Силабус освітнього компонента
Програма навчальної дисципліни

Моделювання механізмів кібербезпеки

Шифр та назва спеціальності
125 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій (320)

Освітня програма
Кібербезпека

Кафедра
Кібербезпеки (328)

Рівень освіти
третій (освітньо-науковий)

Тип дисципліни
Спеціальна (фахова). Обов'язкова

Семестр
2

Мова викладання
Українська

Викладачі, розробники

МІЛЕВСЬКИЙ Станіслав Валерійович
stanislav.milevskyi@khpi.edu.ua
кандидат економічних наук, доцент кафедри кібербезпеки НТУ «ХПІ».

Автор понад 100 наукових та навчально-методичних праць. Науковий Гарант освітньо-професійної програми другого (магістерського) рівня вищої освіти. Провідний лектор з дисциплін: «Основи математичного моделювання систем безпеки», «Англійська мова в академічних застосунках», «Моделювання кіберфізичних дій» у студентів бакалавріата та магістратури.

Детальніше про викладача на сайті кафедри

МІЛОВ Олександр Володимирович
oleksandr.milov@khpi.edu.ua
Доктор технічних наук, професор кафедри кібербезпеки НТУ «ХПІ».

Автор понад 200 наукових та навчально-методичних праць. Науковий керівник з захищених кандидатських робіт, гарант освітньо-професійної програми другого (магістерського) рівня вищої освіти. Провідний лектор з дисциплін: «Математичні основи криптології та криптоаналіз», «Структури даних», «Промисловий та офісний шпіонаж» , «Цифрова криміналістика», у студентів бакалавріата та магістратури, Розділ «Методологія наукової та педагогічної діяльності в науках кіберзахисту» для аспірантів.
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Вивчення дисципліни має на меті формування світогляду, розвитку інтелекту, ерудиції, формування професійних компетенцій зі спеціальності кібербезпека та захист інформації.

Дисципліна "Моделювання механізмів кібербезпеки" орієнтована на розвиток в аспірантів науково-дослідних і практичних навичок у галузі моделювання процесів захисту інформації.

Мета та цілі дисципліни

Формування у аспірантів системи теоретичних знань і практичних навичок з моделювання загроз безпеки, що має на увазі визначення перелік актуальних загроз для конкретної інформаційної системи, на підставі якого приймаються рішення щодо нейтралізації актуальних загроз.

Формат занять

Лекції, практичні роботи, самостійна робота, індивідуальне завдання, консультації. Підсумковий контроль – іспит.

Компетентності

ІК Здатність продукувати нові ідеї, розв'язувати комплексні проблеми професійної та/або дослідницько-інноваційної діяльності у сфері кібербезпеки та захисту інформації, застосовувати методологію наукової та педагогічної діяльності, а також проводити власне наукове дослідження, результати якого мають наукову новизну, теоретичне та практичне значення.
ЗК-2. Здатність до абстрактного мислення, аналізу та синтезу, проведення самостійних досліджень.
ЗК-3. Здатність до виявлення, генерування нових ідей, дослідження та вирішення проблем за професійним спрямуванням.
СК-1. Здатність до застосування сучасних інформаційних і безпекових технологій у сфері захисту інформації, створення комплексних систем захисту інформації;
СК-2. Здатність формулювати наукову проблему, робочі гіпотези досліджуваної проблеми на основі глибокого осмислення наявних і створення нових цілісних знань, а також професійної практики. Використання моделювання механізмів кібербезпеки.
СК-3. Здатність розробляти процеси життєвого циклу інформаційних технологій, виявляти технічні канали витоку інформації, застосовувати засоби захисту інформації.
СК-4. Здатність систематизувати професійні знання в інформаційно-комунікаційних технологіях, моделювання механізмів кібербезпеки.
СК-5. Здатність розробляти та реалізовувати нові конкурентоздатні ідеї в галузі захисту інформації, використовувати методологічні та організаційно-технічні основи забезпечення безпеки.
СК-6. Здатність до розробки технологій та інструментальних засобів аналізу, прогнозування й інформаційно-аналітичної підтримки процесів прийняття рішень щодо забезпечення безпеки інформації.

Результати навчання

РН-5. Вміння та навички критично сприймати та аналізувати існуючі наукові теорії та ідеї, шукати власні шляхи вирішення проблеми та завдань, проводити критичний аналіз власних матеріалів, генерувати власні нові ідеї, приймати обґрунтовані рішення.
РН-8. Вміння використовувати кількісні і якісні методи для проведення наукових досліджень.
РН-11. Вміння розробляти проекти наукових досліджень та моделювати їх структуру, застосовуючи різні способи подання статистичної інформації та результатів.
РН-12. Вміння оцінювати конкурентоспроможність отриманих результатів.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 20 год., практичні роботи – 20 год., самостійна робота – 80 год.

Передумови вивчення дисципліни (пререквізити)

Штучний інтелект та експертні системи, Основи програмування, Комбінаторна оптимізація.

