Силабус освітнього компонента
Програма навчальної дисципліни

Методи та технології інформаційних війн

Шифр та назва спеціальності
257 – Управління інформаційною безпекою

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Освітня програма
Управління інформаційною безпекою

Кафедра
Кібербезпеки (328)

Рівень освіти
Бакалавр

Тип дисципліни
Профільна підготовка, Вибіркова

Семестр
4

Мова викладання
Українська

Викладачі, розробники

ЄВСЕЄВ Сергій Петрович
serhii.yevseiev@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–4. Здатність спілкуватися державною мовою як усно, так і письмово.
КЗ–5. Здатність спілкуватися іноземною мовою.
КЗ–6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
КЗ–7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.
ФК-2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.
ФК-3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.
ФК-5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.
ФК-6. Здатність використовувати іноземну мову для отримання додаткових знань і умінь з питань управління інформаційною безпекою, взаємодіяти з іноземними партнерами.
ФК-7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації.
ФК-8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах.
ФК-9. Здатність організації реагування на загрози на об'єктах критичної інфраструктури, установах та підприємствах.
ФК-10. Здатність забезпечувати неперервність бізнесу згідно з встановленою політикою інформаційної безпеки.
ФК-11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.

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-4. Вільно спілкуватися державною мовою.
ПРН-5. Вільно спілкуватися іноземною мовою у межах потреби своєї професійної діяльності.
ПРН-6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки
ПРН-7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.
ПРН-8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки.
ПРН-10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.
ПРН-11. Вміти забезпечувати процеси захисту та функціонування системи управління інформаційною безпекою та захисту інформації на основі практик, навичок та знань, щодо інфраструктури кіберфізичних систем та інформаційних потоків.

ПРН-12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
ПРН-13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах.
ПРН-14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
ПРН-16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.
ПРН-17. Вміти розв'язувати задачі управління інфораційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.
ПРН-18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.
ПРН-19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах.
ПРН-20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
ПРН-21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.
ПРН-22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.

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 проєкти, 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 соціальнихон-лайн мережах.
Тема 3. Українське законодавство в галузі інформаційної політики та безпеки.
Нормативно-правові акти, що прямо регулюють питанняінформаційної 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. 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

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
Роман КОРОЛЬОВ