СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Загальна інформація про навчальну дисципліну

Повна назва навчальної дисципліни	Сучасні інформаційно-комунікаційні технології в кібербезпеці
Повна офіційна назва закладу вищої освіти	Сумський державний університет
Повна назва структурного підрозділу	Факультет електроніки та інформаційних технологій. Кафедра кібербезпеки
Розробник(и)	Ободяк Віктор Корнелійович, Барченко Наталія Леонідівна
Рівень вищої освіти	Другий рівень вищої освіти, НРК – 7 рівень, QF-LLL – 7 рівень, FQ-EHEA – другий цикл
Семестр вивчення навчальної дисципліни	16 тижнів протягом 2-го семестру
Обсяг навчальної дисципліни	Обсяг становить 5 кред. ЄКТС, 150 год. Для денної форми навчання 32 год. становить контактна робота з викладачем (16 год. лекцій, 16 год. лабораторних занять), 118 год. становить самостійна робота. Для дистанційної форми навчання 150 год. становить самостійна робота.
Мова викладання	Українська

2. Місце навчальної дисципліни в освітній програмі

Статус дисципліни	Вибіркова навчальна дисципліна для освітньої програми "Інформатика"
Передумови для вивчення дисципліни	Сховища даних, Реінжиніринг та верифікація програмного забезпечення
Додаткові умови	Додаткові умови відсутні
Обмеження	Обмеження відсутні

3. Мета навчальної дисципліни

Метою навчальної дисципліни є досягнення студентами сучасного мислення та системи спеціальних знань у галузі кібербезпеки та здатності їх використовувати в інформаційно-комунікаційних системах

4. Зміст навчальної дисципліни

Тема 1 Загальні положення щодо захисту інформації Основи національної безпеки держави. Основні положення інформаційної безпеки. Базові поняття забезпечення захисту інформації в інформаційно-комунікаційних системах

Тема 2 Системи захисту інформації Будова систем захисту інформації. Теоретичні основи захисту інформації. Типові вразливості систем і аналіз причин їх появи. Шкідливе програмне забезпечення.
Тема 3 Захист інформації в інформаційно-комунікаційних системах Основи безпеки інформації в комп'ютерних мережах. Засоби захисту в розподілених інформаційно-комунікаційних системах.

5. Очікувані результати навчання навчальної дисципліни

Після успішного вивчення навчальної дисципліни здобувач вищої освіти зможе:

РН1	Аналізувати конкретні інформаційні системи на предмет інформаційної безпеки та оцінювання її ризиків та розробляти концепцію інформаційної безпеки підприємства
РН2	Розробляти вимоги та обирати для впровадження заходи захисту інформації
РН3	Володіти засобами виявлення небезпек
РН4	Впроваджувати засоби захисту інформації

7. Роль освітнього компонента у формуванні соціальних навичок

Загальні компетентності та соціальні навички, формування яких забезпечує навчальна дисципліна:

СН1	Здатність використовувати інформаційні та комунікаційні технології.
СН2	Здатність застосовувати знання у практичних ситуаціях.
СН3	Здатність оцінювати та забезпечувати якість виконуваних робіт.
СН4	Здатність приймати обґрунтовані рішення.
СН5	Здатність оцінювати та забезпечувати якість виконуваних робіт.

8. Види навчальних занять

Тема 1. Загальні положення щодо захисту інформації
Лк1 "Основи національної безпеки держави і основні положення інформаційної безпеки" Основні поняття національної безпеки. Характеристика основних видів національної безпеки. Система забезпечення національної безпеки в Україні. Поняття інформаційної безпеки. Загрози інформаційній безпеці. Методи і засоби забезпечення інформаційної безпеки
Лк2 "Базові поняття забезпечення захисту інформації в інформаційно-комунікаційних системах. Загрози безпеці інформаці" Структура і склад автоматизованої системи. Основні терміни. Комплекс засобів захисту. Класифікація загроз. Модель загроз. Модель порушника

Лб1 "Аналіз ризиків інформаційної безпеки та побудова концепції інформаційної безпеки підприємства"

Системна характеристика. Ідентифікація загроз. Ідентифікація вразливостей. Аналіз управління. Визначення правдоподібності. Аналіз впливу (втрата цілісності, втрата системи, втрата конфіденційності). Визначення ризиків. Рекомендації управління. Документовані результати

Тема 2. Системи захисту інформації

Лк3 "Будова систем захисту інформації"

Рівні інформаційно-комунікаційної системи. Функціональні сервіси безпеки і механізми, що їх реалізують. Основні підсистеми комплексу засобів захисту

Лк4 "Теоретичні основи захисту інформації і шкідливе програмне забезпечення"

Загальні поняття теорії захисту інформації. Позначення, аксіоми та визначення. Основні типи політик безпеки. Математичні моделі безпеки. . Класифікація шкідливого програмного забезпечення. Програмні закладки. Комп'ютерні віруси. Мережні хробаки. “Троянські коні”. Спеціальні хакерські утиліти. Запобіжні заходи проти створення, розповсюдження і проникнення в інформаційно-комунікаційні системи вірусів та інших засобів атак

Лк5 "Захищені операційні системи"

Загрози безпеці операційних систем. Підходи до створення захищених операційних систем. Адміністративні заходи захисту. Адекватна політика безпеки. Типова архітектура комплексу засобів захисту операційних систем (КЗЗ ОС)

Лк6 "Засоби захисту в операційній системі Windows"

Відповідність вимогам стандартам безпеки. Архітектура операційної системи Windows. Розмежування доступу.

