**Силабус освітнього компонента**
Програма навчальної дисципліни

# Методи та технології інформаційних війн

**Шифр та назва спеціальності**
F5 – Кібербезпека та захист інформації

**Інститут**
ННІ комп`ютерних наук та інформаційних технологій

**Спеціалізація**

**Кафедра**
Кібербезпеки (328)

**Освітня програма**
Кібербезпека

**Тип дисципліни**
Вибіркова

**Рівень освіти**
Перший (бакалаврський)

**Форма навчання**
Денна, заочна

**Семестр**
4

**Мова викладання**
Українська, англійська

## Викладачі, розробники


**ЄВСЕЄВ Сергій Петрович**

serhii.yevseiev@khpi.edu.ua
Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».

Лауреат національної премії імені Бориса Патона.
Кількість наукових публікацій: понад 351, з них патентів на корисну модель 44, 11 монографій, з яких 10 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 149 статтей у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus, гарант освітньо-професійної програми "Кібербезпека" першого (бакалаврського) рівня вищої освіти.

Детальніше про викладача на сайті кафедри

## Загальна інформація

### Анотація

Навчальна дисципліна "Методи та технології інформаційних війн" є вибірковою навчальною дисципліною. Дисципліна досліджує проблематику забезпечення національного суверенітету держави внаслідок розгортання інформаційних війн, насамперед у глобальному інформаційному просторі. Це зумовлює необхідність створення ефективної системи забезпечення інформаційної безпеки людини, суспільства та держави.

## Мета та цілі дисципліни

Оволодіння студентами комплексом знань в області інформаційного впливу на масову свідомість, ознайомлення з теорією та практикою інформаційних війн, принципами захисту від них, вивчення інструментів і чинників руйнування свідомості громадян і суспільств в цілому. Формування професійної компетентності майбутніх фахівців з національної безпеки у сфері кіберзахисту, достатньої для подальшої роботи за фахом та необхідної для розвитку кар'єри.

## Формат занять

Лекції, лабораторні заняття, самостійна робота, консультації. Підсумковий контроль – диференційований залік.

## Компетентності

ЗК1. Здатність застосовувати знання у практичних ситуаціях.
ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.
ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово.
ЗК4. Здатність спілкуватися іноземною мовою.
ЗК5. Здатність вчитися і оволодівати сучасними знаннями.
ЗК6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
ЗК7. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.
СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.

## Результати навчання

РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.
РН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.
РН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.
РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.
РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.
РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення та передачі сигналів тощо, принципи, методи і поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.
РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.
РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
РН17. Забезпечувати функціонування системи управління кібербезпекою та захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.

### Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 16 год., лабораторні роботи – 32 год., самостійна робота – 72 год.

### Передумови вивчення дисципліни (пререквізити)

Вища математика, Фізичні основи технічних засобів розвідки.

### Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проєкти, майстер-класи.

## Програма навчальної дисципліни

### Навчальні заняття

#### Лекції

| Теми лекцій | Кількість годин |
|---|---|
| **Тема 1. Розвиток інформаційно-комунікаційних технологій та історія інформаційних конфліктів.** Еволюція інформаційно-комунікаційних технологій. Приклади інформаційних воєн XX – початку XXI століття. | 2 |
| **Тема 2. Теоретичні основи інформаційної війни: методологія, моделі та понятійний апарат.** Базові моделі інформаційних воєн у соціальних мережах. Методологічні засади та ключові поняття сучасних інформаційних конфліктів. | 2 |
| **Тема 3. Нормативно-правове регулювання інформаційної безпеки в Україні.** Аналіз українського законодавства у сфері інформаційної політики та безпеки: прямі та опосередковані нормативно-правові акти. | 2 |
| **Тема 4. Планування інформаційних операцій: стратегія, тактика та психотехнології.** Стратегічне й тактичне планування інформаційних процесів. Формування меседжів для інформаційних кампаній. Використання сучасних психотехнологій у протистояннях. | 2 |
| **Тема 5. Ідеологія та психологія інформаційної війни в онлайн-середовищі.** Психологічні механізми впливу на суспільство. Алгоритмізація та формалізація процесів інформаційних атак. Умови реалізації інформаційних операцій. | 2 |
| **Тема 6. Інструменти та технології ведення інформаційної війни у соціальних мережах.** Типологія інформаційних операцій у форматі Web 2.0 та 3.0. Використання інтернет-реклами, мобільних технологій та інших засобів як інструментів інформаційної атаки. | 2 |
| **Тема 7. Методи оцінки ефективності та моніторинг інформаційних процесів.** Методи аналізу та оцінки ефективності інформаційних процесів. Інструменти базового моніторингу, соціологічні опитування та експрес-методи оцінки в онлайн-середовищі. | 2 |

| | |
|---|---|
| **Тема 8. Гібридні війни та мережеві проекти в інформаційних операціях.** Роль соціальних мереж та інтернет-технологій у гібридних війнах. Структура та функціонування мережевих проєктів. Використання медіа-вірусів як інформаційної зброї. | 2 |
| **Загальна кількість годин** | **16** |

