Інформаційний пакет освітніх компонент навчального плану
освітньо-професійної програми _____
(назва)

Освітнього рівня _____бакалавр_____

Спеціальності __125 Кібербезпека_____

Галузь знань __12 Інформаційні технології_____

1. Назва освітньої компоненти __Основи безпеки комп'ютерних мереж_____
(назва дисципліни)

2. Тип основна

3. Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінар	Практичних занять	Лабораторних занять	Самостійна підготовка
	5	150	18	-	18	18	96
4. Взаємозв'язок у структурно-логічній схемі							
Освітні компоненти, які передують вивченню	1. Комп'ютерні мережі 2. Безпека безпроводових, мобільних та хмарних технологій						
Освітні компоненти для яких є базовою	1. Комплексні системи захисту інформації 2. Кібербезпека банківських та комерційних структур						
5. Компетенції відповідно до ОПП та вимог роботодавців:							
Компетенції відповідно до ООП							
Знати			**Вміти**				
1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та кібербезпеки.			1. Розробляти проектну документацію щодо програмних та програмно-апаратних комплексів захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем. Виконувати аналіз реалізації прийнятої політики інформаційної та кібербезпеки.				
2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та кібербезпеки.			2. Розробляти та аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах				

	передачі даних. Застосовувати в професійній діяльності знання, навички та практики щодо структур сучасних обчислювальних систем, методів і засобів обробки інформації. Виконувати аналіз програмного забезпечення з метою оцінки на відповідність встановленим вимогам інформаційної та кібербезпеки в інформаційно-телекомунікаційних системах.
3. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та кібербезпеки.	3. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних системах. Забезпечувати введення підзвітності системи управління доступом інформаційних ресурсів і процесів в системах.
4. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та кібербезпеки.	4. Обирати основні методи та засоби захисту інформації відповідно до вимог сучасних стандартів інформаційної та кібербезпеки, та критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії захисту інформації. Використовувати інструментальні засоби оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційних та інформаційно-телекомунікаційних системах.
5. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження.	5. Вирішувати задачі управління процесами забезпечення безперервності бізнесу з використанням процедур резервування програмного забезпечення та безпосередньо інформаційних ресурсів. Виконувати аналіз налаштувань елементів інформаційних систем та комунікаційного обладнання.
6. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та кібербезпеки.	6. Забезпечувати процеси моніторингу доступу до ресурсів і процесів інформаційно-телекомунікаційних систем. Забезпечувати конфігурування та функціонування систем моніторингу ресурсів та процесів в інформаційно-телекомунікаційних системах.
7. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та кібербезпеки.	7. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних та інформаційно-телекомунікаційних системах. Аналізувати ефективність систем виявлення та протидії несанкціонованого доступу до ресурсів і процесів в інформаційно-телекомунікаційних системах.
Компетенції відповідно до вимог роботодавців	
1. Базові знання роботи мереж: IP-адреса, статична та динамічна маршрутизація, моделі ISO OSI, TCP	1. Пошук вразливостей за допомогою спеціалізованого ПЗ і їх усунення

2. Комунікаційне обладнання та супутнє програмне забезпечення, наприклад маршрутизатори, мережеві сервери, комп'ютерні інтегровані голосові системи, виявлення / запобігання вторгнень, брандмауери, шлюзи, фільтрація вмісту, шифрування, запобігання втратам даних та інші технології інформаційної безпеки	2. Навики роботи з IDS / IPS, брандмауерами, розширеними системами виявлення зловмисних програм та іншими платформами кібербезпеки
3. Технологія віртуальної локальної мережі (VLAN)	3. Налаштування і підтримка локальних мережних сервісів
4. Системи або служби управління вразливістю.	4. Проведення розслідування потенційних шахрайських дій/операцій
5. Технологія Брандмауери, антивірусні рішення, понімання принципів роботи комп'ютерної та сетевої безпеки, система обнаруженого входу	5. Адміністрування та розгортання віртуалізації
6. Протоколи взаємодії мережевого обладнання	6. Налаштування та адміністрування мережевого обладнання

6. Результати навчання відповідно до ОПП

1. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.
2. Виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах.
3. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.
4. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій
5. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв’язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.
6. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і кібербезпеки.
7. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
8. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.
9. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.
10. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.
11. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.
12. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.

