**КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**
**ІМЕНІ ТАРАСА ШЕВЧЕНКА**

**Навчально-науковий інститут журналістики**

Кафедра соціальних комунікацій

**«ЗАТВЕРДЖУЮ»**
Заступник декана/директора
з навчально-виховної роботи
_____ В.М. Корнєєв
«01» 08 2021 року

# РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

# ДІЇ В КІБЕРПРОСТОРІ

**для студентів**

| | |
|---|---|
| галузь знань | **06 журналістика** |
| спеціальність | 061 журналістика |
| освітній рівень | магістр |
| освітня програма | *стратегічні комунікації* |
| вид дисципліни | вибіркова |

| | |
|---|---|
| Форма навчання | денна |
| Навчальний рік | 2021/2022 |
| Семестр | 3 |
| Кількість кредитів ECTS | 3 |
| Мова викладання, навчання та оцінювання | українська |
| Форма заключного контролю | екзамен |
| Викладач: | Юрій ГАВРИЛЕЦЬ |

Пролонговано: на 2022/2023 н.р. _____ (Волобуєва А. М.) «№ 1» 30 серпня 2022 р.
(підпис, ПІБ, дата)

на 202_/202_ н.р. _____ (Волобуєва А. М.) «№__» _____ 202__р.
(підпис, ПІБ, дата)

**КИЇВ – 2021**

Розробник: Юрій ГАВРИЛЕЦЬ, к. н. із соц. ком., асистент кафедри соціальних комунікацій

ЗАТВЕРДЖЕНО
Зав. кафедри соціальних комунікацій
_____ (Юрій БОНДАР)
(підпис) (прізвище та ініціали)

Протокол № 16 від «29» червня 2021 р.

Схвалено науково-методичною комісією Інституту журналістики

Протокол від «31» серпня 2021 року

Голова науково-методичної комісії _____ (Анастасія ВОЛОБУЄВА)

«31» серпня 2021 року

# ВСТУП

**1. Мета дисципліни** – сформувати систему знань про основні загрози інформаційній безпеці, кіберзлочинність, способи протидії цим загрозам, а також про те, як висвітлюють поважні медіа проблематику кіберзлочинності.

**2. Попередні вимоги до опанування або вибору навчальної дисципліни (*за наявності*):** володіти знаннями з теорії масової комунікації, основ журналістики та розумінням природи Інтернету та онлайн-оточення в наш час.

**3. Анотація навчальної дисципліни**:

Під час навчання студенти опановують базові знання про основні дії сучасної людини у кіберпросторі. Зокрема, про основні загрози, які у цифрову добу постають перед нами. Для студентів-медійників важливо також уміти критично оцінювати журналістські матеріали про кіберзлочини у ключі дотримання професійних та етичних стандартів у висвітленні цієї проблематики.

Дисципліна покликана розвивати навички абстрактного мислення, аналізу та синтезу, конкретизувати розуміння комунікаційної мети в кіберпросторі, виявляти та вирішувати проблеми в реалізації медіапроєктів, присвяченим кіберзлочинам, проводити дослідницьку та/або інноваційну діяльність, а також точно і зрозуміло доносити власні висновки.

**4. Завдання (навчальні цілі)**:

- сформувати поняття про дії людини в кіберпросторі як основу життя та роботи сучасної цифрової людини;
- опанувати базові знання про різновиди кіберзлочинів, їхню еволюцію та їхній вплив на появу, скажімо, антивірусної галузі як критично важливого елемента у системі протидії кіберзлочинності;
- здатність усебічно аналізувати журналістські матеріали про кіберзлочини, пояснювати сильні та слабкі сторони кожного матеріалу у контексті дотримання професійних стандартів журналістики;
- розуміння сучасних механізмів інформаційних шпигунства, тероризму та війни та особливості ведення цих видів діяльності в Інтернеті.

***5. Результати навчання за дисципліною:***

| **Результат навчання (1. знати; 2. вміти; 3. комунікація; 4. автономність та відповідальність)** | | **Форми (та/або методи і технології) викладання і навчання** | **Методи оцінювання та пороговий критерій оцінювання (за необхідності)** | **Відсоток у підсумковій оцінці з дисципліни** |
|---|---|---|---|---|
| **Код** | **Результат навчання** | | | |
| *1.1* | *Розуміти історичний контекст виникнення кіберзлочинів та основних стадій їх еволюції.* | *Лекції, семінарські заняття* | *Модульна робота 1* | *10* |
| *1.2* | *Знати основні види кіберзлочинів та їхні особливості.* | *Лекції, семінарські заняття, самостійна робота* | *Залік* | *10* |
| *1.3* | *Знати механізм здійснення шпигунства, тероризму та комунікативної війни в Інтернеті.* | *Лекції, семінарські заняття* | *Модульна робота 2* | *10* |
| *2.1* | *Вміти всебічно аналізувати журналістські матеріали про кіберзлочини.* | *Семінарські заняття* | *Модульна робота 3* | *10* |

