Силабус освітнього компонента
Програма навчальної дисципліни

Сучасні проблеми постквантової криптографії

Шифр та назва спеціальності
F5 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Спеціалізація

Кафедра
Кібербезпеки (328)

Освітня програма
Кібербезпека

Тип дисципліни
Наукова підготовка, Обов'язкова

Рівень освіти
Другий (магістерський)

Форма навчання
Денна

Семестр
2

Мова викладання
Українська

Викладачі, розробники

ЄВСЕЄВ Сергій Петрович

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

Лауреат національної премії імені Бориса Патона.
Кількість наукових публікацій: понад 351, з них патентів на корисну модель 44, 11 монографій, з яких 10 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 149 статтей у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus. Гарант освітньо-професійної програми "Кібербезпека" першого (бакалаврського) рівня вищої освіти. Провідний лектор з дисциплін: Математичні основи криптології, Комп`ютерні мережі, Основи криптографічного захисту, Методи криптоаналізу, Основи кібербезпеки, Сучасні проблеми постквантової криптографії, Основи наукових досліджень, Цифрова криміналістика, Етичний хакінг у студентів бакалавріата та магістратури, Методологія наукової та педагогічної діяльності в науках кіберзахисту для аспірантів.

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Дисципліна "Сучасні проблеми постквантової криптографії" зосереджена на вивченні методів і алгоритмів криптографії, стійких до атак з використанням квантових комп'ютерів. Курс охоплює основні концепції і проблеми, пов'язані з постквантовою криптографією, включаючи: огляд квантових комп'ютерів; класи криптографічних проблем; аналіз існуючих алгоритмів; стандартизацію та реалізацію; вивчення нових розробок у постквантовій криптографії, дослідження нових напрямків та інновацій.

Мета та цілі дисципліни

Метою дисципліни є надати студентам знання і навички, необхідні для розуміння та розробки криптографічних систем, які можуть протистояти потенційним загрозам з боку квантових комп'ютерів.

Формат занять

Лекції, лабораторні заняття, самостійна робота, консультації. Підсумковий контроль – диференційований залік.

Компетентності

КЗ-1. Здатність застосовувати знання у практичних ситуаціях.
КЗ-2. Здатність проводити дослідження на відповідному рівні.
КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу.
КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт.
КЗ–5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
КФ1. 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.
КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.
КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.
КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.
КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ11. Здатність здійснювати наукові та/або прикладні дослідження у галузі інформаційної безпеки та/або кібербезпеки із застосуванням сучасних експериментальних і теоретичних методів моделювання процесів, формувати науково-технічну звітність.

Результати навчання

РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.
РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
РН5. 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.
РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.
РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.
РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.
РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.
РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.

РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.
РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.
РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.
РН24. Планувати та виконувати наукові та прикладні дослідження у сфері інформаційної безпеки та/або кібербезпеки із застосуванням сучасних технологій, експериментальних і теоретичних методів і моделей теорії прийняття рішень, системного аналізу, оптимізації процесів, математичної статистики.
РН25. Оцінювати ефективність та практичну цінність результатів наукових і практичних досліджень та інновацій.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 16 год., практичні роботи – 32 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Аналіз шкідливих програм, Алгоритми та структури даних, Основи криптографічного захисту.

Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проєкти, майстер-класи.

Програма навчальної дисципліни

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Основи постквантової криптографії. Основи постквантової криптографії. Вплив квантових комп'ютерів на традиційну криптографію.	2
Тема 2. Постквантові алгоритми на основі крипто-кодових конструкцій Мак-Еліса та Нідеррайтера. Гібридні системи захисту на збиткових кодах. Слабкі та квантовостойкі традиційні геші і шифри у підквантовому світі.	2
Тема 3. Криптографічні задачі та стійкість до квантових атак. Проблема факторизації та її квантові аналоги. Проблема дискретного логарифму та квантові атаки.	2
Тема 4. Многократне виділення та інші алгоритми.	2

