



Силабус освітнього компонента

Програма навчальної дисципліни



Методи та технології інформаційних війн

Шифр та назва спеціальності

256 – Національна безпека (за окремими сферами забезпечення і видами діяльності)

Інститут

ННІ комп'ютерних наук та інформаційних технологій

Освітня програма

Національна безпека у сфері кіберзахисту

Кафедра

Кібербезпеки (328)

Рівень освіти

Бакалавр

Тип дисципліни

Профільна підготовка, Вибіркова

Семестр

4

Мова викладання

Українська

Викладачі, розробники



ЄВСЕЄВ Сергій Петрович

serhii.yevseyev@khpi.edu.ua

Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 350, з них патентів на корисну модель 42, 17 монографій, з яких 9 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 163 статті у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Менеджмент інформаційної безпеки», «Введення в мережі», «Безпека банківських систем», «Гібридні війни та національна безпека», «Аудит та моніторинг корпоративних мереж», «Blockchain: основи та приклади застосування», «Основи смарт-контрактів», «Основи кібербезпеки» у студентів бакалавріата та магістратури, Розділ «Методи і технології моніторингу та аудиту інформаційної безпеки», «Методи побудови постквантових криптосистем», «Новітні технології забезпечення кібербезпеки на основі технології блокчейн» для аспірантів.

[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 роботи, самостійна робота, консультації. Підсумковий контроль – залік.

Компетентності

КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу.

КЗ-7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ФК-2. Здатність аналізувати виклики та загрози національній безпеці за напрямками професійної діяльності, синтезувати інформацію щодо розроблення та реалізації елементів стратегій у визначальних сферах національної безпеки (політичній, економічній, соціальній, гуманітарній).

ФК-5. Здатність використовувати історичний досвід військових та політичних стратегій іноземних держав з метою вирішення завдань з національної безпеки.

ФК-6. Здатність використовувати іноземну мову для отримання додаткових знань і умінь з питань національної безпеки, взаємодіяти з іноземними партнерами.

ФК-7. Здатність визначати необхідні правові та організаційні заходи врегулювання конфліктів, пов'язаних із забезпеченням національної безпеки.

ФК-8. Здатність використовувати механізми забезпечення національної безпеки у її визначальних сферах.

ФК-9. Здатність використовувати знання щодо безпекової складової зовнішньої політики України та інших держав.

ФК-10. Здатність засвоювати основні теоретичні поняття та набуття практичних навичок дослідження, підготовки документів та їх використання в управлінській діяльності.

ФК-11. Здатність використовувати практичні навички, тактику та прийоми роботи з людьми в інтересах службової діяльності.

ФК-12. Здатність виконувати заходи територіальної оборони, а також цивільного захисту у межах професійної компетентності.

ФК-13. Здатність оцінювати вплив глобальних проблем і трансформацій геополітичного та гео економічного простору на національну безпеку.

ФК-14. Здатність здійснювати моніторинг зовнішньої та внутрішньої політики держави у контексті забезпечення національної безпеки, готувати пропозиції щодо підвищення її ефективності.

Результати навчання

ПРН-3. Вміти за допомогою абстрактного мислення, аналізу та синтезу оцінювати результати професійної діяльності та забезпечувати її якість, бути критичним і самокритичним, наполегливим щодо поставлених завдань і взятих зобов'язань.

ПРН-5. Вільно спілкуватися іноземною мовою у межах потреби своєї професійної діяльності.

ПРН-7. Вміти виявляти, ставити та вирішувати професійні завдання, вміти узагальнювати отримані результати, обробляти та аналізувати інформацію з різних джерел, оформлювати і презентувати результати досліджень відповідно до вимог.

ПРН-8. Вміти використовувати інформаційні та комунікаційні технології і на цій основі формувати ефективні системи інформаційно-аналітичного забезпечення підтримки прийняття рішень щодо запобігання, протидії та нейтралізації загроз національній безпеки.

