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

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

ЗАТВЕРДЖУЮ

Гарант освітньої програми
_____ О.О. Ілляшенко
(підпис) (ініціали та прізвище)

« 31 » серпня 2023 р.

РОБОЧА ПРОГРАМА ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Управління інформаційною безпекою
(назва навчальної дисципліни)

Галузь знань: 12 "Інформаційні технології"
(шифр і найменування галузі знань)

Спеціальність: 125 "Кібербезпека"
(код та найменування спеціальності)

Освітня програма: Безпека інформаційних і комунікаційних систем
(найменування освітньої програми)

Форма навчання: денна

Рівень вищої освіти: перший (бакалаврський)

Харків 2023 рік

Розробник: Лисицький К.Є. ст.викладач кафедри 503, phd, _____
(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 « 27 » 08 2023 р.

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, напрям підготовки, рівень вищої освіти</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td></tr>
<tr><td>Кількість кредитів – 4</td><td rowspan="9">Галузь знань
12 "Інформаційні технології"
(шифр та найменування)

Спеціальність
125 "Кібербезпека"
(код та найменування)

Освітня програма
Управління інформаційною безпекою
(найменування)

Рівень вищої освіти:
перший (бакалаврський)</td><td>Цикл загально-професійної підготовки</td></tr>
<tr><td>Кількість модулів – 2</td><td rowspan="2">Навчальний рік
2023/2024</td></tr>
<tr><td>Кількість змістових модулів – 2</td></tr>
<tr><td>Індивідуальне завдання: не передбачено</td><td rowspan="2">Семестр: 7-й</td></tr>
<tr><td>Загальна кількість годин – 48/120</td></tr>
<tr><td rowspan="5">Кількість тижневих годин для денної форми навчання:
аудиторних – 3
самостійної роботи студента – 4.5</td><td>Лекції [1)]32 год.</td></tr>
<tr><td>Практичні, семінарські
0 год.</td></tr>
<tr><td>Лабораторні[1)]
16 год.</td></tr>
<tr><td>Самостійна робота
72 год.</td></tr>
<tr><td>Індивідуальні завдання:
не передбачено</td></tr>
<tr><td>Вид контролю:
модульний контроль, залік</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить:

Для денної форми навчання – 48/72.

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

2. Мета та завдання навчальної дисципліни

Мета діяльності: є формування у студентів теоретичних знань та практичних навичок у галузі аудита та управління інцидентами інформаційної безпеки, використовуючи існуючі міжнародні стандарти з інформаційної безпеки.

Завдання (ОК 29): застосовувати знання до вирішення задач аудиту та управління інцидентами інформаційної безпеки, опираючись на існуючі міжнародні стандарти; обирати потрібні організаційні та інженерно-технічні заходи, засоби і методи реагування на інциденти; аналізувати інциденти та удосконалювати політику інформаційної безпеки організацій.

Компетентності, які набуваються. Дисципліна має допомогти сформувати у студентів такі компетентності.

Загальні компетентності

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.**Фахові компетентності.**

КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

Програмні результати навчання. В результаті вивчення дисципліни студенти мають досягти такі програмні результати навчання:

ПРН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.

ПРН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

ПРН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.

ПРН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.

ПРН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.

ПРН 14.. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.

ПРН 21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

ПРН 28 Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.

ПРН 29 Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.

Пререквізити – дисципліна базується на: ОК23 «Нормативно-правове забезпечення інформаційної безпеки», ОК28 «Комплексні системи захисту інформації: проектування, впровадження, супровід»

Кореквізити – дисципліна є базовою для: ОК29 «Управління інформаційною безпекою»

3. Програма навчальної дисципліни

Модуль 1’

Змістовний модуль 1. Аудит та управління інцидентами інформаційної безпеки.

ТЕМА 1. **Аудит інформаційної безпеки**

Аудит інформаційної безпеки. Види аудиту. Основні складові системи аудиту інформаційної безпеки. Нормативне забезпечення аудиту інформаційної безпеки.

ТЕМА 2. **Внутрішній аудит СМІБ за вимогами ISO/IEC 27001 та ISO 19011**

Загальна характеристика внутрішніх аудитів СМІБ**.** Розробка програми внутрішнього аудиту на рік. Розробка плану аудиту протягом року. Розробка анкет відповідно до критеріїв аудиту. Підготовка до проведення аудиту на місці. Розробка звіту про аудит. Розробка корегувальних та запобіжних заходів. Перевірка виконання заходів і аналіз результативності. Підготовка звіту для вищого керівництва.

