СІЛАБУС
НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Аналіз і дослідження методів виявлення вразливостей пристроїв Інтернету речей»

Шифр та назва спеціальності	**123 – Комп'ютерна інженерія**	**Факультет**	**Комп'ютерні та інформаційні технології**
Назва освітньо-наукової програми	**Комп'ютерна інженерія**	**Кафедра**	**Розподілених інформаційних систем і хмарних технологій**

ВИКЛАДАЧ

Пігнастий Олег Михайлович, *pihnastyi@gmail.com*

Доктор технічних наук, професор кафедри Розподілених інформаційних систем і хмарних технологій НТУ «ХПІ». Автор понад 300 наукових та навчально-методичних праць. Провідний лектор з дисциплін: «Теорія ймовірності», «Системний аналіз», «Нейрокомп'ютинг»

ЗАГАЛЬНА ІНФОРМАЦІЯ ПРО ДИСЦИПЛІНУ

Анотація	Дисципліна спрямована на оволодіння теоретичними основами задач багатофакторної аутентифікації, методів розв'язання задач програмування мережевого захисту інформації, методів резервного копіювання даних
Мета та цілі	Оволодіння аспірантами базовими знаннями та навичками щодо сучасних принципів, методів та алгоритмів кіберзахисту для здійснення контролю і планування заходів щодо захисту систем від кіберзагроз для теоретичної та практичної підготовки до виконання дисертаційної роботи.
Формат	Лекції, лабораторні роботи, консультації. Підсумковий контроль - іспит
Результати навчання	Проводити власні наукові дослідження задач аналізу вразливостей пристроїв Інтеренету речей, навчитися моделювати ситуації, що виникають при цьому в організації чи на підприємстві , та шукати шляхи їх вирішення
Обсяг	Загальний обсяг дисципліни 120 год.: лекції – 20 год., лабораторні роботи – 20 год., самостійна робота – 80 год.
Пререквізити	«Математичні методи обчислювального інтелекту та машинного навчання», «Математичне та комп'ютерне моделювання складних систем»
Вимоги викладача	Аспірант зобов'язаний відвідувати всі заняття згідно розкладу, не спізнюватися. Дотримуватися етики поведінки. Працювати з навчальної та додатковою літературою, з літературою на електронних носіях і в Інтернеті. При пропуску лекційних занять проводиться усна співбесіда за темою. Відпрацьовувати практичні заняття при наявності допуску викладача. З метою оволодіння необхідною якістю освіти з дисципліни потрібно відвідуваність і регулярна підготовленість до занять. Без особистої присутності аспіранта підсумковий контроль не проводиться.

СТРУКТУРА ДИСЦИПЛІНИ

Лекція 1	Проблеми безпеки та конфіденційності. Інтернет-речі, як платформа для атак.	**лабораторна робота 1**	Зловмисні пристрої Cloud-supported IoT.	**Самостійна робота**	Статус конфіденційності.
Лекція 2	Визначення принципів конфіденційності в IoT.	**лабораторна робота 2**	Машинне навчання в інтернеті речей. Моделі машинного навчання. Випадковий ліс. Байєсовські моделі. Згорткові нейронні мережі. Рекурентні нейронні мережі		Локалізація та відстеження. Профілювання.
Лекція 3	Загрози конфіденційності в IoT. Ідентифікація				Єтапи життєвого циклу. Інвентаризація атаки. З'єднання..
Лекція 4	Конвертування даних, що зберігає конфіденційність.				Консорціуми з персональних мереж. Bluetooth SIG. Thread Group. Альянс Zigbee
Лекція 5	Розподіл даних, що зберігають конфіденційність.	**лабораторна робота 3**	Аналіз даних в IoT і порівняння / оцінка методів машинного навчання.		Консорціуми за протоколами Open Connectivity Foundation і Allseen Alliance. OASIS. Object Management Group. IPSO Alliance
Лекція 6	Веб-приватна потокова модель. Візуальний захист приватності.	**лабораторна робота 4**	Управління ключами і модулі TPM. Адресний простір в процесорі і пам'яті. Безпека зберігання даних.		Консорціуми з глобальних обчислювальних мереж. Weightless SIG . LoRa Alliance.
Лекція 7	Безпека та конфіденційність у підтримці хмарних інтернет-речей. Доступ до хмари.				Консорціуми з туманним і граничним обчисленням. OpenFog. EdgeX Foundry
Лекція 8	Анатомія кібератак на IoT-пристрої. Mirai. Stuxnet	**лабораторна робота 5**	Асиметрична криптографія. Криптографічний хеш. Інфраструктура відкритого ключа. Мережевий стек		Анонімність на основі груп.
Лекція 9	Управління ключами і модулі TPM. Адресний простір в процесорі і пам'яті. Безпека зберігання даних.				Ланцюжкова реакція
Лекція 10	Криптографія. Симетрична криптографія.				Споживання інформації: потоки, обробка та озера

