



Силабус освітнього компонента

Програма навчальної дисципліни



Фізичні основи технічних засобів розвідки

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

Обов'язкова

Рівень освіти

Перший (бакалаврський)

Форма навчання

Денна, заочна

Семестр

2

Мова викладання

Українська, англійська

Викладачі, розробники



КОРОЛЬОВ Роман Володимирович

korolevrv01@ukr.net

Кандидат технічних наук, доцент, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 40, з яких 1 навчальний посібник, 23 статті у закордонних виданнях та фахових виданнях України, 10 патентів на корисну модель. Провідний лектор з дисциплін: «Фізичні основи технічних засобів розвідки», «Основи стеганографічного захисту інформації», «Корпоративні мережі та системи доступу», «Безпека та аудит бездротових та рухомих мереж», гарант освітньо-професійної програми "Управління інформаційною безпекою" першого (бакалаврського) рівня вищої освіти.

[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 заняття, самостійна робота, консультації. Підсумковий контроль – іспит.

Компетентності

ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.

ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово.

ЗК5. Здатність вчитися і оволодівати сучасними знаннями.

СК9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.

Результати навчання

РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.

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.

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.

РН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування та контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.

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 проекти, майстер-класи.

Програма навчальної дисципліни

Навчальні заняття

Лекції

Теми лекцій

Кількість годин

Тема 1. Види інформації. Види інформації, які підлягають технічному захисту.	4
Тема 2. Основи розвідувальної діяльності. Види розвідки за призначенням. Види розвідки (воєнної) за масштабами завдань. Види розвідки за завданнями, силами, засобами і способами.	4
Тема 3. Радіoeлектронна розвідка Діапазони електромагнітних хвиль. Особливості радіoeлектронної розвідки. Класифікація радіoeлектронної розвідки.	2
Тема 4. Оптична розвідка. Засоби оптичної розвідки. Визначення відстаней за рахунок використання оптичних засобів розвідки. Основи роботи приладів нічного бачення.	4
Тема 5. Акустична розвідка. Класифікація акустичних каналів витоку інформації. Фізична природа, середовище поширення і спосіб перехвату інформації. Фізичні перетворювачі. Вплив небезпечних акустичних сигналів на технічні системи.	2
Тема 6. Кібернетична розвідка. Принципи кібернетичної розвідки. Вимоги до кібернетичної розвідки. Основні типи засобів кіберрозвідки та зв'язків між ними.	2
Тема 7. Фізичні основи радіаційної розвідки. Поняття радіаційної розвідки. Поняття радіоактивності. Прилади радіаційної розвідки.	4
Тема 8. Хімічна розвідка. Основні показники безпеки хімічної речовини. Основні завдання хімічної розвідки. Методи для індикації отруйних речовин та отрут.	4
Тема 9. Фізичні основи гідроакустичної розвідки. Гідролокатори та їх призначення. Завдання гідроакустичної розвідки. Розповсюдження звуку в морському середовищі. Гідроакустичні засоби розвідки та спостереження.	4
Тема 10. Фізичні основи сейсмічної розвідки. Поняття сейсмічної розвідки. Джерела виникнення пружних хвиль. Методи вивчення глибинних зон Землі.	2
Загальна кількість годин	32

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти α
Тема 1. Захист інформації від витоку технічними каналами. Технічний засіб захисту мовної інформації. Основні типи технічних каналів витоку інформації (електромагнітні, акустичні, віброакустичні) та їх класифікація. Принципи екранування та заземлення як пасивні методи захисту від побічних випромінювань. Активні методи захисту (просторовий шум, лінійний шум) застосовуються для блокування витоку мовної інформації? Технічні засоби захисту мовної інформації (акустичні екрани, шумогенератори) та їх характеристики.	8	0,1

