Черкаський державний технологічний університет

Факультет інформаційних технологій і систем

Кафедра інформаційної безпеки та комп’ютерної інженерії

СИЛАБУС

навчальної дисципліни

СТВОРЕННЯ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА ОСНОВІ ISO 27000

| Освітній рівень  | Другий (магістерський) |
| --- | --- |
| Статус дисципліни | Вибіркова |
| Спеціальність  | усіх спеціальностей  |
| Освітня програма | усіх освітніх програм |
| Обсяг дисципліни  | 4 кредити ECTS (120 годин) |
| Види аудиторних занять | Лекції, практичні заняття |
| Індивідуальні завдання  |  |
| Форма семестрового контролю | Залік |
| Мова викладання  | Українська |

| Предмет дисципліни | Система методів та практик аналізу, оцінки і управління загрозами для побудови систем управління інформаційною безпекою. |
| --- | --- |
| Мета викладання дисципліни | Полягає в отриманні здобувачами вищої освіти знань та вмінь з теорії та практики побудови систем управління інформаційною безпекою в організаціях, установах, підприємствах. Отримання ґрунтовних знань для впровадження програми аудиту системи управління інформаційної безпеки, аналізу досягнення цілей аудиту та можливості для її вдосконалення. |
| Результати навчання | 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 Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних побудови систем управління інформаційною безпекою (автоматизованих) системах.Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах дотримання режиму секретності з фіксуванням результатів у відповідних документах. |
| Тематичний план дисципліни | Тема 1. Завдання організаційного забезпечення захисту інформації. Аналіз і оцінка загроз інформаційної безпеки об'єкта.Тема 2. Структура стандарту ISO 27001.Тема 3. Аналіз зовнішні та внутрішні проблеми, які впливають на інформаційну безпеку організації.Тема 4. Методологія оцінки ризиків.Тема 5. Складання плану лікування ризику.Тема 6. Моніторинг, вимірювання, аналіз та оцінка стану інформаційної безпеки та ефективності ISMS.Тема 7. Вступ до Додатку A стандарту ISO 27001.Тема 8. Внутрішній та зовнішній аудит.Тема 9. Організація внутрішнього аудиту. Елементи внутрішнього аудиту. Припущення аудитора. |
| Політика дисципліни | *Політика щодо відвідування.* Відвідування лекційних занять, лабораторних робіт та контрольних заходів є обов’язковими. Якщо здобувач вищої освіти пропустив заняття або отримав незадовільну оцінку, то він має відпрацювати пропущене або нескладене шляхом вивчення матеріалів з відповідної теми, виконання практичних завдань, які розглядалися під час заняття, виконання тематичного тесту для самоконтролю та написання конспекту з подальшим захистом під час індивідуальної консультації. Організація навчання здобувачів вищої освіти, які навчаються за індивідуальним графіком, здійснюється згідно «Положення про навчання за індивідуальним графіком у Черкаському державному технологічному університеті» (http://tiny.cc/88iiuz). Здобувач вищої освіти має підтримувати зворотній зв’язок із викладачем на всіх етапах вивчення дисципліни.*Політика щодо дедлайнів та перескладання.* Здобувачі вищої освіти звітують про виконання лабораторних завдань під час лабораторного заняття із відповідної теми. Роботи здобувачів вищої освіти (лабораторні, самостійні, індивідуальні тощо), які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (75% від можливої максимальної кількості балів за певний вид діяльності). Модульні контрольні роботи проводяться у формі тестів в письмовій формі або із застосуванням можливостей системи підтримки дистанційного навчання ЧДТУ у терміни, передбачені робочою програмою дисципліни. Здобувачу вищої освіти надається 2 спроби для проходження тесту. У разі одержання незадовільної оцінки за поточну модульну контрольну роботу (менш 60 % правильних відповідей), перескладання відбувається у формі усної співбесіди з теоретичних питань модулю.*Політика щодо академічної доброчесності.* Здобувачі вищої освіти мають свідомо дотримуватися «Кодексу академічної доброчесності Черкаського державного технологічного університету» (http://tiny.cc/b8iiuz), використовувати у навчальній та дослідницькій діяльності лише перевірені чи достовірні джерела інформації, грамотно посилатися на них. Під час проведення контрольних заходів не допускається залучення здобувачами вищої освіти зовнішніх джерел інформації, крім дозволених для використання.*Політика зарахування результатів неформальної освіти.* Визнання результатів навчання, отриманих в умовах неформальної/інформальної освіти здійснюється згідно «Положення про порядок визнання у Черкаському державному технологічному університеті результатів навчання, отриманих в умовах неформальної / інформальної освіти» (http://tiny.cc/d8iiuz). |

| Прізвище, ім’я, по батькові | Миронюк Тетяна Василівна |
| --- | --- |
| Науковий ступінь | к.т.н. |
| Наукове звання | доцент |
| Посада | доцент |
| Місце роботи | Черкаський державний технологічний університет, кафедра інформаційної безпеки на комп’ютерної інженерії |
| Адреса кафедри | м.Черкаси, бул. Шевченка, 460, к.604 |
| Контактний телефон | (097) 8818279 |
| Профайл викладача | *https://ibki.chdtu.edu.ua/staff/myronyuk-tetyana-vasylivna/* |
| e-mail: | *t.myroniuk @chdtu.edu.ua* |
| Профайл дисципліни |  |
| Розклад консультацій  | *https://ibki.chdtu.edu.ua/debts/* |