ЛІТЕРАТУРА ТА НАВЧАЛЬНІ МАТЕРІАЛИ

Основна

1. Roberto Minerva, Abyi Biru, and Domenico Rotondi. IEEE: Towards a definition of the Internet of Things (IoT). http://iot.ieee.org/ , May 2015. Last accessed December 09, 2016.
2. Chema Alonso, Antonio Guzmán, Andrey Nikishin, John Moor, Luis Muñoz Jaime Sanz, Belisario Contreras, and Bertrand Ramé. Scope, scale and risk like never before: Securing the Internet of Things. Technical report, Telefónica and ElevenPaths, 2016.
3. Сэмюэл Грингард, Характеристики Интернет вещей. Будущее уже здесь, : монографія / Сэмюэл Грингард. – Москва: Альпина Паблишер, 2016, - 188с

Додаткова

1. Баранов А.А., Інтернет речей: теоретико-методологічні основи правового регулювання, 2018, 344с.
2. Samuel Greengard, The Internet of IOT (MIT Press Essential Knowledge series), 2015, 230 P.
3. Cuno Pfister, Getting Started with the Things: Connecting Sensors and Microcontrollers to the Cloud, 2011, 194 P.

ПЕРЕЛІК ЗАПИТАНЬ ДЛЯ ПІДГОТОВКИ ДО ІСПИТУ

Тема 1. Що таке інтернет-речі. Проблеми безпеки та конфіденційності. Інтернет-речі, як платформа для атак. Визначення принципів конфіденційності в IoT. Статус конфіденційності. Тема 2. Забезпечення конфіденційності для користувачів IoT на етапі їх проектування. Загрози конфіденційності в IoT. Ідентифікація. Локалізація та відстеження. Профілювання. Єтапи життєвого циклу. Інвентаризація атаки. З'єднання. Конвертування даних, що зберігає конфіденційність. Анонімність на основі груп. Розподіл даних, що зберігають конфіденційність. Диференціальна конфіденційність. Атаки на диференціальну приватність.

ПЕРЕЛІК ОБЛАДНАННЯ

Комп’ютери

СИСТЕМА ОЦІНЮВАННЯ

Розподіл балів для оцінювання успішності аспіранта

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою
90-100	A	відмінно
82-89	B	добре
74-81	C	
64-73	D	задовільно
60-63	E	
35-59	FX	незадовільно з можливістю повторного складання
0-34	F	незадовільно з обов'язковим повторним вивченням дисципліни

Нарахування балів

Бали нараховуються за наступним співвідношенням:

- лабораторні роботи: 30% семестрової оцінки;
- самостійна робота: 20% семестрової оцінки;
- іспит: 50% семестрової оцінки

НОРМИ АКАДЕМІЧНОЇ ЕТИКИ

Аспірант повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при нерозв'язності конфлікту доводитися до співробітників відділу аспірантури.

Сілабус за змістом повністю відповідає робочій програмі навчальної дисципліни