Силабус освітнього компонента
Програма навчальної дисципліни

Шпигунство в кіберпросторі

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
Професійна підготовка, Вибіркова

Рівень освіти
Другий (магістерський)

Форма навчання
Денна

Семестр
3

Мова викладання
Українська

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 " Шпигунство в кіберпросторі " є вибірковою навчальною дисципліною. Дисципліна включає базові положення щодо проблеми забезпечення кібербезпеки і національної безпеки. Розкриваються питання щодо завдань кіберзахисту та шляхів його забезпечення в умовах інформаційної війни. Вивчається поняття кібершпигунство як вид кіберзлочинності, який полягає в несанкціонованому проникненні в комп'ютерні системи, мережі або пристрої для збору конфіденційної або секретної інформації.

Мета та цілі дисципліни

Надати студентам глибоке розуміння принципів, методів і інструментів, що використовуються в кібершпигунстві, а також розвинути навички захисту інформаційних систем від таких загроз.

Студенти повинні навчитися розпізнавати потенційні загрози, аналізувати атаки, використовувати засоби кіберзахисту та впроваджувати заходи безпеки.

Формат занять

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

Компетентності

КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.
КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.
КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.

Результати навчання

РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.
РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.
РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.
РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.
РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.

РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.
РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 16 год., лабораторні роботи – 32 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Безпека та анонімність роботи в Інтернеті, Аналіз шкідливих програм.

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. Кіберпростір і кібербезпека. Національна безпека і особливості захисту інформації у кіберпросторі. Розкривається поняття кіберпростору як нового середовища протистояння. Аналізуються ключові аспекти кібербезпеки, її роль у системі національної безпеки та основні підходи до захисту інформації.	2
Тема 2. Сучасна технічна розвідка. Інформаційна війна і національна безпека. Правова основа забезпечення інформаційної безпеки в Україні. Огляд сучасних методів технічної розвідки, інформаційних операцій та їх впливу на безпеку держави. Вивчення ролі інформаційної війни у гібридних конфліктах. Аналіз нормативно-правової бази, що регулює кібербезпеку, захист державних інформаційних ресурсів та протидію кіберзагрозам.	2
Тема 3. Інформаційно-комунікаційні системи як об'єкт захисту. Вивчаються принципи побудови та захисту ІКС, основні вразливості та механізми протидії несанкціонованому доступу до інформації.	2
Тема 3. Поняття кіберзлочинність та кібертероризм. Розгляд основних видів кіберзлочинів, їх класифікації та прикладів. Аналіз загроз кібертероризму для державних і приватних структур.	2
Тема 5. Вступ до кібершпигунства. Методи кібершпигунства. Технології захисту від кібершпигунства. Ознайомлення з поняттям, історією та сучасними формами кібершпигунства. Визначення цілей, суб'єктів та об'єктів шпигунської діяльності у кіберпросторі. Розгляд технічних і соціальних методів шпигунства: фішинг, сніфінг, ін'єкції, соціальна інженерія, використання бекдорів і шпигунських програм.	2