## Лабораторні заняття

| Теми лабораторних занять | Кількість годин | Вагові коефіцієнти $a$ |
|---|---|---|
| **Тема 1. Еволюція форм та методів ведення інформаційної війни.** Вивчення історії розвитку ведення інформаційної війни. | 4 | 0,1 |
| **Тема 2. Інформаційна війна: сутність, засоби реалізації, результати та можливості протидії.** Вивчення досвіду ведення сучасних інформаційних війн (на прикладі російської експансії в український простір). | 4 | 0,1 |
| **Тема 3. Сучасні інформаційні он-лайн мережеві війни.** Вивчення особливостей ведення сучасної інформаційної он-лайн мережевої війни. | 4 | 0,1 |
| **Тема 4. Ведення інформаційної війни у соціальних он-лайн мережах.** Вивчення базових прийомів в інформаційних війнах на прикладі україно-російського протистояння. | 4 | 0,1 |
| **Тема 5. Оцінка ефективності інформаційних процесів в інтернет-просторі.** Вивчення методів та засобів моніторингу ситуації в інтернет-просторі. | 4 | 0,1 |
| **Тема 6. Моніторинг та ідентифікація достовірності контенту в мережі Інтернет та соціальних он-лайн мережах.** Вивчення процесу моніторингу та ідентифікації достовірності контенту в мережі Інтернет та соціальних он-лайн мережах. | 4 | 0,1 |
| **Тема 7. Інноваційні засоби ведення гібридних війн.** Вивчення інноваційних засобів ведення гібридних війн на прикладі сучасних конфліктів. | 4 | 0,1 |
| **Тема 8. Он-лайн мережеві проекти.** Вивчення процесу розробки інформаційних он-лайн мережевих проектів. | 4 | 0,1 |
| **Загальна кількість годин** | **32** | $\sum_{i=1}^{n} a_i = 0{,}8$ |

## Контрольні роботи

| Теми контрольних робіт | Вагові коефіцієнти $b$ |
|---|---|
| **Тема 1. Теоретичні основи та правові аспекти інформаційних війн.** Робота передбачає вивчення історії виникнення та розвитку інформаційних воєн, аналіз основних понять і моделей, а також розгляд правових аспектів | 0,1 |

| | |
|---|---|
| інформаційної безпеки в Україні та світі. | |
| **Тема 2. Методи та технології ведення інформаційних війн.** Робота орієнтована на аналіз сучасних технологій і тактик інформаційних операцій, використання соціальних мереж та інтернет-ресурсів, методи психологічного впливу, а також оцінку ефективності й моніторинг інформаційних процесів у контексті гібридних воєн. | 0,1 |
| **Загалом** | $\sum_{i=1}^{m} b_i$=0,2 |

### Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

**Опрацювання теоретичного матеріал**

| Теми для самостійного вивчення | Кількість годин |
|---|---|
| **Тема 1. Історія інформаційних війн у XX – поч. XXI ст.** Дослідження ключових інформаційних конфліктів і ролі медіа у їх перебігу. | 8 |
| **Тема 2. Понятійний апарат інформаційної війни.** Основні терміни, моделі та методологічні підходи до вивчення інформаційних протистоянь. | 8 |
| **Тема 3. Законодавча база України у сфері інформаційної політики.** Аналіз нормативно-правових актів, що регулюють питання інформаційної безпеки. | 7 |
| **Тема 4. Стратегії та тактики ведення інформаційних операцій.** Методи створення та поширення меседжів у мас-медіа та соціальних мережах. | 7 |
| **Тема 5. Психологічні методи впливу в інформаційних війнах.** Техніки маніпуляції свідомістю, створення фейкових наративів і пропаганди. | 7 |
| **Тема 6. Соціальні мережі як інструмент інформаційної війни.** Використання Facebook, Instagram, TikTok, X (Twitter) для поширення впливу. | 7 |
| **Тема 7. Інформаційні операції у форматі Web 2.0 та 3.0.** Особливості застосування нових інтернет-технологій у сучасних конфліктах. | 7 |
| **Тема 8. Методи оцінки ефективності інформаційних кампаній.** Моніторинг інформаційного простору, аналітичні інструменти та опитування. | 7 |
| **Тема 9. Фейки, дезінформація та deepfake-технології.** Технології створення неправдивого контенту та способи їх ідентифікації. | 7 |
| **Тема 10. Медіа-віруси як зброя інформаційної війни.** Механізми створення, поширення та вплив на масову свідомість. | 7 |
| **Загальна кількість годин** | **72** |

## Неформальна освіта

Здобувач має можливість перезарахувати окремі теми або курс шляхом: проходження професійних курсів чи тренінгів, онлайн-освіти, професійних стажувань, у сфері, що відповідає навчальним цілям дисципліни.
Для зарахування необхідно надати: сертифікат (електронний або друкований) про проходження курсу/стажування, опис програми тренінгу із зазначенням змісту тем, обсягу та тривалості.

