



Силабус освітнього компонента Програма навчальної дисципліни



Основи криптографічного захисту

Шифр та назва спеціальності

256 – Національна безпека (за окремими сферами забезпечення і видами діяльності)

Інститут

ННІ комп'ютерних наук та інформаційних технологій (320)

Освітня програма

Національна безпека у сфері кіберзахисту

Кафедра

Кібербезпеки (328)

Рівень освіти

Бакалавр

Тип дисципліни

Спеціальна (фахова), Обов'язкова

Семестр

4

Мова викладання

Українська

Викладачі, розробники



ЄВСЕЄВ Сергій Петрович

serhii.yevseiev@khu.edu.ua

Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХП».

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

Навчальна дисципліна "Основи криптографічного захисту" є обов'язковою навчальною дисципліною. Дисципліна спрямована на вивчення симетричних та асиметричних методів шифрування інформації, їх використання; видів криптоаналізу та можливість його застосування.

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 роботи, самостійна робота, консультації. Підсумковий контроль – залік.

Компетентності

КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу.

КЗ-4. Здатність спілкуватися державною мовою як усно, так і письмово.

КЗ-7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ФК-1. Здатність використовувати безпекові режими під час виконання службових обов'язків.

ФК-8. Здатність використовувати механізми забезпечення національної безпеки у її визначальних сферах.

ФК-11. Здатність використовувати практичні навички, тактику та прийоми роботи з людьми в інтересах службової діяльності.

Результати навчання

ПРН-3. Вміти за допомогою абстрактного мислення, аналізу та синтезу оцінювати результати професійної діяльності та забезпечувати її якість, бути критичним і самокритичним, наполегливим щодо поставлених завдань і взятих зобов'язань.

ПРН-4. Вільно спілкуватися державною мовою.

ПРН-7. Вміти виявляти, ставити та вирішувати професійні завдання, вміти узагальнювати отримані результати, обробляти та аналізувати інформацію з різних джерел, оформлювати і презентувати результати досліджень відповідно до вимог.

ПРН-8. Вміти використовувати інформаційні та комунікаційні технології і на цій основі формувати ефективні системи інформаційно-аналітичного забезпечення підтримки прийняття рішень щодо запобігання, протидії та нейтралізації загроз національній безпеці.

ПРН-9. Вміти використовувати безпекові режими під час виконання службових обов'язків.

ПРН-10. Вміти аналізувати виклики та загрози національній безпеці за напрямками професійної діяльності та синтезувати інформацію щодо розроблення та реалізації стратегій у визначальних сферах національної безпеки (політичній, економічній, соціальній, гуманітарній).

ПРН-12. Вміти застосовувати знання з основ теорії національної безпеки, зокрема: оцінювати обстановку, рівень викликів та загроз національній безпеці.

ПРН-16. Використовувати у професійній діяльності окремі елементи механізму впливу та взаємодії у процесі забезпечення окремих складових національної безпеки.

ПРН-17. Вміти використовувати отримані знання щодо безпекової складової зовнішньої політики України та інших держав.

ПРН-18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.

ПРН-19. Вміти використовувати у професійній діяльності методи та інструменти організації соціальної взаємодії, співробітництва та розв'язання конфліктів у сфері професійної діяльності, практичні навички, тактику та прийоми, роботи з людьми в інтересах службової діяльності: працювати у команді з позицій лідера, радника (консультанта), помічника, планувати використання часу та визначати стимули і бар'єри ефективної роботи, здійснювати розподіл (делегування) функцій, повноважень і відповідальності між виконавцями.

Обсяг дисципліни

Загальний обсяг дисципліни 150 год. (5 кредитів ECTS): лекції – 32 год., лабораторні роботи – 32 год., самостійна робота – 86 год.

Передумови вивчення дисципліни (пререквізити)

Математичні основи криптології, Вища математика (спеціальні глави).

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 проекти, майстер-класи.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Теоретичні основи захисту інформації.

Основні поняття. Моделі секретних систем. Основні завдання системи безпеки. Симетричні та несиметричні криптосистеми. Режими роботи симетричних криптосистем.

Тема 2. Протоколи автентичності. Цифровий підпис.

Механізми автентичності. Класифікація цифрового підпису. Методи гешування. Механізми автентифікації на основі використання програмно-апаратних засобів. Автентифікація Kerberos.

Тема 3. Протоколи суворої автентифікації.

Класифікація методів 2 FA. Рівні достовірності автентифікації. Загрози на 2 FA. Двофакторна автентифікація в Linux.

Тема 4. Система PGP.

Основні функції системи. Класифікація ключів. Механізми забезпечення автентичності та конфіденційності. Система довіри.

Тема 5. Основи технології PKI.

Основні функції та склад технології. Фізична та логічна топологія. Криптоперіод. Основні механізми технології на основі симетричних та несиметричних криптосистем.

