Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Кафедра програмного забезпечення комп'ютерних систем

МЕРЕЖЕВА АРХІТЕКТУРА ТА БЕЗПЕКА IOT ПРИСТРОЇВ

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни	
Рівень вищої освіти	***Другий (магістерський)***
Галузь знань	*12 Інформаційні технології*
Спеціальність	*121 Інженерія програмного забезпечення*
Освітня програма	*Інженерія програмного забезпечення мультимедійних та інформаційно-пошукових систем*
Статус дисципліни	*Вибіркова*
Форма навчання	*Очна (денна)*
Рік підготовки, семестр	*2 рік підготовки, 3 семестр*
Обсяг дисципліни	*Лекції: 36 год., комп'ютерний практикум: 18 год., самостійна робота: 66 год.*
Семестровий контроль/ контрольні заходи	*Залік, модульна контрольна робота, календарний контроль*
Розклад занять	*Згідно розкладу поточного навчального року (rozklad.kpi.ua)*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	Лектор: *к.т.н., доцент, Олещенко Любов Михайлівна, oleshchenkoliubov@gmail.com* Комп'ютерний практикум: *к.т.н., доцент, Олещенко Любов Михайлівна, oleshchenkoliubov@gmail.com*
Розміщення курсу	Google classroom. Доступ надається зареєстрованим студентам.

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Вивчення дисципліни «Мережева архітектура та безпека IoT пристроїв» дозволяє сформувати у здобувачів вищої освіти компетенції, необхідні для розв'язання практичних задач професійної та наукової діяльності, пов'язаної з проєктуванням мереж IoT пристроїв та забезпеченням безпеки пристроїв IoT.

***Метою** вивчення дисципліни «Мережева архітектура та безпека IoT пристроїв» є формування у студентів здатностей програмно налаштовувати пристрої IoT для їх безпечного функціонування у мережі заданої топології.*

***Предметом** дисципліни «Мережева архітектура та безпека IoT пристроїв» є протоколи, технології та програмні методи створення мереж пристроїв IoT.*

*Після засвоєння дисципліни «Мережева архітектура та безпека IoT пристроїв» **результатами навчання** є:*

знання:

- *протоколів і стандартів IoT;*
- *архітектур мереж IoT;*
- *параметрів безпеки мереж IoT та їх налаштування.*

уміння:

- *проєктувати мережі пристроїв IoT у середовищі моделювання Packet Tracer, налаштовувати параметри безпеки мереж IoT та виконувати тестування запрограмованих пристроїв IoT у мережі заданої топології.*

досвід:

- *проєктування мереж IoT, забезпечення безпеки та цілісності даних пристроїв IoT;*
- *розроблення програмного забезпечення пристроїв IoT для їх функціонування у мережі заданої топології.*

Вивчення дисципліни «Мережева архітектура та безпека IoT пристроїв» сприяє формуванню у здобувачів вищої освіти, які навчаються за освітньою програмою «Інженерія програмного забезпечення мультимедійних та інформаційно-пошукових систем» компетентностей, необхідних для розв'язання практичних задач професійної діяльності, пов'язаної з використанням технологій безпроводових мереж та програмування для побудови систем IoT та забезпечення їх безпеки:

ЗК01 Здатність до абстрактного мислення, аналізу та синтезу.

ЗК03 Здатність проводити дослідження на відповідному рівні.

ФК02 Здатність розробляти і реалізовувати наукові та/або прикладні проєкти у сфері інженерії програмного забезпечення.

2. Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Успішному вивченню дисципліни «Мережева архітектура та безпека IoT пристроїв» передує вивчення дисциплін «Операційні системи», «Програмування» та «Організація комп'ютерних мереж» навчального плану підготовки бакалаврів за спеціальністю 121 Інженерія програмного забезпечення.

Дисципліна «Мережева архітектура та безпека IoT пристроїв» забезпечує виконання курсових проєктів та магістерських дисертацій за спеціальністю 121 «Інженерія програмного забезпечення».

