Силабус освітнього компонента
Програма навчальної дисципліни

Захист від технічних розвідок

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
Вибіркова

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна, заочна

Семестр
6

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

Дисципліна «Захист від технічних розвідок» вивчає методи виявлення, запобігання та протидії загрозам технічної розвідки на об’єктах критичної інфраструктури. Розглядаються способи збору та аналізу інформації, організаційні та технічні заходи захисту, контроль доступу, електромагнітна безпека, шифрування каналів зв’язку, а також аудит та оцінка ефективності заходів захисту. Студенти набувають практичних навичок захисту інформаційних ресурсів і реагування на спроби технічного шпигунства.

Мета та цілі дисципліни

Формування у студентів знань і практичних навичок для виявлення, запобігання та протидії загрозам технічної розвідки, а також забезпечення інформаційної безпеки об'єктів критичної інфраструктури та захисту ресурсів організацій від шпигунських та кіберактивностей.

Формат занять

Лекції, лабораторні заняття, самостійна робота, консультації. Підсумковий контроль – диференційований залік.

Компетентності

ЗК1. Здатність застосовувати знання у практичних ситуаціях – використання методів виявлення та протидії технічній розвідці на практиці.
ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.
ЗК5. Здатність вчитися і оволодівати сучасними знаннями – вивчення нових технічних засобів розвідки та методів їхнього виявлення.
СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації
СК4. Здатність забезпечувати захист інформації в інформаційних системах згідно встановленої політики кібербезпеки та захисту інформації.
СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо).
СК9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.
СК10. Здатність виконувати моніторинг, аналізувати та виявляти вразливості – включаючи контроль технічних каналів витоку та виявлення засобів розвідки.

Результати навчання

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.
РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення та передачі сигналів тощо, принципи, методи і поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.
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.
РН9. Вміти застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
РН12. Застосовувати методи захисту інформації в інформаційних системах згідно встановленої політики інформаційної безпеки.
РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних та програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних систем та\або інфраструктури організації в цілому.
РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.

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.
РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору та інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 12 год., лабораторні роботи – 24 год., самостійна робота – 84 год.

Передумови вивчення дисципліни (пререквізити)

Основи криптографічного захисту , Основи кібербезпеки, Комп'ютерні мережі.

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

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Вступ до технічної розвідки та загрози. Ознайомлення з поняттям технічної розвідки, основними методами збору інформації та потенційними загрозами для організацій і державних об'єктів.	2
Тема 2. Методи збору та аналізу інформації. Розгляд відкритих і прихованих джерел інформації, технік спостереження, перехоплення сигналів і аналізу даних для виявлення уразливостей.	2
Тема 3 Фізичний захист об'єктів та обмеження доступу. Принципи організації охорони, контроль доступу, периметральний захист, сигналізаційні системи та заходи протидії несанкціонованому проникненню.	2
Тема 4. Електромагнітна та інформаційна безпека. Методи захисту від перехоплення електромагнітних випромінювань, засоби екранізації, шифрування каналів зв'язку та безпечне використання інформаційних систем.	2
Тема 5. Контрзаходи проти технічного шпигунства. Організаційні, технічні та правові заходи для виявлення, запобігання та реагування на спроби технічної розвідки.	2
Тема 6. Аудит та оцінка ефективності заходів захисту. Методи перевірки систем захисту від технічної розвідки, аудит безпеки, тестування на проникнення та оцінка ризиків.	2
Загальна кількість годин	**12**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Виявлення каналів витоку інформації. Ознайомлення з основними технічними каналами розвідки та методами визначення потенційних загроз.	4	0,1
Тема 2. Аналіз методів збору даних противником. Практичне дослідження способів перехоплення інформації (радіо-, акустичні та візуальні канали) та оцінка їх ефективності.	4	0,1
Тема 3. Організація системи фізичного захисту об'єкта. Моделювання заходів контролю доступу, периметральної охорони та використання сигналізаційних систем.	4	0,1
Тема 4. Захист від електромагнітних випромінювань. Вивчення методів екранізації, фільтрації та інших технічних засобів запобігання перехопленню сигналів.	4	0,1
Тема 5. Реалізація контрзаходів проти технічного шпигунства. Виконання практичних завдань з організаційних та технічних заходів захисту, моделювання сценаріїв виявлення спроб розвідки.	4	0,1
Тема 6. Аудит системи захисту від технічної розвідки. Практичне проведення перевірки ефективності встановлених заходів, оцінка вразливостей та формування рекомендацій.	4	0,1
Загальна кількість годин	**24**	$\sum_{i=1}^{n} a_i = 0{,}6$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Вступ до технічної розвідки, методи збору та аналізу інформації, фізичний захист об'єктів. Робота спрямована на перевірку знань щодо основних понять технічної розвідки, джерел інформаційних загроз, а також уміння аналізувати методи збору даних і застосовувати принципи організації фізичного захисту об'єктів.	0,2
Тема 1. Електромагнітна та інформаційна безпека, контрзаходи проти технічного шпигунства, аудит та оцінка захисних заходів. Робота перевіряє розуміння засобів захисту від електромагнітних випромінювань, знання організаційних і технічних контрзаходів проти шпигунства та здатність оцінювати ефективність систем захисту за допомогою аудиту та тестування.	0,2
Загалом	$\sum_{i=1}^{m} b_i = 0{,}4$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріал

Теми для самостійного вивчення	Кількість годин
Тема 1. Основи безпеки бездротових мереж. Основні принципи безпеки бездротових мереж (CIA-тріада) та їх застосування в Wi-Fi. Архітектура бездротових мереж (WLAN, WPAN) та ключові компоненти безпеки.	8
Тема 2. Загрози та вразливості в бездротових мережах. Основні загрози бездротовим мережам (eavesdropping, man-in-the-middle) та приклади атак. Як класифікуються вразливості в бездротових мережах за типами (конфігураційні, протоколні).	8
Тема 3 Протоколи шифрування в Wi-Fi мережах. Еволюція протоколів шифрування Wi-Fi (WEP, WPA, WPA3) та їх сильні/слабкі сторони. Роль EAP (Extensible Authentication Protocol) у аутентифікації користувачів Wi-Fi.	10
Тема 4. Безпека мобільних мереж (GSM, UMTS). Ключові механізми безпеки в GSM (A3/A8 алгоритми) та їх вразливості до атак. Шифрування в UMTS (KASUMI) та методи захисту від IMSI-catching.	8
Тема 5. Безпека мереж LTE та 5G. Нові функції безпеки в 5G (network slicing, SUCI) порівняно з LTE. Протоколи аутентифікації в LTE (EPS-AKA) та ризики SS7-атак.	8
Тема 6. Методи аудиту бездротових мереж. Проводення пентестингу в бездротових мережах (використання інструментів як Aircrack-ng). Стандарти аудиту (ISO 27001, NIST) для оцінки безпеки WLAN.	8
Тема 7. Системи виявлення вторгнень у бездротових мережах. Принципи роботи WIPS (Wireless Intrusion Prevention System) та їх інтеграцію. Методи виявлення аномалій (signature-based, anomaly-based) застосовуються в мобільних мережах.	8
Тема 8. Безпека Bluetooth та NFC технологій. Вразливості Bluetooth (BlueBorne, KNOB) та методи їх пом'якшення. Механізми безпеки NFC (контактна аутентифікація) та ризики relay-атак.	8
Тема 9. Аудит безпеки IoT у бездротових мережах. Як проводити аудит безпеки IoT-пристроїв (Zigbee, Z-Wave) на вразливості? Рекомендації для сегментації мереж IoT для мінімізації ризиків.	8
Тема 10. Стандарти та регуляції безпеки бездротових мереж. Міжнародні стандарти (IEEE 802.11, 3GPP) регулюють безпеку бездротових та рухомих мереж. Роль GDPR та інших регуляцій у аудиті мобільних мереж.	10
Загальна кількість годин	**84**

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

1. Онлайн-курс CISCO «Introduction to Cybersecurity» https://www.netacad.com/courses/introduction-to-cybersecurity?utm_source=chatgpt.com.

Література, навчальні матеріали та інформаційні ресурси

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
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
0,6	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:

$$О = П \cdot k_1 + K \cdot k_2 + І \cdot k_3 + Пк \cdot k_4$$

де: П – середньозважена середня оцінка за поточний контроль
І – оцінка за виконання індивідуального завдання
K – середньозважена оцінка за контрольні роботи
Пк – оцінка за підсумковий контроль

$$П = \frac{П_1 \cdot a_1 + П_2 \cdot a_2 + ... + П_n \cdot a_n}{\sum_{i=1}^{n} a_i}$$

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

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

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (П, K, І,...) виставляються за 100-бальною шкалою згідно з положенням «Про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої освіти» НТУ «ХПІ».

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

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

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