Силабус освітнього компонента
Програма навчальної дисципліни

Фізичні основи технічних засобів розвідки

Шифр та назва спеціальності
256 – Національна безпека (за окремими сферами забезпечення і видами діяльності)

Інститут
ННІ комп`ютерних наук та інформаційних технологій (320)

Освітня програма
Національна безпека у сфері кіберзахисту

Кафедра
Кібербезпеки (328)

Рівень освіти
Бакалавр

Тип дисципліни
Спеціальна (фахова), Обов'язкова

Семестр
2

Мова викладання
Українська

Викладачі, розробники

КОРОЛЬОВ Роман Володимирович

korolevrv01@ukr.net
Кандидат технічних наук, доцент, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 80, з них патентів на корисну модель 12, 1 колективна монографія, 2 навчальних посібника, 65 статті у закордонних виданнях та фахових виданнях України, з них 5 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Бездротова та мобільна безпека», «Основи стеганографії», «Бізнес інтелліджанс» , «Фізичні основи технічних засобів розвідки» у студентів бакалавріата та магістратури.

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Фізичні основи технічних засобів розвідки" є обов'язковою навчальною дисципліною. Дисципліна спрямована на набуття студентом теоретичних знань та практичних навичок щодо фізичних основ технічних засобів розвідки у сфері кіберзахисту.

Мета та цілі дисципліни

Освоєння студентами системи фундаментальних теоретичних знань, прикладних навичків використання основних фундаментальних фізичних уявлень щодо продуктів інформаційних технологій та різноманітних технічних засобів інтелекту, практична робота з широким спектром сучасних фізичних та електронних пристроїв, розвиток самостійного мислення студентів, необхідних для їхнього майбутнього, кар'єри.

Формат занять

Лекції, лабораторні роботи, самостійна робота, консультації. Підсумковий контроль – іспит.

Компетентності

КЗ–3. Здатність до абстрактного мислення, аналізу та синтезу.
КЗ–4. Здатність спілкуватися державною мовою як усно, так і письмово.
КЗ–7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
КЗ–8. Здатність використовувати інформаційні та комунікаційні технології і на цій основі формувати ефективну систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо запобігання, протидії та нейтралізації загроз національній безпеці.
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–3. Здатність використовувати знання щодо ролі, місця та призначення політичних та безпекових інститутів України для ефективного здійснення заходів при виконанні обов'язків з питань забезпечення національної безпеки.
ФК–4. Здатність демонструвати та застосовувати знання з основ теорії 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.

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–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 напрямами професійної діяльності та синтезувати інформацію щодо розроблення та реалізації стратегій у визначальних сферах національної безпеки (політичній, економічній, соціальній, гуманітарній).
ПРН–11. Вміти пояснювати роль, місце та призначення політичних та безпекових інститутів України для ефективного здійснення заходів при виконання обов'язків з питань забезпечення національної безпеки.
ПРН–12. Вміти застосовувати знання з основ теорії національної безпеки, зокрема: оцінювати обстановку, рівень викликів та загроз національній безпеці.
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.

Обсяг дисципліни

Загальний обсяг дисципліни 150 год. (5 кредитів ECTS): лекції – 32 год., лабораторні роботи – 32 год., самостійна робота – 86 год.

Передумови вивчення дисципліни (пререквізити)

Вища математика, Основи програмування.

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. Фізичні основи захисту інформації.
Захист інформації від витоку технічними каналами. Інженерно-технічний захист інформації. Технічний засіб захисту мовної інформації.
Тема 2. Принципи функціонування каналів кібернетичної розвідки несанкціонованого отримання інформації.
Принципи кібернетичної розвідки.
Тема 3. Принципи функціонування каналів кібернетичної розвідки несанкціонованого отримання інформації
Канали несанкціонованого отримання інформації.
Тема 4. Акустична розвідка.
Класифікація акустичних каналів витоку інформації. Фізична природа, середовище поширення і спосіб перехвату інформації. Фізичні перетворювачі. Вплив небезпечних акустичних сигналів на технічні системи.
Тема 5. Напрями забезпечення інформаційної безпеки.
Класифікація технічних каналів витоку інформації. Канали витоку інформації ЕОМ. Матеріально-речові канали інформації. Лінії зв'язку.
Тема 6. Методи та засоби знищення інформації.
Індустріальні перешкоди. Спеціальний силовий вплив. Спеціальний силовий вплив на мережу живлення. Вірусні методи знищення інформації.
Тема 7. Технічні методи та засоби захисту інформації.
Класифікація технічних засобів захисту. Захист від радіозакладок. Методи та засоби захисту від радіомікрофонів. Захист від лазерних систем акустичної розвідки.Захист ліній зв'язку. Способи виявлення апаратури перехоплення інформації. Техніка для захисту телефонних каналів. Екранування приміщень. Засоби захисту інформації. Принципи побудови систем захисту інформації. Програмні засоби захисту інформації.
Тема 8. Програмні методи захисту інформації.
Програми зовнішнього захисту. Проблеми регулювання використання ресурсів. Програми захисту програм. Метод визначення факту інформаційного втручання.
Тема 9. Способи та засоби несанкціонованого отримання інформації з автоматизованих систем.
Несанкціоноване отримання інформації з автоматизованих систем. Захист інформації в автоматизованих системах. Методи захисту інформації.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Фізичні основи захисту інформації.
Тема 2. Принципи функціонування каналів кібернетичної розвідки несанкціонованого отримання інформації.
Тема 3. Акустична розвідка.
Тема 4. Напрями забезпечення інформаційної безпеки.
Тема 5. Методи та засоби знищення інформації.
Тема 6. Технічні методи та засоби захисту інформації.
Тема 7. Програмні методи захисту інформації.
Тема 8. Способи та засоби несанкціонованого отримання інформації з автоматизованих систем.