3. Зміст навчальної дисципліни

Дисципліна «Мережева архітектура та безпека IoT пристроїв» передбачає вивчення таких тем:

Тема 1. Архітектурні моделі IoT.

Тема 2. Безпека IoT пристроїв.

Залік.

4. Навчальні матеріали та ресурси

Базова література:

1. *Олещенко Л. М., Хіцко Я.В. Програмування пристроїв Інтернету речей: лабораторний практикум: навчальний посібник для студентів спеціальності 121 «Інженерія програмного забезпечення» / КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, 2019. – 47 с.*
2. *Технології інтернету речей. Навчальний посібник [Електронний ресурс]: навч. посіб. Для студ. спеціальності 126 «Інформаційні системи та технології», спеціалізація «Інформаційне забезпечення робототехнічних систем» / Б. Ю. Жураковський, І.О. Зенів; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 12,5 Мбайт). – Київ: КПІ ім. Ігоря Сікорського, 2021. – 271 с.*

Додаткова література:

1. *Finardi A. IoT Simulations with Cisco Packet Tracer // Електронний ресурс. Режим доступу: https://www.theseus.fi/bitstream/handle/10024/150158/Andrea%20Finardi%20%20Master%20of%20Engineering%20%20Information%20technology.pdf?sequence=1&isAllowed=y*
2. *Leading the IoT // Електронний ресурс. Режим доступу: https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf*
3. *Changing the programming paradigm for the embedded in the IoT domain // Електронний ресурс. Режим доступу: http://ieeexplore.ieee.org/document/7389059/?arnumber=7389059*
4. *Things and Components available in Packet Tracer 7.2 // Електронний ресурс. Режим доступу: https://www.packettracernetwork.com/internet-of-things/pt7-iot-devices-configuration.html*
5. *IOT attacks // Електронний ресурс. Режим доступу: https://www.educative.io/answers/what-are-iot-attacks*

Матеріали знаходяться у вільному доступі в Інтернеті.

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

№ з/п	Тип навчального заняття	Опис навчального заняття
	Тема 1. Архітектурні моделі IoT.	
1	*Лекція 1. Основні поняття IoT (Інтернету речей). Історія IoT. Архітектура IoT.*	*Основні поняття IoT. Використання IoT. Історія Інтернету Речей. IoT в промисловості. Екосистема IoT. Архітектура IoT.*
2	*Лекція 2. Еталонна модель IoT.*	*Стандарти сумістності IoT. Еталонна модель IoT від MCE-T. Еталонна модель від Всесвітнього форуму IoT. Модель NIST Special Publication 800-183. Модель Industrial Internet of Things Reference Architecture.*
3	*Лекція 3. IoT платформи.*	*Поняття IoT платформа. Платформа Linux Foundation. Платформа AggreGate. Платформа Everyware Cloud.*
4	*Лабораторна робота 1. Програмування пристроїв IoT засобами Cisco Packet Tracer.*	*Завдання: У середовищі Packet Tracer змоделювати топологію для домашньої мережі згідно сценарію за варіантом та запрограмувати пристрої для їх функціонування у мережі та взаємодії з мережевими пристроями. Усі пристрої, домашні планшети та сервери IoT підключені до домашньої бездротової мережі. Кожен пристрій підключений до бездротового маршрутизатора. Налаштувати DHCP, WLAN. Усі бездротові пристрої необхідні для використання однакових ідентифікаторів SSID, пароля та стандартних налаштувань DHCP. Також потрібно налаштувати DNS-сервер для перекладу URL-адреси домашньої сторінки IoT у власну IP-адресу сервера IoT. Виконати тестування запрограмованих пристроїв.*

