Силабус освітнього компонента
Програма навчальної дисципліни

Методи побудови постквантових криптосистем

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
Вибіркова,

Семестр
4

Мова викладання
Українська

Викладачі, розробники

ЄВСЄЄВ Сергій Петрович
serhii.yevseiev@khpi.edu.ua
Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 350, з них патентів на корисну модель 42, 17 монографій, з яких 9 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 163 статті у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Менеджмент інформаційної безпеки», «Введення в мережі», «Безпека банківських систем» , «Гібридні війни та національна безпека», «Аудит та моніторинг корпоративних мереж», «Blockchain: основи та приклади застосування», «Основи смарт-контрактів», «Основи кібербезпеки» у студентів бакалавріата та магістратури, Розділ «Методи і технології моніторингу та аудиту інформаційної безпеки», «Методи побудови постквантових криптосистем», «Новітні технології забезпечення кібербезпеки на основі технології блокчейн» для аспірантів.
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Вивчення дисципліни спрямовано на формування світогляду, розвитку інтелекту, ерудиції, формування професійних компетенцій зі спеціальності кібербезпека; оволодіння методами побудови постквантових криптосистем.

Мета та цілі дисципліни

Формування у аспірантів системи теоретичних знань і практичних навичок з основ, принципів та методів побудови, використання постквантових алгоритмів в системах захисту інформації.

Формат занять

Лекції, лабораторні роботи, самостійна робота, індивідуальне завдання, консультації.
Підсумковий контроль – залік.

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-1.Здатність до професійного спілкування іноземною мовою.
ЗК-4. Здатність працювати в міжнародному науковому просторі, розробляти та управляти науковими проектами.
СК-1. Здатність до застосування сучасних інформаційних і безпекових технологій у сфері захисту інформації, створення комплексних систем захисту інформації.
СК-3. Здатність розробляти процеси життєвого циклу інформаційних технологій, виявляти технічні канали витоку інформації, застосовувати засоби захисту інформації.
СК-5. Здатність розробляти та реалізовувати нові конкурентоздатні ідеї в галузі захисту інформації, використовувати методологічні та організаційно-технічні основи забезпечення безпеки.

Результати навчання

РН-1. Вміння формувати і аргументовано відстоювати власну думку з різних проблем філософії науки та методології наукового пізнання, бути критичним і самокритичним.
РН-2. Вміння вести дискусії, здійснювати публічні промови, робити повідомлення і доповіді з питань дисертаційного дослідження, аргументовано викладати власну точку зору державною та іноземною мовами.
РН-3. Вміння читати оригінальну наукову літературу на іноземній мові, опрацьовувати та оформляти інформацію. Вміння та навики працювати з сучасними бібліографічними і реферативними базами даних, а також наукометричними платформами (наприклад, Scopus, Web of Science, Web of Knowledge та ін.).
РН-4. Знання, розуміння, вміння та навички використання правил цитування та посилання на використані джерела, правил оформлення бібліографічного списку, розуміння змісту і порядку розрахунків основних кількісних наукометричних показників ефективності наукової діяльності (індекс цитування, індекс Гірша (h-індекс), імпакт-фактор (ІФ, або IF)).
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-9. Вміння та навички спілкуватися в діалоговому режимі з широкою науковою спільнотою та громадськістю в галузі наукової та/або професійної діяльності з метою обговорення дискусійних питань, результатів досліджень, узгодження дій і спільної роботи на конференціях, симпозіумах, наукових семінарах, доводити результати досліджень та інновацій до колег, публічно представляти, захищати результати своїх досліджень, обговорювати їх і дискутувати з науково-професійною спільнотою, використовувати сучасні засоби візуальної презентації результатів дослідження..
РН-10. Володіння предметною базою знань та сучасними техніками дослідження, здатність створювати та інтерпретувати нові знання.
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.
РН-13. Вміння узагальнювати і критично оцінювати результати, отримані вітчизняними і зарубіжними дослідниками.
РН-14. Вміння приймати обґрунтовані рішення, бути здатним їх оцінювати та забезпечувати якість виконуваних робіт.

Обсяг дисципліни

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

Передумови вивчення дисципліни (пререквізити)

Математичні методи, моделі та інформаційні технології у наукових дослідженнях. Моделювання механізмів кібербезпеки.

