

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»  
Кафедра кібербезпеки та математичного моделювання

# **СИСТЕМИ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ**

## **МЕТОДИЧНІ ВКАЗІВКИ**

до практичних занять та виконання розрахунково-графічної роботи  
для здобувачів  
першого (бакалаврського) рівня вищої освіти  
освітньо-професійної програми «Кібербезпека»  
спеціальності 125 Кібербезпека та захист інформації

Обговорено і рекомендовано  
на засіданні кафедри кібербезпеки та  
математичного моделювання  
Протокол №4 від 15 квітня 2024 р.

Чернігів 2024

Системи охорони державної таємниці. Методичні вказівки до практичних занять та виконання розрахунково-графічної роботи для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. – Чернігів: НУ «Чернігівська політехніка», 2024 – 26 с.

Укладачі: ЛАРЧЕНКО МАРИНА ОЛЕКСАНДРІВНА, доцент кафедри кібербезпеки та математичного моделювання, кандидат юридичних наук, доцент.  
ТКАЧ ЮЛІЯ МИКОЛАЇВНА, завідувач кафедри кібербезпеки та математичного моделювання, доктор педагогічних наук, професор

Відповідальний за випуск – ТКАЧ ЮЛІЯ МИКОЛАЇВНА,  
завідувач кафедри кібербезпеки та  
математичного моделювання,  
доктор педагогічних наук, професор

Рецензент – ШЕЛЕСТ МИХАЙЛО ЄВГЕНОВИЧ,  
професор кафедри кібербезпеки та математичного моделювання,  
доктор технічних наук, професор

## ЗМІСТ

<b>ЗАГАЛЬНІ ЗАСАДИ</b> .....	5
1. РОБОЧА ПРОГРАМА (у скороченому вигляді).....	9
1.1 Опис навчальної дисципліни.....	9
1.2 Мета навчальної дисципліни.....	9
1.3 Критерії оцінювання результатів навчання .....	11
1.4 Засоби діагностики результатів навчання.....	12
1.5 Програма навчальної дисципліни.....	12
1.6 Розподіл балів, які отримують студенти.....	14
1.7 Рекомендована література .....	15
<b>ПЛАНИ ПРАКТИЧНИХ ЗАНЯТЬ</b> .....	18
1. Поняття, значення і правова основа охорони державної таємниці .....	18
<b>1.1 Вирішувані питання</b> .....	18
1.2 Основні поняття .....	18
2. Інформація та її види .....	18
<b>2.1 Вирішувані питання</b> .....	18
2.2 Основні поняття .....	18
3. Компетенції державних органів та органів місцевого самоврядування у сфері охорони державної таємниці. Служба безпеки України.....	19
<b>3.1 Вирішувані питання</b> .....	19
3.2 Основні поняття .....	19
4. Планування заходів щодо охорони державної таємниці.....	19
<b>4.1 Вирішувані питання</b> .....	19
4.2 Основні поняття .....	19
5. Організація і проведення аналітичної роботи з виявлення і блокування можливих каналів витоку секретних відомостей.....	20
<b>5.1 Вирішувані питання</b> .....	20
5.2 Основні поняття .....	20
6. Основні технічні канали витоку секретної інформації.....	20
<b>6.1 Вирішувані питання</b> .....	20
6.2 Основні поняття .....	20
7. Кримінально-правові засоби забезпечення збереження державної таємниці .....	20
<b>7.1 Вирішувані питання</b> .....	20
7.2 Основні поняття .....	21
<b>РОЗРАХУНКОВО-ГРАФІЧНА РОБОТА</b> .....	21
1. Методичні вказівки до підготовки РГР.....	21
2. Орієнтовний план теоретичної частини роботи.....	21

<b>ДОДАТОК.....</b>	<b>23</b>
<b>РЕКОМЕНДОВАНА ЛІТЕРАТУРА .....</b>	<b>24</b>
<b>ІНФОРМАЦІЙНІ РЕСУРСИ.....</b>	<b>26</b>

## ЗАГАЛЬНІ ЗАСАДИ

Методичні рекомендації до практичних занять, що проводяться для студентів 4-го курсу ОП «Кібербезпека та захист інформації», спрямовані на вирішення таких **головних завдань**:

1) створення умов для реалізації єдиного підходу до організації практичної роботи під час семінарських занять та самостійної роботи студентів;

2) сприяння формуванню у студентів навичок самостійної навчальної, науково-дослідної й практичної роботи; сприяння розвитку й поглибленню професійних, наукових і практичних інтересів;

3) сприяння формуванню професійних якостей, знань, умінь і навичок майбутніх фахівців; створення умов для гармонійного творчого розвитку особистості студента.

Практичні заняття та самостійна робота з дисципліни «Системи охорони державної таємниці» є невід'ємною складовою навчання здобувачів вищої освіти зі спеціальності 125 «Кібербезпека та захист інформації». На вивчення зазначеної дисципліни відведено 120 годин. Аудиторні заняття складають 30 годин, у т.ч. лекцій – 16 год., практичних занять – 14 год. Самостійна робота складає 90 години.

Метою курсу «Системи охорони державної таємниці» є формування у майбутніх фахівців з кібербезпеки системи знань, навичок та вмінь у сфері забезпечення охорони державної таємниці.

Згідно з вимогами освітньо-професійної програми студенти повинні:

### **1) знати:**

- концептуальні основи організації формування та забезпечення системи охорони державної таємниці;

- складові елементи системи охорони державної таємниці;

- основні об'єкти та суб'єкти системи охорони державної таємниці;

- міжнародно-правові нормативні акти щодо охорони державної таємниці;

- механізми та процедури захисту прав особи в інформаційно-правовій сфері;

- види й підстави юридичної відповідальності за порушення законодавства про охорону державної таємниці.

