СИЛАБУС

Кафедра кібербезпеки та математичного моделювання

Назва курсу	Аудит та управління інцидентами інформаційної безпеки
Мова викладання	українська
Викладач (-і)	Ткач Ю.М., завкафедри кібербезпеки та математичного моделювання, д.пед.н., професор
Профайл викладача (-ів)	https://mmi.stu.cn.ua/personal-kafedry/ ORCID 0000-0002-8565-0525
Контакти викладача	(063) 594 22 94 tkachym79@gmail.com

1. **Анотація курсу** -

Предметом навчальної дисципліни "Аудит та управління інцидентами інформаційної безпеки" 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.

Об'єкт навчальної дисципліни – безпека інформаційних систем.

Організаційні форми, методи й засоби забезпечення високої фундаментальної, професійної і практичної спрямованості та диференційованого підходу навчання студентів: для ефективної організації навчальних занять використовуються такі форми роботи, як розповідь, навчальна лекція, практична робота, дискусія, робота з книгою та в Інтернеті, постановка завдання, планування процесу виконання, ілюстрування, демонстрування, регулювання й контроль, аналіз підсумків практичної роботи.

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.

ЗМІСТОВИЙ МОДУЛЬ 1. АУДИТ СИСТЕМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ТЕМА 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.

ТЕМА 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.

ТЕМА 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.

ТЕМА 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

ТЕМА 5. 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.

ТЕМА 6. Стандарти, рекомендації та кращі світові практики щодо управління інцидентами інформаційної безпеки

Визначення показників ефективності процесу управління інцидентами інформаційної безпеки.

ТЕМА 7. 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.

ТЕМА 8. 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.

ТЕМА 9. 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.

ТЕМА 10. 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.

2. 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.

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:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

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

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

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

КФ 1. Здатність розробляти та впроваджувати законодавчу, нормативно-правову базу, державні і міжнародні вимоги, а також інтегрувати, аналізувати і використовувати сучасні світові практики та стандарти з метою здійснення професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

КФ 3. Здатність до проектування, впровадження, супроводження інформаційних мереж і ресурсів, інфраструктури установи, архітектури використання інформаційних технологій (хмарних), а також бізнес/операційних процесів з метою якісного функціонування інформаційно-комунікаційних систем (комутативних або без комутативних), згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації.

КФ 4. Здатність розробляти, впроваджувати та аналізувати заходи, щодо резервування інформаційних ресурсів, розробки планів відновлення штатного

функціонування інфраструктури організації в цілому, які викликані реалізацією різного класу кібератак, виявленням і реєстрацією інцидентів та нештатних ситуацій.

КФ 5. Здатність розробляти, планувати, аналізувати та впроваджувати систему доступу до інформаційних ресурсів, а також систему аудиту і контролю ефективності функціонування інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації.

КФ 6. Здатність розробляти та впроваджувати заходи протидії кіберінцидентам, а також аналізувати, здійснювати процедури управління та контролю інцидентами, організовувати та проводити розслідування, надавати рекомендації щодо заходів їх попередження та протидії.

КФ 7. Здатність розробляти, впроваджувати, супроводжувати системи аудиту та моніторингу якості бізнес/операційних процесів функціонування організації та системи управління інформаційною безпекою та/або кібербезпекою за вітчизняними і світовими нормами та стандартами.

Завдання полягає у:

- 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.

3. Результати навчання

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

ПРН 2. планувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;

ПРН 3. використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;

ПРН 4. аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;

ПРН 6. діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі у напрямах найкращих практик, технічних вимог та рекомендацій з управління інформаційною безпекою та /або кібербезпекою;

ПРН 7. проектувати, впроваджувати, та супроводжувати інформаційно-комунікаційні системи, а також забезпечувати захист інформаційних ресурсів

мереж (мережева безпека) та всієї інфраструктури установи на базі сучасних моделей, методів і засобів передачі даних в комутативних або без комутативних каналах зв'язку, хмарного простору, протоколів обміну даними, мережного устаткування, тощо ;

ПРН 9. розробляти, впроваджувати та аналізувати заходи, щодо резервування інформаційних ресурсів, розробки планів відновлення штатного функціонування інфраструктури організації в цілому, які викликані реалізацією різного класу кібератак, виявленням і реєстрацією інцидентів та нештатних ситуацій;

ПРН 10. розробляти, планувати, аналізувати та впроваджувати систему доступу до інформаційних ресурсів, інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно - апаратних комплексів, підсистем, програмного забезпечення, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації;

ПРН 11. розробляти, впроваджувати, супроводжувати системи аудиту та моніторингу (контролю) якості бізнес/операційних процесів функціонування організації та системи управління інформаційною безпекою та/або кібербезпекою за вітчизняними і світовими нормами та стандартами;

ПРН 12. розробляти, впроваджувати та супроводжувати процеси належного функціонування системи моніторингу інформаційних ресурсів і бізнес процесів в інфраструктурі організації.

Дисципліну можна вважати такою, що засвоєна, якщо ЗВО:

1) **знає**:

— 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.

2) **вміє**:

— самостійно складати програму аудиту;
— самостійно управляти програмою аудиту;
— самостійно оцінювати діяльність з управління інформаційною безпекою організації.

4. Обсяг курсу.

