Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

Кафедра комп'ютерних систем, мереж і кібербезпеки (№ 503)
(назва кафедри)

**ЗАТВЕРДЖУЮ**

Голова НМК

(підпис) Д.М. Крицький (ініціали та прізвище)

« 31 » серпня 2023 р.

# РОБОЧА ПРОГРАМА ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Гарантоздатні хмарні системи
(назва навчальної дисципліни)

**Галузь знань:** 10 «Природничі науки», 11 «Математика та статистика», 12 «Інформаційні технології», 15 «Автоматизація та приладобудування», 16 «Хімічна та біоінженерія», 17 «Електроніка та телекомунікації», 19 «Архітектура та будівництво»
(шифр і найменування галузі знань)

**Спеціальність:**
(код та найменування спеціальності)

**Освітні програми:**
(найменування освітньої програми)

**Форма навчання:** денна

**Рівень вищої освіти:** другий (магістерський)

**Харків 2023 рік**

Розробник: Горбенко Анатолій Вікторович, професор, д.т.н., професор _____
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Робочу програму розглянуто на засіданні кафедри комп'ютерних систем, мереж і кібербезпеки
(назва кафедри)

Протокол № 1 від « 30 » серпня 2023 року

Завідувач кафедри д.т.н., професор _____ В.С. Харченко
(науковий ступінь та вчене звання) (підпис) (ініціали та прізвище)

## 1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, спеціалізація, рівень вищої освіти</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td>Денна форма навчання</td></tr>
<tr><td>Кількість кредитів – 3</td><td rowspan="6">Галузь знань:<br>10 «Природничі науки»,<br>11 «Математика та статистика»,<br>12 «Інформаційні технології»,<br>15 «Автоматизація та приладобудування»,<br>16 «Хімічна та біоінженерія»,<br>17 «Електроніка та телекомунікації»,<br>19 «Архітектура та будівництво»</td><td>Вибіркова</td></tr>
<tr><td>Модулів – 1</td><td rowspan="2">Навчальний рік<br>2023/2024</td></tr>
<tr><td>Змістовних модулів – 2</td></tr>
<tr><td>Індивідуальне науково-дослідне завдання: немає</td><td rowspan="2">Семестр</td></tr>
<tr><td>Загальна кількість годин – денна – 481)/90</td><td>2-й</td></tr>
<tr><td rowspan="10">Тижневих годин для денної форми навчання:<br>аудиторних – 3<br>самостійної роботи здобувача – 2,7</td><td rowspan="10">Рівень вищої освіти:<br>другий (магістерський)</td><td>Лекції1)</td></tr>
<tr><td>0 години</td></tr>
<tr><td>Практичні/Семінари1)</td></tr>
<tr><td>48 годин</td></tr>
<tr><td>Лабораторні1)</td></tr>
<tr><td>0 годин</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>42 годин</td></tr>
<tr><td>Вид контролю</td></tr>
<tr><td>Залік</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить *48/42*.

[1)] Аудиторне навантаження може бути зменшене або збільшене на одну годину в залежності від розкладу занять.

## 2. Мета та завдання навчальної дисципліни

**Мета:** отримання студентами, необхідних компетенцій для спілкування іноземної мової з технічними фахівцями; пошук, систематизація та презентація знань за фахом з іноземних інформаційних ресурсів у різній формі: аудіо, відео або друкованих.

**Завдання:**

- вивчення іноземіної технічної термінології за фахом;
- отримання навичок комунікації з іноземними технічними фахівцями з використанням базових мовних компетенцій: читання, письмо, сприйняття на слух та усне спілкування.

**Компетентності, які набуваються:** Дисципліна має допомогти сформувати у здобувачів такі загальні та спеціальні компетентності:

- Здатність до абстрактного мислення, аналізу і синтезу.
- Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
- Здатність спілкуватися іноземною мовою.
- Здатність представляти результати власних досліджень та/або розробок у вигляді презентацій, науково-технічних звітів, статей і доповідей на науково-технічних конференціях.