### **2) вміти:**

- самостійно працювати із нормативно-правовими актами у сфері охорони державної таємниці;

- правильно кваліфікувати правопорушення у інформаційно-правовій сфері;

- готувати рекомендації, пропозиції до проектів керівних документів у сфері забезпечення охорони державної таємниці;
- аналізувати діяльність органів влади і управління, юридичних та фізичних осіб щодо дотримання вимог законодавства з питань охорони державної таємниці;
- на основі моніторингу та аналізу пропонувати організаційно-правові заходи підвищення ефективності діяльності управлінських структур щодо охорони державної таємниці.

*Самостійна робота* студентів містить у собі:

- підготовку до аудиторних занять (лекційних та практичних);
- виконання відповідних завдань з навчальної дисципліни протягом семестру;
- самостійну роботу над окремими темами навчальної дисципліни відповідно до навчально-тематичного плану;
- підготовку до практичних занять та виконання завдань, передбачених робочою програмою дисципліни;
- підготовку до усіх видів контрольних випробувань (залікових, підсумкових тощо);
- участь у студентських наукових і науково-практичних конференціях, семінарах тощо;
- інші види діяльності, що ініціюються та здійснюються інститутом, факультетом, кафедрою й органами студентського самоврядування.

Організацію роботи здобувачів вищої освіти здійснює кафедра, лектор, а також самі студенти. З власної ініціативи кафедра може проводити студентські навчальні й наукові заходи (конференції, олімпіади, симпозіуми тощо).

Самостійна робота виконується здобувачами вищої освіти під керівництвом викладача, який здійснює аудиторну роботу в цій навчальній групі. Самостійна робота здобувачів вищої освіти повинна мати такі головні ознаки:

- бути виконаною особисто здобувачем вищої освіти або студентською підгрупою (командою), де кожен її член самостійно виконує свою частину колективної роботи;
- бути закінченою розробкою, де розкриваються й аналізуються актуальні проблеми з певної теми або її окремих аспектів;
- демонструвати достатню компетентність автора в розкритті питань, що досліджуються;
- мати навчальну, наукову або практичну спрямованість і значимість;
- містити певні елементи новизни;
- самостійна письмова робота оформлюється відповідно до вимог кафедри.

**Ключові слова:** охорона державної таємниці; секретна інформація; процедура віднесення інформації до державної таємниці; звод відомостей, що

становлять державну таємницю; розголошення державної таємниці; розслідування випадків розголошення державної таємниці; кримінально-правова охорона державної таємниці.

### ***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.

### ***Поради з планування і організації вивчення навчальної дисципліни***

Практична робота здобувача є одним із важливих засобів оволодіння навчальним матеріалом у час, вільний від обов'язкових навчальних занять. Зміст практичної роботи при вивченні дисципліни «Системи охорони державної таємниці» визначається робочою програмою дисципліни, завданнями та вказівками викладача, даними методичними вказівками. Головною метою практичної роботи є закріплення, розширення та поглиблення набутих у процесі аудиторної роботи знань, вмінь та навичок, а також самостійне вивчення та засвоєння нового матеріалу під керівництвом викладача. Питання, що виникають у здобувачів стосовно виконання запланованих завдань, вирішуються на консультаціях, які проводяться згідно графіку, затвердженого кафедрою кібербезпеки та математичного моделювання НУ «Чернігівська політехніка».

Практична робота здобувачів під час вивчення навчальної дисципліни «Системи охорони державної таємниці» включає такі форми:

- опрацювання теоретичних основ прослуханого лекційного матеріалу;
- вивчення окремих тем і питань, які передбачені для самостійного опрацювання;
- підготовка до практичних занять;
- систематизація вивченого матеріалу дисципліни перед проведенням модульних контрольних заходів;
- підготовка наукової статті (есе) за програмою дисципліни;
- підготовка доповідей та участь в наукових студентських конференціях, круглих столах, тощо.

Всі завдання самостійної роботи здобувачів поділяються на обов'язкові та вибіркові, виконуються у встановлені терміни, з відповідною максимальною оцінкою та передбачають певні форми звітності щодо їх виконання. Обов'язкові завдання виконуються кожним без винятку

здобувачем у процесі вивчення навчальної дисципліни, вибірккові завдання є альтернативними.

Після виконання обов'язкових та вибіркових завдань у встановлені терміни студент звітує викладачеві, а набрані ним бали враховуються як кількість балів за поточну успішність в навчальній роботі.

Оцінювання результатів поточної роботи (завдань, що виконуються на практичних заняттях та консультаціях, результати самостійної роботи студентів) проводиться за такими критеріями (у відсотках від кількості балів, виділених на завдання із заокругленням до цілого числа):

а) 100 % - завдання виконано правильно, вчасно і без зауважень;

а) 80 % - завдання виконано повністю і вчасно, проте містить окремі несуттєві недоліки (розмірності, висновки, оформлення тощо);

а) 60 % - завдання виконане повністю, але містить суттєві помилки у розрахунках або в методиці;

б) 40 % - завдання виконане частково та містить суттєві помилки методичного або розрахункового характеру;

б) 0 % - завдання не виконане.

У процесі вивчення здобувачами дисципліни «Системи охорони державної таємниці» передбачено наступні види роботи викладачів зі здобувачами:

- індивідуальні консультації за графіком, затвердженим кафедрою кібербезпеки та математичного моделювання;

- перевірка виконання індивідуальних завдань поточного контролю та модульних контрольних робіт;

- індивідуальні консультації зі здобувачами з метою підвищення рівня їхньої підготовки та розвитку індивідуальних здібностей, результатом яких може бути підготовка наукових доповідей, статей.

