Силабус освітнього компонента
Програма навчальної дисципліни

Шпигунство в кіберпросторі

Шифр та назва спеціальності
125 – Кібербезпека та захист інформації

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

Освітня програма
Освітньо-наукова програма Кібербезпека

Кафедра
Кібербезпеки (328)

Рівень освіти
Магістр

Тип дисципліни
Професійна підготовка, Вибіркова

Семестр
3

Мова викладання
Українська

Викладачі, розробники

КОРОЛЬОВ Роман Володимирович
korolevrv01@ukr.net
Кандидат технічних наук, 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 " 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 роботи, самостійна робота, консультації. Підсумковий контроль – 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 кредитів ECTS): лекції – 32 год., лабораторні роботи – 16 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

Теми лекційних занять

Тема 1. Кіберпростір і кібербезпека. Національна безпека і особливості захисту інформації у кіберпросторі.
Тема 2. Сучасна технічна розвідка. Інформаційна війна і національна безпека.
Тема 3. Правова основа забезпечення інформаційної безпеки в Україні.
Тема 4. Інформаційно-комунікаційні системи як об'єкт захисту.
Тема 5. Поняття кіберзлочинність та кібертероризм.
Тема 6. Вступ до кібершпигунства.
Тема 7. Методи кібершпигунства.
Тема 8. Види атак і шкідливого програмного забезпечення.
Тема 9. Приклади та аналіз відомих атак.
Тема 10. Технології захисту від кібершпигунства.
Тема 11. Правові та етичні аспекти кібершпигунства.
Тема 12. Майбутні загрози кібершпигунства.
Тема 13. Практичні аспекти забезпечення кібербезпеки та кібероборони.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1 Аналіз фішингових атак та соціальної інженерії.
Тема 2. Виявлення та аналіз шкідливого програмного забезпечення (Malware).
Тема 3. Використання систем виявлення вторгнень (IDS) для захисту від кібершпигунства.

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. 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

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
- лабораторні роботи: 20% семестрової оцінки;
- самостійна робота: 10% семестрової оцінки;
- контрольна робота: 30% семестрової оцінки;
- залік: 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 Станіслав МІЛЕВСЬКИЙ