Міністерство освіти і науки України
Національний університет «Чернігівська політехніка»
Навчально-науковий інститут електронних та інформаційних технологій
Кафедра кібербезпеки та математичного моделювання

РОБОЧА ПРОГРАМА
Управління фінансово-економічною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Ткач Ю.М.
(підпис) (прізвище та ініціали)

«26» серпня 2025 р.

Розробник (-и): Мехед Д.Б., доцент, кандидат педагогічних наук, доцент _____
(прізвище та ініціали, посада, науковий ступінь і вчене звання) (підпис)

Робочу програму навчальної дисципліни обговорено на засіданні кафедри кібербезпеки та математичного моделювання

Протокол від «26» серпня 2025р. №6

Узгоджено з гарантом освітньої програми: _____ Ткач.Ю.М.
(підпис) (прізвище та ініціали)

---

1. Загальна інформація про дисципліну.

Тип дисципліни	*Вибіркова*
Мова викладання	українська
Рік навчання та семестр	2025-2026 навчальний рік, І семестр, ОП Кібербезпека за спеціальністю F5 Кібербезпека та захист інформації галузь знань F Інформаційні технології
Викладач (-і)	Мехед Дмитро Борисович, доцент кафедри кібербезпеки та математичного моделювання, кандидат педагогічних наук.
Профайл викладача (-ів)	https://mmi.stu.cn.ua/personal-kafedry/
Контакти викладача	Т.м. +38(063) 690-80-00, E-mail: d.mekhed@stu.cn.ua

2. Анотація курсу.

Дисципліна "Управління фінансовою безпекою" є вибірковою частиною програми підготовки магістрів ОП Кібербезпека за спеціальністю F5 Кібербезпека та захист інформації, галузь знань F Інформаційні технології. Курс надає фундаментальні знання та практичні навички з аналізу фінансових загроз, методів їх попередження та управління фінансовими ризиками в організаціях.

Загальна тематика курсу охоплює: принципи та методи управління фінансовою безпекою; міжнародні стандарти і правові аспекти управління фінансовими ризиками (ISO 22301, ISO 27001, GDPR тощо); методи захисту фінансової інформації від шахрайства, корупції та кіберзагроз; фінансові інструменти для мінімізації ризиків; аналіз фінансових операцій та фінансових звітів на наявність підозрілих або незаконних транзакцій.

Підхід до викладання орієнтований на поєднання теоретичних основ та практичних кейсів, включаючи аналіз реальних фінансових інцидентів. Значна увага приділяється розвитку аналітичного мислення, вмінню визначати фінансові загрози та впровадженню заходів для їх запобігання.

Курс готує спеціалістів, здатних професійно здійснювати управління фінансовою безпекою, аналізувати фінансові ризики та застосовувати інструменти для мінімізації фінансових загроз на підприємствах.

3. Мета та цілі курсу.

Мета курсу – формування у студентів системного розуміння управління фінансовою безпекою, аналізу фінансових загроз та впровадження методів захисту від фінансових ризиків, а також розвиток практичних навичок використання спеціалізованого програмного забезпечення для аналізу фінансових даних.

Цілі курсу:

- Розвиток у студентів здатності аналізувати фінансові загрози та ризики, які можуть вплинути на організаційну фінансову безпеку.
- Ознайомлення студентів з міжнародними стандартами та найкращими практиками управління фінансовими ризиками та забезпеченням фінансової безпеки.
- Формування навичок використання сучасних інструментів та методів для захисту фінансової інформації та запобігання фінансовим шахрайствам.
- Розвиток практичних умінь у застосуванні фінансових стратегій і заходів для мінімізації фінансових загроз в умовах постійних змін в інформаційному середовищі.
- Здобуття навичок проведення фінансового аналізу та оцінки ефективності заходів з фінансової безпеки для прийняття обґрунтованих управлінських рішень.
- Формування вмінь розробляти політики та стратегії управління фінансовими ризиками в організаціях для забезпечення їх стабільності та стійкості до внутрішніх і зовнішніх загроз.