Тема 2. Канали несанкціонованого отримання інформації. Класифікації каналів несанкціонованого отримання інформації (технічні, організаційні, програмні). Канали витоку через кабельні лінії зв'язку (індукційні, контактні, паразитні модуляції). Як функціонують канали несанкціонованого доступу через бездротові мережі (Wi-Fi, Bluetooth) та методи їх виявлення? Канали витоку візуальної інформації (відеоспостереження, оптичні пристрої) та заходи протидії. Ризики несанкціонованого отримання інформації з носіїв даних (HDD, SSD) та способи їх мінімізації? Оформлення результатів аналізу.	8	0,1
Тема 3. Акустична розвідка. Методи акустичної розвідки (лазерна вібраційна, контактна мікрофонія) використовуються для перехоплення мовної інформації. Принципи роботи акустичних пристроїв прослуховування (дистанційні мікрофони, параболічні антени). Як виявляти акустичні канали витоку за допомогою спеціалізованого обладнання (детектори лазерного випромінювання)? Заходи захисту від акустичної розвідки (звукоізоляція, активне шумозаглушення). Роль віброакустичних каналів у акустичній розвідці та методи їх блокування в приміщеннях?	8	0,1
Тема 4. Методи та засоби знищення інформації. Методи знищення інформації на магнітних носіях (демагнітизація, фізичне руйнування) та їх стандарти (NIST SP 800-88). Засоби знищення даних у сервісах передачі даних (шифрування, стирання ключів) для VoIP та відеоконференцій. Як забезпечується безпечне знищення інформації в хмарних сервісах (SaaS, PaaS) для голосу та відео? Ризики витоку інформації в VoIP-сервісах (SIP-атаки, перехоплення RTP-пакетів) та методи протидії.	8	0,1
Загальна кількість годин	32	$\sum_{i=1}^n a_i = 0,4$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Контрольна робота за матеріалами лекційних занять. Види інформації, які підлягають технічному захисту. Діапазони електромагнітних хвиль. Особливості радіоелектронної розвідки. Класифікація радіоелектронної розвідки. Класифікація акустичних каналів витоку інформації. Фізична природа, середовище поширення і спосіб перехвату інформації. Фізичні перетворювачі. Вплив небезпечних акустичних сигналів на технічні системи.	0,1
Тема 2. Контрольна робота за матеріалами лекційних занять. Поняття радіаційної розвідки. Поняття радіоактивності. Прилади радіаційної розвідки. Гідролокатори та їх призначення. Завдання гідроакустичної розвідки. Розповсюдження звуку в морському середовищі. Гідроакустичні засоби розвідки та спостереження.	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. Основи електромагнітних принципів розвідки Які фізичні закони (закон Фарадея, рівняння Максвелла) лежать в основі електромагнітної розвідки сигналів. Принципи генерації та прийому побічних електромагнітних випромінювань від електронних пристроїв.	9
Тема 2. Акустичні основи технічних засобів розвідки Як поширюються звукові хвилі в різних середовищах (повітря, тверде тіло) та їх роль у акустичній розвідці. Фізичні параметри звуку (частота, амплітуда, інтенсивність) та їх вплив на ефективність прослуховування.	9
Тема 3. Оптичні принципи розвідки Закони оптики (дифракція, інтерференція) застосовуються в оптичних системах для дистанційного спостереження. Принципи роботи лазерних оптичних детекторів для перехоплення вібрацій скла чи поверхонь.	9
Тема 4. Радіолокаційні та мікрохвильові засоби Як рівняння радарного рівняння визначають дальність виявлення об'єктів у радіолокаційній розвідці? Фізичні ефекти (ефект Доплера, рефлексія) у мікрохвильовій розвідці рухомих цілей.	9
Тема 5. Віброакустична розвідка. Які фізичні моделі вібрацій (гармонічні коливання, резонанси) використовуються для перехоплення віброакустичних сигналів? Принципи лазерної вібраційної розвідки та обмеження через атмосферні перешкоди.	9
Тема 6. Фізичні канали витоку інформації Як класифікуються фізичні канали витоку (температурні, механічні) за носіями енергії? Фізичні механізми "паразитної" модуляції в кабельних лініях та методи їх посилення для розвідки.	9
Тема 7. Сенсори та детектори в розвідці Фізичні принципи (п'єзоелектричний ефект, термоелектричний) лежать в основі сенсорів для виявлення прихованих пристроїв. Робота детекторів неоновими лампами для пошуку електромагнітних полів.	8
Тема 8. Теплове та інфрачервоне сканування Як закон Стефана-Больцмана застосовується в інфрачервоній розвідці для виявлення теплових сигнатур? Фізичні обмеження тепловізорів (атмосферна абсорбція, роздільна здатність) у реальних умовах.	8
Тема 9. Принципи маскування сигналів у розвідці Фізичні методи (дисперсія, реверберація) використовуються для маскування акустичних та електромагнітних сигналів. Ефекти інтерференції для створення "білих" шумів у технічних засобах розвідки.	8
Тема 10. Сучасні фізичні тенденції в розвідувальних технологіях Як квантові ефекти (квантова запутаність) впливають на майбутні засоби фізичної розвідки? Фізичні виклики (шум, ентропія) у нанорозмірних сенсорах для прихованого моніторингу.	8

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. Лаптев О.А., Савченко В.А., Шуклін Г.В. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності: Навчальний 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: Навчальний 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 КРИПТОГРАФІЧНОГО 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>
8. Гоков О.М. Фізичні основи технічних засобів розвідки: навчальний посібник /О.М.Гоков. – Харків, 2022. – 255 с.

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

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
0,4	0,2		0,4

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:

$$O = \Pi \cdot k_1 + K \cdot k_2 + I \cdot k_3 + \Pi_k \cdot k_4$$

де: Π – середньозважена середня оцінка за поточний контроль

I – оцінка за виконання індивідуального завдання

K – середньозважена оцінка за контрольні роботи

Π_k – оцінка за підсумковий контроль

$$\Pi = \frac{\Pi_1 \cdot a_1 + \Pi_2 \cdot a_2 + \dots + \Pi_n \cdot a_n}{\sum_{i=1}^n a_i}$$

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

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

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Шкала оцінювання

Поточні оцінки за кожну складову (Π , K , I , ...) виставляються за 100-бальною шкалою згідно з [положенням «Про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої](#)

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B

освіти» НТУ «ХПІ».

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

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