	Лекційні заняття (год)	Практичні заняття (год)	Викладач
1. Правила кібербезпеки та соціальна інженерія (реально 2)			Шишацький А.В.
Правила кібербезпеки та кібергігієни. Платіжна безпека. Захист акаунтів. Паролі. Багатофакторна автентифікація. VPN-сервіси. Сторінки в соціальних мережах. Правила безпечних он-лайн покупок. Телефонне шахрайство. Приватність даних і міжнародні регуляції: GDPR. Ведення обліку чутливих даних та ресурсів (asset register). Життєвий цикл даних та ресурсів, утилізація даних.	2		
2. Основні положення інформаційної безпеки та кібербезпеки (реально 1)			Криволап А.В.
Основні складові інформаційної безпеки. Види інформаційної безпеки, класифікація, система забезпечення. Тріада CIA. Поняття кібератаки, кібертероризму. Мета деструктивних інцидентів у сфері високих технологій. Характерні особливості та класифікація кібератак. Об'єкти впливу кібератак. Основні чинники, що формують джерела загроз національній безпеці та інтересам України. Основні засади забезпечення інформаційної та кібербезпеки. Загальна характеристика кіберпростору. Основні методи забезпечення інформаційної безпеки.	2		
Управління доступами. Ідентифікація, автентифікація, авторизація. Принцип найменших привілеїв. Принцип розділення обов'язків. Контроль доступу: дискреційний, обов'язковий, на основі ролей, правил. Класифікація та кластеризація даних. Види заходів кібербезпеки: технічні, адміністративні, фізичні. Пожежна безпека комп'ютерного обладнання. Створення внутрішньої політики кібербезпеки організації.	2		
3. OSINT: основні принципи та безпечний пошук інформації в інтернеті (реально 3)			Супрун О.М.
Історія OSINT та методологія пошуку інформації. Робота з пошуковими системами та головні відмінності пошукових систем. Особливості роботи з інформацією та основні методи фактчекінгу. Поняття безпеки у цифровому просторі та як забезпечити власну безпеку при пошуку інформації. Основні поняття у роботі з мережевою інфраструктурою. Пошук контактів і соцмереж та «червоні прапорці» для людей та компаній. Google Dorks	2		
4. Криптографічний захист інформації (реально 8)			Криволап А.В.

Основні терміни та визначення. Класифікація криптографічних систем. Вимоги до шифрів криптографічного захисту інформації. Принципи Керкхоффса. Різниця між шифруванням, кодуванням, хешуванням.	2		
Деякі алгоритми шифрування. AES, еліптичні криві, RSA. Порівняння швидкодії. Цифровий підпис (схема, алгоритм). Протокол Діффі-Геллмана (схема, алгоритм). Використання шифрування в TLS як приклад.	2		
5. Основні поняття операційних систем (реально 4)			Ченцов О.І.
Основи Linux. Базове розуміння ОС сімейста UNIX/Linux. Базові команди.	2	2	
Базовий курс по Асемблеру	2	4	
6. Комп'ютерні віруси та антивірусний захист (реально 5)			Бучик С.С.
Основні поняття. Ознаки діяльності комп'ютерних вірусів. Класифікація комп'ютерних вірусів, їх коротка характеристика. Способи зараження комп'ютерними вірусами. Методи захисту від комп'ютерних вірусів. Антивірусні програми, їх характеристика.	2	2	
Антивірусне програмне забезпечення: встановлення, можливості, недоліки. Базовий аналіз шкідливого ПЗ: статичні та динамічні методи		2	
7. Поняття про локальну та глобальну комп'ютерні мережі (реально 6)			Шишацький А.В.
Поняття комп'ютерних мереж. Апаратні і програмні засоби мереж. Топології локальних мереж. Служби глобальної мережі Internet. Протоколи мереж. Ідентифікація комп'ютерів в мережі. Мережі: TLS з точки зору безпеки, forward secrecy. MITM, DDoS атаки. Хмарні сервіси: поняття SaaS, IaaS, PaaS. Поняття DMZ.	4		
Захист організацій: встановлення, налаштування та основні проблеми міжмережного екрану (фаєрволу, брандмауреру)		2	
8. Вразливості Web-безпеки (реально 9)			Супрун О.М.
Вразливості веб-серверів. Типи атак на веб-сервери. Інструменти атак на веб-сервери. SQL-ін'єкції. Міжсайтовий скриптінг. Зламана автентифікація і керування сесіями. Небезпечні прямі посилання на об'єкти. Підробка міжсайтових запитів. Невірне налаштування безпеки. Недостатній захист транспортного рівня. Неперевірені перенаправлення та пересилання.	4	4	
9. Етичний хакінг (реально 7)			Бучик С.С.
Основні вразливості CVE (демонстрація + пом'якшення + вплив). Огляд CVE. Публічні експлоіти.	2	2	

Programming (python, c++, WinAPI, asm…).Basic web prog. Базовий огляд деяких мов програмування з ухилом на хакінг (Python, C/C++/C# WinAPI, Асемблер)	4	4	
10. Розрахунок та управління ризиками (реально 10)			Супрун О.М.
Способи оцінки інформаційних ризиків. Сучасні підходи до оцінки ризиків інформаційних технологій. Рівняння ризику, робота з ним. Методика оцінки ризиків NIST 800-30 “Керівництво з інформаційними ризиками ІТсистем” (блок-схема оцінювання ризику). Кіберматриця. Оцінки ризиків: CRAMM, Cobra.	2	2	
Управління ризиками: прийняття, уникнення, передача, знешкодження. Поняття моделі загроз. Міжнародні сертифікації з кібербезпеки для організацій: ISO 27001, SOC-2, PCI DSS. Реагування на інциденти, побудова плану реагування і відновлення роботи. Збір даних про інцидент. Важливість моніторингу та логів.	2		