4. Результати навчання (ПС «Кібероператор»):

Знання:

- Студенти повинні знати основні принципи та методи управління фінансовими ризиками та загрозами.
- Студенти повинні розуміти міжнародні стандарти та правові аспекти фінансової безпеки, зокрема нормативно-правову базу, що регулює фінансову діяльність.
- Студенти повинні володіти знаннями щодо сучасних інструментів та технологій захисту фінансової інформації, а також методів фінансового аналізу.

Уміння:

- Студенти повинні вміти здійснювати фінансовий аналіз організацій, визначати та оцінювати фінансові ризики та загрози.

- Студенти повинні вміти розробляти та впроваджувати стратегії та заходи для захисту фінансової інформації.
- Студенти повинні вміти застосовувати методи оцінки ефективності систем фінансової безпеки та здійснювати корекційні заходи у разі необхідності.
- Студенти повинні вміти аналізувати фінансові загрози, що виникають у сфері інформаційних технологій, та розробляти відповідні стратегії для їх мінімізації.
- Студенти повинні вміти проводити оцінку фінансових ризиків та обґрунтовувати фінансові рішення на основі комплексного аналізу.

ПРН 2. Інтегрувати знання для вирішення складних задач у сфері безпеки у мультидисциплінарних контекстах.
ПРН 9. Аналізувати, розробляти і супроводжувати систему управління інформаційною/кібербезпекою організації.
ПРН 10. Забезпечувати безперервність бізнес-процесів, аналізувати ризики та уразливості.
ПРН 16. Приймати обґрунтовані рішення з організаційно-технічних питань у складних і непередбачуваних умовах.

5. Пререквізити. Відсутні.

6. Обсяг курсу:

Вид заняття	Загальна кількість годин
Лекції	16/6
Лабораторні заняття	16/6
Самостійна робота	88/108
Індивідуальне завдання – розрахунково-графічна робота	
Всього кредитів	4

Лекційні, лабораторні заняття, розрахунково-графічна робота, самостійна робота – з використанням системи дистанційного навчання Moodle, Teams, рекомендованих джерел, відеоматеріалів тощо.

7. Тематика курсу.

Лекції (16 годин):

 Вступ до фінансової безпеки (2 год)

- Поняття фінансової безпеки та її значення для організацій.
- Основні складові фінансової безпеки: захист фінансових активів, управління ризиками, забезпечення стабільності.

 Фінансові ризики та загрози (2 год)

- Визначення фінансових ризиків та загроз.
- Класифікація фінансових ризиків: кредитні, валютні, процентні, операційні тощо.
- Методи і підходи до оцінки фінансових загроз.

 Міжнародні стандарти і правові аспекти фінансової безпеки (2 год)

- Міжнародні стандарти управління фінансовими ризиками (ISO 31000, COSO тощо).
- Правові норми, що регулюють фінансову безпеку (Закон України про фінансові послуги, боротьба з фінансовими злочинами тощо).

- Важливість дотримання стандартів та законодавчих вимог для забезпечення безпеки.

 Методи та інструменти захисту фінансової інформації (2 год)

- Основні методи захисту фінансової інформації: криптографія, багатофакторна автентифікація, шифрування.
- Використання сучасних інструментів для захисту інформаційних систем у фінансових організаціях.

 Аналіз фінансових загроз у контексті інформаційних технологій (2 год)

- Вплив кіберзагроз на фінансову безпеку організації.
- Кіберзлочинність, шахрайство та інші загрози, що виникають внаслідок використання інформаційних технологій.
- Методи мінімізації кіберзагроз у фінансових установах.

 Фінансовий аналіз і оцінка ефективності систем фінансової безпеки (2 год)

- Інструменти фінансового аналізу для оцінки фінансової безпеки.
- Ключові показники ефективності системи фінансової безпеки (KPI, ROA, ROE тощо).
- Підходи до оцінки ризиків та визначення необхідних заходів для їх мінімізації.

 Управління фінансовими кризами та фінансовою стабільністю (2 год)

- Стратегії управління фінансовими кризами: попередження, реакція на кризу та відновлення стабільності.
- Методи і технології для забезпечення фінансової стійкості організації в умовах фінансових труднощів.

 Розробка стратегії фінансової безпеки організації (2 год)

- Розробка та впровадження стратегії фінансової безпеки для організацій різних типів.
- Оцінка внутрішніх і зовнішніх факторів ризику та побудова політики безпеки.
- Практичні приклади створення та впровадження стратегій фінансової безпеки.

