МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ
УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ
УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

КАФЕДРА
КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНОГО
ЗАБЕЗПЕЧЕННЯ

Г.В. ФОРОС, І.О. БИКОВ


# Навчально -методичні рекомендації до вивчення навчальної дисципліни "ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ"

для здобувачів вищої освіти
освітнього ступеня «магістр»
галузь знань 26 Цивільна безпека
спеціальність 262
Правоохоронна діяльність

м. Одеса
2024

**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ**

**ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ**

**КАФЕДРА КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ**

**Г.В. ФОРОС, І.О. БИКОВ**

# Навчально -методичні рекомендації до вивчення навчальної дисципліни «ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ»

**для здобувачів вищої освіти освітнього ступеня «магістр» галузь знань 26 Цивільна безпека спеціальність 262 Правоохоронна діяльність**

**2024 рік**

Схвалено та рекомендовано до друку
кафедрою кібербезпеки та інформаційного забезпечення
(протокол № 12 від 17 травня 2024 року)

Рецензенти:
ІСМАЙЛОВ КАРЕН - заступник начальника 5-го відділу (інформаційних технологій та програмування в південному регіоні) (м. Одеса) 3-го управління (інформаційних технологій та програмування) Департаменту кіберполіції Національної поліції України, підполковник поліції, кандидат юридичних наук, доцент
АФОНІН ДМИТРО – завідувач науково-дослідної лабораторії з проблемних питань кримінального аналізу Одеського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Протидія кіберзлочинності: навчально-методичні рекомендації до вивчення навчальної дисципліни / уклад. Г.В. Форос, І.О. Биков / Одеса: ОДУВС, 2024. 44 с.

**ЗМІСТ**

## ПОЯСНЮВАЛЬНА ЗАПИСКА

**Мета** викладання навчальної дисципліни «Протидія кіберзлочинності» є надання теоретичних знань та практичних навичок здобувачам вищої освіти щодо організаційно-правових засад актуальних і важливих питань протидії кіберзлочинності та визначення шляхів удосконалення цього напрямку діяльності.

Основне завдання дисципліни надати здобувачам вищої освіти теоретичну та практичну підготовку з основ кібербезпеки та протидії кіберзлочинності, зокрема: правові засади протидії кіберзлочинності правоохоронними органами України; правові положення і напрямки міжнародного співробітництва у сфері протидії кіберзлочинності; організаційні основи протидії кіберзлочинності правоохоронними органами України; тактику, методи та процедури, які використовуються кіберзлочинцями; принципи конфіденційності, цілісності і доступності, оскільки вони відносяться до станів даних і контрзаходів в області кібербезпеки; технології.

Навчальна дисципліна «Протидія кіберзлочинності» спрямована на надання здобувачам вищої освіти знань та навичок, необхідних для розуміння, виявлення та протидії кіберзлочинності. Курс охоплює широкий спектр питань, починаючи з основних понять кіберзлочинності, її генезису, сутності та характерних рис, як міжнародного соціального явища. Здобувачі вищої освіти дізнаються про вплив кіберзлочинності на суспільну безпеку, правові системи державних органів, правоохоронних органів та громадських організацій. Аналізується характеристика кіберзлочинців, їх класифікація за віком, психофізіологічними особливостями, цілями та об'єктами правопорушення, а також міжнародна класифікація злочинів у сфері сучасних інформаційних технологій.

Правові та організаційні засади протидії кіберзлочинності розглядаються в контексті національного законодавства та міжнародних нормативних актів. Особлива увага приділяється роботі правоохоронних органів України, проблемам та напрямкам удосконалення протидії кіберзлочинності, а також міжнародному співробітництву у цій сфері. Теоретичні аспекти інформаційної безпеки як складової загальної безпеки держави також є ключовими. Здобувачі вищої освіти вивчають методи та засоби забезпечення інформаційної безпеки, включаючи правові, організаційні, технічні, програмні та криптографічні заходи, аналізують еволюцію загроз інформаційної безпеки та методи шахрайства, такі як соціальна

інженерія, скімінг та фішинг.

Аналіз сучасних кіберзагроз включає розгляд різноманітних загроз для інформаційної безпеки, їх можливі наслідки для організацій та користувачів, класифікацію загроз та методи атак, що використовуються кіберзлочинцями. Здобувачі вищої освіти знайомляться з популярними векторами атак, мотиваціями зловмисників та новітніми технологіями, такими як штучний інтелект та блокчейн, що застосовуються для створення складних кіберзагроз. Важливі аспекти кібербезпеки та технічного захисту в умовах швидкого технологічного розвитку охоплюють сучасні виклики та стратегії захисту IT-інфраструктури, мобільних пристроїв та даних у системах IoT. Розглядається роль штучного інтелекту у виявленні та вирішенні кіберзагроз у реальному часі.

Практичні прийоми захисту від кіберзагроз для мобільних пристроїв на різних операційних системах, а також взаємозв'язок інформаційних війн та кібервійн є невід'ємною частиною курсу. Здобувачі вищої освіти вивчають методи виявлення ботів та тролінгу, а також роль інформаційного середовища у контролі над державами та населенням. Розглядаються аспекти соціальної інженерії, психологія маніпуляції користувачами та необхідність їхньої освіти для запобігання соціальним атакам. Курс охоплює методи та інструменти, що використовуються соціальними інженерами, види соціальних атак та рекомендації для їх запобігання, а також технічні та організаційні контрзаходи для захисту від соціально-інженерних атак.

**Перелік компетентностей, формування яких забезпечує вивчення навчальної дисципліни (з ОПП).**

**Інтегральна компетентність:** Здатність розв’язувати задачі дослідницького та/або інноваційного характеру у сфері права. ЗК1. Здатність до абстрактного мислення, аналізу та синтезу. ЗК2. Здатність застосовувати знання у практичних ситуаціях. ЗК5. Здатність вчитися і оволодівати сучасними знаннями. ЗК10. Здатність оцінювати та забезпечувати якість виконуваних робіт.

**Спеціальні компетентності**: СК2. Здатність забезпечувати законність та правопорядок, безпеку особистості, суспільства, держави в межах виконання своїх посадових обов’язків. СК3. Здатність виявляти та аналізувати причини та умови, що сприяють вчиненню кримінальних та адміністративних правопорушень, вживати заходи для їх усунення.. СК10. Здатність аналізувати, оцінювати й застосовувати сучасні інформаційні технології під час

рішення професійних завдань. СК12. Здатність до використання технічних приладів та спеціальних засобів, інформаційно-пошукових систем та баз даних, спеціальної техніки, оперативних та оперативно-технічних засобів, здійснення оперативно-розшукової діяльності.

**Результати навчання:**

РН5. Аналізувати умови і причини вчинення правопорушень, визначати шляхи їх усунення. РН8. Забезпечувати законність та правопорядок, захист прав та інтересів особистості, суспільства, держави з використанням ефективних методів й засобів забезпечення публічної безпеки і порядку в межах виконання своїх посадових обов'язків. РН9. Використовувати у професійній діяльності сучасні інформаційні технології, бази даних та стандартне і спеціалізоване програмне забезпечення. РН10. Користуватись державною системою урядового зв'язку, Національною системою конфіденційного зв'язку, формування та реалізації державної політики у сферах кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, визначати цілі, завдання, ресурси, строки, виконавців.

**Міждисциплінарні зв'язки**: навчальна дисципліна «Протидія кіберзлочинності» взаємопов'язана з наступними дисциплінами: «Сучасні інформаційні технології», «Кримінально-правова та кримінологічна характеристика кіберзлочинності», «Кримінальний аналіз».

## 2. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, освітній ступінь</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>Денна</td><td>Заочна</td></tr>
<tr><td rowspan="2">Кількість кредитів - 4</td><td>Галузь знань<br>26 Цивільна безпека</td><td colspan="2" rowspan="2">Вибіркова</td></tr>
<tr><td rowspan="6">Спеціальність<br>262 Правоохоронна діяльність</td></tr>
<tr><td rowspan="5">Загальна кількість годин: 120</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>1-й</td><td>2-й</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td>2-й</td><td>3-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="6"></td><td rowspan="6">Освітній ступінь:<br>магістр</td><td>14 год</td><td>8 год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>26 год</td><td>12 год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>80 год.</td><td>100 год.</td></tr>
<tr><td colspan="2">Вид контролю: залік</td></tr>
</table>

**Тематичний план**
**(денна форма навчання)**

| Назви змістових модулів і тем | Кількість годин | | | | |
|---|---|---|---|---|---|
| | денна форма | | | | |
| | усього | у тому числі | | | |
| | | Лекції | Сем. зан. | ПЗ | Сам.роб. |
| Тема 1. Загальна характеристика кіберзлочинності | 14 | 2 | 2 | | 10 |
| Тема 2. Організаційно-правові засади протидії кіберзлочинності | 14 | 2 | 2 | | 10 |
| Тема 3. Інформаційна безпека та захист інформації | 14 | 2 | 2 | 2 | 10 |
| Тема 4. Класифікація та аналіз сучасних кіберзагроз | 14 | 2 | 2 | | 10 |
| Тема 5. Кібербезпека та основні принципи технічного захисту в умовах постійного технологічного розвитку | 25 | 2 | 2 | 2 | 15 |
| Тема 6. Принципи безпечної роботи з мобільними пристроями. Безпека в умовах інформаційної війни та кібервійни | 25 | 2 | 2 | 4 | 15 |
| Тема 7. Соціальна інженерія та кібербезпека користувачів | 16 | 2 | 2 | 2 | 10 |
| Усього годин | 120 | 14 | 14 | 10 | 80 |

**Тематичний план**
**(заочна форма навчання)**

| Назви змістових модулів і тем | Кількість годин | | | |
|---|---|---|---|---|
| | заочна форма | | | |
| | усього | у тому числі | | |
| | | Лекції | Сем. зан. | Сам.роб. |
| Тема 1. Загальна характеристика кіберзлочинності | 24 | 2 | 2 | 20 |
| Тема 2. Організаційно-правові засади протидії кіберзлочинності | 36 | 2 | 4 | 30 |
| Тема 3. Інформаційна безпека та захист інформації | 36 | 2 | 4 | 30 |
| Тема 4. Принципи безпечної роботи з мобільними пристроями. Безпека в умовах інформаційної війни та кібервійни | 24 | 2 | 2 | 20 |
| Усього годин | 120 | 8 | 12 | 100 |

## 3. ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

### ТЕМА 1. ЗАГАЛЬНА ХАРАКТЕРИСТИКА КІБЕРЗЛОЧИННОСТІ

Кіберзлочинність: генезис, сутність та характерні риси. Кіберзлочинність як міжнародне соціальне явище. Суспільна безпека протиправного посягання на правові системи органів державної влади, правоохоронних органів та громадських організацій.

