(Ф 21.01 - 03)

Силабус навчальної дисципліни
«Комплексні системи захисту інформації»

Спеціальність: 125 Кібербезпека
Галузь знань: 12 Інформаційні технології

Рівень вищої освіти	Перший (бакалаврський)
Статус дисципліни	Навчальна дисципліна вибіркового компонента фахового переліку
Семестр	Весняний семестр
Обсяг дисципліни, кредити ЄКТС/загальна кількість годин	3 кредити / 90 годин
Мова викладання	українська
Що буде вивчатися (предмет навчання)	Поняття комплексних систем захисту інформації, інформаційних ресурсів з обмеженим доступом та необхідність захисту інформації від несанкціонованого доступу та розповсюдження. Етапи створення комплексних систем захисту інформації (передпроектні роботи, впровадження засобів захисту інформації, атестація та оцінка захищеності інформації). Розробки політики безпеки інформації в ІТС. Виявлення кіберзлочинів (кібератак, комп'ютерних шахрайств, каналів витоку інформації, несанкціонованого доступу до інформації). Заходи з локалізації наслідків несанкціонованого доступу до інформації. Методи та засоби блокування каналів витоку інформації та унеможливлення несанкціонованого доступу до інформації.
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 комплексного захисту інформації, своєчасного 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.
Чому можна навчитися (результати навчання)	- проводити обстеження об'єктів інформаційної діяльності 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; - здійснювати оцінку захищеності інформації на ОІД та в ІТС.

Як можна користуватися набутими знаннями і уміннями (компетентності)	Отримані знання дозволять: - забезпечувати гарантований захист інформації на ОІД 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 ОІД; - проводити аудит кібербезпеки.
Навчальна логістика	**Зміст дисципліни:** Засвоєння порядку створення КСЗІ в ІТС. Опанування порядку обстеження середовища, де циркулює інформація, розробка моделей загроз та порушника, розробка технічного завдання на створення комплексних систем захисту інформації. Впровадження засобів захисту інформації. Організація та проведення державної експертизи та оцінки захищеності інформації на ОІД та в ІТС. Засвоєння методів та форм здійснення кіберзлочинів (кібератак, комп'ютерних шахрайств, каналів витоку інформації, несанкціонованого доступу до інформації). Виявлення кібератак та каналів витоку інформації. Практичні навички з обстеження ІТС та ОІД. Впровадження апаратних, програмних та апаратно-прогамних засобів захисту інформації. Блокування каналів витоку інформації. Організація та проведення розслідувань кіберзлочинів. **Види занять:** лекції, лабораторні заняття **Методи навчання:** навчальні дискусії, практичне навчання **Форми навчання:** очна
реквізити	Базові знання інформаційних технологій та захисту інформації
Пореквізити	Знання з побудови комплексних систем захисту інформації 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:** завідувач кафедри **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 apivder

Розробник С. Лазаренко