Семінарські (16 годин):

1. **Аналіз фінансових ризиків організації** (2 год)

- Практичне застосування методів аналізу фінансових ризиків.
- Оцінка кредитних, валютних та операційних ризиків на прикладах реальних фінансових організацій.
- Розрахунок показників ризиків за допомогою фінансових моделей.

 Оцінка ефективності системи фінансової безпеки (2 год)

- Розрахунок ключових показників ефективності (KPI) для системи фінансової безпеки.
- Аналіз результатів моніторингу фінансових загроз та визначення необхідних заходів щодо покращення захисту.
- Використання спеціалізованих інструментів для оцінки ризиків.

 Використання криптографії та інших інструментів захисту фінансової інформації (2 год)

- Практичне застосування шифрування для захисту фінансових транзакцій.
- Налаштування багатофакторної автентифікації для фінансових платформ.
- Використання інструментів для моніторингу та захисту фінансових даних від несанкціонованого доступу.

 Аналіз фінансових шахрайств та кіберзагроз (2 год)

- Вивчення методів виявлення та протидії фінансовим шахрайствам (наприклад, фішинг, маніпуляції з активами).
- Оцінка кіберзагроз для фінансових систем та розробка заходів щодо їх мінімізації.
- Практичний аналіз випадків кіберзлочинів у фінансових установах.

 Розробка стратегії фінансової безпеки для організації (2 год)

- Створення проекту стратегії фінансової безпеки для реальної чи уявної компанії.
- Визначення фінансових ризиків та загроз для бізнесу.
- Розробка політики безпеки та рекомендацій щодо управління фінансовими загрозами.

 Моделювання фінансової кризи та управління нею (2 год)

- Практичне моделювання фінансової кризи в організації.
- Розробка плану дій для подолання фінансових труднощів та відновлення стабільності.
- Використання інструментів прогнозування для оцінки потенційних фінансових криз.

 Ідентифікація та аналіз фінансових загроз у сфері інформаційних технологій (2 год)

- Аналіз сучасних загроз для фінансових даних, що виникають внаслідок використання інформаційних технологій.
- Оцінка вразливостей інформаційних систем у фінансовому секторі.
- Розробка заходів для захисту фінансових систем від кіберзагроз.

 Практичні кейс-стаді з управління фінансовими ризиками (2 год)

- Розбір реальних або уявних кейсів управління фінансовими ризиками.
- Оцінка застосування різних методів та інструментів для зниження ризиків.
- Дискусія та групова робота над стратегіями управління фінансовою безпекою у складних ситуаціях.

Розрахунково-графічна робота (РГР)

Тема: Аналіз фінансових ризиків та системи управління фінансовою безпекою

1. **Аналіз основних фінансових показників організації.**
   - Визначення ключових фінансових показників для оцінки стабільності бізнесу (прибутковість, ліквідність, рентабельність).
   - Аналіз структури фінансових потоків організації, виявлення можливих ризиків.
2. **Оцінка фінансових ризиків та загроз.**
   - Визначення основних видів фінансових ризиків (кредитні, валютні, ліквідності).
   - Оцінка впливу цих ризиків на бізнес за допомогою фінансових моделей та інструментів.
3. **Аналіз фінансових операцій та їх захист.**
   - Вивчення процесів фінансових операцій, таких як транзакції, переводи коштів, використання платіжних систем.
   - Оцінка механізмів захисту фінансових операцій від шахрайства та маніпуляцій.
4. **Оцінка ефективності фінансових інструментів захисту.**
   - Аналіз застосування криптографії, багатофакторної автентифікації та інших методів захисту фінансових даних.
   - Оцінка ефективності сучасних технологій для забезпечення безпеки фінансових транзакцій.
5. **Аналіз системи управління фінансовими ризиками в організації.**
   - Оцінка методів управління фінансовими ризиками в організації, визначення слабких місць системи.
   - Розробка рекомендацій щодо покращення фінансової безпеки та захисту від загроз.

Ця РГР допоможе студентам закріпити практичні навички з аналізу фінансових ризиків і загроз, а також надасть інструменти для розробки ефективних стратегій з управління фінансовою безпекою в організації.