Контроль практичної роботи здобувачів здійснюється на практичних заняттях у формі поточного контролю, модульних контрольних робіт та перевірки якості виконання домашніх завдань.



## 1. РОБОЧА ПРОГРАМА (у скороченому вигляді)

### 1.1 Опис навчальної дисципліни

Найменування показників	Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень	Характеристика навчальної дисципліни
		Денна форма навчання
Кількість кредитів – 4	Галузь знань 12 – Інформаційні технології	Вибіркова
		<b>Рік підготовки:</b>
Змістових модулів – 2	Спеціальність 125 – Кібербезпека та захист інформації	4
Загальна кількість годин – 120		<b>Семестр</b>
		7
Тижневих годин: аудиторних – 1,875 год. самостійної роботи здобувача – 5,625 год.	Перший (бакалаврський) кваліфікаційний рівень: бакалавр з кібербезпеки та захисту інформації	<b>Лекції</b>
		16 год.
		<b>Лабораторні</b>
		-
		<b>Практичні</b>
		14 год.
		<b>Самостійна робота</b>
90 год.		
		<b>Вид контролю:</b>
		Екзамен

Дисципліна є складовою частиною професійної підготовки та відноситься до навчальних дисциплін циклу «Вибіркові дисципліни» за спеціальністю «Кібербезпека та захист інформації» (бакалавр з кібербезпеки та захисту інформації).

### 1.2 Мета навчальної дисципліни

**Метою** викладання дисципліни «Системи охорони державної таємниці» є ознайомлення студентів з колом питань, пов'язаних із системою охорони державної таємниці. Курс направлений на отримання ключових знань, пов'язаних із організацією та повноваженнями органів, які забезпечують охорону державної таємниці згідно чинного законодавства України.

**Завданнями** курсу є:

- 1) ознайомлення студентів з необхідними джерелами права;
- 2) сприяння глибокому засвоєнню нормативних актів;
- 3) ознайомлення із сукупністю органів захисту державної таємниці, засобів і методів захисту відомостей, що становлять державну таємницю, і їх носіїв, а також заходів, що проводяться в цих цілях.

Оволодіння здобувачами вищої освіти (ЗВО) цими знаннями допоможе їм зорієнтуватися у майбутній професії, сформулювати уявлення про зміст діяльності відповідних органів безпеки.

**Загальний фокус дисципліни** направлений на формування у здобувачів вищої освіти теоретичних знань та практичних навичок щодо поняття та змісту державної таємниці, діяльності органів безпеки, судової та правоохоронної діяльності, загальні питання організації та функціонування систем охорони секретної інформації; аналізу принципів її побудови відповідними органами, які наділені повноваженнями здійснювати діяльність у сфері безпеки.

**Спеціальний фокус дисципліни** направлений на ознайомлення студентів з необхідними джерелами права; сприяння глибокому засвоєнню нормативних актів; ознайомлення із сукупністю органів захисту державної таємниці, засобів і методів захисту відомостей, що становлять державну таємницю, і їх носіїв, а також заходів, що проводяться в цих цілях.

Дисципліна спрямована на досягнення здобувачами ступеня бакалавра з кібербезпеки та захисту інформації зі спеціальності 125 – кібербезпека та захист інформації:

**1) загальні:**

- КЗ 1. Здатність застосовувати знання у практичних ситуаціях.
- КЗ 2. Знання та розуміння предметної області та розуміння професії.
- КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

**2) спеціальні (фахові):**

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

**Очікувані результати навчання з дисципліни**

В процесі вивчення дисципліни студенти повинні отримати такі **програмні результати навчання:**

ПРН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;

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

ПРН 13. Аналізувати проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних;

ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних систем програмно-апаратними засобами та давати оцінку якості прийнятих рішень;

ПРН 34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;

ПРН 35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і/або кібербезпеки;

ПРН 37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації;

ПРН 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів.

### **1.3 Критерії оцінювання результатів навчання**

З тими ЗВО, які до проведення підсумкового семестрового контролю не встигли виконати всі обов'язкові види робіт та мають підсумкову оцінку від 0 до 19 балів (за шкалою оцінювання), проводяться додаткові індивідуальні заняття, за результатами яких визначається, наскільки глибоко засвоєний матеріал, та чи необхідне повторне вивчення дисципліни.

Дисципліну можна вважати такою, що засвоєна, якщо ЗВО:

#### **1) знає:**

- зміст положень Конституції України, які регламентують організацію та діяльність органів безпеки;
- основні принципи системи охорони державної таємниці;
- вільно орієнтується в системі нормативно-правових актів щодо організації та діяльності органів безпеки та вміє правильно тлумачити та застосовувати ці норми при вирішенні практичних ситуацій;

#### **2) вміє:**

- правильно тлумачити і застосовувати норми Конституції України та чинного законодавства, які регламентують принципи функціонування системи охорони державної таємниці;
- аналізувати законодавство України з окремих тем курсу;
- застосовувати положення законодавства при вирішенні поставлених завдань.
- пропонувати організаційно-правові заходи підвищення ефективності роботи систем охорони державної таємниці.

У цьому випадку ЗВО може отримати підсумкову оцінку «задовільно» - 60 балів – Е (в т.ч. й під час ліквідації академічної заборгованості з дисципліни).