ТЕМА 3. **Комплексний аудит інформаційної безпеки**

Основні етапи аудиту безпеки інформаційних систем. Постановка задачі та уточнення обсягу робіт. Збір і аналіз інформації. Проведення аналізу ризиків. Розробка рекомендацій. Оцінка діяльності з управління інформаційною безпекою організації. Основні положення стандарту ISO/IEC 27004:2009. Вимірювання, показники і метрика безпеки.

ТЕМА 4. **Управління інцідентами інформаційної безпеки.**

Базові принципи, терміни та визначення. Цілі управління інцидентами. Стандарти, рекомендації та найкращі світові практики щодо управління інцидентами інформаційної безпеки. Етапи управління інцидентами інформаційної безпеки відповідно до ISO/IEC 27035. Особливості менеджменту інцидентів відповідно до ITIL. Концепція та структура автоматизованої системи управління інцидентами інформаційної безпеки.

Модульний контроль.

Модуль 2

Змістовний модуль 2. Реагування на інциденти та політика інформаційної безпеки.

ТЕМА 5. Огляд стандарту **ISO/IEC 27001 «Інформаційні технології. Методи забезпечення безпеки. Системи менеджменту інформаційної безпеки. Вимоги»**

Приклади вразливостей, які можуть бути використані для реалізації відповідних загроз для комерційної структури. Ідентифікація активів підприємства для оцінки ризиків.

ТЕМА 6. **Функціонування груп реагування на інциденти інформаційної безпеки CERT/CSIRT**

Загальна характеристика діяльності груп CERT/CSIRT. Етапи створення груп CERT/CSIRT. Класифікація груп CERT/CSIRT за галузевою ознакою. Склад команд CERT/CSIRT. Сервіси, що надаються групами реагування на інциденти. Обробка інцидентів інформаційної безпеки групами CERT/CSIRT. Документаційне забезпечення процесу управління інцидентами інформаційної безпеки.

ТЕМА 7. **Політика безпеки інформації**

Методичні підходи до розробки політики інформаційної безпеки підприємства. Порядок розробки політики та етапи.

Модульний контроль.

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. Аудит та управління інцидентами інформаційної безпеки.					
Тема 1. Аудит інформаційної безпеки.	16	4		2	10

Тема 2. Внутрішній аудит СМІБ за вимогами ISO/IEC 27001 та ISO 19011.	16	4		2	10
Тема 3. Комплексний аудит інформаційної безпеки.	16	4		2	10
Тема 4. Управління інцідентами інформаційної безпеки.	16	4		2	10
Разом за змістовним модулем 1	64	16		8	40
Усього годин за модуль 1	64	16		8	40
Модуль 2					
Змістовний модуль 2. Реагування на інциденти та політика інформаційної безпеки.					
Тема 5. *Огляд стандарту* ISO/IEC 27001 «Інформаційні технології. Методи забезпечення безпеки. Системи менеджменту інформаційної безпеки. Вимоги».	20	6		4	12
Тема 6. Функціонування груп реагування на інциденти інформаційної безпеки CERT/CSIRT.	18	6		2	10
Тема 7. Політика безпеки інформації.	18	4		2	10
Разом за змістовним модулем 2	56	16		8	32
Усього годин за модуль 2	56	16		8	32
Усього годин за дисципліною	120	32		16	72

5. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
...	*Не передбачено*	

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	Закріплення матеріалу лекції щодо аудиту інформаційної безпеки.	2
2	Отримання практичних навичок з розроблення документів. Опитувальник, бланк для фіксації результатів внутрішнього аудиту, протокол відхилень.	2
3	Закріплення матеріалу лекції щодо комплексного аудиту інформаційної безпеки	2
4	Отримання практичних навичок з аналізу СМІБ	2
5	Отримання практичних навичок з виявлення вразливостей, які можуть бути використані для реалізації відповідних загроз для комерційної структури.	4

6	Закріплення матеріалу лекції щодо функціонування груп реагування на інциденти інформаційної безпеки CERT/CSIRT	2
7	Отримання практичних навичок аналізу політик інформаційної безпеки	2
	Разом	16

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Опрацювання стандарту CobiT	14
2	Опрацювання стандарту ITIL	14
3	Опрацювання стандарту ISO/IEC 15408	14
4	Опрацювання стандарту ISO/IEC 270001	16
5	Кращі світові практики політик інформаційної безпеки	14
	Разом	72

9. Індивідуальні завдання

№ з/п	Назва теми	Кількість годин
1	2	3
	Не передбачено	

10. Методи навчання

Проведення аудиторних лекцій, лабораторних занять, консультацій, а також самостійна робота студентів за матеріалами, опублікованими кафедрою.