Загальна характеристика кіберзлочинців. Класифікація комп'ютерних злочинців по віку, по психофізіологічним особливостям, по цілі та об’єктам правопорушення.

Класифікація злочинів у сфері використання сучасних інформаційних технологій. Міжнародна класифікація кіберзлочинів.

**Методичні рекомендації**

Для успішного вивчення теми «Загальна характеристика кіберзлочинності» важливо систематизувати підходи до вивчення основних понять, аналізу класифікацій, міжнародних аспектів кіберзлочинності та підготовки до контрольних заходів. Розпочніть з ознайомлення з основними поняттями теми, такими як визначення кіберзлочинності, її форми і прояви. Для цього рекомендується дослідити визначення кіберзлочинності в юридичних і наукових джерелах, ознайомитися з історичними етапами розвитку кіберзлочинності та вивчити міжнародні документи і конвенції, такі як Будапештська конвенція, що регулюють це питання. Основні джерела для цієї частини вивчення можуть включати наукові статті, монографії про історію кіберзлочинності, юридичні документи і міжнародні конвенції, а також вебінари і лекції від експертів у сфері кіберзлочинності.

При вивченні цієї теми здобувачі вищої освіти повинні засвоїти класифікацію кіберзлочинності, розглянути різні види кіберзлочинів, такі як кібератаки, шахрайство і крадіжка даних, а також класифікацію кіберзлочинців за віком, психофізіологічними особливостями та цілями їх діяльності. Дослідження класифікацій варто доповнити аналізом об’єктів правопорушення і типологією кіберзлочинців. Корисними джерелами для цієї частини є навчальні посібники і статті про типологію кіберзлочинності, кейси і практичні приклади різних видів кіберзлочинів.

Після цього важливо здійснити аналіз кіберзлочинності як міжнародного соціального явища. Розглянути соціальні та економічні впливи кіберзлочинності на суспільство, економіку та правові системи, а також вивчіть міжнародну співпрацю в боротьбі з кіберзлочинністю, включаючи обмін інформацією і ресурсами між країнами. Для цього використовуйте міжнародні звіти і дослідження від організацій, таких як Інтерпол, Європейська комісія і ООН, а також книги і статті про соціальні та економічні наслідки кіберзлочинності.

Практичні заняття і обговорення є важливими для закріплення знань. Рекомендується аналізувати конкретні кейси кіберзлочинів, обговорювати їх деталі, причини та наслідки в групах, а також організовувати обговорення на тему кіберзлочинності для обміну думками і аналізу різних аспектів теми.

При **самостійні підготовці** слід вивчити теоретичні аспекти теми, виконати завдання з аналізу і класифікації кіберзлочинів, а також перевірити свої знання за допомогою тестових завдань і питань для самоконтролю. Корисними матеріалами для підготовки є тестові завдання і питання для самоперевірки, попередні залікові питання і відповіді. Форма педагогічного контролю – усне опитування під час проведення семінарського заняття.

***Семінарське заняття 2 години(денна та заочна форма навчання)***

**Учбові питання:**

1. Кіберзлочинність: поняття та сутність, генезис, характерні риси.
2. Класифікація кіберзлочинців за віковими групами, психофізіологічними особливостями, цілями та об'єктами правопорушення.
3. Класифікація кіберзлочинів.

**Питання до самоконтролю:**

1. Що таке кіберзлочинність і які етапи її розвитку можна виділити?
2. Які характерні риси відрізняють кіберзлочинність від традиційних форм злочинності?
3. Як кіберзлочинність впливає на суспільну безпеку та правові системи органів державної влади і правоохоронних органів?
4. Які категорії кіберзлочинців існують і за якими критеріями їх можна класифікувати?

5. Які типи комп'ютерних злочинів найбільш поширені у сфері сучасних інформаційних технологій?
6. Яким чином класифікуються кіберзлочини на міжнародному рівні і які є основні принципи цієї класифікації?
7. Які соціальні та правові наслідки кіберзлочинності для організацій та громадських структур?
8. Вкажіть тенденції розвитку кіберзлочинності прогнозуються на майбутнє і як вони можуть вплинути на нові форми кіберзлочинних активностей.

## ТЕМА 2. ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Правові засади протидії кіберзлочинності правоохоронними органами України. Міжнародне законодавство у сфері протидії кіберзлочинності.

Організаційні засади протидії кіберзлочинності правоохоронними органами України. Проблеми та напрямки удосконалення протидії кіберзлочинності. Суб'єкти протидії кіберзлочинності. Взаємодія та міжнародне співробітництво у сфері протидії кіберзлочинності.

### Методичні рекомендації

При вивченні цієї теми здобувачі вищої освіти повинні зосередитися на розумінні правових основ боротьби з кіберзлочинністю, міжнародних правових інструментах, організаційних аспектах діяльності правоохоронних органів та співпраці на міжнародному рівні. Вивчення цієї теми вимагає комплексного підходу, що включає теоретичне осмислення правових норм та практичний аналіз реальних випадків і стратегій протидії кіберзлочинності.

Особливої уваги заслуговує вивчення правових засад протидії кіберзлочинності в Україні. Для цього необхідно ознайомитись з основними нормативно-правовими актами, що регулюють боротьбу з кіберзлочинністю, розглянути структуру та повноваження органів, відповідальних за протидію кіберзлочинності, зокрема Національної поліції України, Служби безпеки України та інших спеціалізованих відомств. Необхідно встановити роль і функції правоохоронних органів у забезпеченні кібербезпеки, зокрема механізми виявлення, розслідування і запобігання кіберзлочинам. Корисними для цієї частини є офіційні текстів законодавчих актів, нормативні документи,

аналітичні статті про правове регулювання кіберзлочинності та звіти правоохоронних органів.

При вивченні цієї теми здобувачі вищої освіти повинні дослідити специфіку міжнародного законодавства у сфері протидії кіберзлочинності. Досліджуйте міжнародні конвенції, угоди та рекомендації, такі як Будапештська конвенція про кіберзлочинність та її додаткові протоколи, що регулюють міжнародне співробітництво у боротьбі з кіберзлочинністю. Ознайомтесь з міжнародними організаціями, які сприяють боротьбі з кіберзлочинністю, такими як Інтерпол, Європол і ООН. Вивчення цих документів допоможе зрозуміти, як міжнародна спільнота координує свої зусилля у боротьбі з кіберзлочинністю. Використовуйте офіційні документи міжнародних організацій, звіти міжнародних експертів і статті з міжнародного права для поглиблення знань.

Наступним етапом є аналіз організаційних засад протидії кіберзлочинності в Україні. Розгляньте проблеми і напрямки удосконалення організаційної структури і процесів, що пов'язані з кіберзлочинністю. Вивчіть сучасні підходи до вдосконалення системи захисту від кіберзлочинності в Україні, обговоріть існуючі проблеми та можливі рішення. Дослідження цієї частини теми можна здійснити через вивчення статей з аналізом ефективності існуючих механізмів протидії кіберзлочинності, дослідженням державних і приватних ініціатив у сфері кібербезпеки.

При **самостійні підготовці** ознайомитися з практичними аспектами міжнародного співробітництва в сфері протидії кіберзлочинності. Розгляньте приклади міжнародних спільних операцій, успішних кейсів міжнародної кооперації, а також вивчайте стратегії і механізми, які застосовуються для забезпечення ефективного міжнародного співробітництва. Вивчайте звіти міжнародних організацій, наукові статті та кейси, що ілюструють реальні приклади міжнародної співпраці у боротьбі з кіберзлочинністю. Форма педагогічного контролю – усне опитування під час проведення семінарського заняття.

***Семінарське заняття 2 години (денна та заочна форма навчання)***

**Учбові питання:**

1. Правові засади протидії кіберзлочинності в Україні.
2. Міжнародне законодавство у сфері протидії кіберзлочинності.

3. Організаційні засади протидії кіберзлочинності правоохоронними органами України.
4. Проблеми та напрямки удосконалення протидії кіберзлочинності, аналіз ефективності міжнародного співробітництва у цій сфері.

**Питання до самоконтролю:**

1. Вкажіть правові засади протидії кіберзлочинності існують в Україні.
2. Які міжнародні законодавчі акти регулюють протидію кіберзлочинності?
3. Які організаційні засади протидії кіберзлочинності використовуються правоохоронними органами України?
4. Які проблеми виникають у процесі протидії кіберзлочинності та які напрямки удосконалення можна запропонувати?
5. Охарактеризуйте форми та методи міжнародного співробітництва застосовуються у сфері протидії кіберзлочинності.
6. Яким чином відбувається взаємодія між різними країнами впливає на ефективність протидії кіберзлочинності?
7. Назвіть конкретні заходи, що здійснюються в Україні для запобігання кіберзлочинності.
8. Які основні правові та організаційні відмінності існують між протидією кіберзлочинності на національному та міжнародному рівнях?

## ТЕМА 3. ІНФОРМАЦІЙНА БЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

Сутність теорії інформаційної безпеки. Інформаційна безпека як складова загальної безпеки держави. Напрямки інформаційної безпеки. Методи та засоби здійснення інформаційної безпеки: правові, організаційні, технічні, програмні та криптографічні. Кібербезпека як складова інформаційної системи.

Еволюція загроз інформаційної безпеки. Вплив Інтернету на розвиток шкідливих програм. Основні методи шахрайства, якими користуються зловмисники: соціальну інженерію, скімінг, фішинг та їх комбінації. Які правила дозволять суттєво скоротити можливість потрапляння на такі виверти зловмисників.

### Методичні рекомендації

Для ефективного освоєння теми «Інформаційна безпека та захист інформації» важливо зосередитися на основах теорії інформаційної безпеки, методах захисту інформації, еволюції

кіберзагроз та практичних аспектах захисту даних. Вивчення цієї теми передбачає комплексний підхід, що охоплює як теоретичні знання, так і практичні навички.

