



МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
Харківський національний університет внутрішніх справ

Факультет № 4

Кафедра протидії кіберзлочинності

Факультет № 6

Кафедра кібербезпеки та DATA-технологій

ЗАТВЕРДЖЕНО

На спільному засіданні кафедри протидії кіберзлочинності факультету № 4 та кафедри кібербезпеки та DATA-технологій факультету №6 протокол № 2 від 22 червня 2023 р.
Завідувач кафедри
Олександр МАНЖАЙ

ОСНОВИ КІБЕРБЕЗПЕКИ (ОК.05)

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Кафедра	Кафедра протидії кіберзлочинності (https://univd.edu.ua/uk/dir/1740/kafedra-protydii-kiberzlochynnosti)
Контактний телефон	+38 057 7398085 (роб.)
E-mail	kaf-itk@univd.edu.ua
ЛЕКТОР (ЛЕКТОРИ)	
	Манжай Олександр Володимирович , завідувач кафедри протидії кіберзлочинності факультету № 4, к.ю.н., професор toj@univd.edu.ua Лекційний потік: факультет № 4, шифр навчальних груп Ф4-102, 103 Лекційний потік: факультет № 6, шифр навчальних груп Ф6-КБдср-23-1, Ф6-КБдср-23-2
Назва освітньо-професійної програми	Кібербезпека та захист інформації (безпека інформаційних та комунікаційних систем)

	Cybersecurity and information protection (security of information and communication systems)
Рівень вищої освіти	Перший (бакалаврський) (НРК України – 6 рівень та перший цикл вищої освіти Рамки кваліфікацій Європейського простору вищої освіти)
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека та захист інформації
Статус дисципліни	Обов'язкова компонента освітньо-наукової програми, вивчається в 1 семестрі I курсу навчання
Мета вивчення дисципліни	<p>Навчити здобувачів вищої освіти правил поведіння з інформацією у кіберсфері та безпечної роботи із засобами комп'ютерної техніки.</p> <p>Виробити вміння: визначати заходи кібербезпеки для конкретної ситуації; оцінювати загрози та вживати заходів реагування на робочому місці; безпечно поводитись у кіберсфері; організовувати безпечний доступ до пристроїв і програм; критично оцінювати інформацію.</p> <p>Сформувати у здобувачів вищої освіти знання, уміння і навички щодо основних положень та термінів, що стосуються кібергігієни на робочому місці; заходів кібербезпеки на робочому місці; особливостей дотримання правил кібербезпеки в системі публічної служби.</p>
Завдання вивчення дисципліни	Дослідження принципів та методів безпечної роботи в комп'ютерних системах та мережах, ознайомлення з програмами, призначеними для захисту інформації та її носіїв, засвоєння правил налаштування програмного забезпечення, набуття знань і навичок використання технологій для побудови системи кібербезпеки
Обсяг дисципліни в кредитах ECTS/годинах	<p>Кількість кредитів ECTS (загальний обсяг – 90 год.)</p> <p>З них (денна/заочна):</p> <p>- аудиторна робота: 48/8 год.</p> <p>- самостійна робота: 42/82 год.</p>
Форми та види проведення навчальних занять	<p>Форма навчання – денна</p> <p>Види навчальних занять:</p> <ul style="list-style-type: none"> - лекції: 24 год.; - семінарські заняття: 0 год.; - практичні заняття: 12 год.; - лабораторні заняття: 12 год.

	<p>Форма навчання –заочна</p> <p>Види навчальних занять:</p> <ul style="list-style-type: none"> - лекції: 4 год.; - семінарські заняття:0 год.; - практичні заняття: 2 год; - лабораторні заняття:2 год.
Самостійна робота	Опрацювання рекомендованої літератури, підготовка тез доповідей до конференцій, самостійне вирішення практичних завдань.
Індивідуальні завдання	Наукові доповіді, реферати
Необхідне обладнання	Мультимедійне обладнання (ноутбук та проектор), комп'ютерне забезпечення з виходом у мережу Інтернет.
Мова викладання	Українська
Контроль	Поточний та підсумковий контроль Поточний: опитування на практичних заняттях; участь в дискусіях, веб-квестах, обговоренні доповідей, рефератів; підготовка рефератів та доповідей, тестування, виконання самостійних робіт, захист лабораторних робіт. Критерії оцінки поточного контролю викладач повідомляє на першому занятті та перед кожним оцінюванням. Підсумковий контроль: екзамен.
Інтегральна компетентність, загальні компетентності (ЗК)	<p>Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки та/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов</p> <p>ЗК.2 Знання та розуміння предметної області та розуміння професії</p>
Спеціальні компетентності (СК)	
ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ЗА ТЕМАМИ	
<p>ТЕМА № 1 Загальні правила безпечної роботи з пристроями та програмами</p> <p>Захист персональних даних. Безпека мобільних пристроїв. Шкідливе програмне забезпечення. Фізична безпека. Убезпечення від неправдивих повідомлень.</p>	
<p>ТЕМА № 2 Базові правила убезпечення роботи в комп'ютерній мережі</p> <p>Соціальна інженерія. Безпечне користування мережею Інтернет. Безпечне</p>	

