



**Силабус навчальної дисципліни
«Захищеність кіберпростору»**

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



Рівень вищої освіти	Другий (магістерський)
Статус дисципліни	Навчальна дисципліна вибіркового компонента фахового переліку
Курс	1 (перший)
Семестр	2 (другий)
Обсяг дисципліни, кредити ЄКТС/загальна кількість годин	4 кредити / 120 годин
Мова викладання	українська
Що буде вивчатися (предмет навчання)	Поняття захищеності кіберпростору. Методи та засоби дослідження кіберпростору. Забезпечення кібербезпеки, кіберзахисту та розслідування кіберзлочинів. Огляд побудови систем кіберзахисту в Україні та світі. Виявлення кіберзлочинів та локалізація наслідків кібератак. Методи та засоби захисту кіберпростору.
Чому це цікаво/потрібно вивчати (мета)	Захищеність кіберпростору надає можливість сталому розвитку держави, підприємства, установи та особистості. Захист інформаційних ресурсів набуває актуальності в умовах нових загроз. Розголошення будь-якої особистої (приватної) інформації завдає значної шкоди власнику, іміджу підприємства, організації та державі. Тому, опанування методів та засобів захисту кіберпростору є надзвичайно важливим для сучасного фахівця. Курс спрямований на формування теоретичних знань та практичних навичок щодо гарантованого захисту інформації.
Чому можна навчитися (результати навчання)	<ul style="list-style-type: none"> - проводити обстеження об'єктів інформаційної діяльності та ІТС; - розробляти модель загроз та порушника; - виявляти втручання в роботу ІТС (кібератак, комп'ютерних шахрайств, каналів витоку інформації, несанкціонованого доступу до інформації); - виявлення та знешкодження каналів витоку інформації (навмисні, ненавмисні); - впроваджувати засоби захисту інформації.
Як можна користуватися набутими знаннями і уміннями (компетентності)	Отримані знання дозволять: <ul style="list-style-type: none"> - забезпечувати захист кіберпростору; - виявляти кібератаки; - використовувати апаратні, програмні та апаратно-програмні засоби захисту інформації; - проводити оцінку захищеності інформації та аудит кібербезпеки.

Навчальна логістика	<p>Зміст дисципліни: Дослідження кіберпростору. Забезпечення захисту кіберпростору. Заходи з кібербезпеки, кіберзахисту та кіберзлочинів. Правове підґрунтя забезпечення безпеки кіберпростору. Взаємодія державних органів із забезпечення кібербезпеки, кіберзахисту та проведення розслідувань кіберзлочинів. Методи та форми здійснення кіберзлочинів (кібератак, комп'ютерних шахрайств, каналів витоку інформації, несанкціонованого доступу до інформації).</p> <p>Практичні навички з виявлення кібератак та каналів витоку інформації. Застосування технічних та програмних засобів захисту інформації. Знешкодження виявлених каналів витоку інформації. Організація та проведення розслідувань кіберзлочинів.</p> <p>Види занять: лекції, лабораторні заняття</p> <p>Методи навчання: навчальні дискусії, практичне навчання</p> <p>Форми навчання: очна</p>
переквізити	Базові знання інформаційних технологій та захисту інформації
Пореквізити	Знання з дослідження кіберпростору та забезпечення безпеки (виявлення кіберзлочинів - кібератак, комп'ютерних шахрайств, несанкціонованого доступу до інформації) можуть бути використані для створення комплексних систем захисту інформації на ОІД та ІТС, оцінки захищеності інформації в ІТС та проведення аудиту кібербезпеки.
Інформаційне забезпечення з фонду та репозитарію НТБ НАУ	<p>Науково-технічна бібліотека НАУ:</p> <ol style="list-style-type: none"> 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. <p>Репозитарій НАУ: http://er.nau.edu.ua/handle/NAU/9190</p>
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)	 <p>КОЗЛОВСЬКИЙ ВАЛЕРІЙ ВАЛЕРІЙОВИЧ Посада: завідувач кафедри Вчене звання: професор Науковий ступінь: доктор технічних наук Профайл викладача: http://www.kzzi.nau.edu.ua/kozlovskiy-valery-valeryovitch/ Тел.: 406-70-56 E-mail: valerii.kozlovskiy@npp.nau.edu.ua Робоче місце: 11.410</p>
Оригінальність навчальної дисципліни	Авторський курс, викладання українською мовою
Лінк на дисципліну	Код класу у Google Classroom b2hq6d7