Силабус освітнього компонента
Програма навчальної дисципліни

Інформаційно-комунікаційні системи у сфері національної безпеки

Шифр та назва спеціальності
К3 – Національна безпека (за окремими сферами забезпечення і видами діяльності)

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Спеціалізація

Кафедра
Кібербезпеки (328)

Освітня програма
Національна безпека у сфері кіберзахисту

Тип дисципліни
Обов'язкова

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна

Семестр
7

Мова викладання
Українська

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

ПОГАСІЙ Сергій Сергійович

Serhii.Pohasii@khpi.edu.ua

Доктор технічних наук, доцент, професор кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 95, з них патентів на корисну модель 2, 6 монографій, з яких 4 колективних монографій, 4 навчальних посібників, з яких 4 з грифом Міністерства освіти і науки України, 65 статті у закордонних виданнях та фахових виданнях України, з них 11 у наукометричній базі Scopus. Гарант освітньо-науової програми «Кібербезпека» третього (доктор філософії) рівня вищої освіти, провідний лектор з дисциплін: «Аналогові та цифрові електронні пристрої», «Інтернет речей та сервісів», «Безпека хмарних технологій», «Основи побудови та захисту сучасних операційних систем», «Моделювання систем критичної інфраструктури», «Основи побудови та захисту мікропроцесорних систем», «Безпека смарт-технологій та Інтернет-речей», «Інформаційно-комунікаційні системи у сфері національної безпеки» у студентів бакалавріата та магістратури, Розділ «Інформаційна безпека хмарних сервісів», «Сучасні методи захисту соціо-кіберфізичних систем», «Моделювання механізмів кібербезпеки» для аспірантів.
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Інформаційно-комунікаційні системи у сфері національної безпеки" є обов'язковою навчальною дисципліною. Навчальна дисципліна є теоретичною основою сукупності знань та вмінь, що формують профіль фахівця в області кібербезпеки. На базі здобутих знань та умінь фахівець зможе вирішувати професійні задачі, що базуються на сучасних технологіях та методах захисту інформації у сучасних інформаційно-комунікаційних системах та мережах.

Мета та цілі дисципліни

Метою навчальної дисципліни “Інформаційно-комунікаційні системи у сфері національної безпеки” є навчання студентів принципам побудови комплексних систем захисту інформації для формування контуру безпеки бізнес-процесів в інформаційно-комунікаційних системах на основі Інтернет-технологій та застосунків. Результатами вивчення даної дисципліни є придбання навичок з нейтралізації типових мережевих загроз, використання протоколу SNMP для захисту мережі, захисту від шкідливого програмного забезпечення та захист електронної пошти та веб-трафіку.

Формат занять

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

Компетентності

ЗК1. Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого (безпечного) розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
ЗК7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК8. Здатність використовувати інформаційні та комунікаційні технології і на цій основі формувати ефективну систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо запобігання, протидії та нейтралізації загроз національній безпеці.
СК1. Здатність використовувати безпекові режими під час виконання службових обов’язків.
СК4. Здатність демонструвати та застосовувати знання з основ теорії національної безпеки.

СК6. Здатність використовувати іноземну мову для отримання додаткових знань і умінь з питань національної безпеки, взаємодіяти з іноземними партнерами.
СК8. Здатність використовувати механізми забезпечення національної безпеки у її визначальних сферах.
СК13. Здатність оцінювати вплив глобальних проблем і трансформацій геополітичного та геоекономічного простору на національну безпеку.

Результати навчання

РН1. Вміти реалізовувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського суспільства (вільного демократичного) та необхідність його сталого (безпечного) розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
РН3. 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.
РН4. Вільно спілкуватися державною мовою.
РН5. Вільно спілкуватися іноземною мовою у межах потреби своєї професійної діяльності.
РН7. 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.
РН8. 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 безпеки.
РН9. Вміти використовувати безпекові режими під час виконання службових обов'язків.
РН10. Вміти аналізувати виклики та загрози національній безпеці за напрямами професійної діяльності та синтезувати інформацію щодо розроблення та реалізації стратегій у визначальних сферах національної безпеки (політичній, економічній, соціальній, гуманітарній).
РН12. Вміти застосовувати знання з основ теорії національної безпеки, зокрема: оцінювати обстановку, рівень викликів та загроз національній безпеці.
РН14. Вміти читати й розуміти фахову іншомовну літературу, використовуючи її у соціальній і професійній сферах, а також демонструвати культуру мислення та виявляти навички щодо організації культурного діалогу з іноземними партнерами на рівні, необхідному для професійної діяльності.
РН16. Використовувати у професійній діяльності окремі елементи механізму впливу та взаємодії у процесі забезпечення окремих складових національної безпеки.
РН17. Вміти використовувати отримані знання щодо безпекової складової зовнішньої політики України та інших держав.
РН19. 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.
РН21. Вміти оцінювати вплив глобальних проблем і трансформацій геополітичного та геоекономічного простору на національну безпеку, здійснювати моніторинг зовнішньої та внутрішньої політики держави у контексті забезпечення національної безпеки та готувати пропозиції щодо підвищення її ефективності.