Лб2 "Налагодження та оптимізація роботи комп’ютерного робочого місця (КРМ) підприємства"

Передпроектне дослідження. Вивчення структури поточного стану підприємства. Формування вимог до системи. Визначення наявності або відсутності інформаційних систем і їх властивостей. Визначення політики безпеки підприємства. Визначення загроз і портрета можливих атак. Узгодження технічних рішень. Складання рішень щодо заходів інформаційної безпеки підприємства. Проведення робіт з впровадження, імплементації проекту забезпечення інформаційної безпеки в інфраструктурі підприємства. Складання та реалізація послідовності дій щодо впровадження системи інформаційної безпеки. Проведення при необхідності ознайомлення співробітників підприємства з елементами безпеки, а так само з нормативними, методичними нормами. З адміністративної (або інший, якщо підприємство має особливий статус) відповідальністю. Проведення апробації та пуску систем (-и) інформаційної безпеки. Розробка та апробація алгоритму комплексу заходів при частковому або повному виході з ладу елементів інфраструктури підприємства

Лб3 "Вірусне ПЗ та його типи. Антивірусне ПЗ та алгоритми пошуку вірусів. Заходи протидії та видалення вірусного ПЗ"

Завантаження дублікату встановленої операційної системи на віртуальній машині. Завантаження вірусу. Роміщення в віртуальній машиніутиліти для лікування і пакет sysinternals. Ізоляція віртуальної машини від хостової системи. Перенесення архіву вірусу, антивірусних та інших утиліт в копію віртуальної машин. Розпакування архіву з вірусом. Інфікуваня. Дослідження зараження з допомогою SysinternalsSuite. Видалення вірусу і його проявів. Завантаження інших утиліт для аналізу і проведення аналізу. Дослідження дайджестів, рейтингів, властивостей антивірусного ПО. Підбір антивірусу. Встановлення антивірусного програмного забезпечення для пібприємства

Тема 3. Захист інформації в інформаційно-комунікаційних системах

Лк7 "Основи безпеки інформації в комп'ютерних мережах"

Загрози безпеці інформації у мережах. Безпека взаємодії відкритих систем. Сервіси безпеки. Специфічні механізми безпеки. Універсальні механізми безпеки. Керування безпекою

Лк8 "Засоби захисту в розподілених інформаційно-комунікаційних системах"

Архітектура захищених мереж. Міжмережні екрани. Системи виявлення атак. Додаткові інструментальні засоби

Лб4 "Міжмережевий екран. Особливості та налагоджування"

Аналіз поточного стану актуальності і рейтингу різних міжмережевих екранів (МЕ). Встановлення МЕ. Порти, які потрібно закрити. Таблиця правил дозволити / заборонити. Налаштування згідно з таблицями.

Лб5 "Методи захисту інформації на носіях шифруванням"

Аналіз актуальності і рейтингу програмного забезпечення, що здійснює шифрування-на-льоту. Встановлення вибраного. Створення зашифрованого тому. Перевірка швидкості шифрування та дешифрування різних алгоритмів. Забезпечення доступу з допомогою групової політики. Тестування.

Лб6 "Віртуальна приватна мережа. Принципи, налагодження застосування"

Аналіз необхідності віртуальної приватної мережі (VPN). Вибір VPN. Встановлення VPN. Налаштування VPN. Створення нової мережі. підключення іншого персонального комп'ютера. Перевірка з'єднання (створення тунелю)

Лб7 "Резервне копіювання. Забезпечення швидкого відновлення працездатності"

Порівняння методів резервного копіювання. Завантаження системи. Створення завантажувального носія. Переміщення його на основну систему. Підключення до віртуальної машини ще одного віртуального диску. Створення резервної копію розділу. Видалення операційної системи на основному розділі віртуальної машини. Відновлюємо розділу. Перевірка системи

Лб8 "Тестування комп'ютерного робочого місця. Засоби, програмне забезпечення, відновлення працездатності" Утиліти, які обслуговують апаратне забезпечення комп'ютера. Перевірка оперативної пам'яті. Перевірка жорсткого диску. Тестування основних компонентів апаратного забезпечення

9. Стратегія викладання та навчання

9.1 Методи викладання та навчання

Дисципліна передбачає навчання через:

