Силабус освітнього компонента
Програма навчальної дисципліни

Менеджмент інформаційної безпеки

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
2

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

Загальна інформація

Анотація

Навчальна дисципліна "Менеджмент інформаційної безпеки" є нормативною навчальною дисципліною. Дисципліна спрямована на набуття студентом теоретичних знань та практичних навичок щодо управління інформаційною безпекою в інформаційно-телекомунікаційних (автоматизованих) системах для реалізації встановленої політики безпеки.

Мета та цілі дисципліни

Формування у студентів теоретичних знань основних принципів менеджменту управління інцидентами та ризиками на основі вимог міжнародних регуляторів.

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.
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.
СК6. Здатність використовувати іноземну мову для отримання додаткових знань і умінь з питань управління інформаційною безпекою, взаємодіяти з іноземними партнерами.
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.
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.
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 120 год. (4 кредити ECTS): лекції – 16 год., лабораторні заняття – 32 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Математичний аналіз, Лінійна алгебра, Теорія ймовірностей і математична статистика, Дискретна математика, Інформатика, Програмування, Правове регулювання кібербезпеки.

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 та управління інцидентами. Визначення понять інформаційної безпеки, кіберзагроз і критичних інфраструктур. Розгляд реальних інцидентів (кібератаки на АЕС, Carbanak) та сучасних викликів. Ознайомлення зі стандартами ISO/IEC 27001 і ISO/IEC 27035, принципами інцидент-менеджменту та вимогами до управління інцидентами.	2
Тема 2. Менеджмент інцидентів та управління ризиками. Аналіз життєвого циклу IT-систем, оцінка ризиків і вразливостей, визначення загроз та контролю. Вивчення підходів до зменшення ризиків, залишкового ризику та рентабельності заходів безпеки. Стандартизовані методи управління	2

ризиками (ISO/IEC 27001, SDLC).	
Тема 3. Системи менеджменту інцидентів і стандарти ITIL. Концепція побудови систем управління інцидентами ІБ за міжнародними стандартами ITIL. Функціональна структура, принципи та процеси менеджменту інцидентів у сучасних організаціях.	2
Тема 4. CERT/CSIRT — групи реагування на інциденти безпеки. Історія створення, види та структура груп CERT/CSIRT. Мета, принципи роботи, переваги впровадження. Роль таких груп у системі національної та корпоративної безпеки.	2
Тема 5. Інструменти та документація для управління інцидентами ІБ. Документальне забезпечення процесів безпеки (політики, процедури, звіти). Функціонування SOC (Security Operation Center), його моделі та інструменти. Практичні приклади документів та інструментарію реагування на інциденти.	2
Тема 6. Управління ризиками та міжнародні стандарти безпеки. Розгляд міжнародних стандартів ISO 31000, NIST Cybersecurity Framework. Етапи процесу управління ризиками, впровадження рамкових програм, оцінка ефективності заходів кіберзахисту.	2
Тема 7. Політика інформаційної безпеки та система менеджменту ІБ (СМІБ). Розробка, структура та зміст політик ІБ. Основи створення системи менеджменту інформаційної безпеки (СМІБ) відповідно до ISO/IEC 27001. Приклади ефективних і неефективних політик, принципи оцінки результативності.	2
Тема 8. Аудит, моніторинг та реагування на інциденти. Проведення аудиту безпеки, аналіз ризиків, моніторинг мережевих подій. Методи виявлення атак, аналіз попереджень, реагування та документування інцидентів. Основи післяінцидентного аналізу та удосконалення політик безпеки.	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лекцій	Кількість годин	Вагові коефіцієнти a
Тема 1. Розгортання операційної системи для проведення аудиту інформаційної безпеки комп'ютерних мереж та систем. Ознайомлення з налаштуванням спеціалізованого середовища (наприклад, Kali Linux або Security Onion) для аудиту безпеки. Вивчення інструментів для аналізу мережевої активності, журналів подій та контролю цілісності системи.	3	0,1
Тема 2. Інструменти прихованого збору технічної інформації з комп'ютерної системи або мережі. Вивчення методів пасивного збору інформації про мережеву інфраструктуру, використання засобів OSINT і footprinting. Практична робота з інструментами типу Nmap, Netdiscover, theHarvester.	3	0,1
Тема 3. Дослідження вразливостей систем та веб-ресурсів за	3	0,1

допомогою спеціалізованих сканерів вразливостей (Nessus, Vega). Ознайомлення з принципами роботи сканерів вразливостей. Виконання аналізу веб-додатків та мережевих сервісів для виявлення слабких місць і створення звіту з результатами сканування.		
Тема 4. Визначення вразливостей веб-ресурсів та веб-додатків. Сканер вразливостей – Vega. Використання Vega для автоматизованого тестування веб-додатків. Аналіз знайдених вразливостей (XSS, SQL Injection тощо) та пропозиції щодо їх усунення.	3	0,1
Тема 5. Пошук вразливостей та чуттєвої інформації у відкритих ресурсах за допомогою засобу Maltego. Практичне застосування Maltego для збору даних про організації, домени, IP-адреси, користувачів. Формування графових зв'язків між об'єктами для оцінки ризиків витоку інформації.	3	0,1
Тема 6. Збір технічної та чуттєвої інформації за допомогою ПЗ класу – сніфери. Використання програм Wireshark, TCPdump для перехоплення та аналізу мережевого трафіку. Ідентифікація потенційних витоків даних і виявлення підозрілої активності.	3	0,1
Тема 7. Засіб дослідження вразливостей безпровідних мереж Wi-Fi – Aircrack-ng. Дослідження методів атаки на бездротові мережі. Аналіз безпеки Wi-Fi (WEP/WPA), захоплення трафіку та підбір ключів доступу з метою оцінки захищеності.	3	0,1
Тема 8. Правила Snort та правила міжмережевого екрану. Ознайомлення з принципами роботи IDS/IPS систем. Створення, тестування та оптимізація правил Snort. Налаштування міжмережевого екрану для блокування потенційних атак.	3	0,1
Тема 9. Вилучення виконуваного файлу з PCA. Практична робота з Packet Capture Analysis для виділення переданих у мережі виконуваних файлів (EXE). Аналіз отриманих даних для виявлення шкідливого ПЗ.	3	0,1
Тема 10. Інтерпретація даних HTTP та DNS для ізоляції зловмисника. Аналіз мережевого трафіку з метою виявлення шкідливої активності через HTTP та DNS. Визначення джерел загроз і створення сценаріїв реагування.	3	0,1
Тема 11. Обробка інцидентів. Розбір етапів життєвого циклу інциденту безпеки. Практична імітація процесу реагування: виявлення, аналіз, локалізація, усунення та документування інциденту.	2	0,1
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 1{,}1$

