



СИЛАБУС ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ІНТЕРНЕТ РЕЧЕЙ: БЕЗПЕКА ТА ПРИВАТНІСТЬ

Факультет	Інформаційних технологій та кібербезпеки
Кафедра	Кібербезпеки та технічного захисту інформації
Статус навчальної дисципліни	Вибіркова компонента освітніх програм другого (магістерський) рівня вищої освіти
Рекомендовано для спеціальностей	Для всіх ОПІ запроваджених ДУІТЗ
Форма навчання	Денна, заочна

Викладачі

Кільдішев Віталій Йосипович
kildishev@ukr.net



Доцент кафедри кібербезпеки та технічного захисту інформації, кандидат технічних наук,
доцент

Загальна інформація про дисципліну

Анотація до дисципліни	Дисципліна «Інтернет Речей: безпека та приватність» має міждисциплінарний характер. Вона інтегрує комплекс знань, умінь та навичок які охоплюють предметну область фахівців як безпосередньо з кібербезпеки, так і з технічного захисту інформації з відповідними освітніми компонентами. Навчання спрямовано на формування професійних компетенцій, знань, умінь та навичок базових аспектів надійності та безпеки систем на основі
------------------------	--

	Інтернет речей (Internet of-Things або IoT).
Мета дисципліни	формування системи знань студентів в області Інтернет речей та цифрових технологій, та більш широкої категорії, яка називається цифровим перетворенням на базі яких дипломований фахівець зможе забезпечувати розробку, застосування і експлуатацію таких системи на виробництві та в науковій сфері.
Компетентності, формуванню яких сприяє дисципліна	Здатність застосовувати знання у практичних ситуаціях. Здатність проводити дослідження на відповідному рівні. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки; Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури. Здатність ефективно використовувати на практиці різні теорії в області навчання технологіям, засобам та організаційним аспектам безпеки інформаційних і комунікаційних систем та мереж.
Результати навчання	Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах; Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення; Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки; Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
Обсяг дисципліни	Загальний обсяг дисципліни 6 кредитів ЄКТС (180 академічних годин)
Форма підсумкового контролю	Залік
Терміни викладання дисципліни	Відповідно до розкладу занять вибіркового компонент освітньої програми

Програма дисципліни

Тема 1.	<i>Вступ до IoT. Мережі та TCP/IP</i> Розвиток комунікацій – IoT. Огляд трендів IoT. Компоненти IoT пристроїв. IoT інфраструктура. Приклад: Розумний будинок. Типи безпроводових мереж. Компоненти мереж. Стандартизована архітектура протоколів. Архітектура протоколу TCP / IP. Опис рівнів. Деякі протоколи у TCP/IP Suite. Протоколи та номери портів. Інкапсуляція.
Тема 2.	<i>Стандарти протоколів для IoT</i> Інфраструктура Інтернету речей. MAC протоколи. Проблеми проводової мережі. Класифікація бездротових MAC протоколів. WI-FI MAC.

