Силабус освітнього компонента

Програма навчальної дисципліни

Безпека мобільних технологій

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

Науково-професійного спрямування, Вибіркова

Рівень освіти

Другий (магістерський)

Форма навчання

Денна

Семестр

3

Мова викладання

Українська

Викладачі, розробники

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

У сучасному світі мобільні технології стали невід'ємною частиною життя. Водночас з їх розвитком зростають ризики безпеки, які можуть загрожувати особистій інформації та приватності користувачів. Цей курс має на меті ознайомити студентів із основними поняттями безпеки мобільних технологій, методами захисту, а також аналізом загроз і вразливостей.

Мета та цілі дисципліни

Мета курсу — навчити студентів основам безпеки мобільних технологій, їх загрозам та методам захисту, а також надати практичні навички для захисту мобільних пристроїв та даних.

Формат занять

Лекції, лабораторні заняття, самостійна робота, консультації. Підсумковий контроль – диференційований залік.

Компетентності

КЗ–1. Здатність застосовувати знання у практичних ситуаціях.
КЗ–2. Здатність проводити дослідження на відповідному рівні.
КЗ–4. Здатність оцінювати та забезпечувати якість виконуваних робіт.
КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.
КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.
КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.

Результати навчання

РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН2. Інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.
РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.
РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв’язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.

РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.
РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.
РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.
РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.
РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.
РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.
РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.
РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.
РН24. Планувати та виконувати наукові та прикладні дослідження у сфері інформаційної безпеки та/або кібербезпеки із застосуванням сучасних технологій, експериментальних і теоретичних методів і моделей теорії прийняття рішень, системного аналізу, оптимізації процесів, математичної статистики.
РН25. Оцінювати ефективність та практичну цінність результатів наукових і практичних досліджень та інновацій.

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)

Архітектура та захист сучасних операційних систем, Комп'ютерні мережі, Основи програмування, базові уявлення про типи атак, загрози та методи захисту інформаційних систем.

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. Вступ до безпеки мобільних технологій. Ознайомлення з основними поняттями мобільної безпеки, архітектурою мобільних платформ, типами мобільних додатків та середовищами їх виконання. Аналіз основних відмінностей між безпекою мобільних і традиційних комп'ютерних систем.	4
Тема 2. Типи загроз та вразливостей. Віруси, шкідливе ПЗ, фішинг, атаки на безпеку мережі. Приклади реальних атак на мобільні пристрої. Вивчення основних типів загроз для мобільних пристроїв, способів зараження шкідливим ПЗ, фішингових атак та атак на бездротові мережі. Розгляд відомих інцидентів безпеки у сфері мобільних технологій.	4
Тема 3. Безпека операційних систем мобільних пристроїв. Аналіз архітектури безпеки Android, iOS та інших мобільних ОС. Механізми контролю доступу, ізоляції додатків, оновлень системи та управління дозволами користувачів.	2
Тема 4. Методи аутентифікації та шифрування. Розгляд сучасних методів аутентифікації користувачів (PIN, біометрія, токени, багатофакторна аутентифікація). Застосування криптографічних алгоритмів для захисту даних у мобільних пристроях і під час передавання через мережу.	2
Тема 5. Розробка та впровадження політик безпеки для мобільних пристроїв. Оцінка ризиків та відповідність стандартам безпеки. Вивчення принципів створення корпоративних політик безпеки мобільних пристроїв (MDM, BYOD). Методи управління ризиками, аудит безпеки, а також огляд міжнародних стандартів, таких як ISO/IEC 27001, NIST.	2
Тема 6. Майбутні тенденції у безпеці мобільних технологій. Нові технології, такі як IoT, 5G та їх вплив на безпеку. Аналіз викликів і можливостей, пов'язаних із розвитком 5G, Інтернету речей (IoT) та мобільних платіжних систем. Прогнозування майбутніх загроз і напрямів розвитку технологій мобільної безпеки.	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість	Вагові

