Силабус освітнього компонента
Програма навчальної дисципліни

Комплексні системи захисту інформації

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
Обов'язкова

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна, заочна

Семестр
7

Мова викладання
Українська, англійська

Викладачі, розробники

КОРОЛЬОВ Роман Володимирович

korolevrv01@ukr.net
Кандидат технічних наук, доцент, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 40, з яких 1 навчальний посібник, 23 статті у закордонних виданнях та фахових виданнях України, 10 патентів на корисну модель. Провідний лектор з дисциплін: «Фізичні основи технічних засобів розвідки», «Основи стеганографічного захисту інформації», «Корпоративні мережі та системи доступу» , «Безпека та аудит бездротових та рухомих мереж», гарант освітньо-професійної програми "Управління інформаційною безпекою" першого (бакалаврського) рівня вищої освіти.

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Комплексні системи захисту інформації" є обов`язковою навчальною дисципліною. Дисципліна спрямована на придбання навичок з захисту інформації в інформаційно-комунікаційних системах від витоку інформації по технічними каналами зв’язку, порядку проведення обстеження середовищ функціонування інформаційно телекомунікаційних систем.

Мета та цілі дисципліни

Освоєння студентами принципів побудови комплексних систем захисту інформації на основі синтезу організаційних і технічних заходів щодо забезпечення захисту інформації з обмеженим доступом, основ ведення електронного документообігу в умовах сучасних кіберзагроз та витоку технічними каналами, забезпечення захисту інформації від несанкціонованого доступу на основі вимог міжнародних стандартів з інформаційної безпеки, державних нормативних документів з технології захисту інформації.

Формат занять

Лекції, лабораторні роботи, самостійна робота, консультації. Підсумковий контроль – іспит.

Компетентності

ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.
ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово.
ЗК8. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації
СК2. Здатність використовувати інформаційні технологій, сучасні методи і моделей кібербезпеки та систем захисту інформації.
СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.
СК4. Здатність забезпечувати захист інформації в інформаційних системах згідно встановленої політики кібербезпеки та захисту інформації.
СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо).
СК9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.

Результати навчання

РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.
РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.
РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.
РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення та передачі сигналів тощо, принципи, методи і поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.
РН9. Вміти застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
РН10. Вміти використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

РН11. Планувати підготовку та забезпечувати неперервність процесів в організаціях згідно встановленої політики кібербезпеки та з урахування вимог до захисту інформації.
РН12. Застосовувати методи захисту інформації в інформаційних системах згідно встановленої політики інформаційної безпеки.
РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних та програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних систем та\або інфраструктури організації в цілому.
РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.
РН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування та контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.

Обсяг дисципліни

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

Передумови вивчення дисципліни (пререквізити)

Безпека в інформаційно-комунікаційних системах.

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. Нормативно-правове забезпечення організації захисту інформації на об'єктах інформаційної діяльності. Основні поняття у галузі кібербезпеки, принципи та складові національних інтересів у сфері кібербезпеки.	2
Тема 2 Захист інформації в інформаційно-комунікаційних системах від витоку технічними каналами. Технічний канал витоку інформації (ТКВІ) і чому він є загрозою для інформаційно-комунікаційних систем. Основні типи загроз інформаційній безпеці в інформаційно-комунікаційних системах та телекомунікаційних мережах. Роль технічного захисту інформації в загальній системі інформаційної безпеки.	2
Тема 3. Концепція інформаційної безпеки. Основні концептуальні положення системи захисту інформації. Види забезпечення системи захисту інформації. Класифікація загроз.	2
Тема 4. Основні поняття та визначення комплексного захисту інформації. Основні визначення інформації та її захисту відповідно до Закону України "Про	2