Самостійна робота (88 годин):

 Вивчення основних фінансових ризиків (14 годин)

- Ознайомлення з теорією фінансових ризиків: кредитний, ринковий, операційний, валютний, інвестиційний.
- Самостійне вивчення класифікацій фінансових ризиків, джерел їх виникнення та методів аналізу.
- Аналіз реальних прикладів фінансових криз та їхніх причин.

 Методи оцінки фінансової стійкості організацій (16 годин)

- Самостійне вивчення методів оцінки ліквідності, платоспроможності, рентабельності підприємств.
- Аналіз фінансових звітів та виявлення факторів, що впливають на фінансову стійкість організації.
- Порівняння основних методів оцінки фінансового стану (аналіз коефіцієнтів, динамічний аналіз, фінансові моделі).

 Аналіз систем управління фінансовими ризиками (14 годин)

- Огляд існуючих підходів до управління фінансовими ризиками в організаціях.
- Самостійне дослідження механізмів та інструментів для мінімізації фінансових ризиків (страхування, хеджування, резерви).
- Аналіз міжнародних стандартів управління фінансовими ризиками (ISO 31000, COSO).

 Інструменти та методи захисту фінансових даних (14 годин)

- Вивчення основ криптографії, шифрування та інших методів захисту фінансових транзакцій.
- Дослідження методів аутентифікації та авторизації в системах обробки фінансової інформації.
- Ознайомлення з механізмами безпечної передачі фінансових даних в цифровому середовищі (SSL, TLS, VPN).

 Аналіз законодавчих і нормативних аспектів фінансової безпеки (10 годин)

- Самостійне вивчення основних законів і нормативних актів, що регулюють фінансову безпеку (Закон України "Про фінансові послуги", Закон України "Про захист персональних даних" тощо).
- Ознайомлення з міжнародними стандартами і угодами з фінансової безпеки (GDPR, PCI DSS).
- Аналіз судових та правових випадків, пов'язаних із фінансовими шахрайствами та злочинами.

 Поглиблене вивчення інструментів фінансового контролю (10 годин)

- Самостійне дослідження різних інструментів фінансового контролю, таких як аудити, внутрішній контроль, перевірка фінансових звітів.
- Ознайомлення з принципами побудови фінансових політик безпеки на рівні підприємства.
- Оцінка ефективності внутрішніх контрольних процедур щодо виявлення фінансових порушень.

 Розробка стратегії забезпечення фінансової безпеки підприємства (10 годин)

- Самостійне розроблення стратегії управління фінансовою безпекою для вигаданої або реальної компанії.
- Визначення пріоритетів для захисту фінансових активів, стратегічне планування фінансової безпеки.
- Аналіз поточних загроз і розробка плану дій для мінімізації ризиків.

 Практичні заняття з аналізу фінансових інцидентів (10 годин)

- Аналіз реальних або вигаданих випадків фінансових злочинів: шахрайство, крадіжка коштів, фінансові маніпуляції.
- Визначення причин виникнення інцидентів і розробка рекомендацій щодо запобігання їх у майбутньому.
- Використання методів аудиту і аналізу для виявлення потенційних загроз.

8. Система оцінювання та вимоги

Загальна система оцінювання курсу	Оцінювання курсу базується на **накопичувальній системі** та включає: **поточний контроль** (оцінювання лабораторних занять) – 40 балів, **проміжний модульний контроль** – 10 балів, **виконання індивідуального завдання (РГР)** – 10 балів **та підсумковий контроль** – 40 балів. Оцінювання кожного виду діяльності здійснюється окремо відповідно до **досягнення навчальних цілей**.
Вимоги до РГР, КР, КП тощо	**Критерії оцінювання РГР:** 1) відповідність завдання вимогам курсу – **2 балів;** 2) обґрунтування вибору стандартів та методів захисту – **2 балів;** 3) якість аналізу ризиків та оцінка відповідності – **2 балів;** 4) оформлення роботи, відповідність методичним рекомендаціям – **2 балів;** 5) своєчасність здачі роботи – **2 бали.**
Практичні заняття	Оцінка кожного практичного заняття здійснюється за наступними критеріями: 1) виконання практичного завдання – **3 бали;** 2) аналіз отриманих результатів – **1 бал**; 3) належне оформлення звіту – **1 бал.**
Умови допуску до підсумкового контролю	1. Виконання та захист **не менше 50% практичних робіт** (щонайменше 4 із 8). 2. Проходження проміжного модульного контролю. 3. Виконання **розрахунково-графічної роботи** (РГР).