При вивченні цієї теми здобувачі вищої освіти повинні знати основи теорії інформаційної безпеки, дослідити ключові поняття і визначення, такі як «інформаційна безпека», «конфіденційність», «цілісність», «доступність» інформації. Розглянути концепцію інформаційної безпеки як складову частину національної безпеки, ознайомитись з основними напрямками інформаційної безпеки, що включають правові, організаційні, технічні, програмні та криптографічні аспекти захисту інформації. Для цього корисно використовувати підручники з інформаційної безпеки, статті наукових журналів, нормативні документи з області захисту інформації, а також базові огляди в мережі Інтернет.

Особливої уваги заслуговує дослідження методів і засобів забезпечення інформаційної безпеки. Для цього розгляньте основні категорії інструментів та технологій, які використовуються для захисту інформації, такі як антивірусні програми, системи виявлення та запобігання вторгнень (IDS/IPS), засоби шифрування даних, механізми захисту мережі і програмного забезпечення. Важливо також дослідити еволюцію кіберзагроз і їх вплив на сучасні інформаційні системи, сучасні методи шахрайства, такі як соціальна інженерія, фішинг, скімінг та їх комбінації, а також ефективні практики захисту від них.

Необхідно ознайомитись з основними концепціями кібербезпеки, включаючи розгляд актуальних загроз і вразливостей в інформаційних системах, основи сучасних атак, таких як фішинг, експлойти вразливостей, та введення зловмисних програм. Розгляньте новітні технології, такі як штучний інтелект і блокчейн, що використовуються для створення складних кіберзагроз. Для глибшого розуміння цих концепцій скористайтеся науковими статтями, звітами аналітичних агентств і матеріалами з кібербезпеки.

При **самостійні підготовці** слід розглянути конкретні приклади атак на інформаційні системи, наслідки цих атак і стратегії їх запобігання. Розгляньте кейси з реальної практики та спробуйте розробити власні стратегії захисту інформації на основі отриманих знань. Практична частина навчання має включати аналіз реальних випадків кіберзагроз і вивчення методів захисту даних в умовах постійного технологічного розвитку. Форма педагогічного контролю –

усне опитування під час проведення семінарських та практичних занять.

***Семінарське заняття 2 години (денна форма навчання)***
***Практичне заняття 2 години (денна форма навчання)***
***Семінарське заняття 4 години (заочна форма навчання)***

**Учбові питання:**

1. Сутність теорії інформаційної безпеки та її роль як складової національної безпеки.
2. Напрямки інформаційної безпеки (правові, організаційні, технічні, програмні та криптографічні методи та засоби захисту).
3. Еволюція загроз інформаційній безпеці та вплив Інтернету на розвиток шкідливих програм.
4. Основні методи шахрайства, що використовуються зловмисниками (соціальна інженерія, скімінг, фішинг) та правила, які дозволяють знизити ризик потрапляння на такі атаки.

**Питання до самоконтролю:**

1. Що таке інформаційна безпека і які її основні складові?
2. Які напрямки інформаційної безпеки є найбільш критичними для загальної безпеки держави?
3. Які методи та засоби забезпечення інформаційної безпеки існують?
4. Як інформаційна безпека інтегрується в загальну систему безпеки держави?
5. Які загрози інформаційній безпеці є найбільш актуальними сьогодні і як вони еволюціонували з часом?
6. Який вплив Інтернету на розвиток шкідливих програм і які основні методи шахрайства використовуються зловмисниками?
7. Які правила дозволяють суттєво знизити ризики потрапляння на виверти зловмисників, що використовують соціальну інженерію, скімінг і фішинг?
8. Як кібербезпека співвідноситься з інформаційною безпекою і які ключові принципи забезпечення кібербезпеки?

**Практичні завдання:**

1. Знайдіть на сервісі YouTube відео з теми «Основи інформаційної безпеки». Перегляньте відео. Визначьте для себе рекомендації з інформаційної безпеки, які раніше Ви не знали.
2. Зареєструватися та пройти курси «Основи інформаційної безпеки від антивірусної лабораторії Zillya!» Антивірус (zillya.ua/prometheus) або на платформі Prometheus (https://prometheus.org.ua/) пройти курси

«Основи інформаційної безпеки» та «Інформаційна гігієна під час війни». Отримати сертифікати.

## ТЕМА 4. КЛАСИФІКАЦІЯ ТА АНАЛІЗ СУЧАСНИХ КІБЕРЗАГРОЗ

Кіберзагроза: поняття та класифікація. Класифікація кіберзагроз та їх можливі негативні наслідки. Ключові терміни, пов'язані із кіберзагрозами. Класифікація загроз на основі їх характеристик та методів атак.

Методи, що використовуються атакувальниками, включаючи соціально-інженерні та технічні підходи. Аналіз популярних векторів атак, таких як фішинг, експлойти вразливостей, та введення зловмисних програм. Мотивації, що підштовхують зловмисників, такі як фінансовий зиск, індустріальний шпіонаж або групова політична дестабілізація.

Новітні технології (штучний інтелект та блокчейн), що використовуються для створення складних та інтелектуальних кіберзагроз. Випадки сучасних кібератак, з виокремленням їх особливостей, масштабів та наслідків. Стратегії та технікі, спрямовані на передбачення та запобігання кіберзагрозам.

### Методичні рекомендації

Для глибокого розуміння теми «Класифікація та аналіз сучасних кіберзагроз» важливо зосередитися на вивченні спектра кіберзагроз, їхніх характеристик, методів атак і новітніх технологій, що використовуються зловмисниками. Вивчення цієї теми вимагає комплексного підходу, що включає як теоретичні знання, так і практичні навички.

При вивченні цієї теми здобувачі вищої освіти повинні ознайомитися з основами класифікації кіберзагроз. Встановити ключові категорії загроз, такі як шкідливе програмне забезпечення, атаки на мережеву інфраструктуру, атаки на програмне забезпечення і соціальна інженерія. Розглянути, яким чином класифікуються кіберзагрози за їх характеристиками, такими як типи атак, методи проникнення і цілі атак.

Поглиблене вивчення різноманітностей і характеристик сучасних кіберзагроз є важливим для розуміння їх потенційних наслідків для організацій і користувачів. Вивчайте реальні кейси атак, аналізуйте їхні технічні аспекти, методи реалізації і наслідки для цільових систем. Дослідження історії великих кіберінцидентів, таких

як атаки на Microsoft, Yahoo, або SolarWinds, допоможе вам зрозуміти, які вектори атак використовувалися і які наслідки були для цих організацій. Корисні ресурси для цього можуть включати звіти про інциденти, аналітичні статті і дослідження, доступні на таких платформах як *FireEye*, *Symantec*, *Trend Micro*. Необхідно дослідити різноманітні методи атак і технічні рішення, що використовуються для виявлення і захисту від кіберзагроз. Ознайомитися з методами, такими як фішинг, експлойти вразливостей, введення зловмисних програм, а також з інструментами для захисту від них.

При **самостійні підготовці** слід дослідити інноваційні технології, таких як штучний інтелект і блокчейн, що можуть бути використані для створення нових кіберзагроз або для захисту від них. Корисні для цього ресурси включають технічну документацію по інструментам кібербезпеки, а також наукові статті про новітні технології в сфері кіберзахисту.

Форма педагогічного контролю – усне опитування під час проведення семінарського заняття.

***Семінарське заняття 2 години (денна форма навчання)***

**Учбові питання:**

1. Спектр кіберзагроз, що активно загрожують інформаційній безпеці у сучасному інформаційному суспільстві.
2. Характеристики кіберзагроз, їх можливих наслідків для організацій та користувачів, а також ключових термінів, пов'язаних із кіберзагрозами.
3. Методи атак, які використовуються зловмисниками, включаючи соціально-інженерні та технічні підходи.
4. Новітні технології, такі як штучний інтелект та блокчейн, що використовуються для створення складних та інтелектуальних кіберзагроз.

**Питання до самоконтролю:**

1. Вкажіть основні типи кіберзагроз у сучасному інформаційному суспільстві.
2. Як класифікуються кіберзагрози на основі їхніх характеристик та методів атак?
3. Методи використовуються зловмисниками для проведення кібератак.
4. Вкажіть популярні вектори атак є найбільш розповсюдженими у сучасному кіберсередовищі.

5. Які є різновиди мотивацій зловмисників для здійснення кібератак, таких як фінансовий зиск, індустріальне шпигунство та політична дестабілізація?
6. Які новітні технології, зокрема штучний інтелект та блокчейн, використовуються для створення складних та інтелектуальних кіберзагроз?
7. Вкажіть конкретні випадки сучасних кібератак ілюструють їхні особливості, масштаби та наслідки.
8. Які стратегії та техніки спрямовані на передбачення та запобігання кіберзагрозам є найбільш ефективними?

## ТЕМА 5. КІБЕРБЕЗПЕКА ТА ОСНОВНІ ПРИНЦИПИ ТЕХНІЧНОГО ЗАХИСТУ В УМОВАХ ПОСТІЙНОГО ТЕХНОЛОГІЧНОГО РОЗВИТКУ

Аспекти кібербезпеки та основні принципи технічного захисту в умовах технологічного розвитку. Сучасні виклики та стратегії захисту від кіберзагроз у постійно прогресуючому технологічному середовищі.

Сучасні тенденції технологічного розвитку та їх вплив на кібербезпеку. Архітектурні засади побудови ІТ-інфраструктури з урахуванням вимог до безпеки в сучасному технологічному середовищі. Методи та технічні рішення для забезпечення безпеки в хмарних сервісах, які стали ключовим елементом сучасної ІТ-інфраструктури. Методи та технології, спрямовані на захист мобільних пристроїв та даних.

Аналіз викликів та заходів безпеки, пов'язаних із зростанням кількості підключених до Інтернету пристроїв у різних сферах життя. Роль та використання штучного інтелекту для виявлення та вирішення кіберзагроз у реальному часі. Основні принципи роботи та стратегії використання антивірусних і анти-малварних заходів у сучасних технічних системах. Методи та рішення ефективного контролю та захисту великого обсягу даних, що генеруються системами IoT.