інформацію". Види власної інформації у підприємця. Цілі та завдання створення комплексної системи захисту інформації. Об'єкти захисту в інформаційно-телеконікаційній системі.	
Тема 5. Правові підстави та основні положення щодо створення КСЗІ та комплексу ТЗІ в Україні. Структура законодавства України в області захисту інформації. Основні положення правових норм щодо створення КСЗІ та комплексів ТЗІ інформації.	2
Тема 6. Методи, засоби та заходи захисту інформації в ІТС від НСД. Несанкціонований доступ до інформації і способи його здійснення. Основні методи реалізації загроз НСД. Градації доступу до інформації. Аналіз загроз корпоративних мереж. Уразливості і загрози безпровідних мереж. Тенденції розвитку IT-загроз. Модель порушника. Основні принципи реалізації програмно-технічних засобів захисту інформації в ІТС від НСД.	4
Тема 7. Методи, засоби та заходи захисту інформації в ІТС від витоку та руйнування технічними каналами. Класифікація техничних каналів витоку інформації. Класифікація способів прихованого відеоспостереження і зйомки. Причини створення акустичних каналів витоку інформації. Класифікація технічних каналів витоку акустичної інформації. Допоміжні технічні засоби і системи. Об'єкт інформатизації, як об'єкт розвідки. Схема технічного каналу витоку інформації в технічних засобах обробки інформації.	2
Тема 8. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. НД ТЗІ 1.1-005-07. Проведення організаційних, інженерних і технічних заходів на ОІД під час створення комплексу ТЗІ. Державні будівельні норми України ДБН А.2.2-2-96. Основні заходи щодо організації створення комплексу ТЗІ.	4
Тема 9. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації. НД ТЗІ 3.3-001-07. Порядок розроблення пояснювальної записки з ТЗІ. Порядок розроблення та оформлення паспорта на комплекс ТЗІ.	2
Тема 10. Створення комплексів технічного захисту інформації. Атестація комплексів. НД ТЗІ 2.1-001-2001. Атестація комплексу ТЗІ. Етапи атестації. Суб'єкти атестації.	2
Тема 11. Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення. НД ТЗІ 2.1-002-07. Етап «випробування та атестація комплексу ТЗІ». Висновки за результатах випробувань комплексу ТЗІ. Порядок розроблення та оформлення програм і методик випробувань.	4
Тема 12. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 2.5-004-99. Побудова і структура критеріїв захищеності інформації. Довірча конфіденційність. Адміністративна конфіденційність. Критерії конфіденційності.	2
Тема 13. Етапи побудови КСЗІ. НД ТЗІ 3.7-003 -2005. Обґрунтування необхідності створення КСЗІ. Обстеження середовищ функціонування ІТС. Формування завдання на створення КСЗІ. Розробка політики безпеки інформації в ІТС.	2
Загальна кількість годин	**32**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Kali Linux: встановлення, налаштування, розгляд основних інструментів безпеки. Вивчення основних інструментів безпеки які входять до операційної системи Kali Linux.	4	0,1
Тема 2. Дослідження стійкості точок доступу бездротової мережі Wi-Fi. Дослідження стійкості паролів точок доступу бездротової мережі WiFi за рахунок використання основних інструментів безпеки які входять до операційної системи Kali Linux.	4	0,1
Тема 3.Створення словників для дослідження стійкості точок доступу бездротової мережі Wi-Fi. Використання основних інструментів безпеки які входять до операційної системи Kali Linux для створення словників для дослідження стійкості точок доступу бездротової мережі Wi-Fi.	4	0,1
Тема 4. Обстеження об'єкту інформаційної діяльності. Розробка "Акту обстеження об'єкту інформаційної діяльності"	4	0,1
Загальна кількість годин	**16**	$\sum_{i=1}^{n} a_i = 0{,}4$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Основні поняття та визначення комплексного захисту інформації. Основні визначення інформації та її захисту відповідно до Закону України "Про інформацію".	0,2
Загалом	$\sum_{i=1}^{m} b_i$=0,2

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріал

Теми для самостійного вивчення	Кількість годин
Тема 1. Основи інформаційної безпеки. Які основні принципи комплексного захисту інформації в автоматизованих системах. Як класифікуються рівні захисту інформації за стандартами ДСТУ 4145-2002.	8
Тема 2. Криптографічні основи захисту Опишіть симетричні алгоритми шифрування (наприклад, AES) та їх застосування. Яка роль асиметричних алгоритмів (RSA) у цифрових підписах.	8
Тема 3. Захист від несанкціонованого доступу. Назвіть методи аутентифікації (паролі, біометрія) та їх вразливості. Як функціонують системи контролю доступу (RBAC, ABAC).	8
Тема 4. Виявлення та запобігання вторгненням.	8