Огляд многократного виділення як підходу до постквантової криптографії. Розгляд інших інноваційних алгоритмів.	
Тема 5. Оцінка безпеки постквантових алгоритмів. Методи оцінки безпеки постквантових алгоритмів. Порівняння стійкості різних алгоритмів.	2
Тема 6. Стандартизація постквантових криптографічних алгоритмів. Процес стандартизації постквантових алгоритмів. Виклики та переваги стандартизації.	2
Тема 7. Реалізація постквантових криптографічних систем. Практичні аспекти впровадження постквантових алгоритмів. Інтеграція постквантової криптографії в існуючі системи.	2
Тема 8. Перспективи розвитку та нові напрямки. Огляд нових напрямків у постквантовій криптографії. Прогнози та майбутні тренди.	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Квантові алгоритми. Ознайомлення з основними поняттями і властивостями квантових систем, найпростіші квантові алгоритми: квантова монетка, Дойча-Йоші, побудова оракула і визначення типу функцій.	4	0,1
Тема 2. Квантовий протокол. Розподілення ключа BB84. Ознайомлення з квантовим протоколом розподілу ключа BB84 і досліджування його роботи.	4	0,1
Тема 3. Алгоритм Саймона. Вивчення алгоритму Саймона, отримання навичок визначення типу функції за допомогою даного алгоритму.	4	0,1
Тема 4. Алгоритм Шора. Вивчити алгоритму Шора, отримання навичок визначення періоду функції і факторизації чисел.	4	0,1
Тема 5. Верифікація криптографічних алгоритмів. Тестування алгоритмів на предмет коректності та безпекових вразливостей.	4	0,1
Тема 6. Стандартизація та інтеграція постквантових алгоритмів. Розробка та тестування прикладів постквантових алгоритмів, що відповідають стандартам.	4	0,1
Тема 7. Моделювання атаки на криптографічну систему. Моделювання потенційних атак на постквантові криптографічні алгоритми та аналіз їх ефективності.	4	0,1

Тема 8. Використання квантових комп'ютерів у криптографії. Розробка простих квантових алгоритмів для симуляції атаки на криптографічні системи.	4	0,1
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 0{,}8$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Основи постквантової криптографії. Розглядаються фундаментальні принципи постквантової криптографії, її відмінності від класичної криптографії та вплив розвитку квантових комп'ютерів на сучасні криптографічні системи.	0,1
Тема 2. Постквантові алгоритми на основі криптокодових конструкцій Мак-Еліса та Нідеррайтера. Гібридні системи захисту. Вивчаються принципи побудови постквантових криптосистем на базі кодових конструкцій, особливості алгоритмів Мак-Еліса і Нідеррайтера, а також підходи до створення гібридних систем захисту та аналіз їхньої стійкості у квантових умовах.	0,1
Загалом	$\sum_{i=1}^{m} b_i = 0{,}2$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин
Тема 1. Квантові обчислення та принципи дії квантових комп'ютерів Розглядаються основи квантової механіки, кубіти, суперпозиція, заплутаність і квантові логічні елементи, що лежать в основі квантових обчислень.	8
Тема 2. Алгоритми Шора та Гровера: вплив на сучасну криптографію Аналізуються ключові квантові алгоритми, здатні зруйнувати класичні криптографічні схеми (RSA, ECC), та оцінюється їх практичний вплив.	8
Тема 3. Алгебраїчні основи постквантових криптосистем Вивчаються математичні структури (решітки, коди, багатовимірні поліноми), що використовуються в постквантових алгоритмах.	7
Тема 4. Криптосистеми на основі решіток (Lattice-based cryptography) Розглядаються принципи побудови решіткових криптосистем (NTRU, Kyber, Dilithium) та їхня квантова стійкість.	7
Тема 5. Многочленні та геш-функційні постквантові алгоритми Досліджуються системи на основі багаточленних перетворень і хеш-функцій (SPHINCS+, Rainbow), їхні переваги та обмеження.	7
Тема 6. Ізогенійна криптографія Вивчаються криптографічні системи, побудовані на ізогеніях еліптичних кривих	7

(SIKE, CSIDH), їх стійкість і сфери застосування.	
Тема 7. Гібридні криптосистеми у перехідний період до постквантової ери Ознайомлення з комбінованими схемами, що поєднують класичні та постквантові алгоритми для поступового переходу до нових стандартів безпеки.	7
Тема 8. Стандартизація постквантової криптографії (NIST PQC) Вивчається процес стандартизації постквантових алгоритмів NIST, основні фіналісти, критерії відбору та перспективи впровадження.	7
Тема 9. Реалізація постквантових алгоритмів у протоколах TLS/SSL Розглядаються приклади інтеграції постквантових алгоритмів у сучасні протоколи безпечної передачі даних, їх ефективність і сумісність.	7
Тема 10. Перспективи розвитку постквантових технологій у кібербезпеці Аналізуються поточні тенденції, напрями наукових досліджень та можливі сценарії еволюції постквантових систем захисту інформації.	7
Загальна кількість годин	**72**

Неформальна освіта

Здобувач має можливість перезарахувати окремі теми або курс шляхом: проходження професійних курсів чи тренінгів, онлайн-освіти, професійних стажувань, у сфері, що відповідає навчальним цілям дисципліни.
Для зарахування необхідно надати: сертифікат (електронний або друкований) про проходження курсу/стажування, опис програми тренінгу із зазначенням змісту тем, обсягу та тривалості.