#### **1.4 Засоби діагностики результатів навчання**

Засобами оцінювання та методами демонстрування результатів навчання з дисципліни є поточний та семестровий контроль. Поточний контроль складається з опитувань, які проводяться під час лекцій, а також лабораторних/практичних занять. Семестровий контроль проводиться у вигляді екзамену, запитання до якого на початку семестру розміщується у системі дистанційного навчання.

#### **1.5 Програма навчальної дисципліни**

##### **Змістовий модуль I ФОРМУВАННЯ ЗНАНЬ ПРО ЗМІСТ ПОНЯТТЯ «ДЕРЖАВНА ТАЄМНИЦЯ»**

Тема 1. ЗМІСТ, СТРУКТУРА, МЕТОДИ ВИВЧЕННЯ ТА ЗАВДАННЯ КУРСУ. ПОНЯТТЯ ТА ВИДИ ІНФОРМАЦІЇ. (2 год)

1. Завдання, зміст та структура курсу. Об'єкт та предмет курсу «Система охорони державної таємниці». Взаємозв'язок з юридичними та спеціальними дисциплінами. Основна навчальна та наукова література.

2. Понятійні проблеми інституту державної таємниці.

3. Поняття «інформація». Властивості інформації. Види інформації. Поширення інформації. Право на інформацію.

Тема 2. ФУНКЦІОНУВАННЯ СИСТЕМИ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ В УКРАЇНІ: ОРГАНІЗАЦІЙНО-ПРАВОВА СТРУКТУРА, ПРИНЦИПИ ТА ЗАВДАННЯ. (2 год)

1. Організаційно-правова структура системи охорони ДТ.

2. Повноваження окремих державних органів у сфері охорони ДТ.

3. Принципи та завдання системи охорони ДТ.

Тема 3. ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ (СЕКРЕТНОЇ ІНФОРМАЦІЇ). (2 год)

1. Правовий інститут державної таємниці. Створення правових засад.

2. Особливості правового регулювання захисту державної таємниці в Україні та за її межами.

3. Законодавче забезпечення становлення системи охорони державної таємниці в Україні.

Тема 4. ВІДНЕСЕННЯ ІНФОРМАЦІЇ ДО ДЕРЖАВНОЇ ТАЄМНИЦІ. (2 год)

1. Порядок віднесення інформації до державної таємниці.
2. Методичні рекомендації ДЕТ щодо визначення підстав для віднесення відомостей до ДТ та ступеня їх секретності.
3. Загальна характеристика та проблемні аспекти процедури віднесення інформації до державної таємниці.
4. Засекречування та розсекречування носіїв інформації.
5. Методичні рекомендації щодо порядку організації та проведення експертиз на предмет наявності чи відсутності у МНІ відомостей, що становлять ДТ.

Тема 5. МАТЕРІАЛЬНІ НОСІЇ СЕКРЕТНОЇ ІНФОРМАЦІЇ: ПОНЯТТЯ, ВИДИ І ПОРЯДОК ЗБЕРІГАННЯ ПІД ЧАС КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ. (2 год)

1. Поняття та види матеріальних носіїв.
2. Порядок зберігання матеріальних носіїв секретної інформації під час кримінального провадження.

## **Змістовий модуль II ОХОРОНА ДЕРЖАВНОЇ ТАЄМНИЦІ**

Тема 6. ДЕРЖАВНА ПОЛІТИКА У СФЕРІ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ

1. Основні режимно-правові заходи щодо охорони державної таємниці.
2. Організація режиму секретності. Поняття режимно-секретного органу. Організація режимно-секретної роботи на підприємствах, в установах і організаціях України.
3. Допуск і доступ громадян України до державної таємниці.

Тема 7. КОНТРОЛЬ ЗА ДОТРИМАННЯМ РЕЖИМУ СЕКРЕТНОСТІ.

1. Порядок здійснення контролю за дотриманням режиму секретності на підприємстві.
2. Перевірка наявності секретних документів та інших МНСІ як вид контролю.
3. Проведення службових розслідувань за фактами порушень вимог режиму секретності.
4. Відповідальність за порушення законодавства про державну таємницю.

Тема 8. КОМПЕТЕНЦІЇ ДЕРЖАВНИХ ОРГАНІВ ТА ОРГАНІВ МІСЦЕВОГО САМОВРЯДУВАННЯ У СФЕРІ ОХОРОНИ СЕКРЕТНОЇ ІНФОРМАЦІЇ. СЛУЖБА БЕЗПЕКИ УКРАЇНИ.

1. Компетенції державних органів та органів місцевого самоврядування у сфері охорони секретної інформації. Державний експерт з питань таємниць.

2. Служба безпеки України. Завдання і основні засади та напрямки діяльності органів безпеки в Україні. Контроль та нагляд за діяльністю органів безпеки.

3. Структурні підрозділи Служби безпеки України: контррозвідки; захисту національної державності; контррозвідувального захисту інтересів держави в сфері економічної безпеки; контррозвідувального захисту інтересів держави у сфері інформаційної безпеки; охорони державної таємниці та ліцензування.

**Тема 9. ОРГАНІЗАЦІЯ І ПРОВЕДЕННЯ АНАЛІТИЧНОЇ РОБОТИ З ВИЯВЛЕННЯ ТА БЛОКУВАННЯ МОЖЛИВИХ КАНАЛІВ ВИТОКУ СЕКРЕТНИХ ВІДОМОСТЕЙ. (2 год)**

1. Поняття, мета і завдання аналітичної роботи.

2. Організація і методика проведення аналітичної роботи.

**Тема 10. КРИМІНАЛЬНО-ПРАВОВІ ЗАСОБИ ЗАБЕЗПЕЧЕННЯ ЗБЕРЕЖЕННЯ ДЕРЖАВНОЇ ТАЄМНИЦІ. (2 год)**

1. Втрата документів, що містять державну таємницю.