7. План вивчення освітньої компоненти

Змістовний розділ	Вид заняття	Тема	Знати	Вміти	План заняття	Лекція, методична розробка

Розділ 1						
	Лекція 1	Тема 1: Сучасні загрози мережевої безпеки.	1.Що таке мережеві загрози, техніка нейтралізації. 2.Основи безпеки мережі	1. Описувати загрози і атаки різного типу. 2. інструменти і процедури нейтралізації наслідків взаємодії шкідливого ПЗ і поширення мережевих атак	https://www.netacad.com	https://www.netacad.com
	Лекція 2	Тема 2: Забезпечення безпеки мережевих пристроїв	1. Конфігурація безпечного адміністративного доступу 2. Конфігурація авторизації команд с використанням рівнів привілегій і CLI на основі ролей	1. Впровадження захищеного управління і моніторингу мережевих пристроїв. 2. використання автоматичних функцій для забезпечення безпеки на маршрутизаторах під управлінням IOS	https://www.netacad.com	https://www.netacad.com
	Лекція 3	Тема 3: Аутентифікація, авторизація та облік	1. Способи застосування AAA для захисту мережі 2. Серверна аутентифікація AAA і її комунікаційних протоколів	1. Впровадження аутентифікації AAA, в ході якої виконується звірка користувачів з локальної базою даних 2. Конфігурація серверної авторизації і обліку AAA	https://www.netacad.com	https://www.netacad.com
	Практичне заняття 1	Тема 1: Вивчення мережевих атак, а також інструментів для аудиту безпеки і проведення атак	1.Що таке мережеві загрози, техніка нейтралізації. 2.Основи безпеки мережі	1. Описувати загрози і атаки різного типу. 2. інструменти і процедури нейтралізації наслідків взаємодії шкідливого ПЗ і поширення мережевих атак	https://www.netacad.com	https://www.netacad.com
	Практичне заняття 2	Тема 2: Налагодження та дослідження базових засобів захисту мережної операційної системи Cisco IOS та мережного обладнання Cisco	1. Конфігурація безпечного адміністративного доступу 2. Конфігурація авторизації команд с використанням рівнів привілегій і CLI на основі ролей	1. Впровадження захищеного управління і моніторингу мережевих пристроїв. 2. використання автоматичних функцій для забезпечення безпеки на	https://www.netacad.com	https://www.netacad.com

				маршрутизаторах під управлінням IOS		
	Практичне заняття 3	Тема 3: Налаштування аутентифікації AAA на маршрутизаторах Cisco	1. Способи застосування AAA для захисту мережі 2. Серверна аутентифікація AAA і її комунікаційних протоколів	1. Впровадження аутентифікації AAA, в ході якої виконується звірка користувачів з локальної базою даних 2. Конфігурація серверної авторизації і обліку AAA	https://www.netacad.com	https://www.netacad.com
	Лабораторне заняття 1	Тема 1: Налагодження та дослідження засобів протидії атакам MAC-Flooding та MAC-Spoofing у мережі на базі комутаторів Cisco	1.Що таке мережеві загрози, техніка нейтралізації. 2.Основи безпеки мережі	1. Описувати загрози і атаки різного типу. 2. інструменти і процедури нейтралізації наслідків взаємодії шкідливого ПЗ і поширення мережевих атак	https://www.netacad.com	https://www.netacad.com
	Лабораторне заняття 2	Тема 2: Настройка маршрутизаторов Cisco для операций Syslog, NTP и SSH	1. Конфігурація безпечного адміністративного доступу 2. Конфігурація авторизації команд с використанням рівнів привілегій і CLI на основі ролей	1. Впровадження захищеного управління і моніторингу мережевих пристроїв. 2. використання автоматичних функцій для забезпечення безпеки на маршрутизаторах під управлінням IOS	https://www.netacad.com	https://www.netacad.com
	Лабораторне заняття 3	Тема 3: Налагодження та дослідження роботи аутентифікації на основі моделі AAA та протоколів Radius та Tacacs+ у мережі на базі обладнання Cisco	1. Способи застосування AAA для захисту мережі 2. Серверна аутентифікація AAA і її комунікаційних протоколів	1. Впровадження аутентифікації AAA, в ході якої виконується звірка користувачів з локальної базою даних 2. Конфігурація серверної авторизації і обліку AAA	https://www.netacad.com	https://www.netacad.com
	Самостійна робота	Тема 1. Технології захисту інформації при міжмережевій взаємодії Тема 2. Виявлення мережевих атак шляхом	1.Що таке мережеві загрози, техніка нейтралізації. 2.Основи безпеки мережі 3. Конфігурація безпечного адміністративного доступу	1. Описувати загрози і атаки різного типу. 2. інструменти і процедури нейтралізації наслідків взаємодії шкідливого ПЗ і	https://www.netacad.com	https://www.netacad.com

