



Силабус освітнього компонента Програма навчальної дисципліни



Організація документообігу з обмеженим доступом

Шифр та назва спеціальності

K4 – Управління інформаційною безпекою

Спеціалізація

Освітня програма

Управління інформаційною безпекою

Рівень освіти

Перший (бакалаврський)

Семестр

8

Інститут

ННІ комп'ютерних наук та інформаційних технологій

Кафедра

Кібербезпеки (328)

Тип дисципліни

Вибіркова

Форма навчання

Денна

Мова викладання

Українська

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](#)

Загальна інформація

Анотація

Навчальна дисципліна "Організація документообігу з обмеженим доступом" є нормативною навчальною дисципліною. Дисципліна спрямована на набуття студентом теоретичних знань та практичних навичок щодо організації документообігу з обмеженим доступом у сфері кіберзахисту.

Мета та цілі дисципліни

Оволодіння студентами комплексом знань в області ведення обліку, зберігання, використання й знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію з обмеженим доступом.

Формат занять

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

Компетентності

ЗК6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.

СК2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.

СК3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.

СК5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.

СК7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації.

СК8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах.

СК9. Здатність організації реагування на загрози на об'єктах критичної інфраструктури, установах та підприємствах.

СК10. Здатність забезпечувати неперервність бізнесу згідно з встановленою політикою інформаційної безпеки.

СК11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.

Результати навчання

РН3. 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.

РН6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки.

РН7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.

РН8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки.

РН10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.

РН11. Вміти забезпечувати процеси захисту та функціонування системи управління інформаційною безпекою та захисту інформації на основі практик, навичок та знань, щодо інфраструктури кіберфізичних систем та інформаційних потоків.

РН12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

РН13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах.

РН14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.

РН16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.

PH17. Вміти розв'язувати задачі управління інформаційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.

PH18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.

PH19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-комунікаційних системах.

PH20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.

PH21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.

PH22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.

Обсяг дисципліни

Загальний обсяг дисципліни 90 год. (3 кредити ECTS): лекції – 10 год., лабораторні роботи – 20 год., самостійна робота – 60 год.

Передумови вивчення дисципліни (пререквізити)

Інформаційна безпека держави, Кібербезпека. Правові основи та технології, Фізичні основи технічних засобів розвідки.

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 проекти, майстер-класи.

Програма навчальної дисципліни

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Загальнотеоретичні засади правового регулювання інформації з обмеженим доступом. Поняття та правовий зміст персональних даних як об'єкта правової охорони в Україні. Поняття інформації та її ознаки. Інформація з обмеженим доступом у доктрині та праві. Загальна характеристика видів інформації з обмеженим доступом. Поняття персональних даних як об'єкта правової охорони та їх місце у правовідносинах. Загальні вимоги до обробки персональних даних у базах. Державний контроль в сфері обігу персональних даних.	2
Тема 2. Сучасні тенденції використання інформації з обмеженим доступом в установах. Основи технічного захисту інформації в сучасних інформаційних системах. Загрози від несанкціонованого витоку інформації з обмеженим доступом. Особливості кадрового забезпечення підрозділів захисту інформації з обмеженим доступом в установах. Використання заходів моніторингу у сфері захисту інформації з обмеженим доступом. Класи завдань з технічного захисту інформації в інформаційних системах. Захист інформації від витоку технічними каналами. Захист інформації від	2

Тема 3. Особливості поводження з інформацією з обмеженим доступом в процесі підприємницької діяльності. Захист електронної інформації. 2

Поняття, ознаки, принципи та види підприємницької діяльності. Поняття, зміст, загрози та складові безпеки підприємницької діяльності. Захист інформації з обмеженим доступом на підприємстві.

Засоби і методи виявлення та блокування технічних каналів витоку акустичної інформації. Захист акустичної інформації від зняття радіозакладними пристроями. Методи пошуку радіозакладних пристроїв. Захист інформації від витоку по технічних каналах, утворених допоміжними технічними засобами. Захист інформації від несанкціонованого запису звукозаписувальними пристроями. Захист письмової інформації від оптичного зняття.