2. Передавання або збирання відомостей, що становлять конфіденційну інформацію, яка є власністю держави.

3. Кримінальна відповідальність за порушення законодавства про державну таємницю.

### **1.6 Розподіл балів, які отримують студенти**

#### **Поточний модульний контроль**

<b>Модуль за робочим планом дисципліни та форма контролю</b>	<b>Кількість балів</b>
<b>Семестр 1</b>	<b>0... 60</b>
<b>Модуль 1</b>	<b>0... 45</b>
1 Повнота відповідей на запитання на практичних заняттях	0... 5x7
2 Модульне контрольне завдання (тестування)	0... 10
Всього	0... 45
<b>Модуль 2</b>	<b>0... 15</b>
1 Якість підготовки розрахунково-графічної роботи	0... 10
2 Результати захисту розрахунково-графічної роботи	0... 5
Всього	0... 15

#### **Підсумковий семестровий контроль**

<b>Вид контролю</b>	
---------------------	--

	Кількість балів
<b>Семестр 1</b>	<b>0... 100</b>
1 Модульна оцінка за семестр	0... 60
2 Відповіді на запитання під час заліку	0... 40
<b>Всього</b>	<b>0... 100</b>

### Шкала оцінювання: національна та ECTS

Оцінка в балах	Оцінка ECTS		Оцінка за національною шкалою
			для екзамену (диференційовано з заліку)
90 – 100	<b>A</b>	<i>Відмінно</i> – відмінне виконання лише з незначною кількістю помилок	відмінно
82-89	<b>B</b>	<i>Дуже добре</i> – вище середнього рівня, але з деякими поширеними помилками	добре
75-81	<b>C</b>	<i>Добре</i> – в цілому правильне виконання, але з помітними помилками	
66-74	<b>D</b>	<i>Задовільно</i> – виконання в повному обсязі, але зі значною кількістю недоліків	задовільно
60-65	<b>E</b>	<i>Достатньо</i> – виконання відповідно до мінімальних вимог	
0-59	<b>FX</b>	<i>Незадовільно</i> – недостатньо: необхідно допрацювати	незадовільно з можливістю повторного складання

### 1.7 Рекомендована література

1. Оцінювання шкоди національній безпеці України у разі витоку державної таємниці : Монографія / О.Г. Корченко, О.Є. Архипов, Ю.О. Дрейс. – К.: наук.-вид. центр НА СБ України, 2014. – 332 с.

2. Сергійчук В. В. Досвід деяких зарубіжних країн щодо кримінально-правової охорони державної таємниці. Прикарпатський юридичний вісник. Випуск 3(28) том 2, 2019. С. 161 – 165.

3. Грищенко І.В. Досвід країн Східної Європи у сфері охорони державної таємниці. Порівняльно-аналітичне право. 2015. С. 19–22.

4. Зайцева-Калаур І.В. Опорний конспект лекцій з дисципліни «Охорона державної та комерційної таємниці». ТНЕУ. 2018. 147 с.

5. Самойлова О.С. Кримінально-правова характеристика передачі або збирання відомостей, що становлять конфіденційну інформацію, яка є власністю держави: дис. ... канд. юрид. наук: 12.00.08 / Самойлова О.С. – К., 2006. – 18 с.

6. Пастернак М. С. Процедура віднесення інформації до державної таємниці // Інформаційна безпека людини, суспільства, держави. 2012. №1 (8). С.88-93.

7. Дрейс Ю. О. Функціонування системи охорони державної таємниці в Україні: організаційно-правова структура, принципи та завдання // Безпека інформації. 2014. Т. 20. № 2. С. 176-184.

8. Адабаш О. В. Адміністративна відповідальність за порушення режиму державної таємниці [Електронний ресурс] / О. В. Адабаш // Науковий вісник Ужгородського національного університету. Сер.: : Право . - 2014. - Вип. 25. - С. 134-138.

9. Павленко В.С. Охорона державної таємниці у механізмі інформаційної безпеки. Юридичний науковий електронний журнал. № 4/2021. С. 255 – 258.

10. Павленко В.С., Павленко В.П. Система організаційно-правових заходів щодо охорони державної таємниці в Україні. Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки. Том 31 (70) № 6 2020. С. 70 – 74.

11. Галушка Віта, Тіхонов Григорій. Особливості правового регулювання захисту державної таємниці в Україні та за її межами. Підприємництво, господарство і право. 1/2021. С. 205 – 209.

12. Олійник Василь. Понятійні проблеми інституту державної таємниці. Науковий часопис Національної академії прокуратури. 4'2015. С. 129 – 135.

13. Морозова О.О. Правова охорона державної таємниці в Україні. Право. Випуск 32'2017. С. 101 – 105.

14. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII // Голос України. — 2018. — № 121 від 07.07.2018.

15. Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту інформації. Посібник для курсантів ВНЗ МВС України. – К.: Вид. Національної академії внутріш. справ, 2012. – 104 с.

16. Указ Президента України № 449/2014. Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 р. “ Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України ” // [www.president.gov.ua](http://www.president.gov.ua).

17. Указ Президента України № 96/2016. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “ Про Стратегію кібербезпеки України” // [www.president.gov.ua](http://www.president.gov.ua).

18. Указ Президента України від 26.05.2015 р., № 287/2015. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України". Офіц. вид. - К.: Урядовий кур'єр від 29.05.2015, № 95. // [www.president.gov.ua](http://www.president.gov.ua).