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. Лаптєв О.А., Савченко В.А., Шуклін Г.В. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності: Навчальній посібник. – Київ: ДУТ, 2020. – 126 с. https://f.eruditor.link/file/3323808/
2. Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації: Навчальній посібник. – Київ: НТУУ, 2016. – 104 с.
https://ela.kpi.ua/server/api/core/bitstreams/930d9270-2cb1-4c62-a4ce-ab5404d9b90f/content
3. Jacobson D., Idziorek J. Computer security literacy: staying safe in a digital world. – CRC Press, 2016. Sloan R., Warner R. Unauthorized access: The crisis in online privacy and security. – Taylor & Francis, 2017. – С. 401.
https://api.pageplace.de/preview/DT0400.9781439856192_A24452808/preview-9781439856192_A24452808.pdf
4. Iniewski K. (ed.). Semiconductor radiation detection systems. – CRC press, 2018.
https://www.taylorfrancis.com/books/edit/10.1201/9781315218373/semiconductor-radiation-detection-systems-krzysztof-iniewski
5. Mitra S., Gofman M. (ed.). Biometrics in a data driven world: trends, technologies, and challenges. – CRC Press, 2016.
https://www.perlego.com/book/2051516/biometrics-in-a-data-driven-world-trends-technologies-and-challenges-pdf
6. Цифрова схемотехніка та архітектура мікропроцесорів: навчальний посібник / Євсеєв С. П., Дженюк Н.В., Охрименко М.Ю. та ін. – Харків, – Львів: Видавництво ПП «Новий Світ – 2000», 2023. – 513 с.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
7. Євсеєв С.П. КІБЕРБЕЗПЕКА: ЛАБОРАТОРНИЙ ПРАКТИКУМ З ОСНОВ КРИПОГРАФІЧНОГО ЗАХИСТУ / С.П. Євсеєв, О.В. Мілов, О.Г. Король – Львів: «Новий Світ- 2000», 2020 . – 241 с.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju

Додаткова література :

1. Petersen J. K., Taylor P. Handbook of surveillance technologies. – CRC press, 2012.
https://books.google.com.ua/books/about/Handbook_of_Surveillance_Technologies.html?id=Cj_3DwAAQBAJ&redir_esc=y
2. Ball K., Haggerty K., Lyon D. Routledge handbook of surveillance studies. – Routledge, 2012.
https://books.google.com.ua/books/about/Routledge_Handbook_of_Surveillance_Studi.html?id=F8nhCfrUamEC&redir_esc=y
3. Military intelligence: textbook / compilers: D. V. Zaitsev, A. P. Nakonechny, S. O. Pakharev, I. O. Lutsenko; edited by V. B. Dobrovolsky. - Kyiv: Publishing and Printing Center ''Kyiv University'', 2016. - 335 p.
4. Chen L., Gong G. Communication system security. – CRC press, 2012.
https://books.google.com.ua/books/about/Communication_System_Security.html?id=nmjRBQAAQBAJ&redir_esc=y
5. Mallett X., Blythe T., Berry R. (ed.). Advances in forensic human identification. – CRC Press, 2014.
https://api.pageplace.de/preview/DT0400.9781439825167_A23982999/preview-9781439825167_A23982999.pdf

6. Dardari D., Falletti E., Luise M. (ed.). Satellite and terrestrial radio positioning techniques: a signal processing perspective. – Academic Press, 2012.
7. Sapse D., Kobilinsky L. (ed.). Forensic science advances and their application in the judiciary system. – CRC Press, 2011.
https://books.google.com.ua/books/about/Forensic_Science_Advances_and_Their_Appl.html?id=mXMVCzZZxIwC&redir_esc=y
8. Murphy M. J. (ed.). Adaptive motion compensation in radiotherapy. – CRC Press, 2011.
https://books.google.com.ua/books/about/Adaptive_Motion_Compensation_in_Radiothe.html?id=qVPRBQAAQBAJ&redir_esc=y

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;
• іспит: 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