користування електронною поштою. Безпека користування соціальними мережами. Реагування на інциденти безпеки інформації.

Програмні результати навчання (ПРН)	ПРН 15 використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій
	ПРН 30 здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.
	ПРН 53 вирішувати задачі аналізу програмного коду на наявність можливих загроз
Критерії оцінювання результатів навчання	<p>Оцінювання навчальної дисципліни проводиться за результатами поточного та підсумкового контролю:</p> <ul style="list-style-type: none"> - поточний контроль - 50 балів; - підсумковий контроль - 50 балів. <p>Оцінка за поточний контроль складається з оцінювання аудиторної та самостійної роботи здобувача вищої освіти. Оцінка за аудиторну роботу визначається як середнє арифметичне балів, які ним отримані на семінарських заняттях (здобувач має отримати не менш 5 позитивних оцінок) з коефіцієнтом 5. Оцінка за самостійну роботу визначається як середнє арифметичне балів, які отримані здобувачем за: реферати, програми (здобувач має підготувати не менш 2 проектів) з коефіцієнтом 5.</p> <p>Підсумкові бали з навчальної дисципліни визначаються як сума балів, які отримані здобувачем протягом семестру, та балів, які набрані на підсумковому контролі (екзамені).</p>

ШКАЛА ОЦІНЮВАННЯ: НАЦІОНАЛЬНА ТА ECTS

Оцінка в балах	Оцінка за національною шкалою	Оцінка за шкалою ECTS	
		Оцінка	Пояснення

97-100	Відмінно ("зараховано")	А	„Відмінно” – теоретичний зміст курсу освоєний цілком, необхідні практичні навички роботи з освоєним матеріалом сформовані, всі навчальні завдання, які передбачені програмою навчання виконані в повному обсязі, відмінна робота без помилок або з однією незначною помилкою.
94-96			
90-93			
85-89	Добре ("зараховано")	В	„Дуже добре” – теоретичний зміст курсу освоєний цілком, необхідні практичні навички роботи з освоєним матеріалом в основному сформовані, всі навчальні завдання, які передбачені програмою навчання виконані, якість виконання більшості з них оцінено числом балів, близьким до максимального, робота з двома – трьома незначними помилками.
80-84			
75-79		С	„Добре” – теоретичний зміст курсу освоєний цілком, практичні навички роботи з освоєним матеріалом в основному сформовані, всі навчальні завдання, які передбачені програмою навчання виконані, якість виконання жодного з них не оцінено мінімальним числом балів, деякі види завдань виконані з помилками, робота з декількома незначними помилками, або з однією – двома значними помилками.
70-74	Задовільно ("зараховано")	D	„Задовільно” – теоретичний зміст курсу освоєний не повністю, але прогалини не мають істотного характеру, необхідні практичні навички роботи з освоєним матеріалом в основному сформовані, більшість передбачених програмою навчання навчальних завдань виконано, деякі з виконаних завдань, містять помилки, робота з трьома значними помилками.
65-69			
60-64		Е	„Достатньо” – теоретичний зміст курсу освоєний частково, деякі практичні навички роботи не сформовані, частина передбачених програмою навчання навчальних завдань не виконані, або якість виконання деяких з них оцінено числом балів, близьким до мінімального, робота, що задовольняє мінімуму критеріїв оцінки.

