційним загрозам.

Порядок проведення:

1. Вступна частина проводиться з метою ознайомлення студентів з темою тренінгу.
2. Організаційна частина полягає у створенні робочого настрою у колективі студентів.
3. Практична частина реалізується шляхом виконання завдань з певних проблемних питань теми тренінгу.
4. Підведення підсумків. Обговорення результатів виконаних завдань. Обмін думками з питань, що виносились на тренінг.

Перелік проблемних питань для тренінгу:

1. Основні властивості інформації, які визначають її небезпечість.
2. Особисте бачення ролі та місця інформційної безпеки у життєдіяльнсті суспільства у сучасних умовах.
3. Головний принцип, якій забезпечує необхідний рівень інформаційної безпеки
4. Основна об'єктивна причина складності правового забезпечення інформаційної безпеки.
5. Основні суб'єктивні причини складності правового забезпечення інформаційної безпеки.
6. Чинники, які визначають взаємозв`язок понять «інформаційна безпека» та «кібербезпека».

7. Особисте розуміння співвідношення понять «національна безпека», «інформаційна безпека» та «кібернетична безпека».
8. Чинники, які визначають взаємозв`язок інформаційної діяльності та інформаційної безпеки.
9. Суб'єкти інформаційної діяльності та їх вплив на процеси забезпечення інформаційної безпеки.
10. Суб'єкти інформаційної діяльності та їх вплив на процеси забезпечення кібербезпеки.
11. Особливості маніпулювання свідомістю у сучасних умовах.
12. Наведіть приклади проявів інформаційного насильства.
13. Трансформація ролі та значення інформації на різних етапах розвитку людства.
14. Перспективи розвитку та механізми здійснення інформаційного насильства.
15. Механізми впливу інформації на поведінку людини.
16. Роль та значення інформаційних ресурсів у розвитку людства.
17. Тенденції змін у системі доступу до інформаційних ресурсів.
18. Оцінка стану національного інформаційного суверенітету у сучасних умовах.
19. Основні принципові наслідки глобалізації інформаційного простору.
20. Структура нормативно-правової бази забезпечення захисту інформації.

8. Методи навчання

У навчальному процесі використовуються: лекції, практичні та індивідуальні заняття, групова робота, реферування, а також методи опитування, тестування, ділові ігри тощо.

9. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни «Нормативно-правове забезпечення кібербезпеки» використовуються наступні методи оцінювання навчальної роботи студентів:

- поточне тестування та поточне опитування;
- підсумкове модульне тестування та опитування за кожним заліковим модулем;
- оцінювання виконання лабораторних робіт;
- оцінювання самостійної роботи;
- оцінювання відповідей на питання тренінгу;
- ректорська контрольна робота;
- підсумковий екзамен.

10. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100 – бальною шкалою) з дисципліни «Нормативно-правове забезпечення кібербезпеки» визначається як середньозважена величина, в залежності від питомої ваги кожної складової залікового кредиту %:

Модуль 1		Модуль 2		Модуль 3	Модуль 4	Модуль 5
10%	10%	10%	10%	5%	15%	40%
Поточне оцінювання	Модульний контроль 1	Поточне оцінювання	Модульний контроль 2	Тренінги	Самостійна робота	Екзамен
Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт №1-4.	Підсумкове модульне тестування за темами №1-5.	Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт №5-8.	Підсумкове модульне тестування за темами №6-10.	Визначається як середнє арифметичне з оцінок за завдання тренінгу (не менше двох).	Визначається як оцінка за наскрізне завдання самостійної роботи.	1. Теоретичні питання: 2 питання по 20 балів. 2. 15 тестів по 4 бали.

Шкала оцінювання

За шкалою ЗУНУ (сума балів за всі види навчальної діяльності в межах модуля)	**За національною шкалою**	**За шкалою ECTS**
90-100	відмінно	**A** (відмінно)
85-89	добре	**B** (дуже добре)
75-84		**C** (добре)
65-74	задовільно	**D** (задовільно)
60-64		**E** (достатньо)
35-59	незадовільно	**FX** (незадовільно з можливістю повторного складання)
1-34		**F** (незадовільно з обов'язковим повторним курсом)

11. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

№ з/п	Найменування	Номер теми
1.	Електронний варіант лекцій	1-10
2.	Методичні вказівки до виконання практичних робіт (електронний варіант)	1-10
3.	ПК Intel Core i3-540; монітор 19 Samsung; принтер лазерний Canon MF4570.	1-10
4.	Microsoft Windows, Microsoft Office 2013, Mozilla Firefox, FoxitReader, AdobeReader, WinRAR, WinZip, DjVu Viewer, Total Commander	1-10

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Доктрина інформаційної безпеки України: Указ Президента України від 25.02.2017 р. № 47 / Офіційний вісник Президента України. - 2017. - № 5. - С. 15.
2. ДСТУ 3396.0-96 Захист інформації Технічний захист інформації. URL: https://tzi.com.ua/downloads/DSTU%203396.0-96.pdf
3. ДСТУ 3396.2-97 Захист інформації Технічний захист інформації. Терміни та визначення. URL: https://tzi.com.ua/downloads/%D0%94%D0%A1%D0%A2%D0%A3%203396.2-97.docx
4. Закон України «Про державну таємницю» (зі змінами та доповненнями). URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text
5. Закон України «Про захист інформації в інформаційно-комунікаційних системах» (зі змінами та доповненнями). URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
6. Закон України «Про захист персональних даних» (зі змінами та доповненнями). URL:

https://zakononline.com.ua/documents/show/306885___702634

7. Закон України «Про інформацію» (зі змінами та доповненнями). URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
8. Закон України «Про науково-технічну інформацію» (зі змінами та доповненнями). URL: https://zakon.rada.gov.ua/laws/show/3322-12#Text
9. Закон України «Про національну безпеку України» (зі змінами та доповненнями). URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text
10. Закон України «Про основні засади забезпечення кібербезпеки України» (зі змінами та доповненнями). URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
11. Конвенція про кіберзлочинність, ратифікована Верховною Радою України 07.09.2005. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text
12. Конституція України (зі змінами та доповненнями). URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text
13. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. URL: https://tzi.com.ua/downloads/2.5-004-99.pdf
14. Манжай О. В., Манжай І.А. Правові засади захисту інформації: підручник. – Харків: Панов, 2020. – 162 с. URL: http://univd.edu.ua/science-issue/issue/4315
15. Мельник М.І. «Правоохоронні органи та правоохоронна діяльність». -К.: «Атіка», 2019. – 576 с.
16. Постанова від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» (зі змінами та доповненнями). URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text
17. Стратегія воєнної безпеки України: Указ Президента України від 25 березня 2021 року № 121/2021 року. URL: https://zakon.rada.gov.ua/laws/show/121/2021#n8.
18. Стратегія інформаційної безпеки України, затверджена Указом Президента України від 28 грудня 2021 року № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069
19. Стратегія кібербезпеки України: Указ Президента України від 26 серпня 2021 року № 447/2021 року. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text
20. Стратегія національної безпеки України : Указ Президента України від 14 вересня 2020 року. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text
21. Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології: монографія / І. В. Арістова, О. А. Баранов, О. П. Дзьобань та ін.; за заг. ред. проф. К. І. Бєлякова. Київ:КВІЦ, 2019. 344 с..URL:

http://ippi.org.ua/sites/default/files/monografiya_ok_0.pdf