



**Силабус навчальної дисципліни  
«Виявлення закладних пристроїв»**

**Спеціальність: 125 Кібербезпека  
Галузь знань: 12 Інформаційні технології**



<b>Рівень вищої освіти</b>	Перший (бакалаврський)
<b>Статус дисципліни</b>	Навчальна дисципліна вибіркового компонента фахового переліку
<b>Семестр</b>	Осінній семестр
<b>Обсяг дисципліни, кредити ЄКТС/загальна кількість годин</b>	3 кредити / 90 годин
<b>Мова викладання</b>	українська
<b>Що буде вивчатися (предмет навчання)</b>	Загальні методи отримання інформації (легальні, напівлегальні та нелегальні), характеристика каналів витоку інформації, класифікація засобів перехоплення (з'йому) інформації. Методи та засоби (технічні, програмні) виявлення закладних пристроїв і запобігання несанкціонованого отримання інформації.
<b>Чому це цікаво/потрібно вивчати (мета)</b>	Несанкціонований доступ та розголошення приватної інформації завдає значної шкоди власнику, іміджу підприємства, організації. Тому, 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.
<b>Чому можна навчитися (результати навчання)</b>	<ul style="list-style-type: none"> <li>- розуміння підстав утворення каналів витоку інформації;</li> <li>- оволодіння знаннями про методи пошуку та виявлення каналів несанкціонованого витоку інформації;</li> <li>- навчитись використовувати технічні засоби виявлення закладних пристроїв несанкціонованого отримання інформації;</li> <li>- навчитись використовувати програмні засоби виявлення каналів витоку інформації.</li> </ul>
<b>Як можна користуватися набутими знаннями і уміннями (компетентності)</b>	Отримані знання дозволять: <ul style="list-style-type: none"> <li>- виявляти та блокувати канали несанкціонованого витоку інформації;</li> <li>- використовувати технічні засоби виявлення закладних пристроїв;</li> <li>- використовувати програмні засоби виявлення каналів витоку інформації;</li> <li>- забезпечувати гарантований захист інформації.</li> </ul>

<b>Навчальна логістика</b>	<p><b>Зміст дисципліни:</b> 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 та приладів радіолокації нелінійностей.</p> <p><b>Види занять:</b> лекції, лабораторні заняття</p> <p><b>Методи навчання:</b> навчальні дискусії, практичне навчання</p> <p><b>Форми навчання:</b> очна</p>
<b>Преквізити</b>	Базові знання інформаційних технологій
<b>Пореквізити</b>	Знання з виявлення закладних пристроїв можуть бути використані для створення комплексів технічного захисту інформації та комплексних систем захисту інформації
<b>Інформаційне забезпечення з фонду та репозитарію НТБ НАУ</b>	<p><b>Науково-технічна бібліотека НАУ:</b></p> <ol style="list-style-type: none"> <li>Максименко Г.А. Методи виявлення, обробки та ідентифікації сигналів радіозакладних приладів/ Максименко Г.А., Хорошко В.О.// – К.: ООО «Поліграф Консалтинг», 2004. – 317 с.</li> <li>Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. – К.: ТОВ «ТИД ДС», 2002. – 688 с.</li> <li>Хорошко В.А., Чекатков А.А. Методы и средства защиты информации/ Хорошко В.А., Чекатков А.А.//– К.: ЮНИОР, 2003.</li> </ol> <p><b>Репозитарій НАУ:</b>  <a href="http://er.nau.edu.ua/handle/NAU/9190">http://er.nau.edu.ua/handle/NAU/9190</a></p>
<b>Локація та матеріально-технічне забезпечення</b>	Лабораторія спеціалізованих засобів захисту інформації, мультимедійне обладнання, технічні засоби виявлення закладних пристроїв
<b>Семестровий контроль, екзаменаційна методика</b>	Залік, тестування
<b>Кафедра</b>	Засобів захисту інформації
<b>Факультет</b>	Кібербезпеки, комп'ютерної та програмної інженерії
<b>Викладач(і)</b>	<div style="display: flex; align-items: center;">  <div> <p><b>ЛАЗАРЕНКО СЕРГІЙ ВОЛОДИМИРОВИЧ</b></p> <p><b>Посада:</b> завідувач кафедри</p> <p><b>Вчене звання:</b> доцент</p> <p><b>Науковий ступінь:</b> доктор технічних наук</p> <p><b>Профайл викладача:</b> <a href="http://www.kzzi.nau.edu.ua">http://www.kzzi.nau.edu.ua</a></p> <p><b>Тел.:</b> 406-70-56</p> <p><b>E-mail:</b> serhii.lazarenko@npp.nau.edu.ua</p> <p><b>Робоче місце:</b> 11.410</p> </div> </div>
<b>Оригінальність навчальної дисципліни</b>	Авторський курс, викладання українською мовою
<b>Лінк на дисципліну</b>	Код класу у Google Classroom 4dqo44v