



Силабус освітнього компонента

Програма навчальної дисципліни



Ризик-менеджмент

Шифр та назва спеціальності

256 – Національна безпека (за окремими сферами забезпечення і видами діяльності)

Інститут

ННІ комп'ютерних наук та інформаційних технологій (320)

Освітня програма

Національна безпека у сфері кіберзахисту

Кафедра

Кібербезпеки (328)

Рівень освіти

Бакалавр

Тип дисципліни

Профільна підготовка, Вибіркова

Семестр

4

Мова викладання

Українська

Викладачі, розробники



ЄВСЕЄВ Сергій Петрович

serhii.yevseiev@khpi.edu.ua

Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 350, з них патентів на корисну модель 42, 17 монографій, з яких 9 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 163 статті у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Менеджмент інформаційної безпеки», «Введення в мережі», «Безпека банківських систем», «Гібридні війни та національна безпека», «Аудит та моніторинг корпоративних мереж», «Blockchain: основи та приклади застосування», «Основи смарт-контрактів», «Основи кібербезпеки» у студентів бакалавріата та магістратури, Розділ «Методи і технології моніторингу та аудиту інформаційної безпеки», «Методи побудови постквантових криптосистем», «Новітні технології забезпечення кібербезпеки на основі технології блокчейн» для аспірантів

[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 150, з яких 14 навчальних посібників, 48 статей у закордонних виданнях та фахових виданнях України, 8 патентів на корисну модель, 9 у наукометричній базі Scopus. 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 "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, уможлиблюють кваліфіковану оцінку ризиків в умовах широкого використання сучасних методів кібербезпеки.

Формат занять

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

Компетентності

КЗ-7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

КЗ-8. Здатність використовувати інформаційні та комунікаційні технології і на цій основі формувати ефективну систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо запобігання, протидії та нейтралізації загроз національній безпеці.

ФК-1. Здатність використовувати безпекові режими під час виконання службових обов'язків.

ФК-2. Здатність аналізувати виклики та загрози національній безпеці за напрямками професійної діяльності, синтезувати інформацію щодо розроблення та реалізації елементів стратегій у визначальних сферах національної безпеки (політичній, економічній, соціальній, гуманітарній).

ФК-4. Здатність демонструвати та застосовувати знання з основ теорії національної безпеки.

ФК-8. Здатність використовувати механізми забезпечення національної безпеки у її визначальних сферах.

ФК-9. Здатність використовувати знання щодо безпекової складової зовнішньої політики України та інших держав.

ФК-10. Здатність засвоювати основні теоретичні поняття та набуття практичних навичок дослідження, підготовки документів та їх використання в управлінській діяльності.

ФК-11. Здатність використовувати практичні навички, тактику та прийоми роботи з людьми в інтересах службової діяльності.

ФК-13. Здатність оцінювати вплив глобальних проблем і трансформацій геополітичного та гео економічного простору на національну безпеку.

ФК-14. Здатність здійснювати моніторинг зовнішньої та внутрішньої політики держави у контексті забезпечення національної безпеки, готувати пропозиції щодо підвищення її ефективності.

Результати навчання

ПРН-3. 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.

ПРН-7. Вміти виявляти, ставити та вирішувати професійні завдання, вміти узагальнювати отримані результати, обробляти та аналізувати інформацію з різних джерел, оформлювати і презентувати результати досліджень відповідно до вимог.

ПРН-8. Вміти використовувати інформаційні та комунікаційні технології і на цій основі формувати ефективні системи інформаційно-аналітичного забезпечення підтримки прийняття рішень щодо запобігання, протидії та нейтралізації загроз національній безпеці.

ПРН-9. Вміти використовувати безпекові режими під час виконання службових обов'язків.

ПРН-10. Вміти аналізувати виклики та загрози національній безпеці за напрямками професійної діяльності та синтезувати інформацію щодо розроблення та реалізації стратегій у визначальних сферах національної безпеки (політичній, економічній, соціальній, гуманітарній).

ПРН-12. Вміти застосовувати знання з основ теорії національної безпеки, зокрема: оцінювати обстановку, рівень викликів та загроз національній безпеці.

ПРН-16. Використовувати у професійній діяльності окремі елементи механізму впливу та взаємодії у процесі забезпечення окремих складових національної безпеки.

ПРН-17. Вміти використовувати отримані знання щодо безпекової складової зовнішньої політики України та інших держав.

ПРН-18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.

ПРН-19. Вміти використовувати у професійній діяльності методи та інструменти організації соціальної взаємодії, співробітництва та розв'язання конфліктів у сфері професійної діяльності, практичні навички, тактику та прийоми, роботи з людьми в інтересах службової діяльності: працювати у команді з позицій лідера, радника (консультанта), помічника, планувати використання часу та визначати стимули і бар'єри ефективної роботи, здійснювати розподіл (делегування) функцій, повноважень і відповідальності між виконавцями.

ПРН-21. Вміти оцінювати вплив глобальних проблем і трансформацій геополітичного та гео економічного простору на національну безпеку, здійснювати моніторинг зовнішньої та внутрішньої політики держави у контексті забезпечення національної безпеки та готувати пропозиції щодо підвищення її ефективності.