Розподіл балів, які отримують здобувачі вищої освіти

Модуль за тематичним планом дисципліни та форма контролю		Кількість балів
Змістовий модуль 1. Основи фінансової безпеки та управління фінансовими ризиками		**30**
1	Основи фінансової безпеки та ризик-менеджменту	**5**
2	Методи оцінки фінансових ризиків	**5**
3	Інструменти управління фінансовими ризиками	**5**
4	Законодавчі та нормативні аспекти фінансової безпеки	**15**
Змістовий модуль 2. Захист фінансової інформації та інструменти кібербезпеки в фінансовій сфері		**30**
1	Захист фінансових даних та інформації	**5**
2	Кібербезпека в фінансовій сфері	**15**
3	Шифрування фінансових транзакцій і захист персональних даних	**5**
4	Інструменти для забезпечення безпеки електронних платежів	**5**
Усього поточний і проміжний модульний контроль		**60**
Семестровий контроль (Диференційований залік)		**40**
Разом		**0…100**

Шкала оцінювання результатів навчання

<table>
<tr><th rowspan="2">Оцінка в балах</th><th rowspan="2">Оцінка ECTS</th><th colspan="2">Оцінка за національною шкалою (диференційований залік)</th></tr>
<tr><td>для екзамену (диференційованого заліку), курсового проєкту (роботи), практики, атестації</td><td>для заліку</td></tr>
<tr><td>90 – 100</td><td>A (відмінно)</td><td>відмінно</td><td rowspan="5">зараховано</td></tr>
<tr><td>82-89</td><td>B (дуже добре)</td><td rowspan="2">добре</td></tr>
<tr><td>75-81</td><td>C (добре)</td></tr>
<tr><td>66-74</td><td>D (задовільно)</td><td rowspan="2">задовільно</td></tr>
<tr><td>60-65</td><td>E (достатньо)</td></tr>
<tr><td>0-59</td><td>FX (незадовільно)</td><td>незадовільно з можливістю повторного складання</td><td>незараховано з можливістю повторного складання</td></tr>
</table>

9. Обладнання та програмне забезпечення.

При вивченні курсу використовується наступне **обладнання та програмне забезпечення**:

І. Апартне забезпечення:

Персональні комп'ютери або ноутбуки з підтримкою віртуалізації та можливістю роботи з образами дисків та цифровими доказами.

Операційні системи: Windows 10/11 Pro, Linux (Ubuntu, Kali Linux – для аналізу вразливостей), macOS.

Серверне обладнання для моделювання атак, аналізу мережевого трафіку та логів.

Мережеве обладнання (маршрутизатори, комутатори, мережеві екрани) для дослідження атак та аналізу цифрових слідів.

Зовнішні накопичувачі (HDD, SSD, USB-флешки) для роботи з криміналістичними копіями та створення дампів пам'яті.

Мобільні пристрої (Android, iOS) для дослідження мобільної криміналістики.

ІІ. Програмне забезпечення:

1. Для збору та збереження цифрових доказів:

FTK Imager – створення криміналістичних копій дисків.

Autopsy, Sleuth Kit – аналіз файлових систем та структури дисків.

Guymager – криміналістичне копіювання дисків у Linux.

2. Для аналізу файлових систем та метаданих:

X-Ways Forensics – глибокий аналіз файлових систем, відновлення даних.

ExifTool – витягнення метаданих із файлів (зображень, документів, відео).

Bulk Extractor – автоматичний пошук артефактів у файлах (номери кредитних карт, паролі).

3. Для дослідження операційних систем та лог-файлів:

Registry Explorer – аналіз реєстру Windows.

Event Log Explorer – дослідження журналів подій Windows.

Plaso, Timesketch – створення хронологій подій на основі логів системи.

4. Для мережевої криміналістики та аналізу трафіку:

Wireshark – аналіз мережевого трафіку.

Zeek (Bro IDS) – моніторинг і розслідування мережевих атак.

