Силабус освітнього компонента
Програма навчальної дисципліни

Фізичні основи технічних засобів розвідки

Шифр та назва спеціальності
125 – Кібербезпека та захист інформації

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

Освітня програма
Кібербезпека

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 інтелідженс» , «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 1. Здатність застосовувати знання у практичних ситуаціях.
КЗ 2. Знання та розуміння предметної області та розуміння професії.
КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням
КЗ 5. Здатність до пошуку, оброблення та аналізу інформації
КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.
КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.
КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.
КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.
КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.
КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).
КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.
КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.
КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.
КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Результати навчання

РН–1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;
РН–2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;
РН–3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.
РН–4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
РН–5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.
РН–6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.
РН–7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.
РН–8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.

РН–9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.
РН–10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.
РН–11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.
РН–12. Розробляти моделі загроз та порушника.
РН–13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.
РН–14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.
РН–15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
РН–16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.
РН–17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.
РН–18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
РН–19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.
РН–20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.
РН–21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
РН–22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.
РН–23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
РН–24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).
РН–25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.
РН–26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.
РН–27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.
РН–28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.
РН–29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.
РН–30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.

РН–31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.
РН–32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.
РН–33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.
РН–34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.
РН–35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки.
РН–36. Виявляти небезпечні сигнали технічних засобів.
РН–37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.
РН–38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.
РН–39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.
РН–40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.
РН–41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.
РН–42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.
РН–43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.
РН–44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.
РН–45. Застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.
РН–46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.
РН–47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.
РН–48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.
РН–49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.
РН–50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).
РН–51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.
РН–52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.
РН–53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.

РН–54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

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

Сергій ЄВСЕЄВ