Силабус освітнього компонента
Програма навчальної дисципліни

Основи кібербезпеки

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
4

Мова викладання
Українська, англійська

Викладачі, розробники

ЄВСЕЄВ Сергій Петрович

serhii.yevseiev@khpi.edu.ua
Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».
Лауреат національної премії імені Бориса Патона.
Кількість наукових публікацій: понад 351, з них патентів на корисну модель 44, 11 монографій, з яких 10 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 149 статтей у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus, гарант освітньо-професійної програми "Кібербезпека" першого (бакалаврського) рівня вищої освіти.
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Основи кібербезпеки" є вибірковою навчальною дисципліною. Вивчення дисципліни спрямовано на оволодіння необхідними базовими поняттями та правилами безпечної поведінки в мережі, ознайомлення студентів з принципами побудови систем захисту інформації, ознайомлення з основними механізмами послуг безпеки, вивчення менеджменту інформаційної безпеки, навчання студентів основам аудиту інформаційної безпеки, а також вивчення студентами спеціальних механізмів кіберзахисту.

Мета та цілі дисципліни

Навчання студентів принципам побудови систем захисту інформації, дослідженню та використанню сучасних процедур забезпечення надання основних послуг безпеки інформації в кіберпросторі, проведення аудиту поточного стану інформаційної безпеки.

Формат занять

Лекції, лабораторні заняття, самостійна робота, консультації. Підсумковий контроль – іспит.

Компетентності

ЗК1. Здатність застосовувати знання у практичних ситуаціях.
ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.
ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово.
ЗК4. Здатність спілкуватися іноземною мовою.
ЗК5. Здатність вчитися і оволодівати сучасними знаннями.
ЗК7. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.
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
СК2. Здатність використовувати інформаційні технологій, сучасні методи і моделей кібербезпеки та систем захисту інформації.
СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.
СК4. Здатність забезпечувати захист інформації в інформаційних системах згідно встановленої політики кібербезпеки та захисту інформації.
СК5. Здатність відновлювати функціонування інформаційних систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.
СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо).
СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.
СК9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.
СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

Результати навчання

РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.
РН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.
РН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.
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. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
РН10. Вміти використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.
РН11. Планувати підготовку та забезпечувати неперервність процесів в організаціях згідно встановленої політики кібербезпеки та з урахування вимог до 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.
РН14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних систем з використанням процедур резервування згідно встановленої політики безпеки та забезпечувати функціонування спеціального програмного забезпечення, щодо захисту та відновлення інформації;
РН15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.
РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.
РН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об’єктах інформаційної діяльності.
РН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.
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 90 год. (3 кредити ECTS): лекції – 16 год., лабораторні роботи – 16 год., самостійна робота – 58 год.

Передумови вивчення дисципліни (пререквізити)

Вища математика, Комп'ютерні мережі, Інформаційна безпека держави, Алгоритми та структури даних, Розробка веб-додатків.

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 та загроза. **Cisco Networking Academy:** Теоретичні основи захисту інформації. Домени кібербезпеки. Кіберзлочинці проти фахівців з кібербезпеки. Типові загрози. Області розповсюдження загроз. Вплив проблем кібербезпеки на бездротові мережі. Підготовка більшої кількості спеціалістів. Сертифікація з кібербезпеки.	2
Тема 2. Куб кібербезпеки. Симетричні та несиметричні механізми. **Cisco Networking Academy:** Три виміри. Тріада КЦД (CIA). Моделі секретних систем. Безпека традиційної криптографії. Стани даних. Контрзаходи кібербезпеки. Структура управління IT-безпекою.	2
Тема 3. Кібербезпека – загрози, вразливості та атаки. **Cisco Networking Academy:** Шкідливе програмне забезпечення та зловмисний код. Шахрайство. Атаки. Класифікація цифрових підписів. Основні визначення. Механізми автентифікації. Двофакторна автентифікація.	2
Тема 4. Мистецтво захисту таємниць. **Cisco Networking Academy:** Криптографія. Контроль доступу. Приховування даних.	2
Тема 5. Мистецтво забезпечення цілісності даних. **Cisco Networking Academy:** Типи засобів контролю цілісності даних. Цифрові підписи. Сертифікати. Забезпечення цілісності баз даних.	2
Тема 6. Концепція п'яти дев'яток. **Cisco Networking Academy:** Висока доступність. Заходи для поліпшення доступності. Реакція на інцидент. Аварійне відновлення.	2
Тема 7. Захист домену кібербезпеки. **Cisco Networking Academy:** Захист систем та пристроїв. Укріплення захисту серверів. Укріплення захисту мережі. Фізична безпека.	2
Тема 8. Як стати спеціалістом з кібербезпеки. **Cisco Networking Academy:** Домени кібербезпеки. Розуміння етики роботи у кібербезпеці. Наступний крок.	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Cisco Networking Academy: Тема 1. Аутентифікація, авторизація та облік.	2	0,1

