Силабус освітнього компонента
Програма навчальної дисципліни

Безпека та анонімність роботи в Інтернеті

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
Спеціальна (фахова) підготовка, Обов'язкова

Рівень освіти
Другий (магістерський)

Форма навчання
Денна

Семестр
2

Мова викладання
Українська

Викладачі, розробники

ГАВРИЛОВА Алла Андріївна
alla.havrylova@khpi.edu.ua
PhD, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 50, з них патентів на корисну модель 2, 5 монографії, з яких 3 – у рецензованому виданні, що входить до бази даних Scopus, 1 – в іноземному науковому виданні, 2 – у фаховому виданні України; 14 статей, з них 7 наукових статей – у наукових фахових виданнях України, 4 наукові статті – у рецензованих виданнях, що входять до бази даних Scopus, 3 статті – в іноземних наукових виданнях. Лектор з дисциплін: «Презентація та обробка знань», «Основи управління в проєктах галузікібербезпеки та захисту інформації», «Безпека та анонімність роботи в Інтернет» у студентів магістратури

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

У межах даної дисципліни здобувачі вищої освіти отримують знання й розуміння сучасних тенденцій розвитку освіти, критичне та системне мислення, здатність логічно обґрунтовувати позицію, оцінювати ризики, приймати рішення, розв’язувати проблеми, критичне сприйняття інформаційного простору, безпечне використання сучасних технологій та ефективне оперування цифровими інструментами, зокрема соцмережами.

Мета та цілі дисципліни

Формування фундаментального розуміння загроз конфіденційності, цілісності та доступності (КЦД) особистих даних у мережі, застосування технічних та організаційних заходів для захисту робочих станцій та мобільних пристроїв, навичок використання технологій анонімізації та шифрування для приховування особистості та даних, а також правових та етичних аспектів, пов'язаних з кібербезпекою та приватністю.

Формат занять

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

Компетентності

КЗ-1. Здатність застосовувати знання у практичних ситуаціях.
КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт.
КЗ-5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і
політики інформаційної безпеки та/або кібербезпеки організації.
КФ7. Здатність 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.

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 заняття – 32 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Мережева та хмарна безпека, Технології управління безпекою бізнес-процесів, Цифрова криміналістика, Основи управління в проєктах галузі кібербезпеки та захисту інформації.

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. Основи цифрової безпеки. 1. Аналіз актуальних загро 2. Принципи створення надійних паролів та використання менеджера паролів	2
Тема 2. Захист пристроїв та мереж. 1. Налаштування операційних систем та браузерів для максимальної безпеки 2. Використання брандмауерів та антивірусного ПЗ 3. Захист домашніх та публічних Wi-Fi мереж	4
Тема 3. Технології анонімізації та шифрування 1. Принципи роботи та практичне використання VPN-сервісів. 2. Знайомство з Tor Browser та мережею Tor 3. Шифрування файлів та електронної пошти	4
Тема 4. Безпека комунікацій та хмарних сервісів. 1. Правила безпечного використання електронної пошти та месенджерів 2. Безпечне зберігання даних у хмарних сховищах	2
Тема 5. Цифрова гігієна та мінімізація сліду. 1. Управління налаштуваннями приватності в соціальних мережах 2. Методи пошуку та видалення особистих даних з Інтернету	4
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Безпека облікових записів та управління паролями. 1. Налаштування MFA (двофакторної автентифікації 2. Встановлення та використання менеджера паролів 3. Аудит паролів	6	1
Тема 2. Захист браузера та цифрове слідознавство 1. Налаштування приватності в браузері 2. Аналіз цифрового сліду 3. Тестування на унікальність	6	1
Тема 3. Шифрування та анонімізація трафіку. 1. Тестування VPN 2. Робота з Tor 3. Оцінка безпеки підключення	6	1
Тема 4. Захист комунікацій та файлів.	6	1