11. Методи контролю

Проведення поточного контролю, письмового модульного контролю, підсумковий контроль у вигляді іспиту.

12. Розподіл балів, які отримують студенти
12. Критерії оцінювання та розподіл балів, які отримують студенти

12.1. Розподіл балів, які отримують студенти (кількісні критерії оцінювання)

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовий модуль 1			
Активність та присутність на лекціях.	0…1	8	0…8

Виконання і захист практичних робіт. Своєчасність та виконання всіх завдань практичної роботи оцінюється у максимальну оцінку 6 балів.	0...6	4	0...24
Модульний контроль складається з трьох запитань.	0…18	1	0…18
Змістовий модуль 2			
Активність та присутність на лекціях.	0…1	8	0…8
Виконання і захист практичних робіт. Своєчасність та виконання всіх завдань практичної роботи оцінюється у максимальну оцінку 6 балів.	0...6	4	0...24
Модульний контроль складається з трьох запитань.	0…18	1	0…18
Усього за семестр			**0…100**

Білет для іспиту складається з одного теоретичного та одного практичного запитань, максимальна кількість за кожне із запитань, складає 50 балів.

Під час складання семестрового іспиту студент має можливість отримати максимум 100 балів.

Критерії оцінювання роботи студента протягом семестру

Задовільно (60 – 74). Мати мінімум знань та умінь. Відпрацювати та захистити всі лабораторні роботи та домашні завдання. Захистити всі індивідуальні завдання та здати тестування.

Добре (75 – 89). Твердо знать мінімум знань, виконати всі завдання. Показати вміння виконувати та захищати всі лабораторні роботи в обумовлений викладачем строк з обґрунтуванням рішень та заходів, які запропоновано у роботах.

Відмінно (90 – 100). Повно знати основний та додатковий матеріал. Знати всі теми. Орієнтуватися у підручниках та посібниках. Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти застосовувати їх. Безпомилково виконувати та захищати всі лабораторні роботи в обумовлений викладачем строк з докладним обґрунтуванням рішень та заходів, які запропоновано у роботах.

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

Сторінка дисципліни у системі дистанційного навчання «Ментор» [Ел. ресурс]. URL: https://mentor.khai.edu/course/view.php?id=4255

на якому розміщено навчально-методичний комплекс дисципліни, який включає в себе:

- робоча програма дисципліни;
- конспект лекцій (презентації), в тому числі в електронному вигляді, який за змістом повністю відповідає робочій програмі дисципліни;
- журнал успішності.
- Посилання на практики

14. Рекомендована література

Базова

1. Аудит та управління інцидентами інформаційної безпеки : навчальний посібник / [Корченко О.Г., Гнатюк С.О., Казмірчук С.В., Панченко В.М., Мельник С.В.] – Київ, 2014. – 189 с.
2. Управління інформаційною безпекою : Конспект лекцій / [Носок С. О, Фаль О. М, Ткач В.М.] – Київ, 2021. – 258 с.
3. Information security, cybersecurity and privacy protection : ISO/IEC 27001:2022
4. Information security, cybersecurity and privacy protection : ISO/IEC 15408-2:2022
5. Guidelines for auditing management systems : ISO 19011:2018

15. Інформаційні ресурси

1. Аудит та управління інцидентами інформаційної безпеки : навчальний посібник [Электрон. ресурс]. – Режим доступа: https://er.nau.edu.ua/bitstream/NAU/38027/1/Audit%26Incident_15042014.pdf
2. Управління інформаційною безпекою. Конспект лекцій[Электрон. ресурс]. - Режим доступа: https://ela.kpi.ua/items/30243ca5-b522-4179-993c-f32eab6b0fd1
3. Information security, cybersecurity and privacy protection : ISO/IEC 27001:2022 [Электрон. ресурс]. – Режим доступа: https://www.iso.org/standard/27001
4. Information security, cybersecurity and privacy protection : ISO/IEC 15408-2:2022 – Режим доступа: https://www.iso.org/standard/72892.html
5. Guidelines for auditing management systems : ISO 19011:2018 – Режим доступа: https://www.iso.org/standard/70017.html