		аналізу трафіка Тема 3. Профіль безпеки стандарту ISO/OSI.	4. Конфігурація авторизації команд с використанням рівнів привілегій і CLI на основі ролей	поширення мережевих атак 3. Впровадження захищеного управління і моніторингу мережевих пристроїв. 4. використання автоматичних функцій для забезпечення безпеки на маршрутизаторах під управлінням IOS		
Розділ 2						
	Лекція 4	Тема 4: Впровадження технологій брандмауера	1.Списки контролю доступу 2.Технології міжмережевих екранів 3.Зональні міжмережеві екрани	1. Впровадження списків контролю доступу (ACL) для фільтрації трафіку і нейтралізації мережевих атак 2. Налаштування класичного брандмауера для нейтралізації мережевих атак 3. Впровадження зонального брандмауера з використанням інтерфейсу командного рядка (CLI)	https://www.netacad.com	https://www.netacad.com
	Лекція 5	Тема 5: Впровадження системи запобігання вторгнень	1. технології IPS 2. сигнатури IPS 3. впровадження IPS	1. Пояснення способів застосування AAA для захисту мережі 2. Пояснення способів застосування сигнатур для виявлення шкідливого мережевого трафіку 3. Конфігурація операцій Cisco IOS IPS з використанням інтерфейсу командного рядка (CLI).	https://www.netacad.com	https://www.netacad.com
	Лекція 6	Тема 6: Забезпечення	1. Безпека кінцевих	1. Пояснення вразливостей	https://www.net	https://www.

		безпеки локальної мережі (LAN)	пристроїв 2. Фактори, які необхідно враховувати при забезпеченні безпеки на рівні 2	кінцевих пристроїв і способів захисту 2. Впровадження функцій безпеки на рівні 2	acad.com	netacad.com
	Практичне заняття 4	Тема 4: Налаштування розширених списків контролю доступу (ACL).	1.Списки контролю доступу 2.Технології міжмережевих екранів 3.Зональні міжмережеві екрани	1. Впровадження списків контролю доступу (ACL) для фільтрації трафіку і нейтралізації мережевих атак 2. Налаштування класичного брандмауера для нейтралізації мережевих атак 3. Впровадження зонального брандмауера з використанням інтерфейсу командного рядка (CLI)	https://www.netacad.com	https://www.netacad.com
	Практичне заняття 5	Тема 5: Налаштування системи запобігання вторгнень (IPS) в IOS с використанням інтерфейсу командного рядка	1. технології IPS 2. сигнатури IPS 3. впровадження IPS	1. Пояснення способів застосування AAA для захисту мережі 2. Пояснення способів застосування сигнатур для виявлення шкідливого мережевого трафіку 3. Конфігурація операцій Cisco IOS IPS з використанням інтерфейсу командного рядка (CLI).	https://www.netacad.com	https://www.netacad.com
	Практичне заняття 6	Тема 6: Забезпечення безпеки на 2-му рівні	1. Безпека кінцевих пристроїв 2. Фактори, які необхідно враховувати при забезпеченні безпеки на рівні 2	1. Пояснення вразливостей кінцевих пристроїв і способів захисту 2. Впровадження функцій безпеки на рівні 2	https://www.netacad.com	https://www.netacad.com
	Лабораторне	Тема 4: Налаштування	1.Списки контролю доступу	1. Впровадження списків	https://www.net	https://www.