Cisco Networking Academy: Тема 2. Встановити віртуальну машину на персональний комп'ютер.	2	-
Cisco Networking Academy: Тема 3. Виявлення загроз і вразливостей.	2	0,1
Cisco Networking Academy: Тема 4. Використання стеганографії.	2	
Cisco Networking Academy: Тема 5. Злам паролів.	2	0,1
Cisco Networking Academy: Тема 6. Використання цифрових підписів.	2	-
Cisco Networking Academy: Тема 7. Віддалений доступ.	2	-
Cisco Networking Academy: Тема 8. Захист Linux систем.	2	0,1
Загальна кількість годин	**16**	$\sum_{i=1}^{m} b_i$=0,4

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Основи кіберпростору та загрози інформаційній безпеці. Розглядаються поняття кіберпростору, основні домени кібербезпеки, типові загрози та області їх поширення. Аналізуються дії кіберзлочинців і заходи протидії, вплив проблем кібербезпеки на мережеві технології, зокрема бездротові мережі. Вивчаються принципи куба кібербезпеки, тріада КЦД (конфіденційність, цілісність, доступність), стани даних та контрзаходи, а також питання сертифікації фахівців.	0,1
Тема 2. Криптографічні механізми та забезпечення захищеності даних. Вивчаються загрози, вразливості та види атак, методи автентифікації та двофакторної перевірки. Розглядається криптографія як основа захисту, цифрові підписи, сертифікати й засоби контролю цілісності даних. Аналізуються концепція високої доступності «п'яти дев'яток», аварійне відновлення, а також практичні підходи до захисту систем, серверів, мереж і фізичної інфраструктури.	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. Еволюція кіберзагроз. Від перших комп'ютерних вірусів до сучасних кібератак.	6

Тема 2. Домени кібербезпеки. Сфери застосування та їх роль у захисті інформаційних систем.	6
Тема 3. Куб кібербезпеки та тріада КЦД. Конфіденційність, цілісність, доступність у контексті управління ризиками.	6
Тема 4. Симетричні та асиметричні криптосистеми. Принципи роботи, приклади алгоритмів, сильні та слабкі сторони.	6
Тема 5. Соціальна інженерія як інструмент кібератак. Методи маніпуляцій та способи протидії.	6
Тема 6. Шкідливе програмне забезпечення. Класифікація, методи поширення та засоби захисту.	6
Тема 7. Цифрові підписи та сертифікати. Роль у забезпеченні цілісності та автентичності даних.	6
Тема 8. Концепція п'яти дев'яток. Забезпечення високої доступності та безперервності бізнес-процесів.	6
Тема 9. Захист мережевої інфраструктури. Укріплення серверів, мережевих пристроїв і фізичної безпеки.	5
Тема 10. Кар'єра в кібербезпеці. Сертифікації, професійна етика та перспективи розвитку фахівця.	5
Загальна кількість годин	**58**

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 «PaloAlto (Cybersecurity Foundation)»
https://paloaltonetworksacademy.net/course/index.php.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Євсеєв С.П. Кібербезпека: сучасні технології захисту. / Євсеєв С. П, Остапов С. Е., Король О. Г. // Навчальний посібник для студентів вищих навчальних закладів. Львів: "Новий Світ – 2000", 2019. – 678.
http://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf
2. Кібербезпека в сучасному світі : матеріали III Всеукраїнської науково-практичної конференції (м. Одеса, 19 листопада 2021 р.) / за ред. О. В. Дикого ;уклад.: С. А. Горбаченко, Н. І. Логінова. – Одеса, 2020. – 148 с.
http://dspace.onua.edu.ua/handle/11300/15973
3. Лісовська Ю. Кібербезпека. Ризики та заходи. – К.: Кондор, 2019. – 272 с.
http://dcmaup.com.ua/assets/files/kiberbezpeka.pdf
4. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju

5. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
6. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022. – 196 p. https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.

Додаткова література

7. Доктрина інформаційної безпеки України, затверджено Указом Президента України редакція від 30.12.2021 № 47/2017. [Електронний ресурс]. https://zakon.rada.gov.ua/laws/show/47/2017#Text.
8. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України", затверджено Указом Президента України редакція від 26.08.2021 № 447/2021).
https://zakon.rada.gov.ua/laws/show/447/2021#Text
9. ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 1: Introduction and general model.
URL: https://www.iso.org/search.html?q=15408-1.
10. ISO/IEC 15408-2:2022 Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 2: Security functional components. URL: https://www.iso.org/search.html?q=15408-2&hPP=10&idx=all_en&p=0.
11. ISO/IEC 15408-3:2022 Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 3: Security assurance components.
URL: https://www.iso.org/search.html?q=15408-3&hPP=10&idx=all_en&p=0.
12. ISO/IEC 31010:2019 Risk management . URL:
https://www.iso.org/ru/contents/data/standard/07/21/72140.html
13. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements URL:
https://www.iso.org/ru/contents/data/standard/08/28/82875.html
14. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls URL:
https://www.iso.org/ru/contents/data/standard/08/05/80585.html
15. ISO/IEC 27003:2017 Information technology – Security techniques – Information security management systems – Guidance URL:
https://www.iso.org/ru/contents/data/standard/06/34/63417.html
16. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection – Guidance on managing information security risks. URL:
https://www.iso.org/ru/contents/data/standard/08/05/80585.html
17. ISO/IEC 27032:2023 Cybersecurity – Guidelines for Internet security. URL:
https://www.iso.org/ru/contents/data/standard/07/60/76070.html.

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:

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

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