Рекомендовані курси, тренінги, стажування

1. За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. A RIDDLE WRAPPED IN AN ENIGMA. NEAL KOBLITZ AND ALFRED J. MENEZES Department of Mathematics, Box 354350, University of Washington, Seattle, WA 98195 U.S.A URL: https://eprint.iacr.org/2015/1018.pdf
2. Lili Chen, Stephen Jordan, Yi-Kai-Liu, Dustin Moody, Rene Peralta, Ray Perlner, Daniel Smith-Tone. Report on Post – Quatum Cryptography. NISTIR 8105 (DRAFT). URL: https://www.google.com.ua/search?
3. Shor, P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer / P. W. Shor // SIAM J. Comput. – 1997. – 26 (5). – P. 1484–1509. URL: https://fab.cba.mit.edu/classes/862.19/notes/computation/Shor-1999.pdf
4. Аналіз можливостей квантових комп'ютерів та квантових обчислень для криптоаналізу сучасних криптосистем / Ю. І. Горбенко, Р. С. Ганзя // Восточно-Европейский журнал передовых технологий. - 2014. - № 1(9). - С. 8-16. - Режим доступу: http://nbuv.gov.ua/UJRN/Vejpte_2014_1%289%29__3
5. М. Рябий // Безпека інформації. - 2014. - Т. 20, № 3. - С. 236-241. - Режим доступу: http://nbuv.gov.ua/UJRN/bezin_2014_20_3_6

Додаткова література

1. Moody D. Post-Quntum Cryptography: NIST's Plan for the Future. The Seventh International Conference on Post-Quntum Cryptography, Japan, 2016. Режим доступу: https://pqcrypto2016.jp/data/pqc2016_nist_announcement.pdf.

7. Євсеєв С.П. КІБЕРБЕЗПЕКА: КРИПТОГРАФІЯ З PYTHON: навч. посібн. / С.П. Євсеєв, О.В. Шматко, О.Г. Король – Харків: Видавництво «Новий Світ – 2000», 2021. –120 с. https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
8. Євсєєв 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. https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
9. Євсеєв С.П. КІБЕРБЕЗПЕКА: ЛАБОРАТОРНИЙ ПРАКТИКУМ З ОСНОВ КРИПОГРАФІЧНОГО ЗАХИСТУ / С.П. Євсеєв, О.В. Мілов, О.Г. Король – Львів: «Новий Світ- 2000», 2020 . – 241 с. https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju

Система оцінювання

Підсумкова оцінка з освітнього компонента визначається відповідальним лектором за темами, видами занять, тощо у відповідності до силабусу і є інтегральною оцінкою результатів усіх вид навчальної діяльності здобувача вищої освіти. Підсумкова оцінка повинна відображати всі оцінки за складовими навчального процесу з урахуванням їх вагових показників k:

Поточний контроль (практичні, семінарські, лабораторні заняття), k_1	Контрольні роботи (за наявності), k_2	Індивідуальне завдання (за наявності), k_3	Підсумковий контроль (для ОК з іспитом), k_4
0,8	0,2		

Сума коефіцієнтів повинна складати одиницю: $k_1 + k_2 + k_3 + k_4 = 1$. Підбір вагових коефіцієнтів підсумкової оцінки здійснює розробник курсу.
Розрахунок підсумкової оцінки проводиться за формулою:

$$О = П \cdot k_1 + K \cdot k_2 + І \cdot k_3 + Пк \cdot k_4$$

де: П – середньозважена середня оцінка за поточний контроль
І – оцінка за виконання індивідуального завдання
K – середньозважена оцінка за контрольні роботи
Пк – оцінка за підсумковий контроль

$$П = \frac{П_1 \cdot a_1 + П_2 \cdot a_2 + ... + П_n \cdot a_n}{\sum_{i=1}^{n} a_i}$$

де: a_i - ваговий коефіцієнт за кожне практичне (семінарське) або лабораторне заняття.

$$K = \frac{K_1 \cdot b_1 + K_2 \cdot b_2 + ... + K_m \cdot b_m}{\sum_{i=1}^{m} b_i}$$

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (П, K, І,...) виставляються за 100-бальною шкалою згідно з положенням «Про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої освіти» НТУ «ХПІ».

Підсумкова оцінка виставляється відповідно до розрахованої О з округленням до найближчого цілого числа в більшу сторону.

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	FX

	вивчення)	
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	30.08.2025		**Завідувач кафедри** Сергій ЄВСЕЄВ
	30.08.2025		**Гарант ОП** Станіслав МІЛЕВСЬКИЙ