19. Указ Президента України від 17.09.2018 р., № 284/2018 Про рішення Ради національної безпеки і оборони України від 6 вересня 2018 року «Про Договір про дружбу, співробітництво і партнерство між Україною і Російською Федерацією» // [www.rnbo.gov.ua](http://www.rnbo.gov.ua).



20. Указ Президента України від 12.10.2018 р., № 320/2018. Про рішення Ради національної безпеки і оборони України від 12 жовтня 2018 року «Про невідкладні заходи щодо захисту національних інтересів на Півдні та Сході України, у Чорному та Азовському морях і Керченській протоці» // [www.rnbo.gov.ua](http://www.rnbo.gov.ua).

21. Committee on National Security Systems: National Information Assurance (IA) Glossary, CNSS Instruction No. 4009, 26 April 2010.

22. Pipkin, D. (2000). Information security: Protecting the global enterprise. New York: Hewlett-Packard Company.

23. Kiountouzis, E.A.; Kokolakis, S.A. Information systems security: facing the information society of the 21st century. London: Chapman & Hall, Ltd. ISBN 0-412-78120-4

### Нормативна база:

- Кримінальний кодекс України
- Кримінальний процесуальний кодекс України
- Кодекс України про адміністративні правопорушення
- Закон України «Про державну таємницю»
- Закон України «Про інформацію»
- Закон України «Про доступ до публічної інформації»
- Закон України «Про Службу безпеки України»
- Наказ Служби безпеки України від 23.12.2020 № 383 "Про затвердження Зводу відомостей, що становлять державну таємницю"

### Інформаційні ресурси

1. Офіційний портал Верховної Ради України: <http://zakon1.rada.gov.ua/>
2. Урядовий портал (КМУ) : <http://www.kmu.gov.ua/>
3. Офіційний сайт Президента України: <http://www.president.gov.ua/>
4. Офіційний сайт МВС України: <http://mvs.gov.ua/mvs/>
5. Офіційний сайт СБУ України <http://www.sbu.gov.ua/>
6. Офіційний сайт МНС України <http://www.mns.gov.ua/>
7. Офіційний сайт УДО України <http://www.do.gov.ua/>
8. Офіційний сайт ДАІ МВС України <http://www.sai.gov.ua/>
9. Офіційний сайт ВВ МВС України <http://vv.gov.ua/>
10. Офіційний сайт ДСО МВС України <http://dso.gov.ua/>
11. Офіційний сайт Держспецв'язку України <https://cip.gov.ua/ua>
12. Офіційний сайт Управління охорони ДТ Міністерства оборони України <https://www.mil.gov.ua/ministry/struktura-aparatu-ministerstva/ypravlinnia-ohoroni-derzhavnoi-taemniczi.html>

## **ПЛАН ПРАКТИЧНИХ ЗАНЯТЬ**

### ***1. Поняття, значення і правова основа охорони державної таємниці***

#### **1.1 Вирішувані питання**

1. Основні законодавчі та нормативні акти, які регулюють суспільні відносини пов'язані з віднесенням інформації до державної таємниці (секретної інформації): загальна характеристика.
2. Структура та значення Закону України «Про державну таємницю».
3. Загальні положення забезпечення режиму таємності. Визначення термінів.
4. Характеристики інформації, яка може бути віднесена до державної таємниці.

#### **1.2 Основні поняття**

Державна таємниця, секретна інформація, ступені секретності, матеріальні носії секретної інформації, допуск до державної таємниці.

### ***2. Інформація та її види***

#### **2.1 Вирішувані питання**

1. Поняття «інформація». Властивості інформації. Види інформації.
2. Поширення інформації.
3. Інформаційні потреби. Право на інформацію.
4. Особливості технічного захисту інформації.

#### **2.2 Основні поняття**

Інформація, право на інформацію, властивості інформації, поширення інформації, інформаційні потреби, технічний захист інформації.

### ***3. Компетенції державних органів та органів місцевого самоврядування у сфері охорони державної таємниці. Служба безпеки України***

#### **3.1 Вирішувані питання**

1. Компетенції державних органів та органів місцевого самоврядування у сфері охорони секретної інформації. Державний експерт з питань таємниць.

2. Служба безпеки України. Завдання і основні засади та напрямки діяльності органів безпеки в Україні. Контроль та нагляд за діяльністю органів безпеки.

3. Структурні підрозділи Служби безпеки України: контррозвідки; захисту національної державності; контррозвідувального захисту інтересів держави в сфері економічної безпеки; контррозвідувального захисту інтересів держави у сфері інформаційної безпеки; охорони державної таємниці та ліцензування.

#### **3.2 Основні поняття**

Державні органи, органи місцевого самоврядування, державний експерт з питань таємниць, Служба безпеки України, органи безпеки, контррозвідка, захист національної державності, економічна безпека держави, інформаційна безпека держави, охорона державної таємниці.

### ***4. Планування заходів щодо охорони державної таємниці***

#### **4.1 Вирішувані питання**

1. Сутність та завдання планування діяльності РСО. Принципи та методи планування.

2. Етапи планування, зміст та структура планів. Організаційно-методичні заходи.

3. Аналітичні, запобіжні та контрольні-перевірочні заходи. Робота з кадрами.

4. Види і форми планів та контроль за забезпечення їх виконання.

#### **4.2 Основні поняття**

Планування діяльності РСО, етапи планування, організаційно-методичні заходи, аналітичні заходи, запобіжні заходи, контрольні-перевірочні заходи, робота з кадрами.

