Силабус освітнього компонента
Програма навчальної дисципліни

Інформаційна безпека держави

Шифр та назва спеціальності
К4 – Управління інформаційною безпекою

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Спеціалізація

Кафедра
Кібербезпеки (328)

Освітня програма
Управління інформаційною безпекою

Тип дисципліни
Обов'язкова

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна

Семестр
1

Мова викладання
Українська

Викладачі, розробники

КОРОЛЬ Ольга Григорівна
olha.korol@khpi.edu.ua
кандидат технічних наук, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 175, з яких 19 навчальних посібників, 74 статті у закордонних виданнях та фахових виданнях України, 18 патентів на корисну модель, 9 у наукометричній базі Scopus, гарант освітньо-професійної програми «Кібербезпека» другого (магістерського) рівня вищої освіти. Провідний лектор з дисциплін: «Менеджмент інформаційної безпеки», «Національна безпека держави» , «Інформаційна безпека держави», «Комплексний тренінг «Безпека веб-застосунків»», у студентів бакалавріата та магістратури.

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Інформаційна безпека держави" є нормативною навчальною дисципліною. Дисципліна спрямована на дослідження способів, методів, засобів і каналів реалізації загроз національним інтересам на інформаційному рівні та їх своєчасного виявлення, запобігання і нейтралізації.

Мета та цілі дисципліни

Формування теоретичних основ законодавчої бази України та міжнародного суспільства в галузі національної та інформаційної безпеки держави, визначення основних вимог щодо формування підтримки та удосконалення систем управління інформаційної безпеки критичних інформаційно-комунікаційних систем, а також визначення місця і ролі інформаційної безпеки в загальній системі національної безпеки, стану та принципів забезпечення інформаційної безпеки особистості, суспільства та держави.

Формат занять

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

Компетентності

ЗК3. Здатність до абстрактного мислення, аналізу та синтезу.
ЗК4. Здатність спілкуватися державною мовою як усно, так і письмово.
ЗК5. Здатність спілкуватися іноземною мовою.
ЗК6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.
СК4. Здатність прогнозувати реалізації управлінських рішень щодо захисту інформації.
СК5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.
СК8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах.
СК9. Здатність організації реагування на загрози на об'єктах критичної інфраструктури, установах та підприємствах.
СК10. Здатність забезпечувати неперервність бізнесу згідно з встановленою політикою інформаційної безпеки.

Результати навчання

РН3. Вміти за допомогою абстрактного мислення, аналізу та синтезу оцінювати результати професійної діяльності та забезпечувати її якість, бути критичним і самокритичним, наполегливим щодо поставлених завдань і взятих зобов'язань.
РН4. Вільно спілкуватися державною мовою.
РН5. Вільно спілкуватися іноземною мовою у межах потреби своєї професійної діяльності.
РН6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки
РН7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.
РН13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах.
РН14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
РН16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.
РН17. Вміти розв'язувати задачі управління інфораційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.
РН18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.
РН19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах.

РН20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
РН21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.
РН22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.

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)

Вступ до спеціальності. Ознайомча практика.

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. Основи інформаційної безпеки держави. Ключові поняття, цілі та завдання інформаційної безпеки держави. Місце дисципліни у системі підготовки фахівців з кібербезпеки. Структура інформаційної сфери України, національні інтереси та основні нормативно-правові засади забезпечення інформаційної безпеки.	2
Тема 2. Доктрина, структура та складові інформаційної безпеки держави. Поняття та класифікація видів інформаційної безпеки. Доктрина інформаційної безпеки України, державна політика в інформаційній сфері. Механізми, інструменти та суб'єкти забезпечення інформаційної безпеки на рівні держави.	2
Тема 3. Загрози інформаційній безпеці та інформаційні впливи. Класифікація загроз інформаційній безпеці України. Актуальні ризики, включаючи інформаційні операції, маніпуляції, дезінформацію та інформаційне насильство. Проблеми правового реагування на деструктивні інформаційні впливи та їх роль у сучасній політиці й міжнародних відносинах.	2
Тема 4. Інформаційне протиборство, інформаційні війни та кібернетичний вплив. Основи інформаційного протиборства та концепція інформаційної війни. Принципи кібернетичної розвідки та кібернетичного впливу. Поняття та класифікація кібернетичної зброї, методи та засоби її застосування проти держави й критичних інфраструктур.	2
Тема 5. Психологічні операції та інформаційно-психологічна безпека держави. Поняття психологічної війни, методи психологічного впливу та їх застосування у воєнних і гібридних конфліктах. Основи інформаційно-психологічної безпеки,	2