Вивчаються сучасні засоби захисту: антивірусні системи, системи виявлення вторгнень, шифрування, багаторівнева автентифікація та моніторинг активності.	
Тема 6. Види атак і шкідливого програмного забезпечення. Приклади та аналіз відомих атак. Аналіз видів кіберзагроз — вірусів, троянів, руткітів, шпигунських програм, ботнетів; принципи їхньої роботи та розповсюдження. Розбір відомих кейсів кібершпигунства (Stuxnet, SolarWinds, Pegasus тощо), їх наслідків і методів виявлення.	2
Тема 7. Правові та етичні аспекти кібершпигунства. Майбутні загрози кібершпигунства. Обговорюються морально-етичні дилеми, питання законності збору інформації та міжнародні стандарти відповідальності за кібершпигунство. Оцінюються перспективи розвитку шпигунських технологій, загрози з боку штучного інтелекту, квантових обчислень та автономних систем.	2
Тема 8. Практичні аспекти забезпечення кібербезпеки та кібероборони. Формування практичних навичок побудови систем захисту, управління інцидентами, розробки політик безпеки та реагування на кібершпигунські атаки.	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Аналіз фішингових атак та соціальної інженерії. Розглядаються методи і техніки фішингових атак, спрямованих на отримання конфіденційних даних користувачів. Вивчаються механізми соціальної інженерії, психологічні прийоми маніпулювання людьми, а також способи розпізнавання і протидії таким атакам.	8	0,2
Тема 2. Виявлення та аналіз шкідливого програмного забезпечення (Malware). Вивчаються типи, структура та принципи роботи шкідливого ПЗ, методи його розповсюдження й приховування в системах. Розглядаються сучасні інструменти аналізу Malware, включаючи статичний та динамічний аналіз, а також способи виявлення заражень і відновлення системи.	8	0,2
Тема 3. Використання систем виявлення вторгнень (IDS) для захисту від кібершпигунства. Описуються принципи роботи систем виявлення вторгнень (IDS) та їх роль у виявленні кібершпигунської активності. Розглядаються типи IDS (мережеві та хостові), методи виявлення аномалій, налаштування сигнатур та інтеграція IDS у комплексні системи захисту організації.	8	0,2
Тема 4. Методи виявлення та запобігання кібершпигунству на рівні держави та організації. Вивчаються стратегії і механізми державного та корпоративного реагування на кібершпигунські загрози. Розглядаються принципи побудови систем кіберрозвідки, кібероборони та інформаційного моніторингу. Аналізуються методи міждержавної співпраці, роль	8	0,2

CERT/CSIRT центрів і сучасні практики кіберконтррозвідки.		
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 0{,}8$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Основи кібершпигунства та інформаційної безпеки. Метою роботи є формування розуміння структури та ролі кіберпростору у системі національної безпеки, аналіз правових, технічних і організаційних основ захисту інформації, а також ознайомлення з основними проявами кіберзлочинності та кібертероризму.	0,1
Тема 2. Методи, інструменти та протидія кібершпигунству. Контрольна робота спрямована на вивчення сучасних методів кібершпигунства, аналіз типових атак і вразливостей, оцінку інструментів протидії шпигунству та розуміння правових і етичних аспектів діяльності у сфері кіберрозвідки.	0,1
Загалом	$\sum_{i=1}^{m} b_i$=0,2

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин
Тема 1. Еволюція кібершпигунства: від традиційної розвідки до цифрової епохи. Розгляд історичних етапів розвитку шпигунства та його трансформації в умовах цифровізації та глобальної мережевої взаємодії.	8
Тема 2. Архітектура та принципи роботи систем електронного спостереження. Вивчення принципів побудови систем моніторингу, перехоплення трафіку, аналізу комунікацій і контролю даних у кіберпросторі.	8
Тема 3. Кібершпигунські кампанії державного рівня (APT-атаки). Дослідження найвідоміших кампаній APT-груп (Advanced Persistent Threats), їхніх цілей, методів та інструментів.	7
Тема 4. Використання штучного інтелекту у кібершпигунстві. Огляд сучасних технологій машинного навчання, що застосовуються для автоматизації шпигунських дій, аналізу даних і приховування слідів атак.	7
Тема 5. Психологічні аспекти соціальної інженерії. Дослідження методів впливу на людину для отримання конфіденційної інформації. Аналіз технік маніпуляції та факторів уразливості персоналу.	7
Тема 6. Кіберрозвідка у бізнес-середовищі (Competitive Intelligence). Вивчення механізмів збору, аналізу та використання бізнес-даних конкурентів із відкритих джерел (OSINT) та закритих каналів.	7
Тема 7. Технології анонімізації в кібершпигунстві.	7