Обсяг дисципліни

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

Передумови вивчення дисципліни (пререквізити)

Основи програмування, Технології програмування, 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. Сучасні загрози мережевої безпеки. Забезпечення безпеки мережевих пристроїв. Розглядаються основні типи загроз у комп'ютерних мережах: віруси, фішинг, DoS/DDoS-атаки, злам паролів, перехоплення трафіку. Аналізуються методи виявлення та класифікації атак, а також принципи побудови систем захисту від сучасних кіберзагроз. Висвітлюються методи захисту маршрутизаторів, комутаторів та точок доступу. Розглядаються принципи сегментації мережі, контроль доступу, оновлення прошивки та налаштування політик безпеки для захисту інфраструктури.	2
Тема 2. Автентифікація, авторизація та облік. Пояснюються принципи трирівневої моделі AAA (Authentication, Authorization, Accounting). Розглядаються протоколи автентифікації (RADIUS, TACACS+), методи контролю доступу користувачів і ведення журналів дій у мережі.	2
Тема 3. Впровадження технологій брандмауера. Впровадження системи запобігання вторгнень. Аналізуються типи брандмауерів (мережеві, прикладного рівня, гібридні) та принципи фільтрації трафіку. Розглядається налаштування правил доступу, NAT, політик безпеки й інтеграція брандмауера в корпоративну мережу. Розглядаються системи виявлення та запобігання вторгнень (IDS/IPS). Пояснюється принцип їх роботи, механізми аналізу мережевого трафіку, виявлення сигнатур атак і налаштування реакційних дій.	2
Тема 4. Забезпечення безпеки локальної мережі (LAN). Описуються основні засоби захисту LAN: VLAN, контроль доступу на портах (Port Security), 802.1X, сегментація трафіку. Розглядаються методи запобігання MAC-спуфінгу та атак типу Man-in-the-Middle.	2
Тема 5. Криптографічні системи захисту інформації. Вивчаються основи симетричного та асиметричного шифрування, цифрові підписи, сертифікаційні центри (PKI) та управління ключами. Розглядається застосування криптографічних методів у захисті мережевих з'єднань.	2
Тема 6. Впровадження віртуальних приватних мереж (VPN). Розглядаються принципи побудови VPN, типи тунелів (IPSec, SSL, MPLS), механізми шифрування і автентифікації. Пояснюється роль VPN у забезпеченні захищеного віддаленого доступу.	2
Тема 7. Впровадження багатофункціонального пристрою захисту Cisco Adaptive Security Appliance (ASA). Описуються можливості Cisco ASA як комплексного рішення безпеки:	2

брандмауер, VPN, IPS, антивірус, контроль доступу. Аналізується процес налаштування й моніторингу безпеки з використанням ASA.	
Тема 8. Управління безпечною мережею. Вивчаються принципи централізованого моніторингу, управління політиками безпеки, реагування на інциденти. Розглядаються системи SIEM, аудит мережевої безпеки та оцінка ефективності заходів захисту.	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Соціальна інженерія. Вивчення мережевих атак, а також інструменти для аудиту безпеки і проведення атак. Практичне ознайомлення з методами соціальної інженерії, техніками маніпуляції користувачами для отримання конфіденційної інформації. Використання інструментів тестування безпеки (Kali Linux, Metasploit, Nmap) для виявлення вразливостей і проведення етичного аудиту систем.	8	0,1
Тема 2. Захист маршрутизатора для адміністративного доступу. Виконання налаштувань безпечного віддаленого адміністрування маршрутизатора. Розглядаються методи захисту паролів, обмеження доступу через протоколи Telnet/SSH, використання списків контролю доступу (ACL) для підвищення безпеки керування мережею.	6	0,1
Тема 3. Захист адміністративного доступу за допомогою AAA і RADIUS. Ознайомлення з механізмами автентифікації, авторизації та обліку дій користувачів (AAA). Налаштування сервера RADIUS для централізованого управління доступом до мережевих пристроїв, перевірка роботи протоколу й ведення журналів безпеки.	6	0,1
Тема 4. Налаштування зональних міжмережевих екранів. Практична робота з налаштування зонального брандмауера (Zone-Based Firewall) для розмежування трафіку між сегментами мережі. Визначення політик безпеки для різних зон, створення правил доступу та моніторинг мережевих подій.	6	0,1
Тема 5. Налаштування системи запобігання вторгнень (IPS). Вивчення принципів роботи систем IPS. Виконання налаштувань виявлення та блокування підозрілої активності в мережі. Аналіз спрацьовувань системи, дослідження журналів подій і оптимізація параметрів для зменшення кількості хибних спрацювань.	6	0,1
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 0{,}5$

