СИЛАБУС ВИБІРКОВОЇ ДИСЦИПЛІНИ

ІНТЕРНЕТ РЕЧЕЙ: БЕЗПЕКА ТА ПРИВАТНІСТЬ

Факультет	Інформаційних технологій і кібербезпеки
Кафедра	Кібербезпеки та технічного захисту інформації
Статус навчальної дисципліни	**Вибіркова компонента освітніх програм другого (магістерський) рівня вищої освіти**
Рекомендовано для спеціальностей	125 – Кібербезпека та захист інформації
Форма навчання	Денна, заочно-дистанційна

Викладач

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,	– Здатність застосовувати знання у практичних ситуаціях.

формуванню яких сприяє дисципліна	– 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 і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки 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 4 кредити ЄКТС (120 академічних годин), з них: лекцій – 20 год.; практичних занять – 8 год.; лабораторні занять – 12 годин; самостійна робота – 80 год.
Форма підсумкового контролю	Залік
Терміни викладання дисципліни	Відповідно до розкладу занять вибіркових компонент освітньої програми

Програма дисципліни

Тема 1.	***Вступ до IoT. Мережі та TCP/IP*** 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.	***Стандарти протоколів для IoT*** 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). Вузькосмуговий 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

- Методи та засоби захисту інформації [Навчальний посібник] / В.А. Лахно, Є.В. Василіу, В.М. Гладких, В.М. Домрачев, Н.М. Сивкова. – К. : ФОП Ямчинський О.В., 2020. – 445 с.
- 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.
- Дэвид Роуз, Дивовижні технології. Дизайн та інтернет речей, 336 с.
- 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.
- Електронний курс IoT Fundamentals : IoT Security: офіційний курс Академії Cisco. URL: https://www.netacad.com/courses/cybersecurity/iot-security

Інформація про консультації

Щопонеділка протягом 2024/2025 н.р. з 13^{00} до 14^{30} год., ауд. 250

Загальна схема оцінювання

<table>
<tr><td rowspan="2">Сума балів за всі види навчальної діяльності</td><td rowspan="2">Шкала ЄКТС</td><td colspan="2">Оцінка за національною шкалою</td><td rowspan="10">Нарахування балів</td><td>Бали нараховуються таким чином:</td></tr>
<tr><td>для іспиту</td><td>для заліку</td><td rowspan="9">Оцінювання знань здобувачів вищої освіти здійснюється за 100-бальною шкалою і становить: за поточну успішність (участь у практичних заняттях, виконання практичних завдань та контрольних робіт) – 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</td></tr>
<tr><td>90-100</td><td>A</td><td>Відмінно</td><td rowspan="5">зараховано</td></tr>
<tr><td>82-89</td><td>B</td><td rowspan="2">Добре</td></tr>
<tr><td>74-81</td><td>C</td></tr>
<tr><td>64-73</td><td>D</td><td rowspan="2">Задовільно</td></tr>
<tr><td>60-63</td><td>E</td></tr>
<tr><td>35-59</td><td>FX</td><td>Незадовільно з можливістю повторного складання</td><td>Не зараховано з можливістю повторного складання</td></tr>
<tr><td>0-34</td><td>F</td><td>Незадовільно з обов’язковим повторним вивченням дисципліни</td><td>Не зараховано з обов’язковим повторним вивченням дисципліни</td></tr>
</table>

Політика опанування дисципліни

Відвідування: Здобувачі вищої освіти самостійно планують відвідування лекційних занять, що проводяться в межах дисципліни. Присутність на практичних, лабораторних заняттях та контрольних заходах (залік) є обов’язковою. Важливим є своєчасне виконання індивідуальних завдань в межах самостійної роботи, передбачених програмою дисципліни.

Умови зарахування пропущених занять: Відпрацювання академічної заборгованості з дисципліни можливо до початку екзаменаційної сесії (відповідно до розкладу консультацій викладача).

Інші умови: Навчально-методичні матеріали дисципліни розміщені на платформі Moodle.