NetworkMiner – вилучення артефактів із трафіку.

5. Для криміналістики мобільних пристроїв:
MOBILedit Forensic – вилучення даних із мобільних пристроїв.
Oxygen Forensic Detective – аналіз дзвінків, повідомлень, геолокаційних даних.
Cellebrite UFED – відновлення та аналіз даних із мобільних телефонів.
6. Для аналізу шкідливого програмного забезпечення:
IDA Pro – дизасемблювання та аналіз шкідливого коду.
PE Explorer – дослідження виконуваних файлів Windows.
Cuckoo Sandbox – динамічний аналіз підозрілих файлів у віртуальному середовищі.
7. Для складання криміналістичних звітів та документування:
LaTeX, MS Word – підготовка технічної документації та звітів.
CaseNotes – ведення криміналістичних нотаток.
8. Платформи для дистанційного навчання:
Moodle, Microsoft Teams – розміщення навчальних матеріалів, тестування та проведення лекцій.
Google Drive, OneDrive – спільна робота з документами та звітами.
Використання наведеного обладнання та програмного забезпечення дозволяє студентам отримати практичний досвід у сфері цифрової криміналістики та підготуватися до роботи в реальних криміналістичних розслідуваннях.

10. Політики курсу.
У випадку, якщо здобувач протягом семестру не виконав у повному обсязі всіх видів навчальної роботи, має невідпрацьовані лабораторні роботи або не набрав мінімально необхідну кількість балів (25), він не допускається до складання диференційованого заліку під час семестрового контролю, але має право ліквідувати академічну заборгованість у порядку, передбаченому «Положенням про поточне та підсумкове оцінювання знань здобувачів НУ “Чернігівська політехніка”». Повторне складання заліку з метою підвищення позитивної оцінки не дозволяється. У випадку повторного складання заліку всі набрані протягом семестру бали анулюються, а повторний диференційований залік складається у вигляді тестування.
До загальної політики курсу відноситься дотримання принципів відвідування занять у відповідності до затвердженого розкладу, а також вільного відвідування лекційних занять для осіб, які отримали на це дозвіл відповідно до «Порядку надання дозволу на вільне відвідування занять здобувачам вищої освіти НУ «Чернігівська політехніка»». Запорукою успішного вивчення дисципліни є активність та залучення під час проведення лабораторних/практичних та лекційних занять – відповіді на запитання викладача (як один з елементів поточного контролю), задавання питань для уточнення незрозумілих моментів, вирішення практичних завдань. Консультації відбуваються в аудиторіях університету у відповідності до затвердженого розкладу або ж особистих чи групових консультацій (через вбудований форум) на сторінці курсу в системі дистанційного навчання НУ «Чернігівська політехніка».
Політика дедлайнів
Своєчасність здачі лабораторної роботи оцінюється в 0,5 балу за кожну лабораторну роботу. Своєчасність здачі РГР оцінюється в 1 бал. Відповідно, максимальна оцінка за невчасно здані роботи зменшується на зазначену кількість балів. Виключенням може бути наявність поважних причин несвоєчасної здачі зазначених робіт (хвороба, участь в зазначений час в інших видах навчальної, наукової чи організаційної роботи, офіційна робота за фахом тощо).
Політика користування ноутбуками / смартфонами
Прохання до здобувачів тримати смартфони переведеними у беззвучний режим протягом лекційних та практичних занять, так як дзвінки, переписки та спілкування у соціальних мережах відволікають від проведення занять як викладача, так й інших здобувачів. Ноутбуки, планшети та смартфони не можуть використовуватися в аудиторіях під час занять та під час проведення підсумкового контролю (за виключенням проходження тестового контролю в системі Moodle).

Політика заохочень та стягнень

За результатами навчальної, наукової або організаційної діяльності здобувачів вищої освіти за курсом їм можуть нараховуватися додаткові бали – до 10 балів, у залежності від вагомості досягнень. Види позанавчальної діяльності, за якими здобувачі вищої освіти заохочуються додатковою кількістю балів: участь у міжнародних проектах, наукові дослідження, тези, участь у науково-практичних конференціях, винаходи, патенти, авторські свідоцтва за напрямами курсу.

