(Ф 21.01 - 03)

	Силабус навчальної дисципліни «Методи технічного захисту інформації на об'єктах критичної інфраструктури» **Спеціальність: 263 Цивільна безпека** **ОПП Захист об'єктів критичної інфраструктури**	

Рівень вищої освіти	Перший (бакалаврський)
Статус дисципліни	Навчальна дисципліна вибіркового компонента фахового переліку
Курс	3 (третій)
Семестр	4 (четвертий)
Обсяг дисципліни, кредити ЄКТС/загальна кількість годин	3 кредити / 90 годин
Мова викладання	українська
Що буде вивчатися (предмет навчання)	Види, джерела та носії інформації, що підлягають захисту. Законодавче забезпечення інформаційної/кібернетичної безпеки. Система управління інформаційною/кібернетичною безпекою на базі міжнародних вимог та стандартів. Загальна класифікація та характеристика каналів несанкціонованого отримання інформації. Класифікація, загальна характеристика та принципи функціонування засобів несанкціонованого отримання інформації. Методи та засоби виявлення закладних пристроїв. Загальна характеристика та порядок використання технічних засобів захисту інформації на об'єктах інформаційної діяльності.
Чому це цікаво/потрібно вивчати (мета)	Виведення з ладу інформаційних систем та розголошення приватної інформації завдає значної шкоди власнику, іміджу підприємства, організації та державі. Тому, опанування методів та засобів технічного захисту інформації на об'єктах критичної інфраструктури, своєчасне виявлення кібератак, знешкодження наслідків таких атак та унеможливлення несанкціонованого витоку інформації є надзвичайно важливим для сучасного фахівця. Курс спрямований на формування теоретичних знань та практичних навичок щодо гарантованого захисту інформації на об'єктах критичної інфраструктури.
Чому можна навчитися (результати навчання)	- проводити обстеження об'єктів критичної інфраструктури та ІТС; - розробляти модель загроз та порушника; - впроваджувати засоби захисту інформації; - виявляти втручання в роботу ІТС (кібератак, комп'ютерних шахрайств, каналів витоку інформації, несанкціонованого доступу до інформації); - блокувати канали витоку інформації; - забезпечувати захист інформації на об'єктах критичної інфраструктури та ІТС та здійснювати оцінку захищеності інформації.

Як можна користуватися набутими знаннями і уміннями (компетентності)	Отримані знання дозволять: - забезпечувати гарантований захист інформації на об'єктах критичної інфраструктури та в ІТС; - виявляти та блокувати канали витоку інформації; - використовувати апаратні, програмні та апаратно-програмні засоби захисту інформації; - проводити оцінку захищеності інформації в ІТС та на об'єктах критичної інфраструктури.
Навчальна логістика	**Зміст дисципліни:** Визначення інформації, що потребує захисту на об'єктах критичної інфраструктури (ОКІ). Опанування методів та засобів технічного захисту інформації на ОКІ. Ознайомлення з каналами витоку інформації та підстав їх утворення. Оволодіння навичками роботи із засобами та комплексами виявлення закладних пристроїв несанкціонованого отримання інформації. Оволодіння навичками роботи із засобами та комплексами захисту інформації на ОКІ. Засвоєння порядку проведення обстеження і аналізу ОКІ з метою забезпечення захисту інформації. Оволодіння організаційно-технічними заходами щодо захисту інформації на ОКІ. **Види занять:** лекції, лабораторні заняття **Методи навчання:** навчальні дискусії, практичне навчання **Форми навчання:** очна
пререквізити	Базові знання інформаційних технологій та захисту інформації
Пореквізити	Знання із застосування методів технічного захисту ОКІ та виявлення каналів витоку інформації (кібератак, комп'ютерних шахрайств, несанкціонованого доступу до інформації) можуть бути використані для управління інформаційною/кібербезпекою, автоматизованої обробки інформації з обмеженим доступом, оцінки захищеності інформації в ІТС та проведення аудиту кібербезпеки.
Інформаційне забезпечення з фонду та репозитарію НТБ НАУ	**Науково-технічна бібліотека НАУ:** 1. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. 2. НД ТЗІ 3.7-003-2005. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. 3. НД ТЗІ 1.1-005-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення. 4. НД ТЗІ 3.3-001-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації. 5. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. 6. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. 7. НД ТЗІ 2.6-001-11. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. **Репозитарій НАУ:** http://er.nau.edu.ua/handle/NAU/9190

Локація та матеріально-технічне забезпечення	Лабораторія спеціалізованих засобів захисту інформації, мультимедійне обладнання, технічні засоби виявлення закладних пристроїв
Семестровий контроль, екзаменаційна методика	Залік, тестування
Кафедра	Засобів захисту інформації
Факультет	Кібербезпеки, комп'ютерної та програмної інженерії
Викладач(і)	 **ЛАЗАРЕНКО СЕРГІЙ ВОЛОДИМИРОВИЧ, викладачі кафедри** **Посада:** професор кафедри ЗЗІ ФККПІ **Вчене звання:** доцент **Науковий ступінь:** доктор технічних наук **Профайл викладача:** http://www.kzzi.nau.edu.ua **Тел.:** 406-70-56 **E-mail:** serhii.lazarenko@npp.nau.edu.ua **Робоче місце:** 11.410
Оригінальність навчальної дисципліни	Авторський курс, викладання українською мовою
Лінк на дисципліну	Код класу у Google Classroom d2purtu

Завідувач кафедри В. Козловський

Розробник С. Лазаренко