**Очікувані результати навчання.** В результаті вивчення дисципліни здобувачі мають досягти такі результати навчання:

- Здійснювати пошук інформації в різних джерелах для розв’язання задач комп’ютерної інженерії, аналізувати та оцінювати цю інформацію.
- Вільно спілкуватись усно і письмово українською мовою та однією з іноземних мов (англійською, німецькою, італійською, французькою, іспанською) при обговоренні професійних питань, досліджень та інновацій в галузі інформаційних технологій.
- Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію з питань інформаційних технологій і дотичних міжгалузевих питань до фахівців і нефахівців, зокрема до осіб, які навчаються.

**Пререквізити**: дисципліна є обов’язковим компонентом освітньої програми і базується на знаннях, отриманих під час вивчення дисциплін у циклі загальної і професійної підготовки, передбачених навчальним планом спеціальності.

**Кореквізіти**: немає.

## 3. Зміст навчальної дисципліни

**Модуль 1**

**Змістовний модуль 1. Загрози комп'ютерних систем та управління інформаційною безпекою (Computer system threats and information security management)**

**Тема 1. Unix, безкоштовне програмне забезпечення з відкритим кодом і безпека Linux (Unix, Free and Open Source Software, and Linux Security)**
Popular operating systems. Unix and GNU/Linux. Unix/Linux Security. Free and open source software (FOSS). Unix/Linux file system. Basic Unix command shell.

**Тема 2. Шкідливе програмне забезпечення та шкідливий код (Malware and malicious code)**
Malicious and vulnerable software. Types of malware (Viruses, Worms, Trojans and EXE-wrappers, Rootkits, Zombies and Botnets, Spyware and Adware, Scareware and rogue antivirus, Ransomware, Exploit kits). User accounts and access controls. Malware detection.

**Тема 3. Уразливості програмного забезпечення (Software vulnerabilities)**
Definition of Software vulnerability. Local and Remote Vulnerabilities. Exploits and Payloads. Common types of vulnerabilities/payloads. Bind and Reverse Shell. Privilege Escalation. Window of Vulnerability. Vulnerability disclosure. Auditing and permission. Vulnerability mitigation techniques. Metasploit framework (MSF).

**Тема 4. Управління уразливостями та інформаційною безпекою (Vulnerability and Information Security Management)**
Common Vulnerability Scoring System (CVSS). Vulnerability monitoring and analysis. Vulnerability scanning: credential and non-credential scan; scan perspectives. Vulnerability scanners: Nessus, OpenVAS, Nexpose. Web security. Types of Web vulnerabilities.

**Змістовний модуль 2. Життєвий цикл кібератак та засоби запобігання (Lifecycle of cyberattacks and means of prevention)**

**Тема 5. Життєвий цикл кібератак. Збір інформації та сканування (Cyberattacks Lifecycle. Information gathering and Scanning)**
Lifecycle of cyberattacks: Information gathering, Exploitation, Post-Exploitation. Passive Information Gathering: Footrpinting. Whois and DNS services. Active Information Gathering: Network Scan, Port Scan, Enumeration for SW detection, Fingerprinting for OS detection.

**Тема 6. Від сканування до використання вразливостей (From scanning to vulnerability exploitation)**

**Тема 7. Пост-експлуатаційний етап (Post-exploitation)**
Exploitation Methods. Vulnerability and Exploit Databases: Common Vulnerabilities and Exposures (CVE), National Vulnerability Database (NVD), ExploitDB. Exploit frameworks. Metasploit Framework and Armitage. Vulnerability scanners.

**Тема 8. Аудит безпеки: стандарти, відповідність і методології (Security Audits: Standards, Compliance, and Methodologies)**
Security Audit and Penetration Testing. Types of security audits. Security Audit Output. Security Audit Methodologies: Open Source Security Testing Methodology Manual (OSSTMM), Information Systems Security Assessment Framework (ISSAF), NIST Technical Guide to Information Security Testing and Assessment, Penetration Testing Execution Standard (PTES), OWASP Testing Guide, Penetration Testing Framework. Security Standards and Compliance: PCI Data Security Standards (PCI DSS), ISO/IEC 27001

