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

СИЛАБУС
Аудит та управління інцидентами інформаційної безпеки

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

«_26__» __08___ 2024 р.

Розробник (-и): Гребенник. А.Г., старший викладач кафедри кібербезпеки та математичного моделювання _____
(підпис)

Силабус навчальної дисципліни обговорено на засіданні кафедри кібербезпеки та математичного моделювання

Протокол від 26 серпня 2024р. № 7

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

---

1. Загальна інформація про дисципліну.

Тип дисципліни	Обов'язкова
Мова викладання	українська
Рік навчання та семестр	1 рік, 2 семестр 125 Кібербезпека та захист інформації ОПП Кібербезпека
Викладач (-і)	Гребенник. Алла Григорівна, старший викладач кафедри кібербезпеки та математичного моделювання
Профайл викладача (-ів)	https://mmi.stu.cn.ua/personal-kafedry/ https://scholar.google.fi/citations?hl=uk&user=zDx8WrsAAAAJ https://www.scopus.com/authid/detail.uri?authorId=57219054928 https://orcid.org/0000-0002-7464-1412
Контакти викладача	контактний телефон: +380977267613, E-mail: grebennik.alla@gmail.com.

2. Анотація курсу.

Дисципліна є складовою частиною фундаментальної підготовки та відноситься до навчальних дисциплін циклу «Обов'язкові компоненти освітньої програми» за спеціальністю «Кібербезпека та захист інформації» (магістр).

Предметом вивчення навчальної дисципліни є основні поняття, принципи, методи та засоби організації і проведення аудиту інформаційної безпеки, а також процедури управління інцидентами інформаційної безпеки відповідно до вимог найбільш поширених міжнародних стандартів.

Практична та професійна спрямованість дисципліни зумовлена набуттям знань і вмінь щодо проведення об'єктивної оцінки рівня забезпечення безпеки інформаційних систем. Насамперед, це знання та вміння, які дають змогу виявляти, враховувати, реагувати і аналізувати події та інциденти інформаційної безпеки. Без реалізації цих процесів неможливо забезпечити рівень захищеності, адекватний сучасним стандартам і галузевим нормам.

Посилання на курс в MOODLE: https://eln.stu.cn.ua/course/view.php?id=3692

3. Мета та цілі курсу.

Метою викладання дисципліни є формування в студентів системи теоретичних знань та практичних умінь про сучасні наукові концепції, поняття, принципи та методи аудиту інформаційної безпеки, процедури управління інцидентами інформаційної безпеки відповідно до вимог найбільш поширених міжнародних стандартів, що є професійною основою для фахівця в галузі управління інформаційною безпекою.

Завдання вивчення дисципліни полягають в:

– отриманні знань про методику проведення аудиту та моніторингу процесів функціонування інформаційних систем;

– набутті умінь із забезпечення процесів захисту та функціонування інформаційних систем, що базуються на національних та міжнародних стандартах виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.

Під час вивчення дисципліни здобувач вищої освіти (ЗВО) має набути або розширити наступні загальні (КЗ) та фахові (КФ) компетентності, передбачені освітньою програмою спеціальності 125 - Кібербезпека та захист інформації:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 3. Здатність до абстрактного мислення, аналізу та синтезу.

КЗ 4. Здатність оцінювати та забезпечувати якість виконуваних робіт.

КЗ 5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).

КФ 4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.

КФ 7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

КФ 9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.

4. Результати навчання.

Під час вивчення дисципліни ЗВО має досягти або вдосконалити наступні програмні результати навчання (ПРН), передбачені освітньою програмою:

ПРН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

ПРН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

ПРН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

ПРН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

ПРН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

ПРН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.

ПРН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.

ПРН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.