## ***5. Організація і проведення аналітичної роботи з виявлення і блокування можливих каналів витоку секретних відомостей***

### **5.1 Вирішувані питання**

1. Поняття, мета і завдання аналітичної роботи.
2. Організація і методика проведення аналітичної роботи.
3. Рекомендації по запобіганню витокам секретної інформації з використанням сучасних технічних засобів захисту.

### **5.2 Основні поняття**

Аналітична робота, організація аналітичної роботи, методика аналітичної роботи, запобігання витокам секретної інформації, технічні засоби захисту.

## ***6. Основні технічні канали витоку секретної інформації***

### **6.1 Вирішувані питання**

1. Особливості технічного захисту секретної інформації.
2. Пристрої та системи технічної розвідки.
3. Методи та засоби захисту інформації у системах зв'язку та передачі даних.
4. Протидія технічній розвідці ворога в умовах сучасної війни.

### **6.2 Основні поняття**

Технічний захист секретної інформації, системи технічної розвідки, системи зв'язку та передачі даних, протидія технічній розвідці ворога.

## ***7. Кримінально-правові засоби забезпечення збереження державної таємниці***

### **7.1 Вирішувані питання**

1. Втрата документів, що містять державну таємницю.
2. Передавання або збирання відомостей, що становлять конфіденційну інформацію, яка є власністю держави.
3. Відповідальність за порушення законодавства про державну

таємницю.

## 7.2 Основні поняття

Кримінально-правові засоби, злочини в сфері державної безпеки, кримінально-правовий захист державної таємниці, кримінальна відповідальність за розголошення державної таємниці.

### РОЗРАХУНКОВО-ГРАФІЧНА РОБОТА

**Тема 1. Модель представлення системи охорони державної таємниці**

**Тема 2. Модель організації режиму секретності на підприємствах, в установах та організаціях України**

#### *1. Методичні вказівки до підготовки РГР*

Студент на власний розсуд обирає одну з двох запропонованих тем РГР. Розрахунково-графічна робота складається з двох частин: *теоретичної та практичної*.

1. В теоретичній частині студент має описати власне бачення процесу моделювання системи охорони державної таємниці або організації режиму секретності на підприємстві, в установі, організації згідно запропонованого нижче плану.

#### *2. Орієнтовний план теоретичної частини роботи*

##### **План до теми 1**

1. Поняття та види секретної інформації.
2. Компетенції державних органів та органів місцевого самоврядування у сфері охорони державної таємниці.
3. Види заходів щодо охорони державної таємниці.
4. Організація і проведення аналітичної роботи з виявлення і блокування можливих каналів витоку секретних відомостей.
5. Кримінально-правові засоби охорони державної таємниці.

##### **План до теми 2**

1. Основні поняття організації режиму секретності.
2. Основні принципи організації режиму секретності на підприємствах, в установах і організаціях України.
3. Сутність і призначення режимно-секретної роботи.
4. Створення режимно-секретних органів, їх структура і комплектування. Підготовка працівників, робота яких пов'язана з державною таємницею.
5. Завдання та права режимно-секретних органів.

Обсяг теоретичної частини роботи становить від 8 до 10 аркушів друкованого тексту (поля 2x2x2x2, кегль 14, шрифт Times New Roman, інтервал 1,5). Обсяг вказано без урахування титульної сторінки. Зразок титульної сторінки розміщено в додатках до цих Методичних рекомендацій.

II. В практичній частині роботи студент має навести та описати власну модель, побудовану з урахуванням законодавства України, чинних нормативно-правових актів, державних стандартів із захисту інформації, інших джерел та сучасної літератури.

Модель представлення може бути наведена у вигляді блок-схеми, схеми, інтелектуальної карти, факторної таблиці, графічного відображення тощо. Для її представлення можна використовувати різноманітне програмне забезпечення, що дозволяє належним чином візуалізувати практичну розробку. Представлення може бути виконане в кольорі або в чорно-білому варіанті.

Наведена модель має супроводжуватись короткою анотацією (описом), обсягом близько 0,5 – 1,5 друкованої сторінки.

III. В кінці Розрахунково-графічної роботи має бути наведений список використаної студентом літератури з україномовних, англomовних джерел та/або інформаційних джерел, представлених мовами Європейського Союзу.

Розрахунково-графічна робота здається в електронному вигляді через систему дистанційного навчання Moodle. Термін здачі РГР повідомляє викладач.

Загалом РГР оцінюється в 15 балів, з яких 10 балів відводиться на оцінку якості підготовки РГР та 5 балів – оцінка за захист РГР. Захист підготовлених та зданих робіт відбудеться орієнтовно через тиждень після спливу терміну здачі, визначеному викладачем.

**ДОДАТОК**

**Титульна сторінка РГР**

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**  
**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»**  
Навчально-науковий інститут електронних та інформаційних технологій  
Кафедра кібербезпеки та математичного моделювання

**П І П**

## **РОЗРАХУНКОВО-ГРАФІЧНА РОБОТА**

з дисципліни «Системи охорони державної таємниці»

на тему: \_\_\_\_\_

Курс IV Група КБ-20\_

**Перевірила:**

к.ю.н., доц. Ларченко М.О.

