Силабус освітнього компонента
Програма навчальної дисципліни

Захист об´єктів критичної інфраструктури

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
Вибіркова

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна

Семестр
8

Мова викладання
Українська

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

СЕВРЮКОВА Єлизавета Олександрівна

yelizaveta.sevriukova@khpi.edu.ua
PhD,, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 8, з яких 4 статті у фахових виданнях України, 1 у наукометричній базі Scopus, 3 статті у закордонних наукових публікаціях гарант освітньо-професійної програми «Кібербезпека» другого (магістерського) рівня вищої освіти. Провідний лектор з дисциплін: «Захист об´єктів критичної інфраструктури», «Етичний хакінг» , «Ризик-менеджмент», «Блокчейн та смарт-технології в електронному документообігу»», «Protection from technical intelligence

service», «Protection of critical infrastructure objects», у студентів бакалавріата та магістратури.
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Захист об´єктів критичної інфраструктури" є вибірковою навчальною дисципліною. Вивчення дисципліни спрямовано на визначення інформації, що потребує захисту на об'єктах критичної інфраструктури (ОКІ). Опанування методів та засобів технічного захисту інформації на ОКІ. Ознайомлення з каналами витоку інформації та підстав їх утворення. Оволодіння навичками роботи із засобами та комплексами виявлення закладних пристроїв несанкціонованого отримання інформації. Оволодіння навичками роботи із засобами та комплексами захисту інформації на ОКІ. Засвоєння порядку проведення обстеження і аналізу ОКІ з метою забезпечення захисту інформації. Оволодіння організаційно-технічними заходами щодо захисту інформації на ОКІ.

Мета та цілі дисципліни

Навчання студентів принципам визначення загальних вимог до кіберзахисту об'єктів критичної інфраструктури, встановлення переліку базових заходів з кіберзахисту, які повинні бути впроваджені на об'єкті критичної інфраструктури, на основі вимог міжнародних стандартів з інформаційної безпеки, державних нормативних документів з технології захисту інформації, визначення порядку та критеріїв віднесення об'єктів до об'єктів критичної інфраструктури.

Формат занять

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

Компетентності

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.
СК2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.
СК3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.
СК5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.
СК7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації.
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.
СК11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.

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.
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.
РН8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки.
РН10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.
РН11. Вміти забезпечувати процеси захисту та функціонування системи управління інформаційною безпекою та захисту інформації на основі практик, навичок та знань, щодо інфраструктури кіберфізичних систем та інформаційних потоків.
РН12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
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 90 год. (3 кредити ECTS): лекції – 10 год., лабораторні роботи – 20 год., самостійна робота – 60 год.

Передумови вивчення дисципліни (пререквізити)

Вища математика, Математичні основи криптології, Комплексні системи захисту інформації.

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. Загальні вимоги та принципи захисту об'єктів критичної інфраструктури. Фізичний та кіберзахист об'єктів критичної інфраструктури. Розгляд базових вимог до кіберзахисту, національної політики у сфері захисту критичної інфраструктури та ролі нормативно-правових актів. Інструменти фізичної безпеки, сучасні SOC-центри, захист інфраструктурних комунікацій та основні кіберзагрози.	2
Тема 2. Управління кризовими ситуаціями та реагування на інциденти. Моделі оцінювання рівня захищеності, координація дій під час кризових ситуацій, концепції ліквідації наслідків атак та кризове управління.	2
Тема 3. Захист галузевих інфраструктур (телекомунікаційної, енергетичної, фінансової). Основні вразливості та методи захисту у сферах телекомунікацій, енергетики та фінансів. Технології NGFW, UTM, DLP, двофакторна автентифікація та захист транзакцій.	2
Тема 4. Управління ризиками та протидія терористичним загрозам. Методи аналізу ризиків, інструментальні засоби управління ризиками, фактори виникнення терористичних загроз і заходи їх протидії.	2
Тема 5. Міжнародна співпраця у сфері захисту критичної інфраструктури. Роль міжнародних організацій, договорів і стратегій, досвід України та інших країн у створенні системи колективної кібербезпеки.	2
Загальна кількість годин	**10**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти *a*
Тема 1. Вивчення загальних вимог до кіберзахисту об'єктів критичної інфраструктури. Ознайомлення з базовими принципами та нормативними вимогами до організації захисту критичних об'єктів від кіберзагроз.	2	-
Тема 2 Критична інфраструктура за регіонами України. Організаційні засади регіону України як складові національної системи захисту критичної інфраструктури. Дослідження особливостей розподілу об'єктів критичної інфраструктури в регіонах України та їх ролі у національній системі безпеки.	2	-
Тема 3. Складання відомостей про об'єкт критичної інформаційної інфраструктури визначеного регіону України. Практичне завдання зі збору та аналізу інформації про конкретний об'єкт КІІ у визначеному регіоні з метою оцінки його значущості та вразливостей.	2	0,1
Тема 4. Вивчення особливостей національної системи захисту критичної інфраструктури. Огляд структури, функцій та взаємодії суб'єктів у національній системі кіберзахисту критичної інфраструктури.	2	-
Тема 5. Вивчення особливостей формування Технічних вимог на створення спеціалізованого програмного забезпечення «Державний реєстр об'єктів критичної	2	0,1