| | | | | |
|---|---|---|---|---|
| *2.2* | *Вміти визначати фахову основу кожного журналістського матеріалу про кібез-злочини.* | *Семінарські заняття* | *Залік* | *20* |
| *3.1* | *Презентувати результати проведеного проєкту в колективі (робота над порівняльним аналізом двох журналістських розслідувань про кіберзлочини).* | *Самостійна робота* | *Презентація* | *15* |
| *3.2* | *Вміння аргументовано відстоювати висновки власного проєкту.* | *Семінарські заняття* | *Презентація* | *15* |
| *4* | *Критично оцінювати й аналізувати джерела, в яких викладені різні стратегії донесення інформації про кіберзлочини, використовувати здобуті знання у професійній діяльності.* | *Семінарські заняття* | *Залік* | *10* |
| | *Разом* | | | *100%* |

***6. Співвідношення результатів навчання дисципліни із програмними результатами навчання*** *(необов'язково для вибіркових дисциплін які не входять до блоків спеціалізації)*

| **Результати навчання дисципліни (код) Програмні результати навчання (назва)** | **1.1** | **1.2** | **1.3** | **1.4** | **2.1** | **2.2** | **2.3** | **3.1** | **4** |
|---|---|---|---|---|---|---|---|---|---|
| *ПРН3 Писати рецензію на новий інформаційний продукт та/або інноваційний проєкт.* | + | | + | + | + | | | | |
| *ПРН9 Демонструвати здатність знаходити замовників на проведення дослідження чи розробку стратегічних проєктів* | | + | + | | | | + | + | |
| *ПРН16 Писати звіт про роботу медійного колективу з викладенням пропозицій щодо поліпшення професійної діяльності стратегічних аналітиків та експертів у медіа* | | + | | + | | + | | | + |

**7. Схема формування оцінки.**

**7.1 Форми оцінювання студентів:**

**- семестрове оцінювання:**

| | **ЗМ-1, 2** | |
|---|---|---|
| | Min. 36 – балів | Max. 60 − балів |
| Усна відповідь, участь в обговоренні<br>Семінари 1–5 оцінюються в 5 балів | 5x4=20<br>1x4=4 | 8x5=40 |
| Підсумковий проєкт (самостійна робота) | 12 | 20 |

**- підсумкове оцінювання:**

- форма оцінювання – екзамен;
- максимальна кількість балів, які може отримати студент – 40 балів;

**- умови допуску до екзамену:**

за виконання навчальної програми (оцінювання аудиторних завдань і самостійної роботи) студент має отримати впродовж семестру не менше 36 балів. Мінімальна кількість балів за екзамен, які додаються до семестрових – 24 бали.

Студент, який набрав сумарно меншу кількість балів, ніж критично-розрахунковий мінімум 36 балів, до складання екзамену не допускається.

Студент, який пропустив семінарське заняття, але виконав самостійну роботу, може отримати максимум 5, а не 8 балів за цей семінар (у розрахунку за семестр щонайбільше виходить 25 балів замість 40). Бали за невиконаний підсумковий проєкт не компенсуються. Для всіх студентів обов'язковим для отримання екзамену є виконання і презентація результату самостійної роботи (підсумкового проєкту) — порівняльного аналізу 2-х журналістських розслідувань про кіберзлочини.

| | Змістовий модуль 1 | Змістовий модуль 2 | Екзамен | Підсумкова оцінка |
|---|---|---|---|---|
| Мінімум | 18 | 18 | 24 | 60 |
| Максимум | 30 | 30 | 40 | 100 |

**7.2 Організація оцінювання:**

Дисципліна поділена на 2 змістові модулі (частини). Кожен змістовий модуль включає в себе лекції, семінарські заняття та самостійну роботу студентів, які завершуються рейтинговим контролем рівня засвоєння знань програмного матеріалу відповідної частини курсу та певних професійно-дослідницьких навичок. У змістовий модуль 1 (ЗМ1) входять теми 1-2 (семінари 1-2), у змістовий модуль 2 (ЗМ2) – теми 3–5 (семінари 3–5).