5	*Лекція 4. IoT шлюзи.*	*Шлюзи компанії Eurotech. Шлюзи компанії Intel. Шлюзи компанії Huawei. Шлюзи компанії Cisco. Шлюзи компанії NEXCOM. Шлюзи Edge Gateway компанії Dell. Шлюзи Enterprise компанії Hewlett Packard.*
6	*Лабораторна робота 2. Захист хмарних сервісів IoT.*	*Завдання: У середовищі моделювання Packet Tracer зареєструвати чотири пристрої IoT на складі компанії, детектор руху, спрямоване світло та вебкамеру. Додати умови в реєстраційному сервері, щоб при активації детектору руху вмикались націлене спрямоване світло та веб-камера. Налаштувати на маршрутизаторі складну аутентифікацію для безпечного входу на консоль та для віддаленого доступу. Налаштувати ACL, щоб обмежити мережевий трафік між реєстраційним сервером та складом компанії. Налаштувати веб-сервер у мережі постачальника послуг хмарної мережі, щоб забезпечити безпеку передачі даних.*
7	*Лекція 5. Інтелектуальні сенсори.*	*Прості сенсори. Активні та пасивні сенсори. Сенсорно-комп'ютерні системи. Інтелектуальні сенсори. Види механічних сенсорів. Мікросистемні технології. Деформаційні інтелектуальні сенсори. Принципи роботи глобальної системи орієнтування. Сенсори лінійного та кутового переміщення. Інтелектуальні акустичні сенсори. Електричні сенсори.*
8	*Лекція 6. Технології IoT.*	*Індустрія 4.0. Промисловий Інтернет Речей. Smart Factory - розумне виробництво.*
9	*Лекція 7. Технології та протоколи передачі даних в IoT мережах.*	*Технології передачі даних на довгі відстані в IoT мережах. Технологія LoRaWAN. Технологія SigFox. Стандарт NB-IoT. Технологія Weightless-P. Технології передачі даних на короткі відстані в IoT мережах. Технологія Z – Wave. Технологія NFC. RFID. Bluetooth Low Energy. Wi-Fi HaLow. Сенсорні мережі.*
10	*Лекція 8. Протоколи IoT.*	*Протоколи інфраструктури. Протоколи виявлення сервісів. Протоколи рівня додатків. MQTT. CoAP.*
11	*Лекція 9. Технології Smart Home. Загрози безпеки «розумного будинку».*	*Елементи «розумного будинку». Загрози «розумного будинку». Атаки на «розумний будинок».*
12	*Лекція 10. Технології Smart City.*	*Класифікація Smart City. Концепції розумного міста. Основні складові Розумного міста. Технології розумних міст. Стандарти розумного міста. Інформаційні технології та інформаційно-технологічні платформи.*
13	*Лекція 11. Технології Smart Grid.*	*Історія розвитку енергосистем. Можливості модернізації. Системи на базі технологічної платформи Smart Grid. Властивості розумних енергосистем. Технології розумних енергосистем. Дослідження в Smart Grid. Моделювання розумних енергосистем.*

