



Силабус освітнього компонента

Програма навчальної дисципліни

Ризик-менеджмент



Шифр та назва спеціальності

K4 – 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

4

Мова викладання

Українська

Викладачі, розробники



ЄВСЕЄВ Сергій Петрович

serhii.yevseyev@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 статей 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](#)



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.

Загальна інформація

Анотація

Навчальна дисципліна "Ризик-менеджмент" є вибірковою навчальною дисципліною. Дисципліна спрямована на формування фахових компетенцій щодо виявлення, оцінювання та управління ризиками у процесі засвоєння теоретичних та практичних аспектів ризик-менеджменту.

Мета та цілі дисципліни

Оволодіння майбутніми фахівцями компетентностей, що забезпечують ефективне управління ризиками в сучасних кіберсистемах, уможливають кваліфіковану оцінку ризиків в умовах широкого використання сучасних методів кібербезпеки.

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.

PH12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

PH13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах.

PH14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.

PH16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.

PH17. Вміти розв'язувати задачі управління інформаційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.

PH18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.

PH19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-комунікаційних системах.

PH20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.

PH21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.

PH22. 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 – 16 год., лабораторні роботи – 16 год., самостійна робота – 58 год.

Передумови вивчення дисципліни (пререквізити)

Вища математика, Менеджмент інформаційної безпеки, Основи математичного моделювання систем безпеки.

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 проекти, майстер-класи.

Програма навчальної дисципліни

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Основи кібербезпеки та управління ризиками. Основні поняття та визначення у сфері кібербезпеки. Класифікація та ознаки ризиків. Схема та етапи управління ризиками. Методи оцінки ризику та загроз. Ризики безпеки Microsoft.	2
Тема 2. Кіберзагрози та методи їх прогнозування. Шкідливе програмне забезпечення. Типові мережеві атаки (розвідка, доступ, соціальна інженерія). Атаки відмови в обслуговуванні, переповнення буфера,	2

ухилення. Хто атакує мережу та які інструменти використовуються.

Тема 3. Ідентифікація та моніторинг активів інформаційних систем.

2

Ідентифікація інформаційних ресурсів, ПЗ, користувачів і ролей. Оцінка важливості активів. Управління життєвим циклом активів. Моніторинг мережі та інструменти моніторингу.

Тема 4. Управління кризовими ситуаціями та антикризове управління.

2

Ефективне управління кризовими ситуаціями у критичній інфраструктурі. Класифікатор загроз, моделі безпеки. Удосконалення моделі оцінювання рівня захищеності. Координація дій агентів під час криз. Сутність поняття «криза», фази та наслідки кризи. Фактори та класифікація кризових явищ. Антикризова програма та завдання менеджера.

Тема 5. Внутрішні та зовнішні загрози. IDS та IPS.

2

Класифікація кіберінцидентів. Вразливості IP, TCP, UDP, корпоративних сервісів. Системи виявлення та запобігання вторгнень (IDS/IPS). Методи моніторингу системи. Порівняльний аналіз сучасних систем IDS/IPS. Приклади використання (Security Onion).

Тема 6. Моделі загроз та порушників.

2

Механізми деструктивного впливу на інформаційні системи. Модель порушника інформаційної безпеки. Основні канали витоку інформації. Інсайдери: типи, мотивація, способи реалізації атак.

Тема 7. Політика інформаційної безпеки та система менеджменту (СМІБ).

2

Система менеджменту інформаційної безпеки. Послідовність дій при розробці СМІБ. Приклади вдалих і невдалих політик. Бюджетування та витрати на кіберзахист.

Тема 8. Управління інцидентами інформаційної безпеки.

2

Взаємозв'язок понять «інцидент» і «ризик». Зміст процесу управління інцидентами. Причини виникнення інцидентів. Структура та функції команди з розслідування інцидентів. Нормативні документи з управління інцидентами. Виявлення, документування, протидія поширенню. Ідентифікація порушників, зберігання матеріалів, контрольні листи.

Загальна кількість годин

16

Лабораторні заняття

Теми лабораторних занять

**Кількість
годин**

**Вагові
коефіцієнти α**

Тема 1. Встановлення віртуальної машини CyberOps Workstation.

4

0,1

Кібербезпека: практичні приклади. Вивчення відомостей про атаку. Візуалізація "чорних" хакерів. Як стати захисником.

Тема 2 Вивчення процесів, потоків, дескрипторів та реєстру Windows.

4

0,1

Створення облікових записів користувачів. Використання Windows PowerShell. Диспетчер завдань Windows. Моніторинг системних ресурсів у Windows та керування ними.

Тема 3. Відстеження маршруту. Знайомство з Wireshark.

4

0,1

Використання Wireshark для дослідження кадрів Ethernet. Використання Wireshark для спостереження за тристороннім рукописанням TCP. Використання Wireshark для дослідження

захоплених UDP DNS повідомлень. Використання Wireshark для дослідження TCP та UDP захоплених пакетів. Використання Wireshark для дослідження HTTP та HTTPS трафіку. Дослідження DNS-трафіку. Атака на базу даних MySQL. Використання Wireshark для дослідження HTTP та HTTPS трафіку. Дослідження DNS-трафіку. Атака на базу даних MySQL.