	годин	коефіцієнти a
Тема 1. Вивчення типів шкідливого ПЗ та методів його виявлення. Ознайомлення з основними видами мобільного шкідливого програмного забезпечення (трояни, шпигунські програми, рекламне ПЗ). Практична робота з інструментами аналізу ПЗ, виявленням аномальної поведінки додатків та способами її блокування.	6	0,2
Тема 2. Створення документу політики безпеки для мобільних пристроїв. Розробка політики безпеки для організації, що використовує мобільні пристрої. Визначення правил доступу, шифрування даних, оновлення системи та реагування на інциденти безпеки.	6	0,2
Тема 3. Практичне налаштування VPN та Wi-Fi з шифруванням. Встановлення та конфігурація VPN-з'єднань для захисту трафіку. Налаштування Wi-Fi мереж із використанням протоколів WPA2/WPA3, перевірка рівня безпеки з'єднання та захисту даних під час передачі.	5	0,1
Тема 4. Використання інструментів для оцінки безпеки мобільних додатків. Робота з програмами для тестування мобільних додатків (наприклад, MobSF, Drozer). Аналіз дозволів, перевірка вразливостей у коді, виявлення потенційних каналів витоку даних.	5	0,1
Тема 5. Проведення аудиту безпеки реального мобільного пристрою. Перевірка стану безпеки пристрою: оновлення ОС, рівень шифрування, наявність шкідливих додатків, налаштування доступу. Формування звіту з рекомендаціями щодо підвищення безпеки.	5	0,1
Тема 6. Налаштування та тестування двофакторної аутентифікації на прикладі реального сервісу. Практичне впровадження двофакторної аутентифікації (2FA) на прикладі Google, Microsoft або іншого онлайн-сервісу. Аналіз ефективності 2FA у захисті облікових записів користувачів.	5	0,1
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 0{,}8$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Аналіз загроз і вразливостей мобільних пристроїв. Виявлення, класифікація та аналіз типових загроз для мобільних операційних систем (Android, iOS). Студенти досліджують приклади реальних кібератак, аналізують методи поширення шкідливого ПЗ, фішингові атаки, ризики мережевих з'єднань і розробляють рекомендації щодо запобігання цим загрозам.	0,1
Тема 2. Методи захисту мобільних пристроїв та безпека мобільних додатків.	0,1

Робота спрямована на закріплення знань про засоби безпеки мобільних ОС, методи аутентифікації, шифрування та захисту даних користувача. Студенти розробляють модель безпечного середовища для мобільного додатку, оцінюють ефективність політик безпеки та досліджують вплив технологій IoT і 5G на захист мобільних пристроїв.	
Загалом	$\sum_{i=1}^{m} b_i$=0,2

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин
Тема 1. Мобільні загрози в екосистемах Android та iOS. Порівняння підходів до безпеки різних мобільних платформ, особливості їх архітектури та вразливостей.	8
Тема 2. Соціальна інженерія в мобільному середовищі. Методи обману користувачів через фішингові SMS, месенджери, підроблені додатки.	8
Тема 3. Безпечна розробка мобільних додатків (Secure Coding). Принципи безпечного програмування, уникнення типових помилок розробників.	7
Тема 4. Захист мобільних платежів і фінансових додатків. Технології захисту мобільних транзакцій, роль токенізації та біометричної автентифікації.	7
Тема 5. Мобільне шпигунство та стеження: аналіз інструментів Spyware. Дослідження програм для прихованого збору даних і способів їх виявлення.	7
Тема 6. Захист персональних даних у мобільних пристроях.. Методи збереження конфіденційності користувача: шифрування, дозволи, ізоляція додатків.	7
Тема 7. Безпека мобільних мереж (4G, 5G). Особливості архітектури мобільних мереж та нові виклики у сфері безпеки з появою 5G.	7
Тема 8. Використання Mobile Device Management (MDM) систем. Роль MDM у корпоративній безпеці: контроль пристроїв, оновлення, блокування втраченої техніки.	7
Тема 9. Захист мобільних IoT-пристроїв. Проблеми безпеки в екосистемі “розумних” пристроїв, способи виявлення та усунення вразливостей.	7
Тема 10. Правові та етичні аспекти безпеки мобільних технологій. Норми міжнародного та національного законодавства у сфері кібербезпеки мобільних систем.	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. Онлайн-курс CISCO «Network Support and Security» https://www.netacad.com/catalogs/learn?category=course.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Stephen F. McKearin, Mobile Security: A Comprehensive Guide. URL: https://www.google.com.ua/books/edition/Mobile_Device_Security/HmX6QQAACAAJ?hl=ru
2. Shai Aharony and Gilad Keren, The Mobile Security Ecosystem. URL: https://icrc.tau.ac.il/sites/cyberstudies-english.tau.ac.il/files/media_server/cyber%20center/Report%202014-2016.pdf
3. Ross Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems. URL: https://books.google.com.ua/books?id=eo4Otm_TcW8C&printsec=frontcover&redir_esc=y#v=onepage&q&f=false
4. Nikolay Elenkov , Android Security Internals. URL: https://books.google.com.ua/books/about/Android_Security_Internals.html?id=R-9FAQAACAAJ&redir_esc=y
5. Kevin D. Mitnick, The Art of Deception: Controlling the Human Element of Security/ URL: https://books.google.com.ua/books/about/The_Art_of_Deception.html?id=OIy4F-8b_uEC&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
0,8	0,2		

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** Станіслав МІЛЕВСЬКИЙ