### Методичні рекомендації

Для ефективного вивчення теми «Кібербезпека та основні принципи технічного захисту в умовах постійного технологічного розвитку» необхідно поглибити знання про основи кібербезпеки, сучасні виклики у технічному захисті інформаційних систем та методи забезпечення безпеки в умовах швидкого технологічного прогресу.

При вивченні теми слід зазначити, що для попередження правопорушень в кіберпросторі розробники інформаційних та комунікаційних систем передбачають різноманітні засоби захисту інформації та комп'ютерних систем і мереж. Особливу увагу слід приділити проблемам забезпечення кібернетичної безпеки, а також її складовим. Під кібербезпекою ми будемо розуміти комплекс процесів, практичних порад і технологічних рішень, які допомагають захистити важливі системи й дані від несанкціонованого доступу.

Загрози кібернетичній безпеці, з одного боку, є організаційним компонентом системи органів влади, а з іншого - слугують індикатором ефективності її функціонування. Адже реалізація загроз і переростання їх у небезпеки свідчать про неефективність функціонування даної системи, і навпаки. Для початку рекомендується ознайомитися з базовими поняттями кібербезпеки та технічного захисту інформаційних систем. Дослідити основи концепцій кібербезпеки, таких як конфіденційність, цілісність та доступність інформації.

Окремої уваги потребують проблеми визначення сучасних технологічних викликів у сфері кібербезпеки. Вивчайте тенденції у розвитку технологій, такі як вплив хмарних сервісів, мобільних технологій та Інтернету речей на безпеку інформаційних систем. Доречно буде розглянути основні принципи технічного захисту інформаційних систем, архітектурні рішення для побудови безпечних IT-інфраструктур, включаючи мережеві архітектури, системи захисту даних і методи контролю доступу.

При **самостійні підготовці** слід ознайомитись з впливом штучного інтелекту на кібербезпеку та використанням сучасних технологій для забезпечення безпеки інформаційних систем. Дослідити, як штучний інтелект може бути використаний для виявлення кіберзагроз і як новітні технології впливають на розвиток кібербезпеки. Форма педагогічного контролю – усне опитування під час проведення семінарських та практичних занять.

***Семінарське заняття 2 години (денна форма навчання)***
***Практичне заняття 2 години (денна форма навчання)***

**Учбові питання:**

1. Аспекти кібербезпеки та основні принципи технічного захисту в умовах швидкого технологічного розвитку.
2. Аналіз сучасних тенденцій технологічного розвитку та їхнього впливу на кібербезпеку.

3. Методи та технічні рішення забезпечення безпеки в хмарних сервісах та мобільних пристроях.
4. Виклики та заходи безпеки, пов'язані зі зростанням кількості підключених до Інтернету пристроїв у різних сферах життя.
5. Роль штучного інтелекту у виявленні та вирішенні кіберзагроз у реальному часі.

**Питання до самоконтролю:**

1. Які основні принципи технічного захисту інформації в умовах швидкого технологічного розвитку?
2. Які сучасні виклики та стратегії захисту від кіберзагроз існують у постійно прогресуючому технічному середовищі?
3. Вкажіть сучасні тенденції технологічного розвитку впливають на кібербезпеку.
4. Які архітектурні засади побудови ІТ-інфраструктури враховують вимоги до безпеки в сучасному технологічному середовищі?
5. Які методи та технічні рішення забезпечують безпеку в хмарних сервісах, які є ключовими елементами сучасної ІТ-інфраструктури?
6. Які методи та технології використовуються для захисту мобільних пристроїв та даних в умовах активного використання мобільних технологій?
7. Які виклики та заходи безпеки пов'язані зі зростанням кількості пристроїв, підключених до Інтернету, у різних сферах життя?
8. Яку роль відіграє штучний інтелект у виявленні та вирішенні кіберзагроз у реальному часі?
9. Вкажіть стратегії, що використовуються для контролю та захисту великого обсягу даних, що генеруються системами IoT.

**Практичні завдання:**

1. Ознайомтеся з повним текстом порад для безпеки в мережі Інтернет від команди CERT-UA (cert.gov.ua/?p848) та порівняйте їх з правилами інтернет-безпеки від Профспілки працівників освіти і науки України (pon.org.ua/novyny/5427-bezpeka-v-nternet-scho-potrbno-znati.html). Зверніть увагу, які рекомендації збігаються. З якими загрозами вони пов’язані?

## ТЕМА 6. ПРИНЦИПИ БЕЗПЕЧНОЇ РОБОТИ З МОБІЛЬНИМИ ПРИСТРОЯМИ. БЕЗПЕКА В УМОВАХ ІНФОРМАЦІЙНОЇ ВІЙНИ ТА КІБЕРВІЙНИ

Інформаційна безпека мобільних та дистанційних телекомунікацій.Практичні прийоми захисту від кіберзагроз. Загрози втрати конфіденційної інформації з мобільних пристроїв. Захист Android-пристроїв. Захист iOS-пристроїв. Захист пристроїв на базі Windows Phone та інших мобільних ОС.

Бот: поняття, види, цілі та методика виявлення коментару від бота. Тролінг: визначення, ознаки та методика виявлення тролінгу.

Визначення понять: «кібервійна», «інформаційна війна», «інформаційна зброя». Взаємозв'язок інформаційних війн та кібервійн. Інформаційне середовище - спосіб контролю над певною державою чи населенням, механізм контролю свідомості певних кіл громадян.

### Методичні рекомендації

При підготовці до семінарського заняття важливо розглянути ключові аспекти безпеки мобільних технологій і інформаційних війн, а також методи захисту в умовах кіберконфліктів. Варто пам’ятати, що безпека - це процес, а не одноразова дія. В обмін на певні затрати часу та зусилля Ви отримаєте більшу захищеність і спокій. Щоби ваші дані були завжди в безпеці, потрібно постійно здійснювати заходи щодо їх захисту, регулярно перевіряти й оновлювати встановлені програми та використовувати додаткові засоби захисту, коли це потрібно. Складіть власний план захисту, поєднавши кілька методів, щоб забезпечити максимальний захист вашого пристрою.

В процесі підготовки до семінарського заняття необхідно також засвоїти практичні аспекти захисту мобільних пристроїв, зокрема методи захисту Android-пристроїв, iOS-пристроїв та інших мобільних операційних систем. Дослідити специфіку безпеки для різних мобільних платформ та інструменти, які можна використовувати для забезпечення безпеки, такі як антивірусні програми, рішення для захисту даних та техніки захисту інформації.

Ефективність вибраних засобів захисту залежатиме від багатьох факторів, зокрема вашого стилю користування мобільним пристроєм. Встановлення надійного пароля, використання *Touch ID* або *Face ID,* вчасні оновлення ОС і програм, резервне копіювання даних і вихід у мережу через *VPN* - усе це важливі кроки до убезпечення вашої інформації.

Як вказувалось раніше, загрози інформаційній безпеці, з одного боку, є організаційним компонентом системи органів влади, а з іншого - слугують індикатором ефективності її функціонування. Найнебезпечнішими на даному етапі розвитку українського суспільства є інформаційні війни. Для забезпечення кібербезпеки надзвичайно важливо розуміти загрози кіберпростору. Кібернетичні загрози (кіберзагрози) – наявні та/ або потенційно можливі явища і чинники, що створюють небезпеку життєво важливим інтересам людини і громадянина, суспільства і держави, реалізація яких залежить від належного функціонування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем. При цьому можна виділити таку типологію кібернетичних загроз: кібервійна; кібертероризм; кібершпигунство; кіберзлочинність.

Під час **самостійної роботи** слід розглянути яким чином інформаційні війни та кібервійни впливають на суспільство та державу, концепції інформаційних війн, механізми впливу на свідомість громадськості та роль кібервійн у сучасних конфліктах. Також доцільно дослідити методи виявлення ботів і тролінгу в інформаційному середовищі, а також стратегії боротьби з цими загрозами. Формою педагогічного контролю є опитування здобувачів вищої освіти в усній формі під час проведення семінарських та практичних занять.

***Семінарське заняття 2 години (денна форма навчання)***
***Практичне заняття 4 години (денна форма навчання)***
***Семінарське заняття 4 години (заочна форма навчання)***

**Учбові питання:**

1. Практичні прийоми захисту мобільних пристроїв на базі різних операційних систем, таких як Android, iOS та Windows Phone.
2. Аналіз взаємозв'язку інформаційних війн та кібервійн, а також їх впливу на інформаційне середовище, спосіб контролю над певною державою чи населенням.
3. Методи виявлення та протидії тролінгу та ботам, включаючи ознаки тролінгу та способи виявлення коментарів від ботів.
4. Роль інформаційного середовища як механізму контролю свідомості певних кіл громадян та методів захисту від таких впливів.

**Питання до самоконтролю:**

1. Які практичні прийоми захисту від кіберзагроз існують для мобільних пристроїв?

2. Які особливості захисту Android-пристроїв, iOS-пристроїв та пристроїв на базі Windows Phone?
3. Який взаємозв'язок існує між інформаційними війнами та кібервійнами?
4. Що таке боти та як виявити коментар від бота?
5. Які ознаки тролінгу існують та як виявити тролінг?
6. В чому полягає вплив кібервійн та інформаційних війн на інформаційне середовище держав та населення?
7. Охарактеризуйте механізм контролю свідомості використовуються у рамках інформаційних та кібервійн?
8. Які стратегії забезпечення інформаційної безпеки в умовах інформаційної війни та кібервійни є найефективнішими?

**Практичні завдання:**

1. Здійснити виведення проекції екрану смартфона на персональний комп'ютер. Вирішення цього завдання залежить від операційної системи, встановленої на мобільному пристрої та на ПК. В окремих випадках можливості операційної системи дозволяють здійснити безпосереднє виведення інформації з екрану мобільного пристрою без необхідності встановлення додаткового програмного забезпечення.
2. Налаштуйте параметри безпеки для: операційної системи свого мобільного пристрою; облікових записів, прив'язаних до мобільного пристрою; встановлених на мобільному пристрої застосунків.