Політика академічної доброчесності

Академічна доброчесність повинна бути забезпечена під час проходження даного курсу, зокрема при виконанні лабораторних, контрольних та розрахунково-графічних робіт (КР/КП) (принципи описані у Кодексі академічної доброчесності НУ «Чернігівська політехніка»). Списування під час проміжного та підсумкового контролів, виконання практичних завдань на замовлення, підказки вважаються проявами академічної недоброчесності. Від усіх слухачів курсу очікується дотримання академічної доброчесності у зазначених вище моментах. До здобувачів вищої освіти, у яких було виявлено порушення академічної доброчесності, застосовуються різноманітні дисциплінарні заходи (включаючи повторне проходження певних етапів).

Правила перезарахування кредитів

Кредити, отримані в інших закладах вищої освіти, а також результати навчання у неформальній та/або інформальній освіті, можуть бути перезараховані викладачем у відповідності до положення «Порядок визначення академічної різниці та перезарахування навчальних дисциплін у НУ «Чернігівська політехніка»». Визнання результатів навчання у неформальній освіті розповсюджується на окремі змістові модулі (теми) навчальної дисципліни.

11. Рекомендована література.

Базові підручники:

1. Злочини проти інформаційної безпеки держави: поняття, виявлення, досудове розслідування: монографія / І.В. Гора, В.А. Колесник, В.В. Малюк, В.О. Ходанович, А.М. Черняк, Л.І. Щербина. Київ: 7БЦ, 2023. 512 с.

2. Research Trends, Challenges and Emerging Topics in Digital Forensics: A Review of Reviews. Received January 22, 2022, accepted February 16, 2022, date of publication February 24, 2022, date of current version March 10, 2022. URL: https://www.researchgate.net/publication/358837101_Research_Trends_Challenges_and_Emergin_Topics_in_Digital_Forensics_A_Review_of_Reviews

3. Tarun Vashishth. Cyber Forensics Up and Running. A hands-on guide to digital forensics tools and technique. Published by BPB Online WeWork, 2024. 407 p.

4. eForensics Magazine. Workshop. URL: https://eforensicsmag.com/.

5. Bruce Middleton. Cyber Crime Investigator's Field Guide. Third Edition. Chennai, India: CRC Press, 2022. 353 p.

6. Introduction to Forensic and Criminal Psychology. 7th Edition. Dennis Howitt Loughborough University. New York: Pearson Education Limited, 2022. 768 p.

Джерела:

1. ISO/IEC 27037 Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence. URL: https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027037-2012.pdf

2. Репозиторії готових дампів па'яті для аналізу на гітхаб. URL: https://github.com/SecurityNik/CTF, https://github.com/cyph3rryx/Kryptonite-RAM-Dump-Collection, https://www.baeldung.com/linux/dump-memory-image, https://github.com/504ensicsLabs/LiME

3. Образ віртуальної машини Caine, що містить необхідні інструменти в галузі Computer Forensics. URL: https://www.caine-live.net/page5/page5.html

4. Образ віртуальної машини Kali Linux. URL: https://www.kali.org/get-kali/#kali-platforms

5. Платформа для візуалізації та емуляції на MacOS. URL: https://mac.getutm.app/

6. Власний репозиторій з програмним інструментом для трансферу дампів пам’яті в ізольований контейнер Caine для аналізу. URL: https://github.com/urlinka2006/CyberInsight

7. Autopsy – платформа цифрової криміналістики та графічний інтерфейс для The Sleuth Kit та інших інструментів цифрової криміналістики. URL: https://github.com/sleuthkit/autopsy

8. WireShark – найпопулярніший у світі аналізатор мережевих протоколів. URL: https://www.wireshark.org/

9. Sleuth Kit (TSK) – бібліотека та колекція інструментів цифрової криміналістики командного рядка, які дозволяють досліджувати томи та дані файлової системи. Бібліотеку можна включити до більших інструментів цифрової криміналістики, а інструменти командного рядка можна безпосередньо використовувати для пошуку доказів. URL: https://github.com/sleuthkit/sleuthkit

10. BelkaGPT — перший автономний AI-помічник для розслідувань DFIR. URL: https://belkasoft.com/belkagpt?utm_campaign=Police%201&utm_source=Media&utm_medium=Article&utm_term=eforensicsmag&utm_content=belkagpt