Розгляд інструментів приховування ідентичності зловмисників (VPN, TOR, проксі-сервери, криптовалюти) та методів їх виявлення.	
Тема 8. Контршпигунські технології та цифрова форензика. Вивчення засобів виявлення шпигунського ПЗ, цифрового аналізу інцидентів і збору доказів для кіберрозслідувань.	7
Тема 9. Інсайдерські загрози в контексті кібершпигунства. Аналіз ризиків, пов'язаних із діями співробітників організації, що мають доступ до критичних ресурсів. Методи профілактики та контролю.	7
Тема 10. Геополітичні аспекти кібершпигунства та міжнародна кібербезпека. Розгляд ролі кібершпигунства у глобальній політиці, його впливу на міжнародні відносини, безпеку держав і міждержавні конфлікти у кіберпросторі.	7
Загальна кількість годин	**72**

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. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. – К., 2023.– №11 (листопад) . – 300 с. URL: https://ippi.org.ua/sites/default/files/2023-11.pdf
2. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. – 320 с. ISBN 978-617-582-069-8. URL: https://ippi.org.ua/kiberbezpeka-v-informatsiinomu-suspilstvi
3. Методичні матеріали до вивчення навчальної дисципліни «Запобігання кіберзлочинам» (за вибором) студентів першого (бакалаврського) рівня вищої освіти галузі знань 08 «Право» спеціальності 081 «Право» / уклад. О.В. Таволжанський. Харків: Нац. юрид. ун-т ім. Ярослава Мудрого. 2022. 42 с.
4. Кібербезпека в Україні: правові та організаційні питання: матеріали міжн. наук. практ. конф., м. Одеса, 22 листопада 2019 р. Одеса : ОДУВС, 2019. 110 с. URL: https://dspace.oduvs.edu.ua/server/api/core/bitstreams/b6bb5094-5cc3-4439-9ad7-14fa597f3d16/content
5. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект : підручник за заг. ред. д-ра техн. наук, професора В. Б. Толубка. Київ. ДУТ, 2015. 288 с. URL: https://duikt.edu.ua/uploads/p_303_79299367.pdf

Додаткова література

6. Закон України "Про основні засади забезпечення кібербезпеки України" Зведена інформація щодо діяльності угрупування UAC-0010 станом на липень 2023 року. URL: https://cert.gov.ua/article/5160737
7. Ліпкан В.А., Діордіца І.В. Національна безпека України: кримінально-правова охорона : навч. посібник. Київ : КНТ, 2007. 292 с. URL: https://www.lipkan.com/natsionalna-bezpeka-ukrayini-kriminalno-pravova-oho-rona/
8. Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 26 березня 2021 р.). [Електронне видання]. – Київ : НА СБУ, 2021. – 346 с. URL: https://eportfolio.kubg.edu.ua/data/conference/7238/document.pdf
9. Про основні засади забезпечення кібербезпеки України: Закон України від 04.04.2024 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 05.04.2023).
10. Гук О. М., Мурасов Р. К., Фараон С. І., Толмачов І. В. Особливості здійснення кібервпливів, як складової кіберборотьби в умовах збройного протистояння. Матеріали IV Всеукраїнської науково-практичної конференції (м. Київ, 28 лютого 2024 року). Навчально- науковий інститут захисту інформації ДУІКТ. Київ, 2024. 300 с. URL: https://duikt.edu.ua/uploads/p_2661_62255520.pdf (дата доступу: 05.04.2023).
11. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія. Київ: НІСД, 2014. 328 с. URL: https://www.niss.gov.ua/sites/default/files/2015-02/Dubov_mon-89e8e.pdf
8. Стратегічний оборонний бюлетень України: Указ Президента України №473/2021 від 20 серпня 2021 р. URL: https://www.president.gov.ua/documents/4732021-40121 (дата доступу: 05.04.2023).

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
0,8	0,2		

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, *К*, 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** Станіслав МІЛЕВСЬКИЙ