## ТЕМА 7. СОЦІАЛЬНА ІНЖЕНЕРІЯ ТА КІБЕРБЕЗПЕКА КОРИСТУВАЧІВ

Соціальна інженерія як одна з найважливих сфер в кібербезпеці. Сутність та визначення ключових термінів в контексті соціальної інженерії. Інструменти та методи, що використовуються соціальними інженерами для маніпуляції та отримання несанкціонованого доступу. Ключові психологічні аспекти, що використовуються в соціальній інженерії для впливу на користувачів та роблять їх вразливими до атак.

Видів соціальних атак, включаючи фішинг, обман та імперсонацію. Стратегії та рекомендації для користувачів щодо виявлення та запобігання соціальним атакам. Технічніта організаційні контрзаходи для ефективного захисту від соціально-інженерних атак. Взаємодія та обмін інформацією в спільноті для попередження соціальних атак.

**Методичні рекомендації**

При вивченні цієї теми здобувачі вищої освіти повинні засвоїти основні концепції соціальної інженерії, техніки маніпуляцій, та стратегії підвищення обізнаності користувачів для захисту від соціальних атак. Соціальна інженерія є важливою та актуальною темою в сфері кібербезпеки та захисту інформації. Соціальна інженерія (social engineering, соцінжиніринг) – це метод маніпулювання думками та вчинками людей. Він базується на психологічних особливостях особистості та закономірності людського мислення. Іноді можна зустріти трактування соціальної інженерії як методу несанкціонованого отримання доступу до секретних даних, що цілком відповідає дійсності: ряд технік психологічного впливу може застосовуватися законно. Необхідно розглянути різноманітні техніки соціальної інженерії, такі як фішинг, блефи, обман і імперсонація, а також встановити яким чином ці техніки використовуються для отримання несанкціонованого доступу до інформації або систем.

При підготовці до занять з цієї теми необхідно акцентувати увагу на тому факті, що соціальна інженерія широко використовує психологічні техніки для переконання людини надати конфіденційну інформацію. Так, найбільш ефективний метод соціальної інженерії – видавання себе за твоїх родичів або знайомих, яким ти довіряєш у будь-якому випадку. Один з основних аспектів, який притаманний соціальній інженерії – емоції. Зловмисники використовують людські слабкості для того, аби отримати бажане. Їхні повідомлення можуть викликати страх, надію, цікавість і допитливість – будь-що, аби людина довірилась і без питань надала необхідні дані. Шахраї спеціально створюють такі ситуації, які викликають у тебе стрес, страх та паніку, аби ти почав швидко діяти та не задумувався над тим, що відбувається.

Під час **самостійної роботи** слід розглянути стратегії та методи для запобігання соціальним атакам, а також політики безпеки для організацій, які допоможуть уникнути атак через соціальну інженерію. При підготовці до практичного заняття можуть розглянути практичні вправи з виявлення соціальних атак, таких як проведення фішинг-симуляцій або аналіз випадків соціальної інженерії. Це допоможе розвинути навички виявлення і запобігання соціальним атакам. Формою педагогічного контролю є опитування здобувачів вищої освіти в усній формі під час проведення занять.

***Семінарське заняття 2 години (денна форма навчання)***
***Практичне заняття 2 години (денна форма навчання)***

**Учбові питання:**

1. Соціальна інженерія, розкриття її сутності та ключових термінів у контексті кібербезпеки.
2. Розгляд інструментів та методів, що використовуються соціальними інженерами для маніпуляції та отримання несанкціонованого доступу до інформації.
3. Аналіз психологічних аспектів, які використовуються в соціальній інженерії для впливу на користувачів та підвищення їхньої вразливості до атак.
4. Оцінка важливості освіти користувачів у запобіганні соціальним атакам, а також розгляд технічних та організаційних контрзаходів для ефективного захисту від соціально-інженерних атак.

**Питання до самоконтролю:**

1. Що таке соціальна інженерія і які ключові терміни пов'язані з нею?
2. Які інструменти та методи використовуються соціальними інженерами для маніпуляції та отримання несанкціонованого доступу?
3. Вкажіть ключові психологічні аспекти соціальної інженерії впливають на користувачів і роблять їх вразливими до атак.
4. Які основні види соціальних атак, зокрема фішинг, блефи, обман та імперсонація?
5. Які стратегії та рекомендації для користувачів допомагають виявляти та запобігати соціальним атакам?
6. Які технічні та організаційні контрзаходи є ефективними для захисту від соціально-інженерних атак?
7. В чому полягає важливість освіти користувачів для ефективного запобігання соціальним атакам.
8. Як взаємодія та обмін інформацією в спільноті допомагають попереджати соціальні атаки?

**Практичні завдання:**

1. Навчитись ідентифікації атак із застосуванням соціальної інженерії та встановити інструменти збору інформації. Отримати навики збору відкритої інформації.
2. Інструменти збору інформації в Інтернеті. Отримання особистих даних для доступу до соціальних мереж з використанням Social Engineering Toolkit (SET) та Credential Harvest method. Процес визначення цілей соціоінженерної атаки.

## 4. ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ ОСВІТНЬОЇ ДІЯЛЬНОСТІ

Система оцінювання передбачає накопичення 100 балів з кожної навчальної дисципліни, які перераховуються в національну шкалу та шкалу оцінювання ЄКТС.

Встановлюються: максимальні суми балів за виконання завдань у рамках аудиторної та самостійної роботи - 60 балів; за виконання завдань, винесених на підсумковий контроль - 40 балів.

| **Поточний контроль** | | **Підсумковий контроль (ПК)** |
|---|---|---|
| **Аудиторна робота (АР)** (семінарські/практичні заняття та контрольні заходи) | **Самостійна робота (СР)** | ЗАЛІК (З)/ ЕКЗАМЕН (Е) |
| **≤ 40** | **≤ 20** | |
| **≤ 60** | | **≤ 40** |
| **Підсумкова кількість балів = АР+СР+ПК ≤ 100** | | |

Підсумкова кількість балів з навчальної дисципліни за семестр складається, як сума накопичувальних балів за аудиторну та самостійну роботу і отриманих балів під час підсумкового контролю.

Оцінювання компетентностей здобувача вищої освіти з навчальної дисципліни та виставлення підсумкової кількості балів за аудиторну роботу здійснюється шляхом встановлення відповідного рівня знань на кожному навчальному занятті. Підсумкова кількість балів визначається, як сума всіх отриманих під час проведення навчальних занять оцінок («2», «3», «4» та «5») розділена на кількість отриманих таких оцінок за семестр та помножена на коефіцієнт відповідності максимально можливого балу за аудиторну роботу:

$$АР = \frac{\sum О_{АР}}{КО_{АР}} \times 8,$$

де:

АР – підсумкова кількість балів за аудиторну роботу;

$\sum О_{АР}$ – сума всіх отриманих оцінок за аудиторну роботу;

$КО_{АР}$ – кількість отриманих оцінок за семестр за аудиторну роботу;

8 – коефіцієнт відповідності максимально можливого балу за аудиторну роботу.

Оцінювання компетентностей здобувача вищої освіти з навчальної дисципліни та виставлення підсумкової кількості балів за

самостійну роботу здійснюється шляхом встановлення відповідного рівня знань за виконану самостійну роботу. Підсумкова кількість балів визначається, як сума всіх отриманих за самостійну роботу оцінок («2», «3», «4» та «5») розділена на кількість отриманих таких оцінок за семестр та помножена на коефіцієнт відповідності максимально можливого балу за самостійну роботу:

$$СР = \frac{\sum О_{СР}}{КО_{СР}} \times 4,$$

де:

СР – підсумкова кількість балів за самостійну роботу;

$\sum О_{СР}$ – сума всіх отриманих оцінок за самостійну роботу;

$КО_{СР}$ – кількість отриманих оцінок за семестр за самостійну роботу;

4 – коефіцієнт відповідності максимально можливого балу за самостійну роботу.

Здобувач вищої освіти, як додатковий здобуток може отримати додаткові бали, при цьому загальна сума накопичувальних балів не повинна перевищувати 100:

- за наукову роботу в межах навчальної дисципліни до 10-ти балів;
- за проходження тренінгу за тематикою навчальної дисципліни та отриманні сертифікату до 5-ти балів.

Здобувач вищої освіти може отримати оцінку «5» за умови, що він дуже добре орієнтується в матеріалі, приймав активну участь у занятті та надав повну відповідь на питання семінарського заняття, або на додаткове питання науково-педагогічного працівника, навів приклади, висловив та аргументував власну точку зору, або суттєво доповнював більше трьох разів відповіді колег, не допустивши помилок. Також на оцінку «5» може бути оцінено виступ з доповіддю або рефератом, які було підготовлено з використанням декількох джерел інформації, а під час виступу тему розкрито повністю.

Здобувач вищої освіти може отримати оцінку «4» за умови, що він достатньо добре орієнтується в матеріалі, приймає активну участь у занятті, доповнюючи колег, знає основні визначення та факти з теми семінарського заняття, надав правильну, але не зовсім повну відповідь, висловлює власну думку, але не може змістовно її аргументувати, йому складно навести приклади. Також на оцінку «4» може бути оцінено виступ здобувача з доповіддю або рефератом, які було підготовлено з використанням одного джерела інформації, а під час виступу тему розкрито не повністю.

Здобувач вищої освіти може отримати оцінку «3» за умови, якщо не приймає активної участі в семінарському занятті та не висловлює цікавості до матеріалу, йому складно дати визначення понять, відповідає фрагментарно та спутано, допускає помилки, не орієнтується у темі, власної думки не має, або висловлюючи її відмовляється аргументувати. Також на оцінку «3» може бути оцінено виступ здобувача з доповіддю або рефератом, які містять мізерний обсяг інформації, або застарілі данні.

Здобувач вищої освіти може отримати оцінку «2» за умови незнання здобувачем вищої освіти значної частини навчального матеріалу за змістом відповідної теми навчальної дисципліни, що міститься в основних рекомендованих нормативних та базових джерелах, допустив істотні помилки у відповідях на поставлені питання, виявив невміння застосовувати теоретичні положення під час розв'язання практичних задач, відмовився від відповіді та/або не вирішив практичне завдання, не виконав самостійну роботу. Оцінка «2» потребує перескладання.

Умови допуску здобувача вищої освіти до складання підсумкового контролю:

Для денної форми навчання:

- сума балів поточного контролю не менше ніж 36; має не більше двох невідпрацьованих пропусків та/або невідпрацьованих незадовільних оцінок за поточний контроль.