	заняття 4	списків ACL для IP-адрес з метою нейтралізації атак	2.Технології міжмережевих екранів 3.Зональні міжмережеві екрани	контролю доступу (ACL) для фільтрації трафіку і нейтралізації мережевих атак 2. Налаштування класичного брандмауера для нейтралізації мережевих атак 3. Впровадження зонального брандмауера з використанням інтерфейсу командного рядка (CLI)	acad.com	netacad.com
	Лабораторне заняття 5	Тема 4: Налаштування зонального брандмауера (ZPF)	1.Списки контролю доступу 2.Технології міжмережевих екранів 3.Зональні міжмережеві екрани	1. Впровадження списків контролю доступу (ACL) для фільтрації трафіку і нейтралізації мережевих атак 2. Налаштування класичного брандмауера для нейтралізації мережевих атак 3. Впровадження зонального брандмауера з використанням інтерфейсу командного рядка (CLI)	https://www.netacad.com	https://www.netacad.com
	Лабораторне заняття 6	Тема 5: Налаштування системи запобігання вторгнень (IPS)	1. технології IPS 2. сигнатури IPS 3. впровадження IPS	1. Пояснення способів застосування AAA для захисту мережі 2. Пояснення способів застосування сигнатур для виявлення шкідливого мережевого трафіку 3. Конфігурація операцій Cisco IOS IPS з використанням інтерфейсу командного рядка (CLI).	https://www.netacad.com	https://www.netacad.com

	Лабораторне заняття 7	Тема 6: Забезпечення безпеки VLAN на 2-му рівні	1. Безпека кінцевих пристроїв 2. Фактори, які необхідно враховувати при забезпеченні безпеки на рівні 2	1. Пояснення вразливостей кінцевих пристроїв і способів захисту 2. Впровадження функцій безпеки на рівні 2		https://www.netacad.com
	Самостійна робота	Тема 4: Принципи та методи надання доступу до інформаційних ресурсів. Тема 5: Забезпечення безпеки на рівнях моделі OSI Тема 6: Криптографічні системи	1. Криптографічні сервіси 2. Забезпечення базового рівня цілісності і аутентифікації 3. Конфіденційність 4. Криптографія з відкритими ключами	1. Пояснення способів спільного застосування типів шифрування, хешів і цифрових підписів для забезпечення конфіденційності, цілісності і аутентифікації 2. Пояснення способів застосування криптографічних хеш-кодувань для забезпечення цілісності і аутентифікації даних 3. Пояснення способів застосування алгоритмів шифрування для забезпечення конфіденційності даних 4. Пояснення способів застосування інфраструктури відкритих ключів для забезпечення конфіденційності і аутентифікації даних	https://www.netacad.com	https://www.netacad.com
Розділ 3						
	Лекція 7	Тема 7: Впровадження віртуальних приватних мереж (VPN)	1. Мережі VPN 2. Компоненти мережі IPsec VPN і їх функціонування 3. Реалізація мереж Site-to-Site IPsec VPN за допомогою	1. Пояснення призначення мереж VPN 2. Пояснення принципу роботи мереж IPsec VPN 3. Конфігурація мережі	https://www.netacad.com	https://www.netacad.com