Вид заняття	Загальна к-сть годин
лекції	16
практичні	14
самостійна робота (РГР)	90

5. Пререквізити – взаємозв'язок із суміжними дисциплінами: вивчення навчальної дисципліни "Аудит та управління інцидентами інформаційної безпеки" поглиблює знання студентів отримані під час вивчення дисциплін "Менеджмент інформаційної безпеки" (при підготовці фахівців освітньо-кваліфікаційного рівня "бакалавр" за напрямом "Кібербезпека") та "Забезпечення безперервності бізнесу".

6. Система оцінювання та вимоги

Оцінювання проводиться за 100-бальною шкалою.

Бали нараховуються за наступним співвідношенням:

• практичні заняття : 20% семестрової оцінки;

• домашні завдання: 20% семестрової оцінки;

•РГР: 20% семестрової оцінки;

• іспит: 40% семестрової оцінки.

Загальна система оцінювання курсу	Аудит та управління інцидентами інформаційної безпеки
Вимоги до РГР	**Критерії оцінювання написання** 1. Повнота розкриття. 2. Авторський внесок. 3. Актуальність. 4. Практична значимість. 5. Відповідність вимогам оформлення. **Вимоги оформлення** Об'єм 15-25 сторінок. 14 шрифт. Times New Roman. Одинарний інтервал. Робота складається з: - титул – 1 с.; - зміст – 2 с.; - вступ: актуальність, об'єкт, предмет, мета та завдання дослідження. - основна частина: не менше 2 розділів. - висновки формуються відповідно до завдань. **Критерії оцінювання захисту РГР.** *Стартовий бал 15.* Захист РГР триває не більше 10 хвилин. Якщо при захисті доповідач вклався в час, але не розкрив тему, нараховуються мінус бали (залежно від повноти розкриття). За неправильну відповідь на запитання мінус 2 бали, а за неповну відповідь мінус 1 бал. За відсутність презентації мінус 2 бали.
Практичні заняття	**Критерії оцінювання практичних занять** 1. Підготовленість до практичних занять. 2. Самостійність виконання практичних робіт. 3. Повнота розкриття теми. 4. Своєчасність виконання практичних робіт
Умови допуску до	Позитивна оцінка за всіма обов'язковими видами робіт

підсумкового контролю	(практичні заняття та РГР)

7. Політики курсу -

Політика щодо академічної доброчесності: Списування під час контрольних робіт заборонені. Мобільні пристрої дозволяється використовувати лише під час онлайн-тестування та підготовки практичних завдань.

Жодні форми порушення академічної доброчесності не толеруються. У випадку таких подій – реагування відповідно до Положення про академічну доброчесність студентів та науково-педагогічних працівників Чернігівського національного технологічного університету та Методичних рекомендацій для закладів вищої освіти з підтримки принципів академічної доброчесності.

Правила перезарахування кредитів у випадку мобільності, правила перескладання або відпрацювання пропущених занять тощо: відбувається згідно з Положенням про організацію освітнього процесу в ЧНТУ.

Політика щодо дедлайнів та перескладання: роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (75% від можливої максимальної кількості балів за вид діяльності).

Перескладання модулів відбувається за наявності поважних причин (наприклад, лікарняний).

Політика щодо відвідування: Відвідування занять є обов'язковим компонентом оцінювання. За об'єктивних причин (наприклад, хвороба, працевлаштування, міжнародне стажування) навчання може відбуватись в онлайн-формі за погодженням.

8. Рекомендована література

Базова

1. Корченко О.Г. Аудит та управління інцидентами інформаційної безпеки // О.Г. Корченко, С.О. Гнатюк, С.В. Казмірчук, В.М. Панченко, С.В. Мельник. – К.: Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. – 193 с.
2. Аверченков В.И. Аудит информационной безопасности // Учебное пособие для вузов. — 2-е изд., стереотип. — М.: ФЛИНТА, 2011. — 269 с.
3. Бабак В.П. Інформаційна безпека та сучасні мережеві технології: Англо-українсько-російський словник термінів // В.П. Бабак, О.Г. Корченко. – К.: НАУ, 2003. – 670 с.
4. Бармен Скотт. Разработка правил информационной безопасности. М.: Вильямс, 2002. — 208 с.

Допоміжна

1. Юдін О.І. Захист інформації в мережах передачі даних // О.І. Юдін, О.Г. Корченко, Г.Ф. Конахович – К.: Вид-во ТОВ «НВП» Інтерсервіс», 2009. – 716 с.

2. Кулик Н.С. Энциклопедия безопасности авиации; Под. ред. Н.С. Кулика // Н.С. Кулик, В.П. Харченко, М.Г. Луцкий и др. – К.: Техніка, 2008. – 1000с.; ил. – Библиогр.: с. 977-999.

Інформаційні ресурси

Новітні теоретичні та практичні дані й матеріали що стосуються теорії та практики аудиту інформаційної безпеки рекомендується відслідковувати засобом звертання до наступних сайтів:

1. https://eln.stu.cn.ua/course/index.php?categoryid=185
2. http://www.dut.edu.ua/uploads/l_487_83762444.pdf
3. https://tzi.com.ua/audbezib.html
4. http://csecurity.kubg.edu.ua/index.php/journal/article/view/23
5. https://itlogica.com.ua/uk/services/informacionnaja-bezopasnost/
6. http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=281277&cat_id=38837