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

Теми лекційних занять

Тема 1. Основні поняття та визначення у сфері кібербезпеки.

Основні поняття. Класифікація ризиків. Ознаки ризиків. Загальна схема процесу управління ризиками. Етапи управління ризиками. Оцінка ризику. Оцінка загроз і управління. Ризики безпеки Microsoft.

Тема 2. Прогнозування кіберзагроз.

Шкідливе програмне забезпечення. Типові мережні атаки – Розвідка, Доступ та Соціальна інженерія. Мережні атаки – Відмова в обслуговуванні, Переповнення буфера та ухилення. Хто атакує нашу мережу? Інструменти зловмисників.

Тема 3. Ідентифікація активів інформаційних систем.

Ідентифікація інформаційних ресурсів. Ідентифікація програмного забезпечення. Ідентифікація користувачів та ролей. Оцінка важливості активів. Управління життєвим циклом активів. Моніторинг мережі та інструменти моніторингу. Загальні відомості про інструменти моніторингу мережі.

Тема 4. Управління кризовими ситуаціями та ліквідація наслідків.

Ефективне управління кризовими ситуаціями в критичній інфраструктурі. Реалізація концепції на прикладі ОБС України. Класифікатор загроз. Моделі безпеки. Удосконалення моделі оцінювання рівня захищеності. Класифікація зловмисників. Координація дій різних агентів під час кризової ситуації.

Тема 5. Кризис-менеджмент.

Сутність поняття "криза". Функції системи антикризового управління. Ознаки кризи економічного явища. Наслідки кризи. Фази кризи. Сутність факторів. Класифікація кризових явищ. Структурна схема процесу формування антикризової програми. Основні завдання менеджера з антикризового управління.

Тема 6. Внутрішні та зовнішні загрози. Використання IDS та IPS.

Ключові критерії для класифікації кіберінцидентів. Вразливості IP. Вразливості TCP та UDP. IP-сервіси. Корпоративні сервіси. Системи виявлення та запобігання вторгнень. Способи моніторингу системи. Аналіз методів виявлення вторгнень. Оцінювання сповіщень Security Onion. Відомі системи виявлення та запобігання вторгнень. Порівняльний аналіз сучасних систем виявлення та запобігання вторгнень.

Тема 7. Підходи до побудови моделі загроз та порушника.

Механізм деструктивного впливу на інформаційну систему. Модель порушника інформаційної безпеки. Основні канали витоку інформації. Ображені інсайдери. Нелояльні інсайдери. Класифікація інсайдерів по критерію мотивації. Спосіб реалізації атаки (за місцем дії).

Тема 8. Політика системи менеджменту.

Система менеджменту інформаційної безпеки. Орієнтовна послідовність дій при розробці СМІБ. Приклад політики інформаційної безпеки. Приклади невдалих політик. Аналіз витрат на кібербезпеку. Розробка бюджету.

Тема 9. Аналіз логів: збір, агрегація, інтерпретація.

Інструменти для збору лог-даних з різних компонентів мережі та систем. Методи для агрегації лог-файлів з різних джерел в одне централізоване сховище. Нормалізація лог-даних для забезпечення стандартного формату та полегшення їхнього подальшого аналізу. Техніки та алгоритми для виявлення аномалій в логах, які можуть свідчити про кіберзагрози чи інші проблеми. Профілювання мережі та сервера. Загальна система оцінки вразливостей (CVSS). Безпечне керування пристроями.

Тема 10. Управління інцидентами інформаційної безпеки.

Взаємозв'язок понять. Якісна оцінка СМІБ. Зміст процесу управління інцидентами. Причини виникнення інцидентів. Група розслідування інцидентів. Структура команди з розслідування інцидентів інформаційної безпеки. Розробка нормативних документів з управління інцидентами. Виявлення та аналіз інцидентів інформаційної безпеки. Документування інциденту інформаційної безпеки. Протидія поширенню інциденту. Ідентифікація порушника. Зберігання матеріалів. Контрольні листи спостережень.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Встановлення віртуальної машини CyberOps Workstation.

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

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

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.

Використання Wireshark для дослідження кадрів Ethernet. Використання Wireshark для спостереження за тристороннім рукоятискуванням 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.

Самостійна робота

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи студенти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних

робіт, заліків та іспитів. Студентам також рекомендуються додаткові матеріали (відео, статті) для самостійного вивчення та аналізу.

Неформальна освіта

В рамках неформальної освіти згідно відповідного Положення (<http://surl.li/pxssv>), освітня компонента або її окремі теми можуть бути враховано у разі самостійного проходження професійних курсів/тренінгів, отримання громадянської освіти, онлайн освіти, професійного стажування тощо.

Зокрема, окремі теми даної компоненти можуть бути враховано у разі успішного завершення таких курсів CISCO:

Cyber Threat Management

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

Література та навчальні матеріали

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

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:

- лабораторні роботи: 30% семестрової оцінки;
- самостійна робота: 10% семестрової оцінки;
- контрольна робота: 30% семестрової оцінки;
- іспит: 30% семестрової оцінки

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

Студент 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

28.08.2024



Завідувач кафедри

Сергій ЄВСЕЄВ

28.08.2024



Гарант ОП

Андрій ТКАЧОВ