## 4. Структура навчальної дисципліни

| Назва змістовного модуля і тем | Кількість годин | | | | |
|---|---|---|---|---|---|
| | Усього | У тому числі | | | |
| | | л | п | лаб. | с. р. |
| 1 | 2 | 3 | 4 | 5 | 6 |
| **Модуль 1** | | | | | |
| **Змістовний модуль 1. Загрози комп'ютерних систем та управління інформаційною безпекою (Computer system threats and information security management)** | | | | | |
| Тема 1. Unix, безкоштовне програмне забезпечення з відкритим кодом і безпека Linux (Unix, Free and Open Source Software, and Linux Security). | 11 | | 6 | | 6 |
| Тема 2. Шкідливе програмне забезпечення та шкідливий код (Malware and malicious code). | 11 | | 6 | | 5 |
| Тема 3. Уразливості програмного забезпечення (Software vulnerabilities). | 11 | | 6 | | 5 |
| Тема 4. Управління уразливостями та інформаційною безпекою (Vulnerability and Information Security Management). | 12 | | 6 | | 5 |
| Разом за змістовним модулем 1 | 45 | | 24 | | 21 |
| **Змістовний модуль 2. Життєвий цикл кібератак та засоби запобігання (Lifecycle of cyberattacks and means of prevention)** | | | | | |
| Тема 5. Життєвий цикл кібератак. Збір інформації та сканування (Cyberattacks Lifecycle. Information gathering and Scanning). | 11 | | 6 | | 6 |
| Тема 6. Від сканування до використання вразливостей (From scanning to vulnerability exploitation). | 11 | | 6 | | 5 |
| Тема 7. Пост-експлуатаційний етап (Post-exploitation). | 11 | | 6 | | 5 |
| Тема 8. Аудит безпеки: стандарти, відповідність і методології (Security Audits: Standards, Compliance, and Methodologies). | 12 | | 6 | | 5 |
| Разом за змістовним модулем 2 | 45 | | 24 | | 21 |
| **Усього годин** | **90** | | **48** | | **42** |

## 5. Теми семінарських занять

| № з/п | Назва теми | Кількість годин |
|---|---|---|
| 1 | Unix, безкоштовне програмне забезпечення з відкритим кодом і безпека Linux (Unix, Free and Open Source Software, and Linux Security). | 6 |
| 2 | Шкідливе програмне забезпечення та шкідливий код (Malware and malicious code). | 6 |
| 3 | Уразливості програмного забезпечення (Software vulnerabilities). | 6 |

| | | |
|---|---|---|
| 4 | Управління інформаційною безпекою (Information Security Management). | 6 |
| 5 | Життєвий цикл кібератак. Збір інформації та сканування (Cyberattacks Lifecycle. Information gathering and Scanning). | 6 |
| 6 | Від сканування до використання вразливостей (From scanning to vulnerability exploitation). | 6 |
| 7 | Пост-експлуатаційний етап (Post-exploitation). | 6 |
| 8 | Аудит безпеки: стандарти, відповідність і методології (Security Audits: Standards, Compliance, and Methodologies). | 6 |
| | **Разом** | 48 |

## 6. Теми практичних занять

| № з/п | Назва теми | Кількість годин |
|---|---|---|
| 1 | *Не передбачено* | |
| | **Разом** | |

## 7. Теми лабораторних занять

| № з/п | Назва теми | Кількість годин |
|---|---|---|
| 1 | *Не передбачено* | |
| | **Разом** | |

## 8. Самостійна робота

| № з/п | Назва теми | Кількість годин |
|---|---|---|
| 1 | Відпрацювання матеріалів лекційних занять за темою 1 | 6 |
| 2 | Відпрацювання матеріалів лекційних занять за темою 2 | 5 |
| 3 | Відпрацювання матеріалів лекційних занять за темою 3 | 5 |
| 4 | Відпрацювання матеріалів лекційних занять за темою 4 | 5 |
| 5 | Відпрацювання матеріалів лекційних занять за темою 5 | 6 |
| 6 | Відпрацювання матеріалів лекційних занять за темою 6 | 5 |
| 7 | Відпрацювання матеріалів лекційних занять за темою 7 | 5 |
| 8 | Відпрацювання матеріалів лекційних занять за темою 8 | 5 |
| | **Разом** | **42** |

## 9. Індивідуальні завдання

| № з/п | Назва теми | Кількість годин |
|---|---|---|
| 1 | *Не передбачено* | |
| | **Разом** | |

## 10. Методи навчання

Проведення семінарів, консультацій, а також самостійна робота здобувачів з використанням відповідних матеріалів. За кожної темою передбачено проведення семінарів двох типів: 1) вербальна та візуальна презентація матеріалів викладачем іноземною (англійською) мовою за темою семінара та її подальше групове обговорення; 2) пошук та

систематизація знань з іноземних інформаційних ресурсів у різній формі: аудіо, відео або друкованих та написання есе англійською мовою за темою семінара.

