

	<p>Силабус навчальної дисципліни «Автоматизація обробки інформації з обмеженим доступом»</p> <p>Спеціальність: 125 Кібербезпека Галузь знань: 12 Інформаційні технології</p>	
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)	<p>Поняття інформації з обмеженим доступом. Методи та засоби освоєння підходів до створення вбудованих засобів захисту сучасних операційних систем і програмних застосунків. Виявлення причин їх вразливості на основі наявної статистики загроз з метою обґрунтування загальних вимог до механізмів захисту. Оволодіння навичками побудови та проектування систем захисту інформації з обмеженим доступом та архітектурними принципами побудови систем захисту інформації.</p>	
Чому це цікаво/потрібно вивчати (мета)	<p>Захищеність автоматизованих систем обробки інформації надає можливість розвитку всіх сфер як державного і приватного сектору. Підходів до створення вбудованих засобів захисту сучасних операційних систем і програмних застосунків, виявлення причин їх вразливості на основі наявної статистики загроз з метою обґрунтування загальних вимог до механізмів захисту.</p> <p>Тому, оволодіння навичками побудови та проектування систем захисту інформації з обмеженим доступом та архітектурними принципами побудови систем захисту інформації є надзвичайно важливим для сучасного фахівця.</p> <p>Курс спрямований на формування теоретичних знань та практичних навичок щодо основних засоби забезпечення системи захисту.</p>	

<p>Чому можна навчитися (результати навчання)</p>	<ul style="list-style-type: none"> - вирішувати питання щодо здійснення процесу оцінки надійності систем захисту інформації з урахуванням проблем інформаційної безпеки; - формулювати цілі, забезпечувати та контролювати впровадження розроблених заходів управління; - зробити класифікація об'єктів загроз для досягнення цілей організації (підприємства); -провести аналіз ефективності централізовано-розподіленої системи захисту.
<p>Як можна користуватися набутими знаннями і уміннями (компетентності)</p>	<p>Отримані знання дозволяють:</p> <ul style="list-style-type: none"> - аналізувати статистику загроз для операційних систем сімейств Windows і Unix - здійснювати оцінку надійності систем захисту інформації (поняття відмови, часу відновлення тощо). - проектувати системи захисту інформації з обмеженим доступом, а також у складі локальних обчислювальних мереж. - застосовувати засоби апаратного захисту. -контролювати коректність функціонування механізмів захисту з використанням методів контролю цілісності.

<p>Навчальна логістика</p>	<p>Зміст дисципліни: Вимоги до захисту комп'ютерної інформації. Аналіз стану захищеності операційних систем. Підходи до проектування системи захисту. Принципи побудови архітектури системи захисту інформації. Авторизація. методи ідентифікації. Управління доступом до ресурсів. 3 Моделі управління доступом. Реалізація моделей доступу механізмами додаткового та вбудованого захисту. Контроль коректності функціонування механізмів захисту. Методи контролю цілісності. Механізми контролю цілісності файлових об'єктів. Застосування засобів апаратного захисту. Додатковий захист від несанкціонованого доступу.</p> <p>Практичні навички з аналізу стану захищеності операційних систем. Застосування технічних та програмних засобів захисту інформації. Знешкодження виявлених каналів витоку інформації.</p> <p>Види занять: лекції, лабораторні заняття</p> <p>Методи навчання: навчальні дискусії, практичне навчання</p> <p>Форми навчання: очна</p>
<p>ререквізити</p>	<p>Базові знання інформаційних технологій та захисту інформації</p>
<p>Пореквізити</p>	<p>Знання з принципи побудови системи автоматизованої обробки інформації з обмеженим доступом і її архітектури; функціональну модель системи захисту можуть бути використані для створення комплексних систем захисту інформації на ОІД та ІТС, оцінки захищеності інформації в ІТС та проведення аудиту кібербезпеки.</p>

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. ДСТУ 3396.0-96. «Захист інформації. Технічний захист інформації. Основні положення». 6. ДСТУ 3396.1-96. «Захист інформації. Технічний захист інформації. Порядок проведення робіт». 7. НД ТЗІ 3.7-003-05. «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі». 8. НД ТЗІ 1.1-005-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення. 9. НД ТЗІ НД ТЗІ 2.5-008-2002 .Вимоги із захисту службової інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2. 10. Хорошко В. О. Основи інформаційної безпеки : навчальний посібник/ Дудикевич В. Б., Хорошко В. О., Яремчук Ю. Є./ – Вінниця : ВНТУ, 2018. – 316 с. 11. Браїловський М.М. Технології захисту інформації: підручник / Браїловський М.М., Зибін С.В., Пискун І.В., Хорошко В.О., Хохлачова Ю.Є./ – К.: ЦК “Компринт”, 2021. – 296 с. 12. Богуш В.М. Технічний захист інформації: навчальний посібник/ Богуш В.М., Бровко В.Д., Коус О.В., Козюра В.Д./ – Дніпро.: “Ліра-К”, 2022. – 508с.
Локація та матеріально технічне забезпечення	Лабораторія спеціалізованих засобів захисту інформації, мультимедійне обладнання.
Семестровий контроль, екзаменаційна методика	Залік, тестування
Кафедра	Засобів захисту інформації
Факультет	Кібербезпеки, комп'ютерної та програмної інженерії

Викладач(і)	Щербак Тетяна Леонідівна Посада: доцент Вчене звання: доцент Науковий ступінь: кандидат технічних наук Профайл викладача: http://www.kzzi.nau.edu.ua/http://www.kzzi.nau.edu.ua/shterbak-tetyana-leondvna/ Тел.: 406-70-56 E-mail: tetiana.shcherbak@npp.nau.edu.ua Робоче місце: 11.410
Оригінальність навчальної дисципліни	Авторський курс, викладання українською мовою
Лінк на дисципліну	Код класу у Google Classroom