У підсумку ЗВО повинен

1) знати:
- основну термінологію аудиту інформаційної безпеки;
- види аудиту;
- основні складові системи аудиту інформаційної безпеки;
- нормативне забезпечення аудиту інформаційної безпеки;
- загальну характеристику внутрішніх аудитів системи менеджменту інформаційної безпеки;
- принципи проведення внутрішнього аудиту;
- основні етапи аудиту безпеки інформаційних систем;
- методи оцінки компетентності аудиторів;
- принципи побудови систем управління інформаційною безпекою;
- процеси реагування на інциденти інформаційної безпеки та підходи до їх оцінки;

2) вміти:
- складати програму аудиту;
- управляти програмою аудиту;
- оцінювати діяльність з управління інформаційною безпекою організації;
- визначати вразливості інформаційних ресурсів організації та оцінювати ризик їх застосування.

5. Пререквізити.

Передумовою для вивчення дисципліни є наявність базових знань з дисципліни «Стандартизація, сертифікація засобів та комплексів захисту інформації».

6. Обсяг курсу.

Вид заняття	Загальна кількість годин денна/заочна
Лекції	16/6
Практичні заняття	16/6
Самостійна робота	88/108
Індивідуальне завдання – розрахункова графічна робота	
Всього кредитів	4

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

7. Тематика курсу.

Лекції (16/6 годин):

Змістовий модуль 1. Аудит систем інформаційної безпеки.

1. Системи аудиту інформаційної безпеки.

Предмет дисципліни, її цілі та задачі. Структура, завдання і форми контролю, основна література. Основні положення. Термінологія аудиту. Основні види аудиту інформаційної безпеки. Експертний аудит. Активний аудит. Аудит на відповідність стандартам інформаційної безпеки. Діагностичний аналіз Системи менеджменту інформаційної безпеки (СМІБ) за вимогами ISO/IEC 27001.

2. Внутрішній аудит СМІБ.

Завдання аудиту. Мета аудиту. Склад процедури аудиту. Критерії аудиту. Процес усвідомлення аудиту інформаційної безпеки. Програма аудиту інформаційної безпеки. Принципи проведення аудиту. Стандарт CobiT 4.1. Бібліотека інфраструктури інформаційних технологій – ITIL. Стандарт ISO/IEC 15408. Серія стандартів ISO/IEC 2700X. Загальна характеристика внутрішніх аудитів СМІБ. Принципи проведення внутрішнього аудиту. Алгоритм організації та проведення внутрішніх аудитів. Пошук загроз. Моделювання загроз. Позаплановий внутрішній аудит. Приклад вимог до процедур з внутрішнього аудиту. Принципи проведення внутрішнього аудиту. Дев’ять правил успішного проведення аудиту. Управління програмою аудиту. Розробка цілей програми аудиту. Розробка програми аудиту.

3. Комплексний аудит інформаційної безпеки.

Компетентність особи, що здійснює управління програмою аудиту. Встановлення обсягу програми аудиту. Виявлення та оцінювання ризиків для програми аудиту. Розробка процедур для програми аудиту. Визначення ресурсів, необхідних для реалізації програми аудиту. Реалізація програми аудиту. Вибір методів проведення аудиту. Формування команди з аудиту. Моніторинг програми аудиту. Аналіз та удосконалення програми аудиту.

4. Оцінка діяльності з управління інформаційною безпекою організації.

Встановлення цілей, сфери та критеріїв для конкретного аудиту. Покладання відповідальності на керівника команди з аудиту за конкретний аудит. Управління результатами реалізації програми аудиту. Використання записів відповідно до програми аудиту та їх збереження. Специфічні знання та навички аудиторів, пов'язані з особливостями систем менеджменту і галузями економіки.

Змістовий модуль 2. Управління інцидентами інформаційної безпеки.

5. Стандарти, рекомендації та кращі світові практики щодо управління інцидентами інформаційної безпеки.

Базові принципи, терміни та визначення системи менеджменту інцидентами інформаційної безпеки (СМІІБ). Цілі управління інцидентами. Основні заходи створення СМІІБ. Ознаки інциденту інформаційної безпеки. Аналіз інцидентів інформаційної безпеки. Визначення показників ефективності процесу управління інцидентами інформаційної безпеки.

6. Етапи управління інцидентами інформаційної безпеки відповідно до ISO/IEC 27035.

Етапи формування СМІІБ відповідно до моделі PDCA. Модель життєвого циклу процесу УІІБ. Усунення причин, наслідків інциденту і його розслідування.

