



## Силабус освітнього компонента

Програма навчальної дисципліни



# Основи кібербезпеки

### Шифр та назва спеціальності

257 – Управління інформаційною безпекою

### Інститут

ННІ комп'ютерних наук та інформаційних технологій (320)

### Освітня програма

Управління інформаційною безпекою

### 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](mailto: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](#)

## Загальна інформація

### Анотація

Навчальна дисципліна "Основи кібербезпеки" є вибірковою навчальною дисципліною. Вивчення дисципліни спрямовано на оволодіння необхідними базовими поняттями та правилами безпечної поведінки в мережі, ознайомлення студентів з принципами побудови систем захисту інформації, ознайомлення з основними механізмами послуг безпеки, вивчення менеджменту інформаційної безпеки, навчання студентів основам аудиту інформаційної безпеки, а також вивчення студентами спеціальних механізмів кіберзахисту.

## Мета та цілі дисципліни

Навчання студентів принципам побудови систем захисту інформації, дослідженню та використанню сучасних процедур забезпечення надання основних послуг безпеки інформації в кіберпросторі, проведення аудиту поточного стану інформаційної безпеки.

## Формат занять

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

## Компетентності

КЗ-6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

КЗ-7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.

ФК-2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.

ФК-3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.

ФК-5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.

ФК-7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації.

ФК-8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах.

ФК-9. Здатність організації реагування на загрози на об'єктах критичної інфраструктури, установах та підприємствах.

ФК-10. Здатність забезпечувати неперервність бізнесу згідно з встановленою політикою інформаційної безпеки.

ФК-11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.

## 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-6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки.

ПРН-7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.

ПРН-8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційною безпеки.

ПРН-10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.

ПРН-11. 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.

ПРН-12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

ПРН-13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах.

ПРН-14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.

ПРН-16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.

ПРН-17. Вміти розв'язувати задачі управління інформаційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.

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

ПРН-19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-комунікаційних системах.

ПРН-20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.

ПРН-21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.

ПРН-22. 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, Введення в мережі, Менеджмент інформаційної безпеки, Розробка та аналіз алгоритмів.

## **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**

Cisco Networking Academy:

Тема 1. Кібербезпека - світ фахівців і злочинців.

Світ кібербезпеки. Кіберзлочинці проти фахівців з кібербезпеки. Загальні загрози.

Розповсюдження загроз кібербезпеки. Підготовка більшої кількості спеціалістів.

Cisco Networking Academy:

Тема 2. Куб кібербезпеки.

Тріада КІД (CIA). Стани даних. Контрзаходи кібербезпеки. Структура управління IT-безпекою.

Cisco Networking Academy:

Тема 3. Кібербезпека – загрози, вразливості та атак.

Шкідливе програмне забезпечення та зловмисний код. Шахрайство. Атаки.

Cisco Networking Academy:

Тема 4. Мистецтво захисту таємниць.

Криптографія. Контроль доступу. Приховування даних.

Cisco Networking Academy:

Тема 5. Мистецтво забезпечення цілісності даних.

Типи засобів контролю цілісності даних. Цифрові підписи. Сертифікати. Забезпечення цілісності баз даних.

Cisco Networking Academy:

Тема 6. Концепція п'яти дев'яток.

Висока доступність. Заходи для поліпшення доступності. Реакція на інцидент. Аварійне відновлення.

Cisco Networking Academy:

## Тема 7. Захист домену кібербезпеки.

Захист систем та пристроїв. Укріплення захисту серверів. Укріплення захисту мережі. Фізична безпека.

Cisco Networking Academy:

## Тема 8. Як стати спеціалістом з кібербезпеки.

Домени кібербезпеки. Розуміння етики роботи у кібербезпеці. Наступний крок.

### Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

### Теми лабораторних робіт

Cisco Networking Academy:

Тема 1. Аутентифікація, авторизація та облік.

Cisco Networking Academy:

Тема 2. Встановити віртуальну машину на персональний комп'ютер.

Cisco Networking Academy:

Тема 3. Виявлення загроз і вразливостей.

Cisco Networking Academy:

Тема 4. Використання стеганографії.

Cisco Networking Academy:

Тема 5. Злам паролів.

Cisco Networking Academy:

Тема 6. Використання цифрових підписів.

Cisco Networking Academy:

Тема 7. Віддалений доступ.

Cisco Networking Academy:

Тема 8. Захист Linux систем.

### 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:

PaloAlto (Cybersecurity Foundation)

<https://paloaltonetworksacademy.net/course/index.php>.

## Література та навчальні матеріали

### Основна література

1. Євсєєв С.П. Кібербезпека: сучасні технології захисту. / Євсєєв С. П, Остапов С. Е., Король О. Г. // Навчальний посібник для студентів вищих навчальних закладів. Львів: "Новий Світ – 2000", 2019. – 678.

<http://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnologii-zakhystu.pdf>

2. Кібербезпека в сучасному світі : матеріали III Всеукраїнської науково-практичної конференції (м. Одеса, 19 листопада 2021 р.) / за ред. О. В. Дикого ; уклад.: С. А. Горбаченко, Н. І. Логінова. – Одеса, 2020. – 148 с.  
<http://dspace.onua.edu.ua/handle/11300/15973>
3. Лісовська Ю. Кібербезпека. Ризики та заходи. – К.: Кондор, 2019. – 272 с.  
<http://dcmaup.com.ua/assets/files/kiberbezpeka.pdf>
4. 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>
5. 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>
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>.

### Додаткова література

7. Доктрина інформаційної безпеки України, затверджено Указом Президента України редакція від 30.12.2021 № 47/2017. [Електронний ресурс].  
<https://zakon.rada.gov.ua/laws/show/47/2017#Text>.
8. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України", затверджено Указом Президента України редакція від 26.08.2021 № 447/2021).  
<https://zakon.rada.gov.ua/laws/show/447/2021#Text>
9. 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>.
10. 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](https://www.iso.org/search.html?q=15408-2&hPP=10&idx=all_en&p=0).
11. 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](https://www.iso.org/search.html?q=15408-3&hPP=10&idx=all_en&p=0).
12. ISO/IEC 31010:2019 Risk management . URL:  
<https://www.iso.org/ru/contents/data/standard/07/21/72140.html>
13. 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>
14. 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>
15. 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>
16. 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>
17. 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: 20% семестрової оцінки;
- іспит: 40% 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<br>(потрібне додаткове вивчення) | FX   |
| 1–34       | Незадовільно<br>(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 ВСЕЄВ

28.08.2024



Гарант ОП

Роман КОРОЛЬОВ