Силабус освітнього компонента
Програма навчальної дисципліни

Безпека в соціальних мережах

Шифр та назва спеціальності
К4 – Управління інформаційною безпекою

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Спеціалізація

Кафедра
Кібербезпеки (328)

Освітня програма
Управління інформаційною безпекою

Тип дисципліни
Вибіркова

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна

Семестр
8

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.

Детальніше про викладача на сайті кафедри

МІЛЕВСЬКА Тетяна Сергіївна

Tetiana.Milevska@cs.khpi.edu.ua
Старший викладач кафедри кібербезпеки НТУ «ХПІ».

Автор понад 80 наукових та навчально-методичних праць. Проводить лабораторні та практичні занятть з дисциплін: «Основи математичного моделювання систем безпеки», «Основи наукових досліджень», «Комп'ютерні системи, мережі та комунікації», «Інформаційна безпека держави» у студентів бакалавріата та магістратури.

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Безпека в соціальних мережах" є вибірковою навчальною дисципліною. Вивчення цієї дисципліни дає можливість студенту: ознайомитись з правовими аспектами забезпечення інформаційної і кібербезпеки на рівні держави, міжнародному рівні; ознайомитись з принципами побудови соціальних мереж, протоколами обміну даними в кіберпросторі; ознайомитись з сучасними програмними (програмно-апаратними) застосунками забезпечення безпеки персональних даних; навчитися орієнтуватися в сучасних загрозах, їх направленості; навчитися аналізувати ризики використання конфіденційної інформації в соціальних мережах, відрізняти фейкову інформацію в медіапросторі; навчитися орієнтуватися у послугах і механізмах забезпечення безпеки; набути практичних здатностей в забезпеченні безпеки особистих персональних даних в умовах сучасних загроз.

Мета та цілі дисципліни

Засвоєння принципів забезпечення безпеки персональних даних (конфіденційної інформації) в соціальних мережах, використання механізмів послуг безпеки в умовах сучасних загроз.

Формат занять

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

Компетентності

ЗК6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.
СК2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.
СК3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.
СК5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.
СК7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації.
СК8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах.
СК9. Здатність організації реагування на загрози на об’єктах критичної інфраструктури, установах та підприємствах.
СК10. Здатність забезпечувати неперервність бізнесу згідно з встановленою політикою інформаційної безпеки.
СК11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.

Результати навчання

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.
РН6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки.
РН7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.
РН8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки.

РН10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.
РН11. Вміти забезпечувати процеси захисту та функціонування системи управління інформаційною безпекою та захисту інформації на основі практик, навичок та знань, щодо інфраструктури кіберфізичних систем та інформаційних потоків.
РН12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
РН13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах.
РН14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
РН16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.
РН17. Вміти розв'язувати задачі управління інфораційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.
РН18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.
РН19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах.
РН20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
РН21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.
РН22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.

Обсяг дисципліни

Загальний обсяг дисципліни 90 год. (3 кредити ECTS): лекції – 10 год., лабораторні роботи – 20 год., самостійна робота – 60 год.

Передумови вивчення дисципліни (пререквізити)

Інформаційна безпека держави.

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. Огляд безпеки системи. Основні поняття та визначення безпеки. Роль захисту інформації в кіберпросторі, умови функціонування підсистеми безпеки в соціальних	2

(комп'ютерних) мережах та системах. Вимоги щодо безпеки системи, ризики безпеки. Складові та послуги безпеки: конфіденційність, цілісність, доступність, причетність, спостережність. Розподіл послуг безпеки за рівнями моделі ISO/OSI. Критерії захищеності комп'ютерних систем. Національні нормативні акти і міжнародні регулятори системи безпеки.	
Тема 2. Сучасні загрози в соціальних (комп'ютерних) мережах. Формальне визначення криптосистеми. Критерії та показники ефективності. Аналіз основних видів атак, ризиків та вразливих на елементи інформаційних систем в кіберпросторі. Синергія та гібридність сучасних загроз, основні тенденції спрямованості.	2
Тема 3. Механізми забезпечення конфіденційності та цілісності. Механізми забезпечення автентичності. Основи цифрової стеганографії. Принципи побудови симетричного та несиметричного шифрування. Основні критерії їх використання. Блочні симетричні шифри, алгоритми блокового симетричного шифрування DES, ГОСТ-28147, Rijndael, Калина-256. Несиметричні криптосистеми RSA, Ель Гамаля та Діффі – Геллмана. Принципи їх використання с соціальних мережах. Класифікація механізмів автентифікації: MDC-коди, MAC-коди, цифровий підпис. Основні стандарти цифрового підпису. Класифікація механізмів автентифікації на основі методів двофакторній автентифікації. Класифікація загроз на процедури двофакторній автентифікації. Основні вимоги до протоколів двофакторній автентифікації. Основні процедури, які забезпечують безпеку в протоколах двофакторній автентифікації. Класифікація методів цифровій стеганографії з відкритим ключем. Основні методи приховування конфіденційної інформації.	2
Тема 4. Протоколи захисту інформації на мережево. Механізми та протоколи керування ключами в ІВК в соціальних мережах. Захист інформації на мережному рівні. Протоколи захисту та цілісності IPSec, SSL, TLS, їх сутність. Системи захисту PGP та CS MIME. Криптографічні функції. Сумісність на рівні електронної пошти. Захищена електронна пошта. Компоненти та сервіси інфраструктури відкритих ключів. Архітектура і топологія PKI. Основні вимоги стандарту відкритих ключів, управління сертифікатами. Системи PKI. Основні вимоги до політиці PKI.	2
Тема 5. Програмно-апаратні засоби захисту інформації в мережі Internet. Програмно-апаратні (програмні) засоби захистуінформації в мережі Wi-Fi. Програмно-апаратні (програмні) засоби захисту інформації в хмарних технологіях. Основні принципи захисту інформації при підключенні до мережі Інтернет. Використання паролів і механізмів контролю. Основні принципи захисту інформації при підключенні до мережі Wi-Fi. Використання паролів. Основні принципи захисту інформації при використанні хмарних мереж (технологій).	2
Загальна кількість годин	**10**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти *a*
Тема 1. Механізми захисту операційної системи Windows 10. Ознайомлення з вбудованими інструментами безпеки Windows 10, налаштування облікових записів, керування доступом,	4	-