40-59	Незадовільно („не зараховано”)	FX	„Умовно незадовільно” – теоретичний зміст курсу освоєний частково, необхідні практичні навички роботи не сформовані, більшість передбачених програм навчання, навчальних завдань не виконано, або якість їхнього виконання оцінено числом балів, близьким до мінімального; при додатковій самостійній роботі над матеріалом курсу можливе підвищення якості виконання навчальних завдань (з можливістю повторного складання), робота, що потребує доробки
21-40			
1-20		F	„Безумовно незадовільно” – теоретичний зміст курсу не освоєно, необхідні практичні навички роботи не сформовані, всі виконані навчальні завдання містять грубі помилки, додаткова самостійна робота над матеріалом курсу не приведе до значимого підвищення якості виконання навчальних завдань, робота, що потребує повної переробки

Перелік питань, що виносяться на підсумковий контроль

1. Як називається параметр, який можуть підмінити зловмисники під час телефонування, для того щоб особа вважала, що спілкується з довіреним номером?
2. Які заходи слід вжити для убезпечення мобільного пристрою від несанкціонованого фізичного доступу?
3. На Ваш телефон надійшло повідомлення з телефону начальника про прохання надіслати службовий документ на пошту pp_minko_pp@mail.ru. Яких заходів Ви будете вживати?
4. Від невідомого контакта Вам на телефон надійшло повідомлення про те, що в районі Вашого проживання протягом тижня буде вимкнено електроенергію на пів доби. Також було залишено посилання, де можна переглянути графік відключень. При переході за посиланням у телефоні з'явилося попередження про встановлення якоїсь програми (apk) на телефон. Якими будуть Ваші дії?
5. Інструменти ведення пропаганди.
6. Що таке фейк?
7. Ознаки фейків?
8. Способи протидії неправдивим повідомленням.
9. Що належить до персональних даних про особу?
10. Який з видів інформації не належить до інформації з обмеженим доступом?
11. Що таке «інформація про фізичну особу (персональні дані)» відповідно до Закону України «Про інформацію»?

12. Якого головного правила слід дотримуватись для безпечного користування електронною поштою?
13. Загрози під час користування поштовою скринькою.
14. Ви отримуєте листа від представника Адміністрації Президента України. Який з нижченаведених пунктів найбільше викликав би у Вас довіру?
15. Чому листи, які містять у собі пароль для відкриття файлу в застосунку, викликають велику підозру?
16. Ризики використання неліцензованого програмного забезпечення.
17. Що таке вірус-вимагач?
18. Що є ознакою, що Ваш комп'ютер, імовірно, інфіковано вірусом?
19. Чому НЕ рекомендовано вставляти невідомі флеш-носії в комп'ютер своєї установи?
20. Що означає атака «людина посередині»?
21. Що НЕ є загрозою при крадіжці мобільного пристрою?
22. Що таке соціальна інженерія?
23. Що таке фішинг?
24. Ознаки фішингового листа.
25. Ваш друг попросив Вас у месенджері перекинути йому на карту 1000 грн. Ваші дії?
26. Вам потрібно встановити додаток на Ваш комп'ютер. У пошуковій системі Ви побачили декілька посилань, що пропонували завантаження такого додатку. Звідки Ви його будете завантажувати?
27. Користуючись мережею Інтернет з дому, Ви раптово побачили, що спроба дістатись пошукової системи викликала в браузері повідомлення про підозрілий недовірений сертифікат. Що Ви зробите?
28. Чому користування соціальними мережами безкоштовне для користувачів?
29. Які паролі є надійними?
30. Хто відповідає за конфіденційність інформації в соціальних мережах?

ОСНОВНА ЛІТЕРАТУРА З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Навчальна та наукова література:

1. Oles N. How to Catch a Phish: A Practical Guide to Detecting Phishing Emails. Apress Berkeley, CA, 2023. 147 p. DOI: <https://doi.org/10.1007/978-1-4842-9361-4>.
2. Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: наук.-практ. посіб. Київ: К.І.С., 2021. 160 с. URL: <https://rm.coe.int/handbook-pers-data-protect-2021-web/1680a37a69>.
3. Даник Ю. Г., Гришук Р. В. Основи кібернетичної безпеки: монографія. Житомир : ЖНАЕУ, 2016. 636 с.
4. Манжай О. В., Манжай І. А. Правові засади захисту інформації: підручник / вид. друге, переробл. та доповн. Харків : Промарт, 2020. 162 с. з іл. URL: <https://univd.edu.ua/science-issue/issue/4315>

5. Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікованої) програми підвищення кваліфікації: практикум / О. В. Манжай, В. В. Носов. К. : ВАІТЕ, 2021. 106 с.
6. Робочий зошит для учасників тренінгу з питань кібергігієни. Загальна короткострокова програма підвищення кваліфікації / О.М. Барановський, В.В. Гузій, Д.І. Майорников, О.В. Манжай, В.В. Носов. Київ: ВАІТЕ, 2021. 262 с.