інформаційної інфраструктури». Аналіз вимог до проєктування та функціонування державного реєстру КІІ як ключового інструменту моніторингу та контролю.		
Тема 6. Дослідження заходів із забезпечення кіберзахисту критичної інформаційної інфраструктури банків. Вивчення банківських систем як частини КІІ та аналіз специфічних заходів захисту їхньої інформаційної інфраструктури.	2	0,1
Тема 7. Методичні рекомендації щодо розробки поточного та цільового профілю кіберзахисту. Практичне застосування рекомендацій для формування профілів безпеки та порівняння їх з реальним станом кіберзахисту об'єкта.	4	-
Тема 8. Проведення класифікації заходів кіберзахисту об'єктів критичної інфраструктури. Систематизація заходів кіберзахисту за різними критеріями (організаційні, технічні, правові) з метою створення комплексної системи безпеки.	4	0,1
Загальна кількість годин	**20**	$\sum_{i=1}^{n} a_i$=0,4

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Загальні та фізичні аспекти кіберзахисту критичної інфраструктури. Контрольна робота охоплює базові вимоги до кіберзахисту, фізичний захист об'єктів та організацію управління кризовими ситуаціями. Студенти повинні продемонструвати знання про основні загрози, структури SOC, методи запобігання інцидентам та забезпечення безпеки телекомунікаційних мереж.	0,1
Тема 2. Галузеві та міжнародні аспекти захисту критичної інфраструктури. Контрольна робота присвячена захисту електроенергетичної та фінансової інфраструктури, міжнародній співпраці, протидії терористичним загрозам та інструментам управління ризиками інформаційної безпеки. Студенти повинні показати розуміння специфіки загроз, методів захисту та ролі систем управління у забезпеченні кібербезпеки критичних об'єктів.	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. Кіберзагрози для критичної інфраструктури. Вивчення типових кіберзагроз, їх джерел та потенційних наслідків для критичних об'єктів.	6
Тема 2. Системи моніторингу та раннього попередження. Принципи роботи систем моніторингу, аналіз сповіщень та автоматизація реагування на інциденти.	6

Тема 3. Методи оцінки ризиків для критичної інфраструктури. Класифікація ризиків, методи їх кількісної та якісної оцінки, приклади застосування моделей оцінки.	6
Тема 4. Захист енергетичних об'єктів та інфраструктури IoT. Стратегії та технології для захисту енергетичних мереж та IoT-пристроїв від кібератак.	6
Тема 5. Фінансова та банківська кібербезпека. Методи захисту фінансових транзакцій, банківських інформаційних систем та платіжної інфраструктури.	6
Тема 6. Кризис-менеджмент у кібербезпеці. Фази кризових ситуацій, моделі реагування та координація дій різних агентів у випадку інцидентів.	6
Тема 7. Законодавче регулювання та стандарти кіберзахисту. Основні нормативні документи, стандарти ISO/IEC, вимоги державної політики щодо захисту критичної інфраструктури.	6
Тема 8. Технології сегментації та контролю доступу. Сегментація мережі, мікросегментація, двофакторна аутентифікація та принципи обмеження доступу до критичних ресурсів.	6
Тема 9. Міжнародна співпраця у сфері кібербезпеки. Міжнародні організації, договори, механізми обміну інформацією та координації заходів захисту критичної інфраструктури.	6
Тема 10. Аналіз інцидентів та навчання на прикладах. Вивчення практичних кейсів кіберінцидентів, методи розслідування, документування та вдосконалення заходів безпеки.	6
Загальна кількість годин	**60**

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 «CyberOps»
https://www.netacad.com/catalogs/learn?category=course.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX. Дата оновлення: 01.01.2024. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text
2. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518. Дата оновлення: 07.09.2022. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text
3. Деякі питання об'єктів критичної інформаційної інфраструктури: Постанова Кабінету Міністрів України від 9 жовтня 2020 р. № 943. Дата оновлення: 07.09.2022. URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text

4. Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 06 жовтня 2021 року № 601.
https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601
5. Про затвердження форм подання відомостей до державного реєстру об'єктів критичної інформаційної інфраструктури: Наказ Адміністрації Держспецзв'язку від 02.09.2023 №793
https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-pro-zatverdzhennya-form-podannya-vidomostei-do-derzhavnogo-reyestru-ob-yektiv-kritichnoyi-informaciinoyi-infrastrukturi-vid-02-veresnya-2023-roku-793
6. Про затвердження Положення про організацію кіберзахисту в банківській системі України: Постанова Правління Національного банку України від 12.08.2022 № 178. URL: https://zakon.rada.gov.ua/laws/show/v0178500-22#Text
8. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с.
http://kist.ntu.edu.ua/textPhD/tzi.pdf
9. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. http://monograph.com.ua/pctc/catalog/view/64/52/231-1
10. 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. http://monograph.com.ua/pctc/catalog/view/978-617-7319-72-5/978-617-7319-72-5/746-2
11. 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. http://monograph.com.ua/pctc/catalog/view/978-617-7319-57-2/117/419-2.

Додаткова література

12. 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
13. 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
14. 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 .

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