Оцінювання успішності знань студентів здійснюється у двох формах: семестрове оцінювання (семінарські заняття, тести, самостійна робота) і підсумкове оцінювання (екзамен). Успішне виконання завдань за семестр (семінари, самостійна робота) передбачає отримання за роботу не менше 60 % від максимальної оцінки.

**Самостійна робота – підсумковий проєкт** «Порівняльний аналіз 2-х журналістських розслідувань про кіберзлочини». У цьому проєкті метою є виявити переваги та недоліки у професійності висвітлення кіберзлочинів. Бажано порівнювати матеріали, які висвітлюють схожі злочини.

**Оцінювання проєкту:** максимальна кількість балів – 20, що складаються з таких компонентів:

а) повнота фактів - 5 балів; низька повнота – 3 бали.

б) грамотність (граматика, пунктуація, стилістика) – 5 балів; Якщо більше 5 помилок – проєкт НЕ оцінюється;

в) аналітична аргументованість – 5 балів; мінімальна аргументованість – 3 бали.

г) вчасне подання роботи – 5 балів, невчасне подання роботи – 3 бали.

Усі семестрові роботи (семінари, самостійна робота) мають бути подані на кафедру або, за домовленістю з викладачем, надсилатися на електронну пошту в робочий час. На перевірку роботи викладачеві дається один робочий тиждень. Якщо студент із поважної причини пропустив семінар, то він має право його відпрацювати впродовж 14 календарних днів з моменту проведення семінару.

## 7.3 Шкала відповідності оцінок

| | |
|---|---|
| **Відмінно** / Excellent | 90-100 |
| **Добре** / Good | 75-89 |
| **Задовільно** / Satisfactory | 60-74 |

| | |
|---|---|
| **Незадовільно** / Fail | 0-59 |
| **Зараховано** / Passed | 60-100 |
| **Не зараховано** / Fail | 0-59 |

**8. Структура навчальної дисципліни. Тематичний план лекцій і семінарських занять**

| № п/п | Назва теми | Кількість годин | | |
|---|---|---|---|---|
| | | лекції | семінари | Самостійна робота |
| ***Частина 1.*** **Загальні питання інформаційної безпеки** | | | | |
| 1 | **Тема 1.** *Безпека та конфіденційність користувача в мережі.* | 2 | 2 | 8 |
| 2 | **Тема 2.** *Війна в кіберпросторі: сучасні стратегії і тактики.* | 2 | 2 | 8 |
| ***Частина 2.*** **Види інформаційних загроз та способи їм протидіяти** | | | | |
| 1 | **Тема 3.** *Комп'ютерні віруси та специфіка антивірусних програм: як висвітлюються в медіа.* | 2 | 2 | 8 |
| 2 | **Тема 4.** *Кібершпигунство та кібертероризм.* | 2 | 2 | 8 |
| 4 | **Тема 5.** *Даркнет та безпека електронних фінансів.* | 2 | 2 | 8 |
| | Підсумковий проєкт – порівняльний аналіз 2-х журналістських розслідувань про кіберзлочини. | | | 30 |
| | | | | |
| | **ВСЬОГО** | **10** | **10** | **70** |

**Загальний обсяг *90** год.,* в тому числі:
Лекцій **– *10** год.*
Семінари **– *10** год.*
Самостійна робота **- *70** год.*

**9. Рекомендовані джерела:**

***Основна:** (Базова)*


1. Митник, К. (2019). Мистецтво залишатись непоміченим. Хто ще читає ваші імейли? Київ: Наш Формат.
2. Гудмен, М. (2019). Злочини майбутнього. Київ: Наш Формат.
3. Senker, C. (2017). Cybercrime and the Darknet. London, UK: Arcturus.


***Додаткова:***


4. Смаль, Ю. (2019). Як я була ботом. Київ: Комора.
5. Бороган, И., Солдатов, А. (2016). Битва за Рунет: Как власть манипулирует информацией и следит за каждым из нас. Москва: Альпина Паблишер.
6. Рекомендації. Департамент Кіберполіції МВС України. https://cyberpolice.gov.ua/articles/.
7. Marks, J. (September, 28). The Cybersecurity 202: Here are five big things election experts are really worried about. Washington Post. https://www.washingtonpost.com/politics/2020/09/28/cybersecurity-202-here-are-five-big-things-election-experts-are-really-worried-about/.
8. Carns, A. (September, 11, 2020). Who Gets Hurt When the World Stops Using Cash. New York Times. https://www.nytimes.com/2020/09/11/your-money/cash-credit-cards-coronavirus.html.