Силабус освітнього компонента
Програма навчальної дисципліни

Комплексний тренінг «Криптографія та криптоаналіз»

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
Професійна підготовка, Вибіркова

Рівень освіти
Другий (магістерський)

Форма навчання
Денна

Семестр
3

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

Навчальна дисципліна "Комплексний тренінг «Криптографія та криптоаналіз»" є вибірковою навчальною дисципліною. Дисципліна включає принципи, засоби і математичні методи перетворення інформації, з метою приховування сенсу або структури даних, а також для захисту інформації від несанкціонованого використання або підробки. Криптологія традиційно поділяється на криптографію і криптоаналіз. Побудова сучасної криптології як науки грунтується на сукупності фундаментальних понять математики, фізики, теорії інформації. Методи криптографії орієнтовані на створення систем захисту інформації.

Мета та цілі дисципліни

Ознайомлення з теоретичними основами криптології; придбання навичок в практичному використанні, постановці і вирішенні задач шифрування інформації; розуміння суті інформаційних процесів в криптографічних системах; застосування комп'ютерів для вирішення завдань шифрування і дешифрування; розробка і використання математичних і обчислювальних моделей процесів шифрування інформації, їх оптимізація та вироблення напрямків вдосконалення.

Формат занять

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

Компетентності

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.
КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.
КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.

Результати навчання

РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
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.
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.
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.

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)

Математичні основи криптології, Основи криптографічного захисту, Сучасні методи програмування.

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. Вступ до криптографічних методів захисту. Розглядаються основи криптографії, її роль у забезпеченні інформаційної безпеки, базові принципи шифрування та дешифрування, класифікація криптосистем і сфери їх застосування.	2

Тема 2. Диференціальний і лінійний криптоаналіз. Вивчаються методи аналізу симетричних шифрів, принципи побудови атак на блокові шифри, особливості пошуку залежностей між вхідними та вихідними даними.	2
Тема 3. Традиційне шифрування: алгоритми "потрійний" DES. Алгоритм RSA. Аналізуються принципи роботи DES і Triple DES, архітектура алгоритму RSA, генерація ключів, процеси шифрування та розшифрування.	2
Тема 4. Криптографія з використанням еліптичних кривих. Описуються математичні основи еліптичних кривих, їх використання у створенні стійких криптосистем та переваги над класичними алгоритмами з відкритим ключем.	2
Тема 5. Традиційне шифрування і конфіденційність. Розглядаються властивості симетричних шифрів, методи забезпечення конфіденційності даних та способи оцінки криптостійкості алгоритмів.	2
Тема 6. Розподіл ключів. Вивчаються протоколи обміну ключами (зокрема, алгоритм Діффі-Хеллмана), методи захисту від перехоплення та модифікації ключів, роль центрів сертифікації.	2
Тема 7. Криптографія з відкритим ключем. Управління ключами. Описуються принципи криптографічних систем з відкритим ключем, методи управління, зберігання та ротації ключів, інфраструктура відкритих ключів (PKI).	2
Тема 8. Цифрові підписи і протоколи аутентифікації. Вивчаються механізми створення та перевірки цифрових підписів, методи забезпечення цілісності та невідмовності, а також сучасні протоколи аутентифікації користувачів.	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Блокові симетричні шифри. Лабораторна робота передбачає ознайомлення з принципами роботи блокових симетричних шифрів, таких як DES та AES, практичне шифрування та дешифрування повідомлень, аналіз ефективності та безпеки алгоритмів.	8	0,2
Тема 2. Асиметричні криптосистеми. В роботі студенти досліджують принципи асиметричного шифрування, зокрема алгоритми RSA та ElGamal, реалізують шифрування та дешифрування, а також оцінюють стійкість систем до криптоаналітичних атак.	6	0,2
Тема 3. «Pretty Good Privacy» (PGP). Лабораторна робота зосереджена на використанні PGP для забезпечення конфіденційності та цілісності електронної	6	0,2