використання системних оновлень і механізмів шифрування для підвищення рівня захищеності.		
Тема 2 Вивчення можливостей захисту шифрованої файлової системи (EFS) Windows 10, центру безпеки та обслуговування і брандмауера Windows 10. Дослідження можливостей шифрування файлів та папок, моніторингу стану безпеки системи через центр безпеки, а також налаштування правил роботи брандмауера для захисту від несанкціонованого доступу.	4	0,1
Тема 3. Засоби автентифікації користувачів і аналізу безпеки системи. Розгляд механізмів перевірки автентичності користувачів, включаючи паролі, біометрію та багатофакторні методи, а також аналіз журналів безпеки для виявлення загроз і спроб несанкціонованого доступу.	4	0,1
Тема 4. Засоби аналізу захищеності. Використання антивірусних програм, систем моніторингу активності та інструментів для виявлення вразливостей з метою оцінки рівня безпеки операційної системи та виявлення потенційних загроз.	4	0,1
Тема 5. Дослідження стійкості парольного захисту. Аналіз ефективності паролів різної складності, моделювання атак на них (brute force, словникових тощо), дослідження альтернативних способів автентифікації та використання менеджерів паролів.	4	0,1
Загальна кількість годин	**20**	$\sum_{i=1}^{n} a_i$=0,4

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Основи безпеки та сучасні загрози. Розглядаються базові поняття інформаційної безпеки, складові та послуги безпеки, нормативні акти та критерії захищеності, а також аналізуються сучасні загрози, ризики й тенденції розвитку кібератак у соціальних мережах.	0,1
Тема 2. Криптографічні та прикладні механізми захисту. Вивчаються принципи симетричного й несиметричного шифрування, механізми автентифікації та стеганографії, протоколи захисту інформації, інфраструктура відкритих ключів і засоби захисту в Internet, Wi-Fi та хмарних технологіях.	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. Історія розвитку інформаційної безпеки.	6

Етапи становлення підходів до захисту інформації та формування міжнародних стандартів.	
Тема 2. Моделі загроз у соціальних мережах. класифікація атак та приклади реальних інцидентів.	6
Тема 3. Фішинг та соціальна інженерія. Методи впливу на користувачів і способи протидії.	6
Тема 4. Віруси та шкідливе програмне забезпечення в соціальних мережах. Основні типи, механізми поширення та засоби захисту.	6
Тема 5. Політика конфіденційності та захист персональних даних. Вимоги GDPR, українського законодавства та внутрішніх правил соцмереж.	6
Тема 6. Двофакторна автентифікація та сучасні методи автентифікації. Переваги, обмеження й приклади використання.	6
Тема 7. Криптографічні алгоритми у соціальних мережах. Використання симетричного й асиметричного шифрування для захисту даних.	6
Тема 8. Стеганографія та приховування інформації. Практичні методи та приклади застосування.	6
Тема 9. Захист інформації у хмарних технологіях. Ризики, пов'язані з обробкою даних у хмарних сервісах, та способи їхнього зниження.	6
Тема 10. Майбутні тенденції кіберзагроз у соціальних мережах. Прогнозування нових векторів атак та розвиток технологій захисту.	6
Загальна кількість годин	**60**

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. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. Львів: "Новий Світ- 2000", 2019. – 678 с.
https://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf
2. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2020 . – 678 с.
https://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf
3. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. – 320 с.

https://kr-labs.com.ua/books/%D0%9E%D1%81%D0%BD%D0%BE%D0%B2%D0%B8+%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8+%D1%82%D0%B0+%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%BE%D0%B1%D0%BE%D1%80%D0%BE%D0%BD%D0%B8_+%D0%BF%D1%96%D0%B4%D1%80%D1%83%D1%87%D0%BD%D0%B8%D0%BA..PDF
4. Stallings V. Cryptography and Network Security: Principles and Practice, 2nd ed.: Trans. from English - K.: "Williams" Publishing House, 2001. - 672 p.: illustrations. - Paral. title English
https://www.cs.vsb.cz/ochodkova/courses/kpb/cryptography-and-network-security_-principles-and-practice-7th-global-edition.pdf
5. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. http://monograph.com.ua/pctc/catalog/view/64/52/231-1
6. 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. http://monograph.com.ua/pctc/catalog/view/978-617-7319-72-5/978-617-7319-72-5/746-2
7. 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. http://monograph.com.ua/pctc/catalog/view/978-617-7319-57-2/117/419-2.

Додаткова література

8. "Cybersecurity in Social Networks" - Ricardo Jorge Girante Gonçalves
https://run.unl.pt/bitstream/10362/133016/1/TGI0504.pdf
9. "Security and Privacy in Social Networks" – Rajaraman, R. https://books.google.com.ua/books/about/Security_and_Privacy_in_Social_Networks.html?id=rpIYSxjfV7wC&redir_esc=y.

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 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** Роман КОРОЛЬОВ