Для заочної форми навчання: сума балів поточного контролю не менше ніж 36.

З метою підвищення поточного рейтингу успішності здобувач вищої освіти має право перескладати аудиторну та самостійну роботу відповідно до графіку, встановленого науково-педагогічним працівником до підсумкового контролю і не більше двох пропусків та/або незадовільних оцінок з однієї навчальної дисципліни за один робочий день.

Здобувач вищої освіти, який за результатами поточного контролю накопичив менше 60 балів, зобов'язаний складати підсумковий контроль.

Здобувач вищої освіти, який за результатами поточного контролю протягом семестру накопичив 60 балів, має можливість:

- не складати підсумковий контроль і отримати накопичену кількість балів як підсумкову оцінку;
- складати підсумковий контроль відповідно до розкладу.

**Критерії оцінювання знань**

Для тих, хто складає залік критерії оцінювання знань наступні.

Оцінка A,B,C, D, E / "зараховано " виставляється, якщо здобувач вищої освіти виявив достатньо повні знання курсу; вміє узагальнювати теоретичний матеріал, співвідносити загальні знання з конкретними ситуаціями, засвідчив уміння критично оцінювати варіативні підходи щодо сутності поставлених питань, дає правильні, хоча і не завжди повні відповіді на поставлені запитання; висловлює своє ставлення до варіантних теорій щодо сутності явищ; допускає незначні неточності в розкритті окремих теоретичних положень; матеріал викладає не завжди логічно, послідовно і переконливо.

Оцінка FX, F/ "не зараховано " виставляється, якщо здобувач вищої освіти виявив слабкі (відсутність) знання теоретичного програмного матеріалу; не зміг дати визначення основних провідних категорій та явищ; відсутні навички адекватної оцінки норм і теорій; виклад матеріалу непослідовний, нелогічний, фрагментарний, неточний, стислий; повна відсутність переконливості в викладенні матеріалу.

**Шкала оцінювання знань: національна та ECTS**

<table>
<tr><th>За внутрішньою шкалою навчального закладу в балах</th><th colspan="2">За шкалою ECTS /За національною шкалою</th></tr>
<tr><td></td><td colspan="2">Вноситься до відомості</td></tr>
<tr><td></td><td>Екзамен</td><td>залік</td></tr>
<tr><td>90 – 100</td><td>A/Відмінно</td><td rowspan="5">A,B,C, D, E/Зараховано</td></tr>
<tr><td>82-89</td><td>B/Добре</td></tr>
<tr><td>74-81</td><td>C/Добре</td></tr>
<tr><td>64-73</td><td>D/Задовільно</td></tr>
<tr><td>60-63</td><td>E/Задовільно</td></tr>
<tr><td rowspan="2">35-59</td><td>FX/Незадовільно</td><td>Не зараховано</td></tr>
<tr><td colspan="2">з можливістю повторного складання</td></tr>
<tr><td rowspan="2">0-34</td><td>F/Незадовільно</td><td>Не зараховано</td></tr>
<tr><td colspan="2">з обов'язковим повторним курсом</td></tr>
</table>

**Засоби діагностики успішності навчання**

Засоби діагностики успішності навчання з навчальної дисципліни «Протидія кіберзлочинності» включають:

- контрольні питання до семінарських та практичних занять;
- квізи (тести);
- перелік питань до заліку.

## 5. ПИТАННЯ ДЛЯ ПІДСУМКОВОГО КОНТРОЛЮ

1. Основні етапи генезису кіберзлочинності.
2. Характерні риси кіберзлочинності.
3. Яким чином кіберзлочинність впливає на міжнародне соціальне середовище?
4. Основні загрози кіберзлочинності для суспільної безпеки.
5. Які правові системи найбільше піддаються кіберзлочинним посяганням?
6. Класифікація комп'ютерних злочинців за віком та психофізіологічними особливостями.
7. Цілі та об'єкти правопорушень характерні для різних типів комп'ютерних злочинців.
8. Види злочинів у сфері використання сучасних інформаційних технологій найпоширеніші.
9. Міжнародна класифікація кіберзлочинів.
10. Які заходи можна застосувати для ефективної боротьби з кіберзлочинністю на міжнародному рівні?
11. Правові засади протидії кіберзлочинності існують в Україні.
12. Міжнародне законодавство в сфері протидії кіберзлочинності.
13. Організаційні засади протидії кіберзлочинності.
14. Основні проблеми у сфері протидії кіберзлочинності в Україні.
15. Напрямки удосконалення протидії кіберзлочинності можна виділити.
16. Яке значення має міжнародне співробітництво у сфері протидії кіберзлочинності?
17. Як відбувається координація між національними та міжнародними організаціями у боротьбі з кіберзлочинністю?
18. Ключові аспекти правових засад протидії кіберзлочинності в Україні можна виділити.
19. Які методи і стратегії використовуються в Україні для організаційної протидії кіберзлочинності?

20.Які міжнародні ініціативи та договори сприяють ефективній протидії кіберзлочинності?
21.Інформаційна безпека та її основні складові.
22.Яким чином інформаційна безпека впливає на загальну безпеку держави?
23.Основні напрямки інформаційної безпеки.
24.Правові методи здійснення інформаційної безпеки.
25.Технічні та програмні засоби захисту інформації.
26.Криптографічні методи захисту інформації і як вони застосовуються.
27.Охарактеризуйте еволюцію загроз інформаційній безпеці вплинула на сучасні системи захисту.
28.В чому полягає вплив має Інтернет на розвиток шкідливих програм.
29.Основні методи шахрайства використовують зловмисники і як можна їм протидіяти.
30.Вкажіть основні класифікаційні ознаки сучасних кіберзагроз.
31.Класифікація кіберзагроз за їх характеристиками та методами атак.
32.Основні види кіберзагроз і які їх можливі наслідки для організацій та користувачів.
33.Методи соціально-інженерних атак використовуються сучасними кіберзлочинцями.
34.Технічні підходи здійснення атак через експлойти вразливостей.
35.Популярні вектори атак у сучасному кіберпросторі.
36.Як штучний інтелект і блокчейн можуть бути використані для створення складних кіберзагроз?
37.Новітні технології передбачення та запобігання кіберзагрозам.
38.Як можна проаналізувати та вивчити конкретні випадки сучасних кібератак для розробки ефективних стратегій захисту?
39.Основні принципи технічного захисту інформаційних систем в умовах швидкого технологічного розвитку.
40.Сучасні тенденції технологічного розвитку впливають на кібербезпеку.
41.Яким чином побудувати архітектуру IT-інфраструктури з урахуванням вимог до безпеки?
42.Методи технічного захисту інформаційних систем в хмарних.
43.Основні виклики та рішення для забезпечення безпеки мобільних пристроїв.

44.Які новітні технології, такі як штучний інтелект, використовуються для виявлення та запобігання кіберзагрозам?
45.Особливості захисту даних у великих обсягах, що генеруються системами Інтернету речей (IoT).
46.Технічні та організаційні заходи захисту інформації в умовах постійного технологічного розвитку.
47.Стратегії і технічні рішення безпеки в хмарних обчисленнях.
48.Основні принципи роботи антивірусних і анти-малварних програм у сучасних технічних системах.
49.Основні принципи безпечної роботи з мобільними пристроями.
50.Захиди безпеки Android-пристроїв від кіберзагроз.
51.Методи захисту iOS-пристроїв.
52.Безпека мобільних пристроїв на базі Windows Phone та інших мобільних ОС.
53.Основні ознаки бота та засоби їх виявлення в інформаційному середовищі.
54.Методи виявлення і протидії тролінгу в Інтернеті.
55.Особливості та наслідки інформаційних війн та кібервійн для державної безпеки.
56.Технічні та організаційні заходи захисту мобільних пристроїв в умовах інформаційної війни.
57.Соціальна інженерія і які її основні методи використовуються в кіберзлочинності.
58.Вплив соціальної інженерії на кібербезпеку користувачів і організацій.
59.Які психологічні аспекти використовуються в соціальній інженерії для маніпуляції користувачами?
60.Основні види соціальних атак.
61.Технічні та організаційні контрзаходи захисту від соціальних атак.
62.Як освітні програми для користувачів можуть допомогти запобігти соціальним атакам?
63.Стратегії і рекомендації виявлення і запобігання соціальним атакам.
64.Аналіз випадків соціальної інженерії допомагає розробити ефективні заходи захисту.
65.Роль і важливість взаємодії та обміну інформацією в спільноті для попередження соціальних атак.

## 6. ГЛОСАРІЙ

*Автоматизована інформаційна система оперативного призначення (АІС ОП)*- сукупністю програмно-технічних і телекомунікаційних засобів та призначена для накопичення й обробки відомостей, що утворюються в процесі оперативно-розшукової діяльності Національної поліції Україні.

*Автоматизована система (ас)* - сукупність керованого об'єкта й автоматичних керуючих пристроїв, у якій частину функцій керування виконує людина. АС являє собою організаційно-технічну систему, що забезпечує вироблення рішень на основі автоматизації інформаційних процесів у різних сферах діяльності (управління, проектування, виробництво тощо) або їх поєднаннях.

*Автоматизовані інформаційно-пошукові системи* – сукупність методів і засобів, призначених для зберігання та пошуку документів, відомостей про них чи певних фактів.

*Аналіз інформації* – процес обробки інформації, який базується на логічному та креативному мисленні, спрямований на одержання якісно нової інформації у вигляді гіпотез, висновків, припущень, ситуативних картин тощо.

*Аналітик* – 1. Фахівець, що володіє необхідними знаннями та досвідом аналізу управлінських ситуацій, підготовки аналітичних звітів, висновків та пропозицій. 2. Посадова особа підрозділу кримінального аналізу (кримінального аналізу та оперативного моніторингу).

*Аналітична діяльність* – це інтелектуальна творча діяльність, спрямована на одержання та використання нових знань, що здійснюється із застосуванням наукових методів на основі процесу судження від конкретного до загального.

*Аналітичний документ* - вторинний документ, що містить узагальнену інформацію, отриману в результаті всебічного, глибокого та критичного аналізу первинних документів, аргументовану оцінку стану і тенденцій розвитку проблеми, що розвивається.