кореспонденції, генерації ключів, цифрових підписів та шифрування/дешифрування повідомлень.		
Тема 4. Стеганографічні методи захисту інформації. Студенти вивчають методи прихованого передавання інформації в цифрових носіях, досліджують інструменти для стеганографії та аналізують безпеку цих методів.	6	0,1
Тема 5. Алгоритм RSA. Лабораторна робота передбачає детальне вивчення алгоритму RSA, його математичної основи та практичного застосування для шифрування, дешифрування та створення цифрових підписів.	6	0,1
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 0{,}8$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Симетричне та асиметричне шифрування: алгоритми, аналіз і практичне застосування. Контрольна робота передбачає вивчення принципів роботи симетричних і асиметричних криптосистем, аналіз їхньої стійкості до атак, порівняння ефективності та практичне застосування у захисті конфіденційної інформації. Студенти демонструють знання алгоритмів AES, DES, RSA, ElGamal та інших, а також вміння шифрувати та дешифрувати дані в навчальних прикладах.	0,1
Тема 2. Криптографічні протоколи та цифрові підписи: захист інформації та управління ключами. Контрольна робота охоплює вивчення криптографічних протоколів обміну даними та методів цифрового підпису, їх застосування для забезпечення автентичності, цілісності та конфіденційності інформації. Студенти аналізують алгоритми підпису, протоколи генерації та обміну ключами, а також демонструють практичні навички реалізації протоколів у навчальних сценаріях.	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. Сучасні симетричні шифри. AES, Camellia, Blowfish; принципи роботи, переваги та недоліки, сфери застосування.	8
Тема 2. Сучасні асиметричні алгоритми. ElGamal, ECC, Diffie-Hellman; порівняння стійкості та ефективності.	8
Тема 3. Методи криптоаналізу сучасних алгоритмів. Аналіз стійкості до диференційного та лінійного криптоаналізу.	7

Тема 4. Цифрові підписи та електронні сертифікати. Структура, алгоритми генерації та перевірки, застосування у PKI.	7
Тема 5. Протоколи обміну ключами. Diffie-Hellman, Kerberos, протоколи на базі асиметричної криптографії.	7
Тема 6. Гомоморфне шифрування. Принципи роботи, практичні застосування, переваги для безпечної обробки даних.	7
Тема 7. Квантова криптографія та постквантові алгоритми. Основні концепції, стійкість до квантових атак.	7
Тема 8. Криптографічні геш-функції та їх використання. SHA-2, SHA-3, BLAKE2; застосування для перевірки цілісності даних.	7
Тема 9. Атаки на криптографічні системи. Side-channel attacks, brute-force, timing attacks; способи захисту.	7
Тема 10. Застосування криптографії у сучасних інформаційних системах. Blockchain, IoT, захист хмарних сервісів, електронна комерція.	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. 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. [Електронний ресурс]. – Режим доступу : https://acrobat.adobe.com/id/urn%3Aaaid%3Asc%3AEU%3A3c427761-01ab-4365-88f6-37f76ca508c5/?x_api_client_id=chrome_extension_viewer&bookmarkAcrobat=true&x_api_client_location=bookmark&filetype=application%2Fpdf&viewer%21megaVerb=group-discover
2. 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. [Електронний ресурс]. – Режим доступу : http://library.hneu.edu.ua/storage/new-arrivals-books/December2020/.pdf2.pdf
3. Остапов С. Е. Основи криптографії: навчальний посібник / С. Е. Остапов, Л. О. Валь. – Чернівці: Книги–ХХІ, 2008. – 188 с. [Електронний ресурс]. – Режим доступу : https://ru.scribd.com/document/678969380/%D0%9E%D1%81%D1%82%D0%B0%D0%BF%D0%BE%D0%B2-%D0%A1-%D0%95-%D0%92%D0%B0%D0%BB%D1%8C-%D0%9B-%

D 0 % 9 E - % D 0 % 9 E % D 1 % 8 1 % D 0 % B D % D 0 % B E % D 0 % B 2 % D 0 % B 8 - % D 0 % 9 A % D 1 % 8 0 % D 0 %B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97-2009
4. Oleshchuk V. A. On Public-Key Cryptosystem Based on Church-Rosser String-Rewriting Systems // Computing and Combinatorics: First Annual International Conference, COCOON '95. — Springer, 1995. — С. 264–269. [Електронний ресурс]. – Режим доступу : https://eprint.iacr.org/2004/220.pdf
5. Вербіцький О. В. Вступ до криптології. — Л. : ВНТЛ, 1998. — 248 с. [Електронний ресурс]. – Режим доступу : https://www.twirpx.com/file/593876/.

Додаткова література

6. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. [Електронний ресурс]. – Режим доступу : https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
7. 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. [Електронний ресурс]. – Режим доступу : https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
8. 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. [Електронний ресурс]. – Режим доступу : 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 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 30.08.2025 **Завідувач кафедри** Сергій ЄВСЕЄВ

30.08.2025 **Гарант ОП** Станіслав МІЛЕВСЬКИЙ