7. Особливості менеджменту інцидентів відповідно до ITIL.

Місце процесу управління інцидентами серед усіх процесів ITIL. Основні етапи управління інцидентами відповідно до ITIL. Варіанти категорування інцидентів відповідно до ITIL. Концепція та структура автоматизованої системи управління інцидентами інформаційної безпеки. Інтеграційна платформа автоматизованої системи

управління інцидентами інформаційної безпеки. Апаратно-програмні засоби моніторингу і аудиту. Апаратно-програмні засоби захисту. Сховище інформації про ІІБ. Аналітичні інструменти і засоби генерації звітів.

8. Функціонування груп реагування на інциденти інформаційної безпеки CERT/CSIRT.

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

Практичні роботи (16/6 годин):

1. Основні види аудиту інформаційної безпеки. Діагностичний аналіз Системи менеджменту інформаційної безпеки (СМІБ) за вимогами ISO/IEC 27001.
2. Внутрішній аудит СМІБ. Розробка програми аудитів підприємства на рік. Складання плану внутрішнього аудиту. Підготовка опитувальника для проведення внутрішнього аудиту. Складання протоколу відхилень. Розробка звіту про аудит.
3. Розробка технічного завдання та проведення комплексного аудиту інформаційної безпеки підприємства.
4. Оцінка діяльності з управління інформаційною безпекою організації. Розробка аудиторського звіту. Розробка рекомендацій щодо вдосконалення системи захисту інформації.
5. Стандарти, рекомендації та кращі світові практики щодо управління інцидентами інформаційної безпеки.
6. Етапи управління інцидентами інформаційної безпеки відповідно до ISO/IEC 27035.
7. Особливості менеджменту інцидентів відповідно до ITIL.
8. Функціонування груп реагування на інциденти інформаційної безпеки CERT/CSIRT.

Розрахунково-графічна робота (РГР)

Тема: Аудит комп'ютерних систем. Засоби аналізу мережевої безпеки (сканери вразливостей).

Самостійна робота (88/108 годин):

1. Системи аудиту інформаційної безпеки.
2. Внутрішній аудит СМІБ.
3. Комплексний аудит інформаційної безпеки.
4. Оцінка діяльності з управління інформаційною безпекою організації.
5. Стандарти, рекомендації та кращі світові практики щодо управління інцидентами інформаційної безпеки..
6. Етапи управління інцидентами інформаційної безпеки відповідно до ISO/IEC 27035.
7. Особливості менеджменту інцидентів відповідно до ITIL.
8. Функціонування груп реагування на інциденти інформаційної безпеки CERT/CSIRT.

8. Система оцінювання та вимоги

Загальна система оцінювання курсу	Оцінювання курсу базується на накопичувальній системі та включає: поточний контроль (оцінювання практичних 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	Критерії оцінювання РГР: 1) виконання завдання – 5 балів; 2) якість виконання завдання – 2 бали; 3) оформлення роботи, відповідність методичним рекомендаціям – 2 бали; 4) своєчасність здачі роботи – 1 бал.

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. 2. Проходження проміжного модульного контролю. 3. Виконання розрахунково-графічної роботи.

Розподіл балів, які отримують здобувачі вищої освіти

Модуль за тематичним планом дисципліни та форма контролю		**Кількість балів**
Змістовий модуль 1. Аудит систем інформаційної безпеки		
1	Виконання практичних робіт	**0…20**
2	Проміжний модульний контроль	**0…10**
Змістовий модуль 2. Управління інцидентами інформаційної безпеки		
1	Виконання практичних робіт	**0…20**
2	Виконання індивідуального завдання (РГР)	**0…10**
Усього поточний і проміжний модульний контроль		**60**
Семестровий контроль (Екзамен)		**40**
Разом		**0…100**

Шкала оцінювання результатів навчання

Оцінка в балах	**Оцінка ECTS**	**Оцінка за національною шкалою (диференційований залік)**	
		для екзамену (диференційованого заліку), курсового проєкту (роботи), практики, атестації	для заліку
90 – 100	**A** (*відмінно*)	відмінно	зараховано
82-89	**B** (*дуже добре*)	добре	
75-81	**C** (*добре*)		
66-74	**D** (*задовільно*)	задовільно	
60-65	**E** (*достатньо*)		
0-59	**FX** (*незадовільно*)	незадовільно з можливістю повторного складання	незараховано з можливістю повторного складання

9. Політики курсу.