принципи безпеки у психосфері, сили та засоби протидії психологічним атакам.	
Тема 6. Інтернет-простір, соціальні мережі, кіберцивілізація та глобальна інформаційна безпека. Особливості правовідносин в Інтернеті. Проблеми глобалізації інформаційного простору, кіберсоціалізації та мережевої мобілізації. Кіберзлочинність та кібертероризм: визначення, міжнародні акти, українське законодавство. Загрози для держави в умовах кіберцивілізації.	2
Тема 7. Захист персональних даних і конфіденційної інформації в державі. Види персональних даних, принципи їх захисту, європейська система GDPR. Національні нормативні документи, механізми державної політики щодо забезпечення конфіденційності та безпеки персональної інформації громадян.	2
Тема 8. Правові засади, стратегічні документи та юридична відповідальність у сфері інформаційної безпеки. Стратегічні документи України: Стратегія національної безпеки, Стратегія кібербезпеки, Доктрина інформаційної безпеки, Концепція розвитку сектору безпеки і оборони. Правова відповідальність за порушення в сфері інформаційної безпеки (адміністративна, кримінальна, цивільна). Законодавчі норми щодо кібербезпеки та інформаційної сфери.	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти *a*
Тема 1. Порівняння даних за допомогою хешу. Вивчення принципів створення хеш-значень та їх застосування для перевірки цілісності файлів. Практичне порівняння хешів різних алгоритмів (MD5, SHA-1, SHA-256) та аналіз їх стійкості.	4	0,1
Тема 2. Методи та шляхи збору та обробки інформації. «Що було зроблено?». Ознайомлення з методами OSINT, аналіз джерел інформації, способи верифікації даних. Практичне завдання щодо збору цифрових слідів і підготовки короткого звіту про отримані результати.	4	0,1
Тема 3. Створення та збереження надійних паролів. Практичні методики формування стійких паролів, використання менеджерів паролів, впровадження багатофакторної автентифікації. Оцінка надійності паролів за допомогою спеціальних інструментів.	3	0,1
Тема 4. Резервне копіювання даних до зовнішнього сховища. Виконання резервного копіювання локальних даних у хмарні та фізичні зовнішні сховища. Порівняння різних способів бекапу та перевірка відновлення інформації.	3	0,1
Тема 5. Інформаційне протиборство. Хто володіє вашими даними? Аналіз цифрових слідів, що залишаються в Інтернеті. Дослідження політик конфіденційності сервісів, оцінка ризиків витоку персональних даних та моделювання загроз визначеному профілю користувача.	3	0,1