### Рекомендовані курси, тренінги, стажування

За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

## Література, навчальні матеріали та інформаційні ресурси

### Основна література


1. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. Дата оновлення: 31.12.2023. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
2. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. Дата оновлення: 27.10.2022. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
3. Сучасні інформаційні війни в мережевому он-лайн просторі: навчальний посібник / О.В.Курбан. – Київ: ВІКНУ, 2016. – 286 с.
http://www.interinf.chnu.edu.ua/res//interinf/Inf%20vijny.pdf
4. Бебік В.М. Інформаційно-комунікаційний менеджмент у глобальному суспільстві: психологія, технології, техніка паблік рілейшнз: монографія / В.М. Бебік. – Київ: МАУП, 2005. – 440 с.
https://kpdi.edu.ua/biblioteka/%D0%86/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE-%D0%BA%D0%BE%D0%BC%D1%83%D0%BD%D1%96%D0%BA%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B8%D0%B9%20%D0%BC%D0%B5%D0%BD%D0%B5%D0%B4%D0%B6%D0%BC%D0%B5%D0%BD%D1%82%20%D0%91%D0%B5%D0%B1%D0%B8%D0%BA%20%D0%92.%D0%9C..pdf
5. Березовец Т. Анексія: Острів Крим. Хроніки «гібридної війни» / Т.Березовець. – Київ: Брайт Стар Паблішінг, 2015. – 392 с.
http://resource.history.org.ua/item/0010325
6. Васютинський В.О. Психологічні виміри спільноти: монографія / В.О. Васютинський. – Київ: Золоті ворота, 2010. – 119 с.
https://www.ispp.org.ua/backup_ispp/1426077022.pdf
7. Вєдєнєєв Д.В. Гострі когті орла. Сили спеціальних операцій США: історія та сучасність: монографія / Д.В. Вєдєнєєв, Г.С. Биструхін, А.І.Семука. – Київ: К.І.С., 2010. – 400 с.
https://issuu.com/pubkis/docs/gostri_kihti_orla


### Додаткова література


8. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements URL:
https://www.iso.org/ru/contents/data/standard/08/28/82875.html
9. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls URL:
https://www.iso.org/ru/contents/data/standard/08/05/80585.html
10. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection – Guidance on managing information security risks. URL:
https://www.iso.org/ru/contents/data/standard/08/05/80585.html.


## Система оцінювання

Підсумкова оцінка з освітнього компонента визначається відповідальним лектором за темами, видами занять, тощо у відповідності до силабусу і є інтегральною оцінкою результатів усіх вид навчальної діяльності здобувача вищої освіти. Підсумкова оцінка повинна відображати всі оцінки за складовими навчального процесу з урахуванням їх вагових показників $k$:

| Поточний контроль (практичні, семінарські, лабораторні заняття), $k_1$ | Контрольні роботи (за наявності), $k_2$ | Індивідуальне завдання (за наявності), $k_3$ | Підсумковий контроль (для ОК з іспитом), $k_4$ |
|---|---|---|---|

| | |
|---|---|
| 0,8 | 0,2 |

Сума коефіцієнтів повинна складати одиницю: $k_1 + k_2 + k_3 + k_4 = 1$. Підбір вагових коефіцієнтів підсумкової оцінки здійснює розробник курсу.
Розрахунок підсумкової оцінки проводиться за формулою:

$$О = П \cdot k_1 + K \cdot k_2 + І \cdot k_3 + Пк \cdot k_4$$

де: П – середньозважена середня оцінка за поточний контроль
І – оцінка за виконання індивідуального завдання
$K$ – середньозважена оцінка за контрольні роботи
Пк – оцінка за підсумковий контроль

$$П = \frac{П_1 \cdot a_1 + П_2 \cdot a_2 + ... + П_n \cdot a_n}{\sum_{i=1}^{n} a_i}$$

де: $a_i$ - ваговий коефіцієнт за кожне практичне (семінарське) або лабораторне заняття.

$$K = \frac{K_1 \cdot b_1 + K_2 \cdot b_2 + ... + K_m \cdot b_m}{\sum_{i=1}^{m} b_i}$$

де: $b_i$ - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (П, $K$, І,... ) виставляються за 100-бальною шкалою згідно з положенням «Про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої освіти» НТУ «ХПІ».

Підсумкова оцінка виставляється відповідно до розрахованої О з округленням до найближчого цілого числа в більшу сторону.

**Шкала оцінювання**

| Сума балів | Національна оцінка | ECTS |
|---|---|---|
| 90–100 | Відмінно | A |
| 82–89 | Добре | B |
| 75–81 | Добре | C |
| 64–74 | Задовільно | D |
| 60–63 | Задовільно | E |
| 35–59 | Незадовільно (потрібне додаткове вивчення) | FX |
| 1–34 | Незадовільно (потрібне повторне вивчення) | F |

## Норми академічної етики і політика курсу

Здобувач вищої освіти повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту.
Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

## Погодження

Силабус погоджено 30.08.2025

**Завідувач кафедри**
Сергій ЄВСЕЄВ

30.08.2025

**Гарант ОП**
Сергій ЄВСЕЄВ