Опишіть принципи роботи систем IDS/IPS у мережах. Які етапи реагування на інциденти безпеки (Incident Response).	
Тема 5. Захист технічними каналами витоку. Назвіть типи технічних каналів (акустичні, електромагнітні) та методи блокування. Як застосовуються пасивні методи захисту (екранування).	8
Тема 6. Організаційні заходи захисту. Які політики безпеки (політика паролів, аудит) є ключовими в комплексних системах. Як проводити оцінку ризиків інформації (методологія OCTAVE).	8
Тема 7. Фізичний та мережевий захист. Опишіть засоби фізичного захисту (контроль доступу до приміщень). Які протоколи шифрування трафіку (IPSec, SSL/TLS) у мережах.	6
Тема 8. Захист від шкідливого ПЗ. Назвіть типи шкідливого програмного забезпечення (віруси, трояни) та антивірусні стратегії. Як застосовуються системи виявлення аномалій для моніторингу.	6
Тема 9. Сертифікація та стандартизація. Які вимоги до сертифікації систем захисту інформації в Україні. Як ISO 27001 впливає на побудову комплексних систем.	6
Тема 10. Сучасні загрози та перспективи. Опишіть загрози в хмарних системах (DDoS, інсайдерські атаки). Які тенденції розвитку (AI у захисті, квантове шифрування).	6
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

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

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. Дата оновлення: 31.12.2023. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
2. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. Дата оновлення: 27.10.2022. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
3. Указ Президента України: Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України": Указ Президента України від 6 травня 2015 року № 287/2015. Дата оновлення: 16.09.2020. URL: https://zakon.rada.gov.ua/laws/show/287/2015#Text
4. Про національну безпеку: Закон України від 21.06.2018 № 2469-VIII. Дата оновлення: 31.03.2023. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

5. Указ Президента України: Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" № 96/2016. Дата оновлення: 28.08.2021. URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text
6. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 № 1229. Дата оновлення: 04.05.2008. URL: https://zakon.rada.gov.ua/laws/show/1229/99#Text
7. ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення. URL: https://tzi.com.ua/downloads/DSTU%203396.0-96.pdf
8. ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт. URL: https://tzi.com.ua/downloads/DSTU%203396.1-96.pdf
9. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованих системах, наказ ДСТСЗІ СБУ від 04.12.2000 № 53 (Зміна № 1 наказ Адміністрації Держспецзв'язку від 28.12.2012 № 806).
https://tzi.com.ua/downloads/1.4-001-2000.pdf
10. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 28.04.99 № 22 (Зміна № 1 наказ від 28.12.2012 № 806).
https://tzi.com.ua/downloads/2.5-004-99.pdf
11. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблювальної інформації від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 28.04.99 № 22 (Зміна № 1 наказ від 15.10.2008 № 172).
https://tzi.com.ua/downloads/2.5-005%20-99.pdf
12. НД ТЗІ 3.6-003-16 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.
13. НД ТЗІ 3.7-003-2023 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі (наказ Адміністрації від 28.10.2023 № 924).
https://www.cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-pro-vnesennya-zmin-do-normativnogo-dokumenta-sistemi-tekhnichnogo-zakhistu-informaciyi-nd-tzi-3-7-003-2005-vid-28-zhovtnya-2023-roku-924
14. НД ТЗІ 1.6-004-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що становить державну таємницю.
https://zakononline.com.ua/documents/show/83554__83554
15. Information Security Handbook for Network Beginners. National Center of Incident Readiness and Strategy for Cybersecurity (NISC) ver. 2.11e.
https://www.coursehero.com/file/55121963/handbook-all-engpdf/
16. 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://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
17. 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

1. ISO/IEC 27001:2022/Amd 1:2024 Information security, cybersecurity and privacy protection – Information security management systems – Requirements URL:
https://www.iso.org/ru/contents/data/standard/08/28/82875.html
2. ISO/IEC 27002:2023 Information security, cybersecurity and privacy protection – Information security controls URL:
https://www.iso.org/ru/contents/data/standard/08/05/80585.html
3. ISO/IEC 27005:2023 Information security, cybersecurity and privacy protection – Guidance on managing information security risks. URL:
https://www.iso.org/ru/contents/data/standard/08/05/80585.html.

4. Synergy of building cybersecurity systems: monograph / S. Yevseyev, V. Ponomarenko, O. Laptiev, O. Milov and others. - Kharkiv: PC TECHNOLOGY CENTER, 2021. - 188 p. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
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: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
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: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.

Інформаційні ресурси

1. Указ Президента України: Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" № 96/2016. Дата оновлення: 28.08.2021. URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text
2. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 № 1229. Дата оновлення: 04.05.2008. URL: https://zakon.rada.gov.ua/laws/show/1229/99#Text

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
0,4	0,2		0,4

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

Шкала оцінювання

Сума балів	Національна оцінка	ECTS

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.

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** Сергій ЄВСЕЄВ