Контрольні роботи

Теми контрольних робіт	Вагові

	коефіцієнти b
Тема 1. Організаційно-технічні засади аудиту інформаційної безпеки комп'ютерних систем. Аналіз принципів і методів проведення аудиту безпеки. Визначення основних етапів аудиту, документування результатів, оцінка відповідності системи політиці інформаційної безпеки.	0,1
Тема 2. Аналіз і оцінювання вразливостей мережевих ресурсів засобами спеціалізованого програмного забезпечення. Виконання практичного дослідження вразливостей за допомогою сканерів безпеки (Nessus, Vega, Maltego тощо). Формування звіту з оцінкою ризиків і рекомендаціями щодо підвищення захищеності системи.	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. Нормативно-правове забезпечення аудиту інформаційної безпеки. Огляд законодавчих актів, міжнародних стандартів ISO/IEC 27001, 27002 та інших документів, що регламентують проведення аудиту безпеки.	8
Тема 2. Політика інформаційної безпеки організації. Принципи побудови, структура та роль політики ІБ у забезпеченні захищеності інформаційних систем.	8
Тема 3. Класифікація загроз і вразливостей комп'ютерних систем. Типологія загроз безпеці, методи виявлення вразливостей, їх оцінка та мінімізація ризиків.	7
Тема 4. Методології аудиту інформаційної безпеки. Порівняння міжнародних підходів до аудиту — COBIT, NIST, ITIL. Переваги та недоліки кожного методу.	7
Тема 5. Аналіз журналів подій і моніторинг безпеки. Методи збору, обробки та аналізу логів. Використання SIEM-систем для виявлення інцидентів безпеки.	7
Тема 6. Засоби виявлення вторгнень (IDS/IPS). Принципи роботи, класифікація систем виявлення вторгнень, їхня роль в аудиторських перевірках безпеки.	7
Тема 7. Оцінювання ефективності систем захисту інформації. Методи оцінки ефективності технічних і організаційних засобів захисту, показники ефективності.	7
Тема 8. Управління ризиками інформаційної безпеки. Поняття ризику, методи ідентифікації та оцінки ризиків, розробка плану реагування.	7
Тема 9. Тестування на проникнення (penetration testing). Поняття, етапи проведення тесту на проникнення, інструменти та правила етичного використання.	7
Тема 10. Формування звітності за результатами аудиту інформаційної	7

безпеки. Вимоги до звітів, структура документа, оформлення висновків і рекомендацій щодо усунення недоліків.	
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 Threat Management»

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

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Менеджмент інформаційної безпеки : навчальний посібник для студентів спеціальності 125 "Кібербезпека" / О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук, Ю.М. Ткач, Є.В. Іванченко. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 408 с. : іл.
http://ir.stu.cn.ua/bitstream/handle/123456789/19244/%d0%9c%d0%b5%d0%bd%d0%b5%d0%b4%d0%b6%d0%bc%d0%b5%d0%bd%d1%82%20%d1%96%d0%bd%d1%84%d0%be%d1%80%d0%bc.%20%d0%b1%d0%b5%d0%b7%d0%bf.%20New%20booklet%201.pdf?sequence=1&isAllowed=y
2. 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/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
3. 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/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
4. 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/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju

Додаткова література

5. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems.
https://www.iso.org/ru/standard/27001
6. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України/ [Електронний ресурс].
https://zakon.rada.gov.ua/laws/show/v0365500-11#Text
7. ДСТУ ISO/IEC TR 13335-1:2003 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки інформаційних технологій. [Електронний ресурс].
http://lindex.net.ua/ua/shop/bibl/500/doc/11423
8. ДСТУ ISO/IEC TR 13335-2:2003 Інформаційні технології. Частина 2. Настанови з управління безпекою інформаційних технологій. [Електронний ресурс].
http://www.premier-hs.com.ua/content/dstu-isoiec-tr-13335-22003-nastanovi-z-kieruvannia-biezpiekoiu-informatsiinikh-tiekhnologhii Дата звернення: Декабрь. 7.2017.

9. ДСТУ ISO/IEC TR 13335-3:2003 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 3. Методи управління захистом інформаційних технологій. [Електронний ресурс].
http://lindex.net.ua/ua/shop/bibl/500/doc/11425
10. ДСТУ ISO/IEC TR 13335-4:2005 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 4. Вибірання засобів захисту. [Електронний ресурс].
http://metrology.com.ua/download/iso-iec-ohsas-i-dr/61-iso/290-dstu-iso-iec-tr-13335-4-2005
11. ДСТУ ISO/IEC TR 13335-5:2005 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 5. Настанова з управління мережевою безпекою. [Електронний ресурс].

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