## 11. Методи контролю

Проведення поточного контролю, оцінка письмових робіт, підсумковий контроль у вигляді семестрового заліку, який проводиться у разі відмови студента від балів поточного тестування й за наявності допуску до заліку. В якості завдання студент має підготовити презентацію за однією з тем семінарських зайнять та зробити доповідь іноземної (англійською) мовою. Під час складання семестрового заліку здобувач має можливість отримати максимум 100 балів.

## 12. Критерії оцінювання та розподіл балів, які отримують здобувачі

| Складові навчальної роботи | Бали за одне заняття (завдання) | Кількість занять (завдань) | Сумарна кількість балів |
|---|---|---|---|
| **Змістовний модуль 1** | | | |
| Робота на семінарах | 0…5 | 4 | 0…20 |
| Написання письмових робіт (есе) англійською мовою | 0...8 | 4 | 0...30 |
| **Змістовний модуль 2** | | | |
| Робота на семінарах | 0…5 | 4 | 0…20 |
| Написання письмових робіт (есе) англійською мовою | 0...8 | 4 | 0...30 |
| **Усього за семестр** | | | **0…100** |

### Критерії оцінювання роботи здобувача протягом семестру

**Задовільно (60-74).** Показати необхідний мінімум знань та умінь. Виконати не менше 60% від усіх письмових робіт.

**Добре (75-89).** Твердо знати основні концепції розподілених систем та хмарних обчислень та уміти їх обговорювати іноземною (англійською) мовою. Виконати не менше 80% від усіх письмових робіт.

**Відмінно (90-100).** Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти їх обговорювати іноземною (англійською) мовою.

### Шкала оцінювання: бальна і традиційна

| Сума балів | Оцінка за традиційною шкалою | |
|---|---|---|
| | Іспит, диференційований залік | Залік |
| 90 – 100 | Відмінно | Зараховано |
| 75 – 89 | Добре | |
| 60 – 74 | Задовільно | |
| 0 – 59 | Незадовільно | Не зараховано |

## 13. Методичне забезпечення

Навчально-методичний комплекс дисципліни розміщений у системі дистанційного навчання «Google Classroom».

1. Сторінка дисципліни у системі дистанційного навчання «Mentor» [Ел. ресурс]. URL: https://mentor.khai.edu/course/view.php?id=2148

## 14. Рекомендована література

### Базова


1. Harper, A., Harris, S., Ness, J., et al. Gray hat hacking : the ethical hacker's handbook, 6th ed. – McGraw-Hill, 2022. – 704 p. URL: https://pages.cs.wisc.edu/~ace/media/gray-hat-hacking.pdf
2. Hoffman, H. Ethical Hacking with Kali Linux. – – Independently published, 2020. – 153 p. URL: https://edu.anarcho-copy.org/Against Security - Self Security/Ethical Hacking With Kali Linux Learn Fast How To Hack.pdf
3. OccupyTheWeb. Linux Basics for Hackers. – No Starch Press, 2018. – 248p.


### Допоміжна


1. Minning, E. Kali Linux Hacking, 2nd ed. – Independently published, 2019. – 175 p.


## 15. Інформаційні ресурси

1. 5 Best Free Cyber Security Courses for Beginners to Learn in 2023 [Ел. ресурс]. URL: https://medium.com/javarevisited/5-best-free-cyber-security-courses-for-beginners-a4abec9d5e6c
2. Free Online Cyber Security Courses with Certificates [Ел. ресурс]. URL: https://www.oxfordhomestudy.com/courses/cyber-security-courses/free-cyber-security-courses