*База даних* – це поіменована, структурована сукупність взаємопов'язаних даних, що належать до певної предметної області і зберігається на комп’ютерних носіях, зазвичай разом з прикладною програмою. Основне призначення баз даних – зберігання, накопичення, оновлення і пошук необхідної інформації.

*База стратегічних даних* (БСД) – це стислий системний опис найсуттєвіших стратегічних елементів, що належать до зовнішнього середовища підприємства; вона (БСД) використовується для оцінки поточного становища, застосовується для визначення прояву процесів у майбутньому та для прийняття стратегічних рішень.

*Блокування інформації в системі* - дії, внаслідок яких унеможливлюється доступ до інформації в системі.

*Виток інформації* - результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї.

*Відеоконференція* - це сфера інформаційної технології, що забезпечує одночасно двосторонню передачу, обробку, перетворення і представлення інтерактивної інформації на відстань у реальному режимі часу за допомогою апаратно-програмних засобів обчислювальної техніки, тобто між двома та більше абонентами Для проведення відеоконференцій використовується така технологія, як відеоконференцзв'язок.

*Візуальна форма електронного документа* - відображення даних, що він містить, електронними засобами або на папері у формі, придатній для сприймання його змісту людиною.

*Віртуальний простір* - простір, що моделюється за допомогою комп'ютера, у якому перебувають відомості про особи, предмети, факти, події, явища і процеси, представлені в математичному, символьному або будь-якому іншому виді й рухи, що перебувають у процесі, по локальних і глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального устрою, а також іншого носія, спеціально призначеного для їхнього зберігання, обробки й передачі.

*Документ* - матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі.

*Доступ до інформації в системі* - отримання користувачем можливості обробляти інформацію в системі.

*Електронне (віртуальне) судочинство* - проведення судового процесу з використанням сучасних комп'ютерних та телекомунікаційних технологій.

*Єдина інформаційна система МВС* - багатофункціональна інтегрована автоматизована система, що безпосередньо забезпечує реалізацію функцій її суб'єктів, інформаційну підтримку та супроводження їх діяльності і становить сукупність взаємозв'язаних функціональних підсистем, програмно-інформаційних комплексів, програмно-технічних та технічних засобів телекомунікації, які забезпечують логічне поєднання визначених інформаційних ресурсів, обробку та захист інформації, внутрішню та зовнішню інформаційну взаємодію.

*Єдиний реєстр досудових розслідувань (ЄРДР)* - це створена за допомогою автоматизованої системи електронна база даних, відповідно до якої здійснюється збирання, зберігання, захист, облік,

пошук, узагальнення даних про кримінальні правопорушення та хід досудового розслідування у кримінальних провадженнях.

*Захист інформації* - сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

*Збір інформації* – діяльність суб'єкта, в ході якої він здійснює пошук і отримання відомостей про потрібний йому об'єкт.

*Знищення інформації в системі* - дії, внаслідок яких інформація в системі зникає.

*Інтеграція інформаційних ресурсів єдиної інформаційної системи МВС* - комплекс методів та процедур, спрямованих на логічне функціональне об'єднання інформаційних ресурсів єдиної інформаційної системи МВС у визначених форматах, за узгодженими показниками, для їх автоматизованої обробки, використання та надання користувачам в уніфікованому вигляді.

*Інтегрована інформаційно-телекомунікаційна система «Аркан»* - це сукупність організаційно-розпорядчих заходів, програмно-технічних та телекомунікаційних засобів, що забезпечують обробку інформації (уведення, приймання, отримання, передавання, реєстрація, зберігання) щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон України, та автоматизований доступ до інформаційних ресурсів (баз даних) суб'єктів системи «Аркан».

*Інтегрована інформаційно-телекомунікаційна система «Гарт-1»* - це сукупність організаційно-розпорядчих заходів, програмно-технічних та телекомунікаційних засобів, що забезпечують обробку інформації (уведення, записування, зчитування, зберігання, знищення, приймання, передавання) щодо прикордонного контролю осі і транспортних засобів, які перетинають державний кордон України, та автоматизований доступ до інформації, що зберігається в базах даних системи "Гарт-1".

*Інтерпол* - міжнародна організація кримінальної поліції, створена у 1923 р., штаб-квартира його розташована в м. Ліоні (Франція). Вищим керівним органом Інтерполу є Генеральна асамблея, на якій обираються робочі органи Інтерполу - Генеральний секретаріат і Виконавчий комітет. Поліцейський відділ Генерального Секретаріату через свої підвідділи підтримує зв'язки з національними центральними бюро (НЦБ) Інтерполу, організовує їхню взаємодію, надає та збирає оперативну інформацію. НЦБ Інтерполу виконує завдання координації взаємодії правоохоронних органів країни з компетентними органами зарубіжних держав щодо

ведення боротьби із злочинністю, що має транснаціональний характер або виходить за межі країни.

*Інформаційна система* - сукупність організаційних і технічних засобів для збереження та обробки інформації з метою забезпечення інформаційних потреб користувачів.

*Інформаційна безпека* – це стан захищеності інформаційного простору, що забезпечує формування та розвиток цього простору в інтересах особистості, суспільства та держави

*Інформаційна війна*: 1) дії з метою досягнення інформаційної переваги шляхом застосування заходів для експлуатування, підриву, знищення, дестабілізації і руйнування інформаційного потенціалу противника і його функцій; 2) міри з метою захисту власних інформаційних ресурсів і телекомунікаційних систем; 3) дії з метою використання інформаційних ресурсів і телекомунікаційних систем іншої сторони для досягнення цілей і інтересів, наприклад електронна війна (інформаційна війна в оборонному і військовому контексті), війна в Інтернеті (інформаційна війна в більш широкому суспільному контексті).

*Інформаційна мережа* – мережа, призначена для обробки, зберігання та передачі даних.

*Інформаційна технологія (ІТ)* – це комплекс методів і процедур, за допомогою яких реалізуються функції збирання, передавання, оброблення, зберігання та доведення до 3 користувача інформації в організаційно-управлінських системах з використанням обраного комплексу технічних засобів.

*Інформаційне забезпечення* - це: 1) комплекс організаційних, правових, технічних і технологічних заходів, засобів та методів, котрі забезпечують в процесі управління і функціонування системи інформаційні зв'язки та елементів (суб'єктів і об'єктів) шляхом оптимальної організації інформаційних масивів баз даних і знань; 2) діяльність, що організується в рамках управління, спрямована на проектування, функціонування та вдосконалення інформаційних систем, що забезпечують ефективне виконання задач управління; 3)органічна єдність роботи щодо визначення змісту, обсягів, якості інформації, необхідної для здійснення управління, а також заходів щодо раціональної організації процесів для здійснення управління, а також заходів щодо раціональної організації процесів збирання, систематизації, накопичення та обробки цієї інформації шляхом.

*Інформаційне забезпечення на досудових стадіях* - це виокремлені напрями, в яких розробка і впровадження конкретних засобів сприяє ефективному виявленню, дослідженню і фіксації джерел інформації у передбаченому законом порядку з метою формування на їх основі доказів

про обставини вчинення злочинів, методи їх встановлення та використання у кримінальному провадженні.

*Інформаційне забезпечення сфери оперативно-розшукової діяльності* виступає як необхідна передумова здійснення оперативно-тактичних заходів, що забезпечують у конкретних умовах оперативної обстановки (ситуації) успішне попередження, розкриття злочинів, розшук осіб, а також інтереси кримінального судочинства.

*Інформаційний продукт (продукція)* - створена виробником сукупність документованої інформації, відомостей, даних і знань, яка призначена для забезпечення інформаційних потреб користувача.

*Інформаційний простір (національний)* - інформаційне середовище, в якому здійснюються інформаційні процеси та інформаційні відносини щодо створення, збирання, відображення, реєстрації, накопичення, збереження, захисту і поширення інформації, інформаційних продуктів та інформаційних ресурсів, на яке розповсюджується юрисдикція держави.

*Інформаційний ресурс* – це сукупність документів в інформаційних системах.

*Інформаційні ресурси єдиної інформаційної системи МВС* - визначені групи взаємозв'язаних задокументованих одиниць інформації, які формуються і об'єднуються в автоматизованих інформаційних системах суб'єктів єдиної інформаційної системи МВС за певними ознаками.

*Інформаційно-аналітична діяльність:* 1) сукупність дій на основі концепцій, методів, засобів, нормативно-методичних матеріалів для збору, накопичення, обробки та аналізу даних з метою обґрунтування та прийняття рішень. 2) специфічний різновид інтелектуальної, розумової діяльності людини, в процесі якої внаслідок певного алгоритму послідовних дій з пошуку, накопичення, зберігання, обробки, аналізу первинної інформації утворюється нова, вторинна аналітична інформація у формі аналітичної довідки, звіту, огляду, прогнозу тощо.

*Інформаційно-аналітичне забезпечення це* – сукупність дій та заходів … для збору, нагромадження, обробки та аналізу даних на основі інформаційних технологій, у процесі реалізації якого особливої ваги набуває систематичність визначення кола питань, що виникають у процесі базової діяльності споживача інформації, їх аналіз та прогнозування тенденцій розвитку.

*Інформаційно-аналітичні документи* містять інформацію, що є підставою для прийняття певних рішень, тобто ініціюють управлінські рішення, дозволяють обирати той або інший спосіб управлінського впливу.

*Інформаційно-телекомунікаційна система* - сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле.

*Інформаційно-телекомунікаційна система «Інформаційний портал Національної поліції України»* - сукупність технічних і програмних засобів, призначених для обробки відомостей, що утворюються у процесі діяльності Національної поліції України та її інформаційно-аналітичного забезпечення.

*Інформація* - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

*Інформація з обмеженим доступом це* – відомості конфіденційного або таємного характеру, правовий статус яких передбачений діючим законодавством України, які визнані такими відповідно до встановлених юридичних процедур і право на обмеження доступу до яких надано власнику таких відомостей.

*Інформація моніторингова* - інформація, що надходить у систему управління по каналам зворотного зв'язку і відображає реакцію керованої системи на управляючі впливи.

*Кібербезпека* - безпека інформації та інфраструктури в цифровому середовищі, що її забезпечує. Кібербезпека передбачає досягнення і збереження властивостей безпеки в ресурсах організації або користувачів, що спрямовані на запобігання відповідним кіберзагрозам.