1. Безпечні месенджери 2. Шифрування файлів 3. PGP-ключі		
Тема 5. Безпека хмарних сховищ та мобільних пристроїв. 1. Безпека хмарних сховищ та мобільних пристроїв 2. Аудит хмарного сховища 3. Налаштування приватності на мобільному пристрої 4. Безпечне скидання даних.	8	2
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 6$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Фундаментальні основи кібербезпеки та шифрування	5
Тема 2. Анонімність, приватність та правові аспекти	5
Тема 3. Безпека інфраструктури та мобільності	5
Загалом	$\sum_{i=1}^{m} b_i$=15

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин
Тема 1. Криптографія та захист даних. 1. Порівняльний аналіз алгоритмів шифрування. 2. Практика PGP/GnuPG	14
Тема 2. Поглиблена анонімність та обхід цензури 1. Розширена конфігурація Tor 2. Концепція "Цифрового відбитка" 3. Безпечні операційні системи	16
Тема 3. Соціальна інженерія та людський фактор 1. Аналіз сучасних технік фішингу 2. Оцінка ризиків, пов'язаних з публікацією даних	14
Тема 4. Правові та етичні аспекти 1. Міжнародні норми приватності 2. Юридичні аспекти VPN та Tor	14
Тема 5. Безпека мобільних пристроїв 1. Безпека застосунків та дозволи 2. Техніки захисту від шпигунського ПЗ	14
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

За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Вишняков В. М. Захист інформації в комп'ютерних системах: навч. посіб. / В М. Вишняков; – Київ. Нац. Ун-т буд-ва і архіт. - Київ: КНУБА, 2022. – 119 с. https://repositary.knuba.edu.ua/handle/123456789/11349
2. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems –Requirements / International Organization for Standardization. – Geneva : ISO, 2022. https://hightable.io/iso-27001
3. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection – Information security controls / International Organization for Standardization. – Geneva : ISO, 2022. https://dnv.com/training/iso-27002
4. Tor Project. Tor Browser Manual. – [Електронний ресурс]. – Режим доступу: https://tb-manual.torproject.org/ (Дата звернення: 05.11.2025). – (Офіційна документація мережі Tor).
5. Electronic Frontier Foundation (EFF). Surveillance Self-Defense. – [Електронний ресурс]. – Режим доступу: https://ssd.eff.org/ (Дата звернення: 05.11.2025). – (Посібник із самозахисту від стеження).
6. Signal Foundation. Technical Whitepaper. – [Електронний ресурс]. – Режим доступу: https://signal.org/docs/ (Дата звернення: 06.11.2025). – (Документація щодо протоколу наскрізного шифрування).

Додаткова література

1. Google. Google Safety Center: How We Keep Your Data Secure. – [Електронний ресурс]. – Режим доступу: https://safety.google/security/ (Дата звернення: 06.11.2025).
2. Європейський Союз. Регламент (ЄС) 2016/679 Європейського парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб щодо обробки персональних даних і про вільний рух таких даних (GDPR). – [Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu/legal-content/UK/TXT/?uri=CELEX:32016R0679 (Дата звернення: 07.11.2025).
3. NIST. NIST Special Publication 800-63B: Digital Identity Guidelines. – [Електронний ресурс]. – Режим доступу: https://doi.org/10.6028/NIST.SP.800-63b (Дата звернення: 07.11.2025). – (Рекомендації щодо цифрової ідентифікації та автентифікації).
4. VeraCrypt. Official Documentation. – [Електронний ресурс]. – Режим доступу: https://www.veracrypt.fr/en/documentation.html (Дата звернення: 07.11.2025). – (Інструкції з використання програмного забезпечення для шифрування дисків).
5. GnuPG (GNU Privacy Guard). The GNU Privacy Handbook. – [Електронний ресурс]. – Режим доступу: https://www.gnupg.org/gph/en/manual.html (Дата звернення: 07.11.2025). – (Керівництво з використання PGP).

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
0,6	0,4		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** Станіслав МІЛЕВСЬКИЙ