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. Теоретичні основи побудови постквантових алгоритмів.
Теоретичні основи квантової механіки. Побудова постквантового комп'ютера. Квантові алгоритми Гровера та Шора.
Тема 2. Математичні основи побудови постквантових алгоритмів.
Вимоги до алгоритмів постквантової криптографії.
Тема 3. Постквантові алгоритми на основі крипто-кодової конструкції Мак-Еліса.
Теоретичні вимоги, основи побудови. Аналіз енергоємності та стійкості.
Тема 4. Постквантові алгоритми на основі крипто-кодової конструкції Нідеррайтера.
Теоретичні вимоги, основи побудови. Аналіз енергоємності та стійкості.
Тема 5. Побудова гібридних постквантових алгоритмів.
Теоретичні вимоги, основи побудови. Аналіз енергоємності та стійкості.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Формування вимог до постквантових алгоритмів на основі аналізу результатів конкурсу NIST.
Тема 2. Побудова алгоритмів на основі збиткових кодів.
Тема 3. Побудова еліптичних кодів. Побудова постквантового алгоритму на основі крипто-кодової конструкції Мак-Еліса.
Тема 4. Побудова еліптичних кодів. Побудова постквантового алгоритму на основі крипто-кодової конструкції Нідеррайтера.
Тема 5. Побудова гібридних постквантових алгоритмів. Побудова постквантового алгоритму.

Самостійна робота

Самостійна робота аспіранта 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. О. О. Кузнецов, С. П. Євсеєв, та С. В. Кавун Захист інформації та економічна безпека підприємства. Монографія. Харків, Україна: Вид. ХНЕУ, 2009. URL: https://drive.google.com/file/d/16FGhHZf0CYHtJvYvmvNwbEIh9VfSkKDE/view?usp=sharing
2. 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.
3. S. Yevseiev and other “Development of Niederreiter hybrid crypto-code structure on flawed codes” Eastern-European Journal of Enterprise Technologies, 1/9 (97). p. 27 –37, 2019 URL: https://drive.google.com/file/d/168NcM_G7jTZJIohsFFAzmvzZ9sqZgCLL/view?usp=sharing
4. 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.
5. С. П. Євсеєв, О. Ю. Йохов, та О. Г. Король Гешування даних в інформаційних системах. Монографія. Харків, Україна: Вид. ХНЕУ, 2013. URL: https://drive.google.com/file/d/1JIg1YT-nIILr91t6f4xE5VGajNtPvIvb/view?usp=sharing
6. Євсеєв С.П. Кібербезпека: основи кодування та криптографії/ С.П. Євсеєв, О.В. Мілов, С.Е. Остапов, О.В. Сєвєрінов. – Харків: Вид. “Новий Світ-2000”, 2023. – 657 с. URL: https://drive.google.com/file/d/1694khGjEN1-2PvXFQY27IPPc8Sn4BsLC/view?usp=sharing.

Додаткова література

7. S. Yevseiev, H Kots, S Minukhin, O Korol, and A Kholodkova, “The development of the method of multifactor authentication based on hybrid crypto-code constructions on defective codes”, Eastern-European Journal of Enterprise Technologies, 5/9(89), с. 19 – 35, 2017 URL: https://drive.google.com/file/d/1iEx9R2mi5h_Vg2EzQHI4SIsBgo1c_tPj/view?usp=sharing
8. R. J. McEliece, “A Public-Key Criptosystem Based on Algebraic Theory”, DGN Progres Report 42-44, Jet Propulsi on Lab. Pasadena, CA. January – February, p. 114 – 116, 1978. URL: https://drive.google.com/file/d/1-NwBLsc5KXDPnhTLQ8XIKa6DBpfvEioa/view?usp=sharing
9. H. Niederreiter, “Knapsack-Type Cryptosystems and Algebraic Coding Theory”, Probl. Control and Inform. Theory, V.15, p. 19 – 34, 1986.

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
•лабораторні роботи: 20% семестрової оцінки;
•самостійна робота: 30% семестрової оцінки;
•індивідуальне завдання: 20% семестрової оцінки;
•залік: 30% 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