ДОДАТКОВА ЛІТЕРАТУРА З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Навчальна та наукова література:

7. Манжай О. В., Манжай І.А. Що таке кібергігієна? // Протидія кіберзлочинності та торгівлі людьми (18 травня. 2021 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; ГС «Глобальний центр взаємодії в кіберпросторі». Харків : ХНУВС, 2021. С. 65-67.
8. Носов В.В., Манжай О.В. Зміст та методологія практичного навчання з питань кібергігієни // Протидія кіберзлочинності та торгівлі людьми (18 травня. 2021 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; ГС «Глобальний центр взаємодії в кіберпросторі». Харків : ХНУВС, 2021. С. 72-73.
9. Maennel K., Mäses S., Maennel O. Cyber Hygiene: The Big Picture. In: Gruschka N. (eds) Secure IT Systems. NordSec 2018. *Lecture Notes in Computer Science*. 2020. Vol. 11252. Springer, Cham. (DOI: 10.1007/978-3-030-03638-6_18).
10. Pfleeger S. L., Sasse M. A., Furnham A. From Weakest Link to Security Hero: Transforming Staff Security Behavior. *Journal of Homeland Security and Emergency Management*. 2014. Vol. 11. Iss. 4. pp. 489-510. (DOI: 10.1515/jhsem-2014-0035).
11. Review of cyber hygiene practices (December 2016). European Union Agency For Network and Information Security (ENISA). https://www.enisa.europa.eu/publications/cyber-hygiene/at_download/fullReport, p. 4.
12. Vishwanath A., Neo L. S., Goh P., Lee S., Khader M., Ong G., Chin J. Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*. 2020. Vol. 128 (DOI: 10.1016/j.dss.2019.113160).

Нормативно-правові акти:

13. Про критичну інфраструктуру: Закон України від 16.11.2021 р. № 1882-IX. URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text>.
14. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.
15. Про створення Центру протидії дезінформації: Рішення Ради національної безпеки і оборони України від 11 березня 2021 року, введено в дію Указом Президента України від 19 березня 2021 року № 106/2021. URL: <https://zakon.rada.gov.ua/laws/show/106/2021#Text>.

16. Стратегія інформаційної безпеки України, затверджена Указом Президента України від 28 грудня 2021 року № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#Text> (дата звернення: 10.05.2023).
17. Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 року № 447/2021. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#Text> (дата звернення: 10.05.2023).
18. Про захист персональних даних: закон України від 01.06.2010; [із змінами і доповненнями]. *Офіційний вісник України*. 2010. № 49 (09.07.2010), стор. 199, стаття 1604.
19. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: постанова Кабінету Міністрів України № 373 від 29.03.06; [із змінами і доповненнями]. *Офіційний вісник України*. 2006. № 13 (12.04.2006), стор. 164, стаття 878.
20. Про доступ до публічної інформації: закон України від 13.01.2011; [із змінами і доповненнями]. *Офіційний вісник України*. 2011. № 10 (18.02.2011), стор. 29, стаття 446.
21. Про затвердження документів у сфері захисту персональних даних: наказ Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14. *Баланс*. 2014, № 19, С. 5. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#n11.
22. Про інформацію: закон України від 02.10.1992 р.; [із змінами і доповненнями]. *Відомості Верховної Ради України*. 1992. № 48 (01.12.1992). ст. 650.
23. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). *Офіційний вісник Європейського Союзу*. 04.05.2016. L 119. С. 1. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.
24. Про захист інформації в інформаційно-комунікаційних системах. Закон України: від 05.07.1994, № 1170-VII. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>.
25. Про електронні комунікації: Закон України від 16.12.2020 : [із змінами і доповненнями]. *Офіційний вісник України*. 2021. № 6 (21.01.2021). Ст. 306.

Інформаційні ресурси в Інтернеті:

26. Освітній серіал «Основи кібергігієни». URL: <https://osvita.diia.gov.ua/courses/cyber-hygiene>.
27. Ви вмієте розпізнавати фішинг? URL: <https://phishingquiz.withgoogle.com/?hl=uk>.