	Тема 2. Безпека IoT пристроїв.	
14	*Лекція 12. Виклики безпеки IoT. Аналіз моделі загроз для системи IoT.*	*Анатомія атаки IoT. Програмне забезпечення Mirai. Модель безпеки IoT. Моніторинг охорони здоров'я IoT. Безпека в еталонній моделі IoT. Стандартизована архітектура ETSI M2M. Моделювання загроз IoT. NICE Cybersecurity Workforce Framework.*
15	*Лабораторна робота 3. Налаштування безпеки пристроїв IoT.*	*Завдання: У середовищі моделювання Packet Tracer виконати налаштування безпеки пристроїв IoT в мережі заданої топології за допомогою бездротового маршрутизатора.*
16	*Лекція 13. Вразливості та атаки на апаратному рівні.*	*Фізичні вразливості пристроїв IoT. Безпека фізичного пристрою. Уразливості апаратного забезпечення. Уразливості мікропрограм. Уразливості вбудованого програмного забезпечення. Моделі контролю доступу. Керування ідентифікацією пристрою IoT. Шифрування в обмежених системах.*
17	*Лекція 14. Уразливості комунікаційного рівня.*	*Сценарії зв'язку IoT. Ролі пристроїв IEEE 802.15.4. Топології IEEE 802.15.4. Безпека IEEE 802.15.4. Меш-протоколи, які використовують 802.15.4.*
18	*Лекція 15. Уразливості TCP/IP у мережах IoT.*	*Поширені вразливості IP. DoS-атаки. Атаки посилення та відбиття. Атаки ICMP. Атаки підробки IP-адрес. Уразливості TCP. TCP SYN Flood атака. Уразливості UDP. Безпека для комунікаційних протоколів IoT. Модель загроз для комунікаційних технологій IoT. Контрольний список комунікацій IoT.*
19	*Лекція 16. Атаки рівня додатків систем IoT.*	*Уразливості веб- та хмарних програм OWASP. Керування пристроями та програми даних. Рекомендації щодо безпечних веб-додатків і хмарних додатків. Уразливості веб-інтерфейсу. Моделювання загроз на прикладному рівні. Протоколи обміну повідомленнями IoT. Захист MQTT. Захист CoAP.*
20	*Лекція 17. Оцінка вразливості та ризиків у системах IoT.*	*Оцінка ризиків IoT. Загальна система оцінки вразливості. Групи показників CVSS. Базова метрична група CVSS. Компоненти діаграм потоків даних IoT. Стратегії управління ризиками. IoT і блокчейн.*
21	*Лекція 18.Підсумкове заняття.*	*Модульна контрольна робота.*

6. Самостійна робота студента

Дисципліна «Мережева архітектура та безпека IoT пристроїв» ґрунтується на самостійній підготовці до аудиторних занять на теоретичні теми.

№ з/п	*Назва теми, що виноситься на самостійне опрацювання*	*Кількість годин*	*Література*
1	*Підготовка до лекції 1*	*2*	*2, стор. 8-24.*
2	*Підготовка до лекції 2*	*2*	*2, стор. 25-38.*
3	*Підготовка до лекції 3*	*2*	*2, стор. 41-50.*

4	*Підготовка до лабораторної роботи 1*	*4*	*1, стор. 5-30.*
5	*Підготовка до лекції 4*	*2*	*2, стор.52-60.*
6	*Підготовка до лабораторної роботи 2*	*4*	*1, стор. 31-36.*
7	*Підготовка до лекції 5*	*2*	*2, стор.62-104.*
8	*Підготовка до лекції 6*	*2*	*2, стор.111-131.*
9	*Підготовка до лекції 7*	*2*	*2, стор.133-156.*
10	*Підготовка до лекції 8*	*2*	*2, стор.172-188.*
11	*Підготовка до лекції 9*	*2*	*2, стор.189-204.*
12	*Підготовка до лекції 10*	*2*	*2, стор.205-220.*
13	*Підготовка до лекції 11*	*2*	*2, стор.240-255.*
14	*Підготовка до лекції 12*	*2*	*2(дод.), стор.12-27.*
15	*Підготовка до лабораторної роботи 3*	*4*	*4 (дод.)*
16	*Підготовка до лекції 13*	*2*	*5 (дод.)*
17	*Підготовка до лекції 14*	*2*	*5 (дод.)*
18	*Підготовка до лекції 15*	*2*	*5 (дод.)*
19	*Підготовка до лекції 16*	*2*	*5 (дод.)*
20	*Підготовка до лекції 17*	*2*	*5 (дод.)*
21	*Підготовка до модульної контрольної роботи*	*20*	*1, стор. 5-36.* *2, стор. 8-255.* *1-5 (дод.).*

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

- *Відвідування лекційних занять є обов'язковим.*
- *Відвідування занять комп'ютерного практикуму може бути епізодичним та за потреби захисту робіт комп'ютерного практикуму.*
- *Правила поведінки на заняттях: активність, повага до присутніх, відключення телефонів.*
- *Дотримання політики академічної доброчесності.*

8. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

*Протягом семестру студенти виконують **3 комп'ютерні практикуми**.*
Максимальна кількість балів за кожний комп'ютерний практикум: 20 балів.
Бали нараховуються за:
- якість виконання комп'ютерного практикуму: 0-8 бали;
- відповідь під час захисту комп'ютерного практикуму: 0-8 бали;
- своєчасне представлення роботи до захисту: 0-4 бали.
Критерії оцінювання якості виконання:
7-8 балів – робота виконана якісно, в повному обсязі;
5-6 балів – робота виконана якісно, в повному обсязі, але має недоліки;
3-4 бали – робота виконана якісно, але не в повному обсязі, має недоліки;
1-2 бали – робота виконана не якісно, не в повному обсязі, має недоліки;
0 балів – робота виконана не в повному обсязі, або містить суттєві помилки.

Критерії оцінювання відповіді:
7-8 балів – відповідь повна, добре аргументована;
5-6 балів – відповідь неповна, проте добре аргументована;
3-4 бали – у відповіді є незначні помилки;
1-2 бали – у відповіді є суттєві помилки;
0 балів – немає відповіді або відповідь невірна.
Критерії оцінювання своєчасності представлення роботи до захисту:
4 бали – робота представлена до захисту не пізніше вказаного терміну;
0 балів – робота представлена до захисту пізніше вказаного терміну.

Максимальна кількість балів за виконання та захист комп'ютерних практикумів:
20 балів × 3 комп. практ. = 60 балів.

*Завдання на **модульну контрольну роботу** складається з 5 питань – 3 теоретичних та 2 практичних. Відповідь на кожне теоретичне/практичне запитання оцінюється 8 балами.*
Критерії оцінювання кожного теоретичного/практичного запитання модульної контрольної роботи:
7-8 балів – відповідь вірна, повна, добре аргументована;
5-6 балів – відповідь вірна, але неповна або погано аргументована;
3-4 бали – у відповіді є незначні помилки;
1-2 бали – у відповіді є суттєві помилки;
0 балів – немає відповіді або відповідь невірна.
Максимальна кількість балів за модульну контрольну роботу:
8 балів × 3 теоретичні запитання + 8 балів × 2 практичні запитання = 40 балів.

Рейтингова шкала з дисципліни дорівнює:
$R = R_C$ = 60 балів + 40 балів = 100 балів.
За описом: $R = R_{комп.практ} + R_{МКР.}$ = 60+40 балів = 100 балів
Календарний контроль: провадиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу.
На першій атестації (8-й тиждень) студент отримує «зараховано», якщо його поточний рейтинг не менше 50 % від максимальної кількості балів, яку може отримати студент до першої атестації (20 балів).
На другій атестації (14-й тиждень) студент отримує «зараховано», якщо його поточний рейтинг не менше 50 % від максимальної кількості балів, яку може отримати студент до другої атестації (30 балів).
*Семестровий контроль: **залік**.*
Умови допуску до семестрового контролю:
При семестровому рейтингу (r_C) не менше 60 % (60 балів) та зарахуванні усіх робіт комп'ютерного практикуму.
Необхідною умовою допуску до заліку є виконання і захист комп'ютерного практикуму.

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

Кількість балів	*Оцінка*
100-95	Відмінно
94-85	Дуже добре
84-75	Добре
74-65	Задовільно
64-60	Достатньо
Менше 60	Незадовільно
Не виконані умови допуску	Не допущено

9. Додаткова інформація з дисципліни (освітнього компонента)

Наявність сертифікату проходження аналогічного курсу з проєктування IoT та мережевої безпеки IoT оцінюється як 15 балів, написання статей або участь у конференціях/ проєктах за відповідною тематикою також оцінюється як додаткові 5 балів.

Складено к.т.н., доц. Олещенко Л.М.

Ухвалено кафедрою ПЗКС (протокол №8 від 25.01.23)

Погоджено Методичною комісією факультету прикладної математики (протокол № 6 від 27.01.2023)