ПРН-10. Вміти аналізувати виклики та загрози національній безпеці за напрямками професійної діяльності та синтезувати інформацію щодо розроблення та реалізації стратегій у визначальних сферах національної безпеки (політичній, економічній, соціальній, гуманітарній).

ПРН-12. Вміти застосовувати знання з основ теорії національної безпеки, зокрема: оцінювати обстановку, рівень викликів та загроз національній безпеці.

ПРН-13. Вміти використовувати історичний досвід військових та політичних стратегій іноземних держав з метою вирішення завдань з національної безпеки.

ПРН-14. Вміти читати й розуміти фахову іншомовну літературу, використовуючи її у соціальній і професійній сферах, а також демонструвати культуру мислення та виявляти навички щодо організації культурного діалогу з іноземними партнерами на рівні, необхідному для професійної діяльності.

ПРН-15. Вміти визначати необхідні правові та організаційні заходи врегулювання конфліктів, пов'язаних із забезпеченням національної безпеки.

ПРН-16. Використовувати у професійній діяльності окремі елементи механізму впливу та взаємодії у процесі забезпечення окремих складових національної безпеки.

ПРН-17. Вміти використовувати отримані знання щодо безпекової складової зовнішньої політики України та інших держав.

ПРН-18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.

ПРН-19. Вміти використовувати у професійній діяльності методи та інструменти організації соціальної взаємодії, співробітництва та розв'язання конфліктів у сфері професійної діяльності, практичні навички, тактику та прийоми, роботи з людьми в інтересах службової діяльності: працювати у команді з позицій лідера, радника (консультанта), помічника, планувати використання часу та визначати стимули і бар'єри ефективної роботи, здійснювати розподіл (делегування) функцій, повноважень і відповідальності між виконавцями.

ПРН-20. Вміти виконувати заходи територіальної оборони, а також цивільного захисту у межах професійної компетентності.

ПРН-21. Вміти оцінювати вплив глобальних проблем і трансформацій геополітичного та гео економічного простору на національну безпеку, здійснювати моніторинг зовнішньої та внутрішньої політики держави у контексті забезпечення національної безпеки та готувати пропозиції щодо підвищення її ефективності.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 32 год., лабораторні роботи – 16 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 проекти, майстер-класи.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Розвиток інформаційно-комунікаційних технологій у форматі історії інформаційних конфліктів.

Історія розвитку інформаційно-комунікаційних технологій. Інформаційні війни XX - поч. XXI ст.

Тема 2. Теорія інформаційної війни: методологія та понятійний апарат.

Базова модель теорії сучасної інформаційної війни у соціальних он-лайн мережах. Методологічна основа сучасної інформаційної війни у соціальних он-лайн мережах.

Тема 3. Українське законодавство в галузі інформаційної політики та безпеки.

Нормативно-правові акти, що прямо регулюють питання інформаційної безпеки. Нормативно-правові акти, що опосередковано регулюють питання інформаційної безпеки.

Тема 4. Стратегічне та тактичне планування інформаційних протистоянь.

Стратегічний рівень планування інформаційних процесів. Основи тактики планування інформаційних процесів.

Тема 5. Ідеологічні аспекти та психологія сучасної інформаційної он-лайн мережевої війни.

Ідеологія та процеси створення меседжів в інформаційних кампаніях. Сучасні психотехнології в он-лайн інформаційних війнах. Алгоритмізація та формалізація процесів. Структура та ключові умови реалізації інформаційних операцій.

Тема 6. Базові прийоми та інструменти ведення інформаційної війни у соціальних он-лайн мережах.

Загальна характеристика сучасного інтернет-простору. Типологія та класифікація інформаційних операцій формату web 2.0 та 3.0. Базові прийоми в інформаційних війнах. Інтернет-реклама та її застосування в інформаційній війні. Використання мобільних засобів зв'язку як інструмента інформаційної атаки.