	Проблема прихованого терміналу. Складові 802.11 кадру. Інший довільний доступ: IEEE 802.15.4 . Мережеві топології в IEEE 802.15.4 . Протокол Bluetooth. ZigBee. LoRa. Архітектури LoRa та MAC. Мобільні мережі (4/5G). Вузкосмуговий LTE для Інтернету речей.
Тема 3.	Огляд основ кібербезпеки Рівні системи безпеки. Вразливості, загрози та атаки. Типи загроз та атак. Послуги безпеки. Приклад: атака даних CIA. Політика безпеки та механізми. Цілі безпеки. Криптографія. Забезпечення конфіденційності: шифрування симетричним ключем. Шифрування з використанням симетричних ключів. Забезпечення конфіденційності: системи з відкритим ключем (асиметричні). Криптоаналіз. Хеш функції. Забезпечення автентифікації/цілісності. Забезпечення невідновності. Порівняння симетричний ключ ТА відкритий ключ. Порівняння безпека ТА конфіденційність.
Тема 4.	Перегляд роботи з ключами Управління ключами в IoT . Види управління .Симетричне керування ключами (сеанс). Розповсюдження ключів сеансу. Центр розповсюдження ключів. Обмін ключами Діффі-Хеллмана. Через PKC. Алгоритм Діффі-Хеллмана. Активна атака на DH. Автентифікований протокол DH. Управління відкритими ключами. Сертифікат X.509. Сховища сертифікатів. Механізми відкликання та переоформлення сертифікатів.
Тема 5.	Стандарти IoT. Безпека WiFi Безпека необхідна в IoT. Розглянемо захист: IEEE 802.11. Конфіденційність проводового елемента (WEP). Рішення для кращої безпеки IEEE 802.11. IEEE 802.1x. Процес авторизації. Розширений протокол автентифікації (EAP). Захищений доступ до Wi-Fi (WPA). Генерація ключів в WPA2. WPA3.

Список рекомендованих джерел

1. Методи та засоби захисту інформації [Навчальний посібник] / В.А. Лахно, Є.В. Васіліу, В.М. Гладких, В.М. Домрачев, Н.М. Сивкова. – К. : ФОП Ямчинський О.В., 2020. – 445 с.
2. Жураковський Б. Ю., Зенів І.О.Технології інтернету речей: навч. посіб. Київ: КПІ ім. Ігоря Сікорського, 2021. 271 с. • Сторчак К.П. Технології Інтернет речей. Навчальний посібник. – Київ: ДУТ, 2021. 68 с.
3. Дэвид Роуз, Дивовижні технології. Дизайн та інтернет речей, 336 с.
4. Баранов А.А., Інтернет речей: теоретико-методологічні основи правового регулювання. Том І. Сфери застосування, ризики і бар'єри, проблеми правового регулювання, ISBN: 978-966-937-513-1, 2018, 344с.
5. Електронний курс IoT Fundamentals : IoT Security: офіційний курс Академії Cisco. URL: <https://www.netacad.com/courses/cybersecurity/iot security>

Інформація про консультації

Індивідуальні та колективні консультації проводяться в час, визначений за попередньою домовленістю з викладачем через засоби зв'язку.

Загальна схема оцінювання

Сума балів за всі види навчальної діяльності	Шкала ЄКТС	Оцінка за національною шкалою		а н н я	Бали нараховуються таким чином:
		для іспиту	для заліку		Оцінювання знань здобувачів вищої освіти

90-100	A	Відмінно	зараховано	<i>здійснюється за 100-бальною шкалою</i> і становить: за поточну до 60 балів, за результати індивідуального завдання – до 40 балів. При оформленні документів за екзаменаційну сесію використовується таблиця відповідності оцінювання знань здобувачів вищої освіти за різними системами
82-89	B	Добре		
74-81	C			
64-73	D	Задовільно		
60-63	E			
35-59	FX	Незадовільно з можливістю повторного складання	Не зараховано з можливістю повторного складання	
0-34	F	Незадовільно з обов'язковим повторним вивченням дисципліни	Не зараховано з обов'язковим повторним вивченням дисципліни	

Політика опанування дисципліни

Відвідування:

Відвідування та відпрацювання пропущених занять є обов'язковим. Допускаються пропуски занять з поважних причин, які підтверджується документально. За такої умови навчання може відбуватися в режимі он-лайн за погодженням із деканатом.

Дотримання принципів академічної доброчесності:

Політика щодо академічної доброчесності побудована на основі «Положення про академічну доброчесність» в університеті. Списування під час виконання письмових контрольних видів робіт заборонено. Користуватися мобільними пристроями, під час проведення різних видів контролю успішності, дозволяється лише з дозволу викладача.

Умови зарахування пропущених занять:

Відпрацювання пропущених занять проходять в дні згідно графіку консультацій викладачів кафедри.