



Силабус освітнього компонента

Програма навчальної дисципліни



Безпека в соціальних мережах

Шифр та назва спеціальності

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

Інститут

ННІ комп'ютерних наук та інформаційних технологій

Освітня програма

Національна безпека у сфері кіберзахисту

Кафедра

Кібербезпеки (328)

Рівень освіти

Бакалавр

Тип дисципліни

Профільна, Вибіркова

Семестр

8

Мова викладання

Українська

Викладачі, розробники



ЄВСЕЄВ Сергій Петрович

serhii.yevseiev@khpi.edu.ua

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

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](#)



ВОРОПАЙ Наталя Ігорівна

voropay.n@gmail.com

Кандидат технічних наук, доцент кафедри кібербезпеки НТУ «ХПІ».

Автор понад 30 наукових та навчально-методичних праць. Провідний лектор з дисциплін: «Технології програмування Ч.1», «Децентралізовані системи», «Захист об'єктів критичної інфраструктури», «Антивірусний захист інформації», «Блокчейн та смарт-технології в електронному документообігу».

[Детальніше про викладача на сайті кафедри](#)



КОРОЛЬ Ольга Григорівна

olha.korol@khpri.edu.ua

кандидат технічних наук, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 150, з яких 14 навчальних посібників, 48 статей у закордонних виданнях та фахових виданнях України, 8 патентів на корисну модель, 9 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Менеджмент інформаційної безпеки», «Національна безпека держави», «Інформаційна безпека держави», «Комплексний тренінг «Безпека веб-застосунків»», 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 роботи, самостійна робота, консультації. Підсумковий контроль – іспит.

Компетентності

КЗ-1. 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.

КЗ-2. 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.

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

КЗ-8. 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.

ФК-2. Здатність аналізувати виклики та загрози національній безпеці за напрямками професійної діяльності, синтезувати інформацію щодо розроблення та реалізації елементів стратегій у визначальних сферах національної безпеки (політичній, економічній, соціальній, гуманітарній).

ФК-4. Здатність демонструвати та застосовувати знання з основ теорії національної безпеки.

ФК-7. Здатність визначати необхідні правові та організаційні заходи врегулювання конфліктів, пов'язаних із забезпеченням національної безпеки.

ФК–9. Здатність використовувати знання щодо безпекової складової зовнішньої політики України та інших держав. ФК–11. Здатність використовувати практичні навички, тактику та прийоми роботи з людьми в інтересах службової діяльності. ФК–12. Здатність виконувати заходи територіальної оборони, а також цивільного захисту у межах професійної компетентності. ФК–14. Здатність здійснювати моніторинг зовнішньої та внутрішньої політики держави у контексті забезпечення національної безпеки, готувати пропозиції щодо підвищення її ефективності.

Результати навчання

ПРН–1. 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.

ПРН–2. Вміти використовувати 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.

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–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–15. Вміти визначати необхідні правові та організаційні заходи врегулювання конфліктів, пов'язаних із забезпеченням національної безпеки.

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.

ПРН–20. Вміти виконувати заходи територіальної оборони, а також цивільного захисту у межах професійної компетентності.

ПРН–21. Вміти оцінювати вплив глобальних проблем і трансформацій геополітичного та гео економічного 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 90 год. (3 кредити ECTS): лекції – 24 год., лабораторні роботи – 12 год., самостійна робота – 54 год.

Передумови вивчення дисципліни (пререквізити)

Національна 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

Теми лекційних занять

Тема 1. Огляд безпеки системи.

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.

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.

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.

Тема 4. Механізми забезпечення автентичності.

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.

Тема 5. Основи цифрової стеганографії.

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

Тема 6. Протоколи захисту інформації на мережево.

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.

Тема 7. Механізми та протоколи керування ключами в IBK в соціальних мережах.

Компоненти та сервіси інфраструктури відкритих ключів. Архітектура і топологія PKI. Основні вимоги стандарту відкритих ключів, управління сертифікатами. Системи PKI. Основні вимоги до політиці PKI.

Тема 8. Програмно-апаратні засоби захисту інформації в мережі Internet.

Основні принципи захисту інформації при підключенні до мережі Інтернет. Використання паролів і механізмів контролю.

Тема 9. Програмно-апаратні (програмні) засоби захисту інформації в мережі Wi-Fi.

Основні принципи захисту інформації при підключенні до мережі Wi-Fi. Використання паролів.

Тема 10. Програмно-апаратні (програмні) засоби захисту інформації в хмарних технологіях.

Основні принципи захисту інформації при використанні хмарних мереж (технологій).

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Механізми захисту операційної системи Windows 10.

Тема 2. Вивчення можливостей захисту шифрованої файлової системи (EFS) Windows 10, центру безпеки та обслуговування і брандмауера Windows 10.

Тема 3. Засоби автентифікації користувачів і аналізу безпеки системи.

Тема 4. Засоби аналізу захищеності.

Тема 5. Дослідження стійкості парольного захисту.

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. 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-tekhnohii-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-tekhnohii-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

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;
- іспит: 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 ВСЕЄВ

28.08.2024



Гарант ОП
Андрій ТКАЧОВ