**Оцінка** \_\_\_\_\_

Чернігів – 2024

## РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Оцінювання шкоди національній безпеці України у разі витоку державної таємниці : Монографія / О.Г. Корченко, О.Є. Архипов, Ю.О. Дрейс. – К.: наук.-вид. центр НА СБ України, 2014. – 332 с.
2. Сергійчук В. В. Досвід деяких зарубіжних країн щодо кримінально-правової охорони державної таємниці. Прикарпатський юридичний вісник. Випуск 3(28) том 2, 2019. С. 161 – 165.
3. Грищенко І.В. Досвід країн Східної Європи у сфері охорони державної таємниці. Порівняльно-аналітичне право. 2015. С. 19–22.
4. Зайцева-Калаур І.В. Опорний конспект лекцій з дисципліни «Охорона державної та комерційної таємниці». ТНЕУ. 2018. 147 с.
5. Самойлова О.С. Кримінально-правова характеристика передачі або збирання ідомостей, що становлять конфіденційну інформацію, яка є власністю держави: дис. ... канд. юрид. наук: 12.00.08 / Самойлова О.С. – К., 2006. – 18 с.
6. Пастернак М. С. Процедура віднесення інформації до державної таємниці // Інформаційна безпека людини, суспільства, держави. 2012. №1 (8). С.88-93.
7. Дрейс Ю. О. Функціонування системи охорони державної таємниці в Україні: організаційно-правова структура, принципи та завдання // Безпека інформації. 2014. Т. 20. № 2. С. 176-184.
8. Адабаш О. В. Адміністративна відповідальність за порушення режиму державної таємниці [Електронний ресурс] / О. В. Адабаш // Науковий вісник Ужгородського національного університету. Сер.: : Право . - 2014. - Вип. 25. - С. 134-138.
9. Павленко В.С. Охорона державної таємниці у механізмі інформаційної безпеки. Юридичний науковий електронний журнал. № 4/2021. С. 255 – 258.
10. Павленко В.С., Павленко В.П. Система організаційно-правових заходів щодо охорони державної таємниці в Україні. Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки. Том 31 (70) № 6 2020. С. 70 – 74.
11. Галушка Віта, Тіхонов Григорій. Особливості правового регулювання захисту державної таємниці в Україні та за її межами. Підприємництво, господарство і право. 1/2021. С. 205 – 209.
12. Олійник Василь. Понятійні проблеми інституту державної таємниці. Науковий часопис Національної академії прокуратури. 4'2015. С. 129 – 135.
13. Морозова О.О. Правова охорона державної таємниці в Україні. Право. Випуск 32'2017. С. 101 – 105.
14. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII // Голос України. — 2018. — № 121 від 07.07.2018.
15. Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту інформації. Посібник для курсантів ВНЗ МВС України. – К.: Вид. Національної академії внутріш. справ, 2012. – 104 с.



16. Указ Президента України № 449/2014. Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 р. “ Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України ” // [www.president.gov.ua](http://www.president.gov.ua).

17. Указ Президента України № 96/2016. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “ Про Стратегію кібербезпеки України” // [www.president.gov.ua](http://www.president.gov.ua).

18. Указ Президента України від 26.05.2015 р., № 287/2015. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України". Офіц. вид. - К.: Урядовий кур'єр від 29.05.2015, № 95. // [www.president.gov.ua](http://www.president.gov.ua).

19. Указ Президента України від 17.09.2018 р., № 284/2018 Про рішення Ради національної безпеки і оборони України від 6 вересня 2018 року «Про Договір про дружбу, співробітництво і партнерство між Україною і Російською Федерацією» // [www.rnbo.gov.ua](http://www.rnbo.gov.ua).

20. Указ Президента України від 12.10.2018 р., № 320/2018. Про рішення Ради національної безпеки і оборони України від 12 жовтня 2018 року «Про невідкладні заходи щодо захисту національних інтересів на Півдні та Сході України, у Чорному та Азовському морях і Керченській протоці» // [www.rnbo.gov.ua](http://www.rnbo.gov.ua).

21. Committee on National Security Systems: National Information Assurance (IA) Glossary, CNSS Instruction No. 4009, 26 April 2010.

22. Pipkin, D. (2000). Information security: Protecting the global enterprise. New York: Hewlett- Packard Company.

23. Kiountouzis, E.A.; Kokolakis, S.A. Information systems security: facing the information society of the 21st century. London: Chapman & Hall, Ltd. ISBN 0-412-78120-4

### **Нормативна база:**

- [Кримінальний кодекс України](#)
- [Кримінальний процесуальний кодекс України](#)
- [Кодекс України про адміністративні правопорушення](#)
- [Закон України «Про державну таємницю»](#)
- [Закон України «Про інформацію»](#)
- [Закон України «Про доступ до публічної інформації»](#)
- [Закон України «Про Службу безпеки України»](#)
- [Наказ Служби безпеки України від 23.12.2020 № 383 "Про затвердження Зводу відомостей, що становлять державну таємницю"](#)

## ІНФОРМАЦІЙНІ РЕСУРСИ

1. Офіційний портал Верховної Ради України: <http://zakon1.rada.gov.ua/>
2. Урядовий портал (КМУ) : <http://www.kmu.gov.ua/>
3. Офіційний сайт Президента України: <http://www.president.gov.ua/>
4. Офіційний сайт МВС України: <http://mvs.gov.ua/mvs/>
5. Офіційний сайт СБУ України <http://www.sbu.gov.ua/>
6. Офіційний сайт МНС України <http://www.mns.gov.ua/>
7. Офіційний сайт УДО України <http://www.do.gov.ua/>
8. Офіційний сайт ДАІ МВС України <http://www.sai.gov.ua/>
9. Офіційний сайт ВВ МВС України <http://vv.gov.ua/>
10. Офіційний сайт ДСО МВС України <http://dso.gov.ua/>
11. Офіційний сайт Держспецзв'язку України <https://cip.gov.ua/ua>
12. Офіційний сайт Управління охорони ДТ Міністерства оборони України <https://www.mil.gov.ua/ministry/struktura-aparatu-ministerstva/ypravlinnia-ohoroni-derzhavnoi-taemniczi.html>