Тема 4. Використання Wireshark для дослідження кадрів Ethernet.	4	0,1
Розгляд інструменту Wireshark як основного засобу аналізу мережевого трафіку. Основи роботи з інтерфейсом програми, фільтрація та відображення пакетів. Дослідження структури кадру Ethernet: поля MAC-адрес, типу протоколу, даних та контрольної суми. Практичне застосування для виявлення помилок передачі, аналізу мережевих атак та діагностики проблем у локальних мережах.		
Загальна кількість годин	16	$\sum_{i=1}^n a_i=0,4$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Управління ризиками та загрозами в кібербезпеці.	0,1
Перевірка знань студентів щодо основних понять і підходів у сфері кібербезпеки, процесів управління ризиками та прогнозування загроз, а також умінь ідентифікувати активи інформаційних систем, будувати моделі загроз та порушників, аналізувати внутрішні й зовнішні загрози. Особлива увага приділяється кризис-менеджменту, політикам інформаційної безпеки та управлінню інцидентами.	
Тема 2. Оцінка та управління ризиками в організаціях.	0,1
Перевірка знань студентів щодо методів оцінки ризиків, класифікації та пріоритизації ризиків у бізнес-процесах та інформаційних системах. Студенти демонструють вміння застосовувати інструменти моніторингу, аналізувати загрози, а також пропонувати заходи з мінімізації ризиків та формування ефективної політики управління ризиками.	
Загалом	$\sum_{i=1}^m b_i=0,2$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин
Тема 1. Види та класифікація ризиків.	6
Поняття фінансових, операційних, стратегічних та інформаційних ризиків. Основні критерії класифікації.	
Тема 2. Методи ідентифікації ризиків.	6
SWOT-аналіз, методи мозкового штурму, сценарне планування, Check-листи ризиків.	
Тема 3. Оцінка ймовірності та наслідків ризиків.	6
Кількісні та якісні методи оцінки: матриці ризиків, експертні оцінки, статистичні	

моделі.

Тема 4. Квантитативне та якісне управління ризиками.

6

Методи управління ризиками: уникнення, зниження, передача, прийняття ризику.

Тема 5. Моніторинг та контроль ризиків.

6

Використання показників ризику, контрольні точки, системи раннього попередження.

Тема 6. Управління ризиками в інформаційних системах.

6

Ризики кібербезпеки, вразливості програмного та апаратного забезпечення, політики безпеки.

Тема 7. Фінансові ризики та страхування.

6

Види фінансових ризиків, інструменти страхування, хеджування ризиків.

Тема 8. Кризис-менеджмент та планування заходів.

6

Фази кризи, розробка антикризових планів, комунікація під час кризових ситуацій.

Тема 9. Регуляторні та правові аспекти управління ризиками.

5

Законодавчі вимоги, стандарти ISO, GDPR та їх вплив на управління ризиками.

Тема 10. Використання інформаційних технологій у ризик-менеджменті.

5

Програмне забезпечення для оцінки ризиків, моделювання сценаріїв, автоматизація процесів управління ризиками.

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 «Cyber Threat Management»

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

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Ozkaya, Erdal. Learn Social Engineering: Learn the art of human hacking with an internationally renowned expert. Packt Publishing Ltd, 2018.- 557 p.

<https://h.twirpx.link/file/2523887/>

2. Alexander, Michael; Wanner, R. Methods for understanding and reducing social engineering attacks. SANS Inst., 2016, 1: 1-32.

<https://www.giac.org/paper/gccc/270/methods-understanding-reducing-social-engineering-attacks/147205>

3. Hadnagy, Christopher. Social engineering: The science of human hacking. John Wiley & Sons, 2018 - 330 p.

http://repo.darmajaya.ac.id/4637/1/Social%20Engineering_%20The%20Science%20of%20Human%20Hacking%20%28%20PDFDrive%20%29.pdf

4. Ethical Hacking: 3 in 1- Beginner's Guide+ Tips and Tricks+ Advanced and Effective measures of Ethical Hacking Paperback – July 23, 2020 – 456 p.
https://books.google.com.ua/books/about/Ethical_Hacking.html?id=7D3AzQEACAAJ&redir_esc=y
5. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа/. – Львів: "Магнолія 20062, 2018 - 320с.
<https://spadok.org.ua/books/Buryachok-Osnovy-info-ta-ciberbezpeky.pdf>
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>.
7. 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>.
8. 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>.

Додаткова література

1. 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>.
2. 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.
3. 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.
4. ISO/IEC 31010:2019 Risk management . URL:
<https://www.iso.org/ru/contents/data/standard/07/21/72140.html>
5. 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>
6. 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>
7. 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>
8. 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>
9. 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:

$$O = \Pi \cdot k_1 + K \cdot k_2 + I \cdot k_3 + \Pi_k \cdot k_4$$

де: Π – середньозважена середня оцінка за поточний контроль

I – оцінка за виконання індивідуального завдання

K – середньозважена оцінка за контрольні роботи

Π_k – оцінка за підсумковий контроль

$$\Pi = \frac{\Pi_1 \cdot a_1 + \Pi_2 \cdot a_2 + \dots + \Pi_n \cdot a_n}{\sum_{i=1}^n a_i}$$

де: a_i - ваговий коефіцієнт за кожне практичне (семінарське) або лабораторне заняття.

$$K = \frac{K_1 \cdot b_1 + K_2 \cdot b_2 + \dots + K_m \cdot b_m}{\sum_{i=1}^m b_i}$$

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (Π , K , I ,...))

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 O 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