*Комплексна система захисту інформації* - взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації.

*Комп'ютерна інформація* – це текстова, цифрова, графічна чи інша інформація (дані, відомості) про осіб, предмети, події, яка існує в електронному вигляді, зберігається на відповідних електронних носіях і може використовуватися, оброблятися або змінюватися при допомозі ЕОМ (комп'ютерів).

*Комп'ютерні мережі (мережа ЕОМ)* – це об'єднання декількох комп'ютерів (ЕОМ) та комп'ютерних систем, що взаємопов'язані і розташовані на фіксованій території та орієнтовані на колективне використання загальномережевих ресурсів.

*Конфіденційною* є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень.

*Користувачі єдиної інформаційної системи МВС* - фізичні особи та уповноважені посадові особи суб'єктів єдиної інформаційної системи МВС, яким в установленому порядку надано відповідні права доступу до інформації в єдиній інформаційній системі МВС;

*Криптографічний захист інформації* - вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

*Міжнародні злочини* – суспільно небезпечні умисні посягання на життєвоважливі інтереси міжнародного співтовариства, основи існування держав і народів – міжнародний мир і міжнародну безпеку.

*Моделювання* – це метод дослідження різних явищ і процесів, вироблення варіантів управлінських рішень.

*Моніторинг* – комплекс наукових, технічних, технологічних, організаційних та інших засобів, які забезпечують систематичний контроль (стеження) за станом та тенденціями розвитку природних, техногенних та суспільних процесів.

*Надійність джерела інформації* – здатність джерела об'єктивно відтворити обставини, які стали йому відомі (відносно особи) або в ньому (з його допомогою) відобразилися (відносно речових джерел).

*Несанкціоновані дії щодо інформації в системі* - дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства.

*Обробка інформації в системі* - виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів.

*Програмне забезпечення «Акорд»* - сучасний програмний продукт, який забезпечує фіксування запису аудіо та відео судового процесу на базі якого можливе проведення відеоконференцій між сторонами та учасниками процесу.

*Режим доступу до інформації* – це передбачений правовими нормами порядок одержання, використання, поширення і зберігання інформації.

*Сервіс єдиної інформаційної системи МВС* - спеціальний програмний засіб, що забезпечує доступ користувачів єдиної інформаційної системи МВС до інформаційних ресурсів єдиної інформаційної системи МВС.

*Система інформаційного забезпечення* - це сукупність інформаційних підсистем певних обліків, побудованих з урахуванням дотримання таких вимог: наявності нормативно-правової бази; організаційно-кадрового забезпечення інформаційних підрозділів; організації підготовки та перепідготовки кадрів; наявності

відповідних технічних, програмних та телекомунікаційних технологій; матеріально-технічного та фінансового забезпечення.

*Система обробки даних* – комплекс технічних і математичних засобів, що виконує автоматизовану обробку даних.

*Суб'єкти єдиної інформаційної системи МВС* - апарат МВС та його територіальні органи з надання сервісних послуг МВС, Національна гвардія, заклади, установи і підприємства, що належать до сфери управління МВС, центральні органи виконавчої влади, діяльність яких спрямовується і координується Кабінетом Міністрів України через Міністра внутрішніх справ, інші державні органи, які обробляють інформацію в єдиній інформаційній системі МВС для реалізації своїх повноважень;

*Телекомунікаційна система* - сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

*Технічний захист інформації* - вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.

*Технології* – під поняттям технології ми розуміємо загальні знання та опанування засобами, необхідними для виконання якогось ремесла, мистецтва і т.ін. Технології переносять принципи на робочий ґрунт. Їх застосування забезпечує більш легке, швидке, впевнене, більш точне досягнення цілей.

*Функціональні підсистеми єдиної інформаційної системи МВС* – це сукупність технічних засобів та програмних комплексів, які автоматизують службові процеси суб'єктів єдиної інформаційної системи МВС до рівня стандартів операційних процедур та автоматизованого робочого місця користувача, забезпечують формування, зберігання, спільне використання і верифікацію інформаційних ресурсів єдиної інформаційної системи МВС.

## РЕКОМЕНДОВАНА ЛІТЕРАТУРА

### Базова


1. Конституція України від 28 червня 1996 року № 254к/96. URL: https://zakon.rada.gov.ua
2. Кримінальний кодекс України від 05.04.2001 № 2341-14. URL: http://zakon.rada.gov.ua/laws
3. Кримінальний процесуальний кодекс України від 13.04.2012 № 4651-VI URL: https://zakon.rada.gov.ua/laws
4. Кодекс України про адміністративні правопорушення 07.12.1984р. №8073–X URL: http://zakon.rada.gov.ua/laws
5. Цивільний кодекс України від 16. 01.2003р. № 435-IV URL: http://zakon.rada.gov.ua/laws
6. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 01.08.2016 № 80/94-ВР. URL:https://zakon.rada.gov.ua/laws
7. Закон України «Про інформацію» від 02.10.1992 № 2657-12. URL: http://zakon.rada.gov.ua/laws
8. Закон України « Про хмарні послуги» від 17.02.2022 **№** 2075-IX**.** URL: https://zakon.rada.gov.ua/laws
9. Закон України «Про захист персональних даних» від 01.06.2010 № 742297-17. URL: http://zakon.rada.gov.ua/laws
10. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017. № 2163- VIII. URL: http://zakon.rada.gov.ua/laws
11. Указ Президента України «Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України» від 27 січня 2016 р., № 96/2016. URL: http://zakon.rada.gov.ua.
12. Указ Президента України «Про Національний координаційний центр кібербезпеки» від 07.06.2016 № 242/2016. URL: http://zakon.rada.gov.ua.
13. Указ Президента України «Про Стратегію національної безпеки України» від 06.05.2015 № 287/2015. URL: http://zakon.rada.gov.ua.


### Допоміжна


1. Актуальні питання інформаційного права: навч. посіб. /В. Г. Хахановський, О. В. Корнейко. Київ: Нац. акад. внутр. справ, 2024. 258 с.
2. Анонімність в інтернеті. Цифрові цінності: наук.-прак.посібник /авт.кол.: М.Г. Вербенський, В.О. Криволапчук, Д.В. Смерницький та ін. Київ: «Видавництво Людмила, 2022. 48 с.
3. Арістова І.В., Ткаченко В.В. Інформаційне законодавство України: проблеми адаптації до міжнародних правових стандартів: монографія. Київ, 2015. 185 с.
4. Базова безпека вашого мобільного пристрою. URL: https://deepstateua.com/bazova-biezpieka-vashogho-mobilnogho-pristroiu

5. Бурячок В.Л.,. Толубко В. Б, Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект: підручник. за заг. ред. д-ра техн. наук, професора В. Б. Толубка. К.: ДУТ, 2015.288 с
6. Виявлення та розслідування кіберзлочинів: навчально-методичний посібник / О. А. Самойленко. Одеса : 2020. 112 с.
7. Грохольський В.Л., Ісмайлов К.Ю., Форос Г.В. Науково-практичний коментар до Закону України «Про основні засади забезпечення кібербезпеки України» / за заг. ред. д. ю. н., проф. В. Л. Грохольського. Одеса. ОДУВС, 2020. 142 с.
8. Кіберзлочинність: реальна боротьба у віртуальному світі. URL: http://www.imzak.org.ua
9. Ковалів М. В., Єсімов С. С., Ярема О. Г. Інформаційне право України: навчальний посібник. Львів : Львівський державний університет внутрішніх справ, 2022. 416 с.
10. Куліш А.М., Кобзєва Т.А., Шапіро В.С. Інформаційне право України: навчальний посібник. Суми: Сумський державний університет, 2016. 108 с.
11. Куцаєв В.В., Живило Є.О., Срібний С.П., Черниш Ю.О. Розширення термінології сучасного кіберпростору. URL: mino.esrae.ru/pdf/2014/3Sm/1387.doc
12. П’ять основних загроз безпеки, з якими стикаються користувачі смартфонів. URL: https://softico.ua/uk/news/p-yat-osnovnih-zagroz-bezpeki-z-yakimi-stikayutsya-koristuvachi-smartfoniv
13. Рудь І. Закон про кібербезпеку: основні положення, оцінки експертів та розвиток вітчизняного інформаційного простору/ Україна: події, факти, коментарі. 2017. № 19. С. 42–48. URL:http://nbuviap.gov.ua
14. Форос Г.В. Правові основи захисту інформації в кіберпросторі. *Правова держава*. Одеса. № 30. 2018. С. 181-187.
15. Потій О.В., Горбенко Ю.І., Замула О.А., Ісірова К.В. Аналіз методів оцінки і управління ризиками кібер- і інформаційної безпеки URL: https://nure.ua/wp-content/uploads/2021/Scientific_editions/radio_engineering_206/3.pdf
16. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання: монографія. К.: Видавничий дім “Гельветика”, 2017. 168 с.

**Інформаційні ресурси**

1. www.rada.gov.ua – Офіційний сайт Верховної Ради України.
2. http://ippi.org.ua/ - науково-дослідний центр правової інформатики.
3. http://textbooks.net.ua – електронна бібліотека.
4. http://radnuk.info – український юридичний портал «Радник»

Науково-методичне видання

**Форос** Ганна Володимирівна

БИКОВ Ігор Олеговис

«ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ»

Навчально -методичні рекомендації до вивчення навчальної дисципліни

Для здобувачів вищої освіти освітнього ступеня «магістр» галузь знань 26 Цивільна безпека спеціальність 262 Правоохоронна діяльність
Факультету підготовки фахівців для підрозділів кримінальної поліції
Кафедра кібербезпеки та інформаційного забезпечення
факультету підготовки фахівців для підрозділів кримінальної поліції

Підп. до друку 17.05.2024. Формат 60х84/16.
Друк цифровий. Папір офсетний. Гарнітура Times.
Ум.-друк. арк. 2,56 Обл.-вид. арк. 1,95
Надруковано з готового оригінал-макету
Редакційно-видавничий відділ
Одеського державного університету внутрішніх справ
м. Одеса, вул. Успенська,1,
Свідоцтво суб'єкта видавничої справи ДП № 3507 від 25.06.2009