Тема 6. Аналітичне забезпечення інформаційної безпеки. Дослідження ризиків поведінки в Інтернеті (командна робота). Командний аналіз поведінкових сценаріїв користувачів. Визначення ризикових дій у мережі, оцінка ймовірних наслідків та побудова рекомендацій щодо безпечної поведінки онлайн.	3	0,1
Тема 7. Класифікація програмних і криптографічних засобів забезпечення ІБ. Дослідження різних типів програмних рішень: антивірусів, IDS/IPS, VPN, криптопровайдерів. Практичне ознайомлення з алгоритмами шифрування та інструментами криптографічного захисту.	3	0,1
Тема 8. Електронна ідентифікація користувачів. Нормативне забезпечення. Загрози безпеки. Практика роботи з системами електронної ідентифікації (BankID, MobileID, ЕЦП/КЕП). Огляд нормативних документів у сфері ІБ. Аналіз можливих загроз і способів їх мінімізації.	3	0,1
Тема 9. Технічні засоби забезпечення інформаційної безпеки: класифікація та характеристика. Вивчення технічних засобів захисту: міжмережевих екранів, апаратних криптомодулів, систем контролю доступу. Практичне знайомство з принципами їх роботи та налаштування.	3	0,1
Тема 10. Міжнародні стандарти та рекомендації в галузі інформаційної безпеки. Розгляд стандартів ISO/IEC 27000, NIST, рекомендацій ЄС. Практична робота зі структурою стандарту ISO/IEC 27001: аналіз вимог та формування прикладних політик безпеки.	3	0,1
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 1$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Стан, загрози та основні засади забезпечення інформаційної безпеки держави. У роботі необхідно проаналізувати сутність інформаційної безпеки держави, її складові та місце в системі національної безпеки. Розкрити класифікацію основних загроз інформаційній безпеці України, дестабілізуючі фактори, питання інформаційного насильства та маніпуляцій. Дати характеристику Доктрини інформаційної безпеки України та пріоритетам державної політики в інформаційній сфері. Оцінити актуальні ризики для держави в сучасних умовах.	0,1
Тема 2. Інформаційне протиборство, кіберзагрози та правові засади забезпечення кібербезпеки. Контрольна передбачає дослідження основ інформаційного протиборства, концепції інформаційної війни, основ кіберрозвідки та кібернетичного впливу. Необхідно розкрити суть кібернетичної зброї, її класифікацію та методи застосування. Додатково слід проаналізувати правові та нормативні акти у сфері інформаційної та кібербезпеки: Воєнну доктрину, Доктрину інформаційної безпеки, Стратегію кібербезпеки, Закон України «Про основні засади забезпечення кібербезпеки України». Особлива увага — юридичній відповідальності за правопорушення у сфері інформаційної безпеки.	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. Сучасні методи інформаційних операцій та їх вплив на національну безпеку. Аналіз інформаційно-психологічних операцій, цілей, інструментів та реальних прикладів їх застосування.	8
Тема 2. Роль спецслужб у забезпеченні інформаційної безпеки держави. Функції, завдання та приклади діяльності українських та міжнародних служб у сфері кібер- та інформаційної розвідки.	8
Тема 3. Державна політика щодо протидії дезінформації та фейковим новинам. Інструменти моніторингу, виявлення та запобігання поширенню дезінформації.	7
Тема 4. Функціонування національних центрів реагування на комп'ютерні інциденти (CERT/CSIRT). Структура, принципи роботи та приклади діяльності міжнародних CERT.	7
Тема 5. Міжнародне співробітництво у сфері інформаційної та кібербезпеки. Роль НАТО, ЄС, ООН, Будапештської конвенції; міжнародні ініціативи.	7
Тема 6. Пропаганда та контрпропаганда в інформаційному просторі. Історичні та сучасні методи, засоби впливу на громадську думку та механізми протидії.	7
Тема 7. Захист державних інформаційних ресурсів та державних реєстрів. Технічні заходи, організаційні підходи, актуальні загрози цифровим реєстрам.	7
Тема 8. Роль штучного інтелекту у сучасних інформаційних конфліктах. Використання ШІ для дезінформації, кіберрозвідки, автоматичного аналізу даних.	7
Тема 9. Інформаційні ризики глобалізації та цифровізації суспільства. Нові загрози в умовах розвитку соцмереж, IoT, великих даних.	7
Тема 10. Психологічні аспекти кіберсоціалізації та їх вплив на безпеку держави. Формування інформаційної поведінки громадян, мобілізаційні процеси в соцмережах, загрози кіберцивілізації.	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

1. Онлайн-курс CISCO «Cyber Ess»
https://www.netacad.com/catalogs/learn?category=course.

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. – Режим доступу: http://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf.
2. Богуш В. М., Юдін О. К. Інформаційна безпека держави. – К.: “МК-Прес”, 2005. – 432с.
3. Термінологічний довідник з питань технічного захисту інформації / Коженевський С.Р., Кузнецов Г.В., Хорошко В.О., Чирков Д.В. / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2007. – 365 с.
4. Бобало Ю.Я., Горбатий І.В. (ред.) Інформаційна безпека. Навчальний посібник. — Львів : Видавництво Львівської політехніки, 2019. — 580 с. — ISBN 978-966-941-339-0.
https://pdf.lib.vntu.edu.ua/books/2021/Bobalo_2019_580.pdf.
5. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека»/ В.І. Гур’єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. – Ніжин: ФОП Лук’яненко В.В. ТПК «Орхідея», 2018. – 166 с.
http://ir.stu.cn.ua/bitstream/handle/123456789/19246/%d0%86%d0%bd%d1%84%d0%be%d1%80%d0%bc.%20%d0%b1%d0%b5%d0%b7%d0%bf%d0%b5%d0%ba%d0%b0%20%d0%b4%d0%b5%d1%80%d0%b6.%20New%20booklet%201.pdf?sequence=1&isAllowed=y.

Додаткова література

6. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. Дата оновлення: 31.12.2023. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
7. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. Дата оновлення: 27.10.2022. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
8. Указ Президента України: Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України": Указ Президента України від 6 травня 2015 року № 287/2015. Дата оновлення: 16.09.2020. URL: https://zakon.rada.gov.ua/laws/show/287/2015#Text
9. Про національну безпеку: Закон України від 21.06.2018 № 2469-VIII. Дата оновлення: 31.03.2023. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text
10. 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
11. 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
12. 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.
13. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
14. 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. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju

15. 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. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju

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 Роман КОРОЛЬОВ