



Силабус освітнього компонента Програма навчальної дисципліни



Безпека в соціальних мережах

Шифр та назва спеціальності

F5 – Кібербезпека та захист інформації

Спеціалізація

Освітня програма

Кібербезпека

Рівень освіти

Перший (бакалаврський)

Семестр

8

Інститут

ННІ комп'ютерних наук та інформаційних технологій

Кафедра

Кібербезпеки (328)

Тип дисципліни

Вибіркова

Форма навчання

Денна, заочна

Мова викладання

Українська, англійська

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 статей 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 заняття 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

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово.

ЗК4. Здатність спілкуватися іноземною мовою.

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 технології, сучасні методи і моделі 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.

СК5. Здатність відновлювати функціонування інформаційних систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

Результати навчання

РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.

РН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.

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.

PH7. 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.

PH9. 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.

PH10. Вміти використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

PH11. Планувати підготовку та забезпечувати неперервність процесів в організаціях згідно встановленої політики кібербезпеки та з урахування вимог до захисту інформації.

PH12. Застосовувати методи захисту інформації в інформаційних системах згідно встановленої політики інформаційної безпеки.

PH13. 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.

PH14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних систем з використанням процедур резервування згідно встановленої політики безпеки та забезпечувати функціонування спеціального програмного забезпечення, щодо захисту та відновлення інформації.

PH15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.

PH18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

PH19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.

PH21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору та інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

Обсяг дисципліни

Загальний обсяг дисципліни 90 год. (3 кредити ECTS): лекції – 12 год., лабораторні роботи – 24 год., самостійна робота – 54 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.	2
Основні поняття та визначення безпеки. Роль захисту інформації в	

кіберпросторі, умови функціонування підсистеми безпеки в соціальних (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.

2

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.

Тема 3. Механізми забезпечення конфіденційності та цілісності. Механізми забезпечення автентичності.

2

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 Гамала та Діффі – Геллмана. Принципи їх використання в соціальних мережах.

Класифікація механізмів автентифікації: MDC-коди, MAC-коди, цифровий підпис. Основні стандарти цифрового підпису. Класифікація механізмів автентифікації на основі методів двофакторної автентифікації. Класифікація загроз на процедури двофакторної автентифікації. Основні вимоги до протоколів двофакторної автентифікації. Основні процедури, які забезпечують безпеку в протоколах двофакторної автентифікації.

Тема 4. Основи цифрової стеганографії.

2

Класифікація методів цифрової стеганографії з відкритим ключем. Основні методи приховування конфіденційної інформації.

Тема 5. Протоколи захисту інформації на мережево. Механізми та протоколи керування ключами в IBK в соціальних мережах.

2

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 політики PKI.

Тема 6. Програмно-апаратні засоби захисту інформації в мережі Internet. Програмно-апаратні (програмні) засоби захисту інформації в мережі Wi-Fi. Програмно-апаратні (програмні) засоби захисту інформації в хмарних технологіях.

2

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).

Загальна кількість годин

12

Лабораторні заняття

Теми лабораторних занять

Кількість
годин

Вагові
коефіцієнти α

Тема 1. Механізми захисту операційної системи Windows 10. Ознайомлення з вбудованими інструментами безпеки Windows 10, налаштування облікових записів, керування доступом, використання системних оновлень і механізмів шифрування для підвищення рівня захищеності.	6	-
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.	6	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	24	$\sum_{i=1}^n a_i = 0,4$

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

Тема 1. Історія розвитку інформаційної безпеки. Етапи становлення підходів до захисту інформації та формування міжнародних стандартів.	5
Тема 2. Моделі загроз у соціальних мережах. класифікація атак та приклади реальних інцидентів.	5
Тема 3. Фішинг та соціальна інженерія. Методи впливу на користувачів і способи протидії.	5
Тема 4. Віруси та шкідливе програмне забезпечення в соціальних мережах. Основні типи, механізми поширення та засоби захисту.	5
Тема 5. Політика конфіденційності та захист персональних даних. Вимоги GDPR, українського законодавства та внутрішніх правил соцмереж.	5
Тема 6. Двофакторна автентифікація та сучасні методи автентифікації. Переваги, обмеження й приклади використання.	5
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	54

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-tekhnologii-zakhystu.pdf>

2. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2020 . – 678 с.

<https://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnologii-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-](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)

[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](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:

$$O = \Pi \cdot k_1 + K \cdot k_2 + I \cdot k_3 + \Pi_k \cdot k_4$$

де: Π – середньозважена середня оцінка за поточний контроль

I – оцінка за виконання індивідуального завдання

K – середньозважена оцінка за контрольні роботи

Π_k – оцінка за підсумковий контроль

$$\Pi = \frac{\Pi_1 \cdot a_1 + \Pi_2 \cdot a_2 + \dots + \Pi_n \cdot a_n}{\sum_{i=1}^n a_i}$$

де: a_i - ваговий коефіцієнт за кожне практичне (семінарське) або лабораторне заняття.

$$K = \frac{K_1 \cdot b_1 + K_2 \cdot b_2 + \dots + K_m \cdot b_m}{\sum_{i=1}^m b_i}$$

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (Π , K , I ,...) 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 O 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 ЄВСЄЄВ

30.08.2025



Гарант ОП

Сергій ЄВСЄЄВ