У випадку, якщо здобувач протягом семестру не виконав у повному обсязі всіх видів навчальної роботи, має невідпрацьовані практичні роботи або не набрав мінімально необхідну кількість балів (25), він не допускається до складання екзамену 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 екзамену з метою підвищення позитивної оцінки не дозволяється. У випадку

повторного складання екзамену всі набрані протягом семестру бали анулюються, а повторний екзамен 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 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 практичної роботи оцінюється в 0,5 балу за кожну практичну 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 практичних та розрахунково-графічних робіт (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.

Базова

1. Управління інформаційною безпекою. Навчальний посібник / [уклад.: Толюпа С.В., Політанський Л.Ф., Політанський Р.Л., Лесінський В.В.] Чернівці.: Чернівецький нац. ун-т ім. Ю.Федьковича, 2021. – 540 с.

2. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с.

3. Якименко Ю.М., Савченко В.А., Легомінова С.В. Системний аналіз інформаційної безпеки: сучасні методи управління: підручник. Київ: Державний університет телекомунікацій, 2022. – 308 с.

4. Менеджмент інформаційної безпеки : навчальний посібник для студентів спеціальності 125 "Кібербезпека" / О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук, Ю.М. Ткач, Є.В. Іванченко. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 408 с.

5. Козачок В.А., Гайдур Г.І., Гахов С.О., Власенко В.О., Чумак Н.С. Політики безпеки. Навчальний посібник для студентів вищих навчальних закладів – Київ: ДУТ ННІЗІ, 2020. – 167с.

Допоміжна

1. Нестеренко Г. Інформаційна безпека: курс лекцій. Київ: НАУ, 2022. – 102 с.

2.Mike Chapple, David Seidl — *CompTIA CySA+ Study Guide: Exam CS0-002* (2nd ed.) — 2020.

3. ДСТУ ISO 19011:2019. Настанови щодо проведення аудитів систем управління.

4. Микитишин А. Г., Митник М. М., Голотенко О. С., Карташов В. В. Комплексна безпека інформаційних мережевих систем: навч. посіб. – Тернопіль: ФОП Паляниця В. А., 2023. – 324 с.

Інформаційні ресурси

1. Система дистанційного навчання НУ «Чернігівська політехніка». Курс: Аудит та управління інцидентами інформаційної безпеки (ОКЗ). – [Електронний ресурс]. – Режим доступу: https://eln.stu.cn.ua/course/view.php?id=3692

2. Бібліотека та читальний зал НУ «Чернігівська політехніка». – [Електронний ресурс]. – Режим доступу: http://library2.stu.cn.ua

3. Державна служба спеціального зв'язку та захисту інформації України. – [Електронний ресурс]. – Режим доступу: http://www.dsszzi.gov.ua

4. Національна бібліотека ім В.І. Вернадського / [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/ .

5. Стандарти систем управління ІБ серії ISO/IEC 27000. [Електронний ресурс]. Режим доступу: https://www.iso27001security.com/

6. Офіційний портал Верховної Ради України [Електронний ресурс]. – Режим доступу: www.rada.gov.ua/

7. Технічний захист інформації. Аудит безпеки інформаційної безпеки. – [Електронний ресурс]. – Режим доступу: https://tzi.com.ua/audbezib.html

8. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». . – [Електронний ресурс]. – Режим доступу: https://csecurity.kubg.edu.ua/index.php/journal/issue/archive

9. Кваліфікаційний центр інформаційних технологій та кібербезпеки. ДержНДІ технологій кібербезпеки. – [Електронний ресурс]. – Режим доступу: https://qc.csi.cip.gov.ua/uk

10. Prometheus: Платформа масових відкритих онлайн-курсів [Електронний ресурс]. – Режим доступу: https://prometheus.org.