Силабус навчальної дисципліни «ВИЯВЛЕННЯ ЗАКЛАДНИХ ПРИСТРОЇВ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ»

Освітньо-професійної програми: «Системи технічного захисту інформації, автоматизація її обробки»
Галузь знань: 12 «Інформаційні технології»
Спеціальність: 125 «Кібербезпека»

Рівень вищої освіти	Перший (бакалаврський)
Статус дисципліни	Навчальна дисципліна професійної підготовки обов'язкової компоненти ОП
Курс	2 (другий)
Семестр	3 (третій)
Обсяг дисципліни, кредити ЄКТС/години	4 кредити / 120 годин
Мова викладання	українська
Що буде вивчатися (предмет навчання)	Методи та засоби (технічні, програмні) виявлення закладних пристроїв та запобігання несанкціонованому отриманню інформації. Загальні методи отримання інформації (легальні, напівлегальні та нелегальні), характеристика каналів витоку інформації, класифікація засобів перехоплення (з'йому) інформації.
Чому це цікаво/треба вивчати (мета)	Несанкціонований доступ та розголошення приватної інформації завдає значної шкоди власнику, іміджу підприємства, організації. Вивчення методів та засобів виявлення закладних пристроїв, здатність блокування каналів витоку інформації є надзвичайно важливим для сучасного фахівця. Курс спрямований на формування теоретичних знань щодо утворення каналів витоку інформації (природних, штучних) та можливих способів несанкціонованого отримання інформації. Отримання практичних навичок з використання технічних та програмних засобів виявлення закладних пристроїв та блокування каналів витоку інформації.

Чому можна навчитися (результати навчання)	За результатами вивчення навчальної дисципліни здобувачі повинні: *Знати* - призначення, класифікацію та принципи побудови пошукових систем та комплексів; - поняття, класифікацію та підстави утворення каналів витоку інформації; - порядок використання пошукових систем, комплексів та засобів (засобів виявлення закладних пристроїв, відеокамер тощо); - порядок проведення обстеження ОІД, з метою виявлення закладних пристроїв. *Вміти* - самостійно проводити обстеження ОІД, з метою виявлення закладних пристроїв; - самостійно застосовувати пошукові засоби та комплекси; - вести технічну документацію, оформляти результати обстеження ОІД), (виявлення та блокування каналів витоку інформації, виявлення закладних пристроїв).
Як можна користуватися набутими знаннями і уміннями (компетентності)	Отримані знання дозволять: - застосовувати знання у практичних ситуаціях; - виявляти та блокувати канали несанкціонованого витоку інформації; - використовувати технічні засоби (апаратні, програмні, апаратно-програмні) виявлення закладних пристроїв; - аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки; - забезпечувати гарантований захист інформації.
Навчальна логістика	**Зміст дисципліни:** Методи та способи отримання інформації (легальні, напівлегальні, нелегальні). Характеристика каналів витоку інформації (природні, штучні). Методи та способи блокування каналів несанкціонованого витоку інформації. Застосування технічних та програмних засобів виявлення закладних пристроїв. Практичні навички використання детекторів поля, скануючих радіоприймачів (панорамних, аналізуючи), програмно-апаратних комплексів виявлення і вимірювання радіовипромінювань та пошуку закладних пристроїв, оптичних приладів виявлення відеокамер, приладів радіолокації нелінійностей. **Види занять:** аудиторні (лекції, лабораторні заняття), самостійна робота студента. **Методи навчання:** робота в малих групах, семінар-дискусія, мозкова атака, кейс, презентація, рольова гра, дидактична гра, практичне навчання. **Форми навчання:** очна, заочна
Пререквізити	Базові знання із забезпечення кібербезпеки та захисту інформації на ОІД
Пореквізити	Знання будуть використані для опанування дисциплін: «Системи технічного захисту інформації», «Комлексні системи захисту інформації», «Методи та засоби технічного захисту інформації».
Інформаційне забезпечення з репозитарію та фонду НТБ НАУ	**Науково-технічна бібліотека НАУ:** 1. Максименко Г.А. Методи виявлення, обробки та ідентифікації сигналів радіозакладних приладів/ Максименко Г.А., Хорошко В.О.// – К.: ООО «Поліграф Консалтинг», 2004. – 317 с. 2. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. – К.: ТОВ «ТИД ДС», 2002. – 688 с. 3. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации/ Хорошко В.А., Чекатков А.А.//– К.: ЮНИОР, 2003. **Репозитарій НАУ:** http://er.nau.edu.ua **Науково-технічна бібліотека НАУ:** http://www.lib.nau.edu.ua.

Локація та матеріально-технічне забезпечення	Лабораторія спеціалізованих засобів захисту інформації, мультимедійне обладнання, автоматизовані робочі місця, персональні комп'ютери, засоби виявлення закладних пристроїв, засоби технічного захисту інформації.
Семестровий контроль, екзаменаційна методика	Тестування, екзамен
Кафедра	Засобів захисту інформації
Факультет	Кібербезпеки, комп'ютерної та програмної інженерії
Викладач(і)	 **ЛАЗАРЕНКО СЕРГІЙ ВОЛОДИМИРОВИЧ** **Посада:** професор кафедри **Вчене звання:** доцент **Науковий ступінь:** доктор технічних наук **Профайл викладача:** http://www.kzzi.nau.edu.ua/lazarenko-sergy-volodimirovitch/ **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 Class room 4dqo44v