Тема 6. Протоколи цілісності SSL, TLS.

Взаємозв'язок об'єктів критичної інфраструктури з кіберфізичними системами. Структура протоколів SSL, TLS. Функції протоколу SSL. АТАКИ НА SSL/TLS.

Тема 7. Основи постквантової криптографії.

Основні поняття. Основа квантових обчислень. Основні алгоритми квантового криптоаналізу.

Тема 8. Основи теорій інформації та кодування.

Загальна структура системи зв'язку. Моделі двійкового симетричного каналу без пам'яті. Ефективне кодування Хаффмана. Корекція та винахід помилок. Класифікація двійкових кодів. Основні поняття теорії перешкодостійкого кодування. Поля Галуа. Структура кінцевих полів їх властивості. Коди Боуза-Чоудхурі-Хоквінгему.

Тема 9. Основи розкодування.

Алгоритм Берлекемпа-Месі. Приклад.

Тема 10. Постквантові алгоритми на основі крипто-кодових конструкцій Мак-Еліса і Нідеррайтера. Гібридні системи захисту на збиткових кодах.

Класифікація крипто-кодових конструкцій. Еліптичні криві. Основи побудови (формування ключових матриць, формування криптограми). Оцінка стійкості. Шляхи зменшення ємності ключових даних. Формування крипто-кодових конструкцій на алгеброгеометричних (еліптичних) кодах. Основи криптографії на збиткових кодах. Формування гібридних крипто-кодових конструкцій.

Тема 11. Потоків симетричні криптосистеми.

Симетричні криптосистеми. Потоків шифр RC-4. Стійкість. Ініціалізація S-блоку. Потоків шифр PRC-4A. Потоків шифр STRUMOK. Потоків шифр SNOW2.0.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Найпростіші шифри.

Тема 2. Дослідження властивостей режимів роботи блокових шифрів.

Тема 3. Дослідження протоколів автентичності та конфіденційності за допомогою RSA.

Тема 4. Дослідження протоколів цифрового підпису.

Тема 5. Дослідження протоколів системи PGP.

Тема 6. Стеганографічні методи захисту інформації.

Тема 7. Методика NIST STS оцінки статистичних властивостей криптографічних алгоритмів.

Тема 8. Побудова циклічних кодів.

Тема 9. Робота з кубітами. Емуляція вимірювань.

Самостійна робота

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи студенти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт, заліків та іспитів. Студентам 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. Євсєєв С.П. Кібербезпека: сучасні технології захисту. / Євсєєв С.П, Остапов С.Е., Король О.Г. // Навчальний посібник для студентів вищих навчальних закладів. Львів: "Новий Світ- 2000", 2019. – 678. – Режим доступу: <http://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnologii-zakhystu.pdf>.
2. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с.
<http://kist.ntu.edu.ua/textPhD/tzi.pdf>.
3. Bonaventure O. Computer Networking: Principles, Protocols and Practice. - Louvain-la-Neuve: Universite catholique de Louvain (Belgium), 2019. - 272 p.
<https://resources.saylor.org/wwwresources/archived/site/wp-content/uploads/2012/02/Computer-Networking-Principles-Bonaventure-1-30-31-OTC1.pdf>.
4. Євсєєв С.П. Кібербезпека: основи кодування та криптографії/ С.П. Євсєєв, О.В. Мілов, С.Е. Остапов, О.В. Северінов. – Харків: Вид. "Новий Світ-2000", 2023. – 657 с.
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
5. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с.
<http://kist.ntu.edu.ua/textPhD/tzi.pdf>

Додаткова література :

6. Євсєєв С.П. КІБЕРБЕЗПЕКА: ЛАБОРАТОРНИЙ ПРАКТИКУМ З ОСНОВ КРИПТОГРАФІЧНОГО ЗАХИСТУ / С.П. Євсєєв, О.В. Мілов, О.Г. Король – Львів: «Новий Світ- 2000», 2020. – 241 с.
<http://library.hneu.edu.ua/storage/new-arrivals-books/December2020/Yevseiev.pdf>
7. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, F. Vercauteren. Handbook of elliptic and hyperelliptic curve cryptography// Kenneth H. Rosen Ed. 2006. 843 p.
<https://blkcipher.pl/assets/pdfs/Handbook of Elliptic and Hyperelliptic Curve Cryptography.pdf>
8. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. URL:
https://www.researchgate.net/publication/352013398_Synergy_of_building_cybersecurity_systems_Monograph.

9. A. Rukhin, J. Soto. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22, 2000
<https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-22r1a.pdf>.

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:

- лабораторні роботи: 40% семестрової оцінки;
- самостійна робота: 10% семестрової оцінки;
- контрольна робота: 10% семестрової оцінки;
- залік: 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

Студент 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

Андрій ТКАЧОВ