Контрольні роботи

Теми контрольних робіт	Вагові

	коефіцієнти b
Тема 1. Забезпечення безпеки мережевої інфраструктури державних інформаційних систем. Розглядаються принципи побудови захищених мережевих архітектур, методи автентифікації користувачів, політики доступу та управління мережевими пристроями. Аналізуються загрози на рівні маршрутизаторів, комутаторів і шлюзів, а також шляхи їх нейтралізації засобами Cisco, ACL та AAA.	0,1
Тема 2. Сучасні технології виявлення та запобігання кіберзагроз у національних інформаційно-комунікаційних системах. Досліджуються системи брандмауерів, IPS/IDS, VPN і криптографічні методи захисту. Оцінюється ефективність інтеграції багаторівневого захисту, аналізується роль моніторингу безпеки, журналювання та реагування на інциденти у сфері національної безпеки.	0,1
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 побудови безпечної архітектури мережі державних органів. Розгляд принципів побудови багаторівневої мережевої інфраструктури з урахуванням безпеки, зон довіри та сегментації.	8
Тема 2. Протоколи безпечного обміну даними (SSL/TLS, IPsec, SSH). Вивчення механізмів шифрування, автентифікації та захисту переданих даних у національних комунікаційних мережах.	8
Тема 3. Управління ризиками у сфері інформаційно-комунікаційних систем. Оцінювання загроз, вразливостей і впровадження системи управління ризиками у державних структурах.	7
Тема 4. Технології виявлення та реагування на інциденти безпеки (SIEM-системи). Дослідження сучасних рішень для збору, аналізу й кореляції подій безпеки (Splunk, ELK, QRadar).	7
Тема 5. Використання криптографії у захисті інформації на державному рівні. Огляд стандартів шифрування, цифрових підписів і сертифікації ключів у національній системі безпеки.	7
Тема 6. Використання криптографії у захисті інформації на державному рівні. Огляд стандартів шифрування, цифрових підписів і сертифікації ключів у національній системі безпеки.	7
Тема 7. Технології сегментації мережі та контроль доступу (NAC). Розгляд принципів Network Access Control, Zero Trust і засобів контролю пристроїв, що підключаються до мережі.	7
Тема 8. Аналіз шкідливого трафіку та методи його блокування.	7

Вивчення технік виявлення зловмисної активності, застосування фільтрації пакетів та поведінкових моделей.	
Тема 9. Хмарні сервіси та їх роль у національній інформаційній безпеці. Оцінка переваг і ризиків використання хмарних платформ у державних структурах. Моделі безпеки SaaS, PaaS, IaaS.	7
Тема 10. Розроблення політики кіберзахисту організації. Формування нормативних документів, регламентів доступу, планів реагування на кіберінциденти та резервного копіювання.	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. Технології захисту інформації [Електронний ресурс] : підручник для студ. 122 «Комп'ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в інформаційних системах» / Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,04 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с.
https://ela.kpi.ua/server/api/core/bitstreams/c50a89f5-ef09-4821-b7d6-f402882f2bd4/content
2. С. П. Євсеєв. Технології захисту інформації / С. Е. Остапов, С. П. Євсеєв, О. Г.Король. – Чернівці. – Видавничий дом "Родовід", 2014. – 428 с.
http://kist.ntu.edu.ua/textPhD/tzi.pdf
3. Швачич Г.Г., Толстой В.В., Петречук Л.М., Іващенко Ю.С., Гуляєва О.А., Соболенко О.В. Сучасні інформаційно-комунікаційні технології: Навчальний посібник. – Дніпро: НМетАУ, 2017. –230 с.
https://nmetau.edu.ua/file/ikt_tutor.pdf
5. Коробейнікова Т.І., Захарченко С.М. Технології захисту локальних мереж на основі обладнання CISCO. Львів : Вид-во Львів. політехніки, 2021. 232 с.
https://vlp.com.ua/node/20266

Додаткова література

6. Askoxylakis I., Ioannidis S., Katsikas S.K., Meadows C. (eds.) Computer Security -ESORICS 2016, Part I
https://link.springer.com/book/10.1007/978-3-319-45744-4
7. Б. Ю. Жураковський, І.О. Зенів Комп'ютерні мережі. Частина 1. [Електронний ресурс]: навч. посіб. /; КПІ ім. Ігоря Сікорського. – Електронні текстові дані(1 файл: 8,6 Мбайт). Київ : КПІ ім. Ігоря Сікорського, 2020. 336 с.
https://ela.kpi.ua/server/api/core/bitstreams/c4ecfaa7-73d5-498c-a63a-513137ee0aba/content
8. Computer Networks / ред.: P. Gaj, M. Sawicki, A. Kwiecień. Cham : Springer International Publishing, 2019. URL: https://doi.org/10.1007/978-3-030-21952- 9 (дата звернення: 29.11.2023).

9. Куперштейн , Л., Кренцін, М., Дудатьєв, А. і Каплун, В. Аналіз проблем безпеки піринговых мереж // Інформаційні технології та комп'ютерна інженерія. 54, 2 (Чер 2022), 5–14. DOI:https://doi.org/10.31649/1999-9941-2022-54-2-5-1
10. Куперштейн , Л., Кренцін, М. Аналіз тенденцій розвитку піринговых мереж // Вісник ХНУ. Технічні науки. №299(4), 2021. С. 25-29
http://journals.khnu.km.ua/vestnik/wp-content/uploads/2021/11/299-text_2021_4_t.pdf

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
0,2	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 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** Андрій ТКАЧОВ