Особливості дисципліни, методи та технології навчання

Аспірант зобов'язаний відвідувати всі заняття згідно розкладу, не спізнюватися. Дотримуватися етики поведінки. Працювати з навчальною та додатковою літературою, з літературою на електронних носіях і в Інтернеті. При пропуску лекційних занять проводиться усна співбесіда за темою. З метою оволодіння необхідною якістю освіти з дисципліни потрібно відвідуваність і регулярна підготовленість до занять. Без особистої присутності аспіранта підсумковий контроль не проводиться.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. STRIDE and Associated Derivations.
Тема 2. PASTA (The Process for Attack Simulation and Threat Analysis).
Тема 3. LINDDUN (Linkability, Identifiability, Non-Repudiation, Detectability, Disclosure of Information, Unawareness, Non-Compliance).
Тема 4. CVSS (Common Vulnerability Scoring System). Attack Trees.
Тема 5. Quantitative Threat Modeling Method. Trike.
Тема 6. VAST Modeling. OCTAVE. Mitre.

Теми практичних занять

Тема 1. Побудова діаграми потоків даних (DFD).
Тема 2. Побудова високорівневих архітектурних схем.
Тема 3. LINDDUN GO – виявлення загроз конфіденційності (ID.RA-P3).
Тема 4. Persona non Grata. Security Cards. hTMM.
Тема 5. Моделювання загроз в пакеті Microsoft Threat Modeling Tool.
Тема 6. Моделювання в пакеті R: SpatialDeltaGLM.

Теми лабораторних робіт

Лабораторні роботи в рамках дисципліни не передбачені.

Самостійна робота

Самостійна робота здобувачів є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи аспіранти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт, заліків та іспитів. Аспірантам також рекомендуються додаткові матеріали (відео, статті) для самостійного вивчення та аналізу.

Неформальна освіта

В рамках неформальної освіти згідно відповідного Положення (http://surl.li/pxssv), освітня компонента або її окремі теми можуть бути враховано у разі самостійного проходження професійних курсів/тренінгів, отримання громадянської освіти, онлайн освіти, професійного стажування тощо.
За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література та навчальні матеріали

Основна література

1. Cheung, C. Y. Threat Modeling Techniques [Master's Thesis]. Delft University of Technology.November 2016. http://www.safety-and-security.nl/uploads/cfsas/attachments/SPM5440%20%26%20WM0804TU%20-%20Threat%20modeling%20techniques%20-%20CY%20Cheung.pdf
2. Potteiger, B.; Martins, G.; & Koutsoukos, X. Software and attack centric integrated threat modeling for quantitative risk assessment. Pages 99-108. In Proceedings of the Symposium and Bootcamp on the

Science of Security. April 2016. DOI 10.1145/2898375.2898390. URL: https://cs.vuse.vanderbilt.edu/koutsoxd/www/Publications/p99-potteiger.pdf
3. Agrawal, A.; Ahmed, C. M.; & Chang, E. Poster: Physics-Based Attack Detection for an Insider Threat Model in a Cyber-Physical System. Pages 821-823. In Proceedings of the 2018 on Asia Conference on Computer and Communications Security. June 2018. DOI 10.1145/3196494.3201587. URL: https://dl.acm.org/doi/10.1145/3196494.3201587

Додаткова література

1. Allodi, L. & Etalle, S. Towards Realistic Threat Modeling: Attack Commodification, Irrelevant Vulnerabilities, and Unrealistic Assumptions. Pages 23-26. In Proceedings of the 2017 Workshop on Automated Decision Making for Active Cyber Defense. Conference on Computer and Communications Security. November 2017. DOI 10.1145/3140368.3140372. URL: https://arxiv.org/pdf/1801.04569
2. Shostack, A. Threat Modeling: Designing for Security. Wiley, 2014. ISBN 978-1118809990. URL: https://www.google.com.ua/books/edition/Threat_Modeling/YiHcAgAAQBAJ?hl=ru&gbpv=1&dq=Shostack,+A.+Threat+Modeling:+Designing+for+Security.+Wiley,+2014.+ISBN+978-1118809990.&printsec=frontcover
4. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. URL: http://monograph.com.ua/pctc/catalog/view/64/52/231-1
5. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p. URL: http://monograph.com.ua/pctc/catalog/view/978-617-7319-72-5/978-617-7319-72-5/746-2
6. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022. – 196 p. URL: http://monograph.com.ua/pctc/catalog/view/978-617-7319-57-2/117/419-2.

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
•практичні роботи: 20% семестрової оцінки;
•самостійна робота: 30% семестрової оцінки;
•індивідуальне завдання: 10% семестрової оцінки;
•іспит: 40% семестрової оцінки.

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D
60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Здобувач вищої освіти 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 неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту.
Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Погодження

Силабус погоджено

28.08.2024 — Завідувач кафедри
Сергій ЄВСЕЄВ

28.08.2024 — Гарант ОП
Олександр МІЛОВ