МН1	Лекційне навчання
МН2	Практикоорієнтоване навчання
МН3	Самостійне навчання

Дисципліна передбачає навчання через: МН1. Лекційне навчання; МН2. Практикоорієнтоване навчання МН3. Самостійне навчання. Лекції надають студентам матеріали сучасних інформаційно-комунікаційних технологій в кібербезпеці з застосуванням пасивного методу навчання з елементами активного та інтерактивного методів, що є основою для самостійного навчання здобувачів вищої освіти (РН1 - РН4). Лекції доповнюються лабораторними заняттями, що надають студентам можливість застосовувати теоретичні знання для конкретних ситуацій (РН1 - РН4). Самостійному навчанню сприятиме підготовка до лекцій і практичних занять (РН1 - РН4).

Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності

9.2 Види навчальної діяльності

НД1	Робота з підручниками та релевантними інформаційними джерелами
НД2	Оформлення звітів до лабораторних робіт
НД3	Підготовка до атестації

10. Методи та критерії оцінювання

10.1. Критерії оцінювання

Визначення	Чотирибальна національна шкала оцінювання	Рейтингова бальна шкала оцінювання
Відмінне виконання лише з незначною кількістю помилок	5 (відмінно)	$90 \leq RD \leq 100$
Вище середнього рівня з кількома помилками	4 (добре)	$82 \leq RD < 89$

Загалом правильна робота з певною кількістю помилок	4 (добре)	74 ≤ RD < 81
Непогано, але зі значною кількістю недоліків	3 (задовільно)	64 ≤ RD < 73
Виконання задовольняє мінімальним критеріям	3 (задовільно)	60 ≤ RD < 63
Можливе повторне складання	2 (незадовільно)	35 ≤ RD < 59
Необхідний повторний курс з навчальної дисципліни	2 (незадовільно)	0 ≤ RD < 34

10.2 Методи поточного формативного оцінювання

	Характеристика	**Дедлайн, тижні**	**Зворотний зв'язок**
МФО1 Перевірка та оцінювання письмових завдань	Якість виконання робіт	1	Через Mix
МФО2 Експрес-тестування	Опитування та усні коментарі викладача за його результатами	0	Безпосередньо в аудиторії або через Meet
МФО3 Дискусії у фокус-групах	Відстоювання власної думки	0	Безпосередньо в аудиторії або через Meet

10.3 Методи підсумкового сумативного оцінювання

	Характеристика	**Дедлайн, тижні**	**Зворотний зв'язок**
МСО1 Звіт за результатами виконання лабораторних робіт	Перевіряється виконання лабораторних робіт	1	Через Mix
МСО2 Модульний контроль	Проводиться тестування	В день проведення тестування	Безпосередньо в аудиторії або через MIX

Контрольні заходи:

	Максимальна кількість балів	Мінімальна кількість балів	Можливість перескладання з метою підвищення оцінки
2 семестр	**100 балів**		
МСО1. Звіт за результатами виконання лабораторних робіт	**60**		

		60	Не передбачено	Ні
МСО2. Модульний контроль		**40**		
		40	Не передбачено	Ні

11. Ресурсне забезпечення навчальної дисципліни

11.1 Засоби навчання

ЗН1	Мультимедіа, відео- і звуковідтворювальна, проєкційна апаратура (відеокамери, проєктори, екрани, смартдошки тощо)
ЗН2	Комп'ютери, комп'ютерні системи та мережі

11.2 Інформаційне та навчально-методичне забезпечення

Основна література	
1	Кушнерьов, О. С. Безпека інформації [Текст] : конспект лекцій / О. С. Кушнерьов. — Суми : СумДУ, 2021. — 99 с. - https://essuir.sumdu.edu.ua/bitstream-download/123456789/85989/3/Kushnerov.pdf
2	Інформаційна безпека : навч. посіб. / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник та ін.; за заг. ред. Ю. Я. Бобала, І. В. Горбатого. — Львів : Вид-во Львівської політехніки, 2019. — 580 с. - https://pdf.lib.vntu.edu.ua/books/2020/Bobalo_2019_580sec.pdf
3	Бобро, Д. Г. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України [Текст] : аналітична доповідь / Д. Г. Бобро, С. П. Іванюта, С. І. Кондратов, О. М. Суходоля ; ред. О. М. Суходоля. — К. : Нац. ін-т стратегісних досліджень, 2019. — 224 с. - https://niss.gov.ua/sites/default/files/2019-05/Dopov_Suchodolya_print.pdf
Допоміжна література	
4	Cyber Security. Simply. Make it Happen. : Monograph / edit. Abolhassan. – Springer International Publishing, 2017. – ISBN 978-3-319-46528-9 (print); 978-3-319-46529-6 (online). 127 p.
5	Інформаційна безпека України: теорія і практика [Текст] : підручник / В. В. Лизанчук. — Львів : Львівський нац. ун-т ім. І. Франка, 2017. — 728 с.