			CLI	Site-to-Site IPsec VPN (між двома пунктами) з аутентифікацією за допомогою загального ключа з використанням інтерфейсу командного рядка (CLI)		
	Лекція 8	Тема 8: Впровадження багатофункціонального пристрої захисту Cisco Adaptive Security Appliance	1. Основні відомості ASA 2. Конфігурація брандмауера ASA	1. Пояснення того, як пристрій ASA функціонує в якості розширеного брандмауера зі збереженням стану 2. Конфігурація брандмауера ASA	https://www.netacad.com	https://www.netacad.com
	Лекція 9	Тема 9: Управління безпечною мережею	1. Тестування безпеки мережі 2. Розробка комплексної політики безпеки	1. Пояснення різних методів та інструментів, які використовуються для тестування безпеки мережі 2. Пояснення призначення комплексної політики з інформаційної безпеки	https://www.netacad.com	https://www.netacad.com
	Практичне заняття 7	Тема 7: Конфігурація і перевірка IPsec VPN між двома пунктами (site-to-site) за допомогою інтерфейсу командного рядка	1. Мережі VPN 2. Компоненти мережі IPsec VPN і їх функціонування 3. Реалізація мереж Site-to-Site IPsec VPN за допомогою CLI	1. Пояснення призначення мереж VPN 2. Пояснення принципу роботи мереж IPsec VPN 3. Конфігурація мережі Site-to-Site IPsec VPN (між двома пунктами) з аутентифікацією за допомогою загального ключа з використанням інтерфейсу командного рядка (CLI)	https://www.netacad.com	https://www.netacad.com
	Практичне заняття 8	Тема 8: Конфігурація базових налаштувань ASA і міжмережевого	1. Основні відомості ASA 2. Конфігурація брандмауера ASA	1. Пояснення того, як пристрій ASA функціонує в якості розширеного	https://www.netacad.com	https://www.netacad.com

		екрану з використанням інтерфейсу командного рядка (CLI)		брандмауера зі збереженням стану 2. Конфігурація брандмауера ASA		
	Практичне заняття 9	Тема 9: Ускладнене завдання на сукупне використання навичок	1. Тестування безпеки мережі 2. Розробка комплексної політики безпеки	1. Пояснення різних методів та інструментів, які використовуються для тестування безпеки мережі 2. Пояснення призначення комплексної політики з інформаційної безпеки	https://www.netacad.com	https://www.netacad.com
	Самостійна робота	Тема 7: Принципи об'єднання мереж на основі протоколів рівня моделі OSI Тема 8: Дослідження роботи протоколу VTP у мережі на базі комутаторів Cisco Багатофункціональний пристрій забезпечення безпеки Cisco ASA з розширеним функціоналом Тема 9: Моніторинг та безпека мережі	1. ASA Security Device Manager 2. Налаштування VPN в ASA 3. Тестування безпеки мережі 4. Розробка комплексної політики безпеки	1.Впровадження конфігурації брандмауера ASA 2. Налаштування мереж VPN віддаленого доступу на пристрої ASA 3. Пояснення різних методів та інструментів, які використовуються для тестування безпеки мережі 4. Пояснення призначення комплексної політики з інформаційної безпеки	https://www.netacad.com	https://www.netacad.com

8. Мова вивчення освітньої компоненти

(українська, англійська, розділи, що викладаються англійською мовою)

Українська

9. Інформаційне забезпечення освітньої компоненти

Рекомендовані джерела та інші навчальні ресурси: вказати підручники, навчальні посібники не пізніше 2010 року видання, які є у нас у бібліотеці на державній мові; електронні ресурси, посилання, електронна бібліотека ДУТ, іншомовні джерела

1. Tim Boyles. "CCNA Security Study Guide" Wiley Publishing. USA, 2016.
2. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. 5-е издание. СПб: Питер, 2016.
3. Э. Таненбаум, Д. Уэзеролл «Компьютерные сети» 5-е изд. СПб: Питер, 2016.

4. У. Одом «Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101. Маршрутизация и коммутация» , 2016
5. Крэйг Хант TCP/IP. Сетевое администрирование. 3-е издание. СПб-Москва, 2017

10. Методи оцінювання, підсумкові звітності за освітньою компонентою
(заліки, екзамени, курсові проекти, тестування)
Екзамен
11. Матеріально-технічне забезпечення освітньої компоненти
Cisco Packet Tracer 7.2
GNS3 2.1.8
Oracle VirtualBox 5.2.18