Тема 7. Базові методи та засоби оцінки ефективності інформаційних процесів в інтернет-просторі.

Сучасні методи та засоби аналізу інформаційних процесів. Базові методи та засоби оцінки ефективності інформаційних процесів в інтернет-просторі. Методи базового моніторингу. Засоби експрес-опитування у соціальних мережах.

Тема 8. Моніторинг та ідентифікація достовірності контенту в мережі Інтернет та соціальних он-лайн мережах.

Моніторинг та ідентифікація достовірності інформаційного контенту. SMM-аудит.

Тема 9. Соціальні он-лайн мережі в системі сучасних форматів ведення війни.

Гібридна війна: структура та базові прийоми. Сучасні інноваційні засоби ведення гібридних війн. Сучасні інноваційні засоби ведення гібридних війн. Інтернет-технології та соціальні он-лайн мережі в структурі гібридної війни.

Тема 10. Мережеві он-лайн проекти в гібридній війні: структура та принципи функціонування.

Формат та специфіка он-лайн мережевих проектів. Методи та засоби управління проектами. Медіа-віруси та їх використання як інформаційної зброї.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Еволюція форм та методів ведення інформаційної війни.

Вивчення історії розвитку ведення інформаційної війни.

Тема 2. Інформаційна війна: сутність, засоби реалізації, результати та можливості протидії.

Вивчення досвіду ведення сучасних інформаційних війн (на прикладі російської експансії в український простір).

Тема 3. Сучасні інформаційні он-лайн мережеві війни.

Вивчення особливостей ведення сучасної інформаційної он-лайн мережевої війни.

Тема 4. Ведення інформаційної війни у соціальних он-лайн мережах.

Вивчення базових прийомів в інформаційних війнах на прикладі україно-російського протистояння.

Тема 5. Оцінка ефективності інформаційних процесів в інтернет-просторі.

Вивчення методів та засобів моніторингу ситуації в інтернет-просторі.

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.

Тема 7. Інноваційні засоби ведення гібридних війн.

Вивчення інноваційних засобів ведення гібридних війн на прикладі сучасних конфліктів.

Тема 8. Он-лайн мережеві проекти.

Вивчення процесу розробки інформаційних он-лайн мережевих проектів.

Самостійна робота

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи студенти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт, заліків та іспитів. Студентам також рекомендуються додаткові матеріали (відео, статті) для самостійного вивчення та аналізу.

Неформальна освіта

В рамках неформальної освіти згідно відповідного Положення (<http://surl.li/pxssv>), освітня компонента або її окремі теми можуть бути враховано у разі самостійного проходження професійних курсів/тренінгів, отримання громадянської освіти, онлайн освіти, професійного стажування тощо.

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

Література та навчальні матеріали

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. Бебик В.М. Інформаційно-комунікаційний менеджмент у глобальному суспільстві: психологія, технології, техніка публік рілейшнз: монографія / В.М. Бебик. – Київ: МАУП, 2005. – 440 с.
<https://kpd.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. Березовець Т. Анексія: Острів Крим. Хроніки «гібридної війни» / Т.Березовець. – Київ: Брайт Стар Паблішинг, 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. Веденєєв Д.В. Гострі когті орла. Сили спеціальних операцій США: історія та сучасність: монографія / Д.В. Веденєєв, Г.С. Биструхін, А.І.Семука. – Київ: К.І.С., 2010. – 400 с.
https://issuu.com/pubkis/docs/gostri_kiht_i_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

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:

- лабораторні роботи: 40% семестрової оцінки;
- самостійна робота: 10% семестрової оцінки;
- контрольна робота: 10% семестрової оцінки;
- залік: 40% семестрової оцінки.

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

Студент 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

28.08.2024



Завідувач кафедри
Сергій ЄВСЕЄВ

28.08.2024



Гарант ОП
Андрій ТКАЧОВ