Тема 4. Ведення документів, що містять конфіденційну інформацію із грифом “Для службового користування”. Організація роботи з секретними документами. Документ і документаційне забезпечення управління в Україні. 2

Приймання, розгляд та реєстрація документів. Розмноження і розсилання документів. Формування виконаних документів. Використання документів. Знищення документів.

Класифікація та реєстрація документів. Обладнання приміщень для зберігання матеріальних носіїв секретної інформації. Приймання та оброблення кореспонденції. Друкування матеріалів. Оформлення та відправлення документів. Попередній та інвентарний обліки документів.

Система органів держави, державних підприємств і державних установ України. Системи державних органів України. Законодавче регулювання діловодства та документування в державних установах України. Стандартизація, уніфікація та трафаретизація управлінських документів. Документування управлінської інформації в державних установах. Бланки організаційно-розпорядчих документів. Печатки державних установ. Датування і погодження управлінських документів. Затвердження і підписання управлінських документів. Загальні вимоги до тексту управлінських документів. Особливості підготовки та оформлення розпорядчих документів. Засвідчення копій та витягів службових документів. Реєстрація документів. Організація передачі документів та їх виконання та контроль за виконанням документів.

Тема 5. Юридична відповідальність у сфері обігу інформації з обмеженим доступом. 2

Теоретичні засади юридичної відповідальності у сфері обігу інформації з обмеженим доступом. Характеристика правопорушень у сфері обігу інформації з обмеженим доступом. Кримінальні правопорушення у сфері обігу інформації з обмеженим доступом. Адміністративні правопорушення у сфері обігу інформації з обмеженим доступом. Цивільні правопорушення у сфері обігу інформації з обмеженим доступом. Дисциплінарні правопорушення у сфері обігу інформації з обмеженим доступом.

Загальна кількість годин 10

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти α
Тема 1. Організаційна робота із захисту інформації з обмеженим доступом в країнах НАТО і ЄС.	6	0,1
Вивчення принципів та підходів до організації захисту інформації з обмеженим доступом у країнах-членах НАТО та ЄС. Аналіз		

структур, процедур і вимог до безпеки, які забезпечують надійність обміну даними між організаціями.

Тема 2 Вивчення міжнародного стандарту з оцінювання безпеки інформаційних технологій (ISO/IEC 15408).

6

0,1

Ознайомлення з основними положеннями стандарту ISO/IEC 15408 (Common Criteria), принципами оцінювання рівнів довіри до безпеки ІТ-систем та методологією сертифікації програмних і апаратних засобів.

Тема 3. Вивчення організаційної роботи служби захисту інформації в автоматизованих системах.

8

0,1

Дослідження завдань та функцій служби захисту інформації в автоматизованих системах. Розгляд організаційних заходів, процедур доступу, контролю та реагування на інциденти безпеки в інформаційних системах.

Загальна кількість годин

20

$\sum_{i=1}^n a_i = 0,3$

Контрольні роботи

Теми контрольних робіт

Вагові

коефіцієнти b

Тема 1. Правові засади регулювання та класифікація інформації з обмеженим доступом.

0,1

Розглядаються загальнотеоретичні основи правового регулювання інформації з обмеженим доступом. Вивчаються поняття інформації, її ознаки та класифікація, характеристика видів інформації з обмеженим доступом у національному та міжнародному праві.

Тема 2. Захист інформації з обмеженим доступом у сучасних умовах.

0,1

Аналізуються сучасні тенденції використання та захисту інформації з обмеженим доступом в установах та у сфері підприємницької діяльності. Особлива увага приділяється загрозам витоку інформації, організаційним і технічним заходам захисту, а також особливостям кадрового забезпечення відповідних підрозділів.

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. Міжнародний досвід захисту інформації з обмеженим доступом.

8

Ознайомлення з підходами НАТО та ЄС до організації захисту секретної та службової інформації, приклади кращих практик.

Тема 2. Стандарти інформаційної безпеки (ISO/IEC 15408, ISO/IEC 27001).

8

Вивчення основних положень міжнародних стандартів із забезпечення безпеки інформаційних технологій та їх впровадження в установах.

Тема 3. Технічні канали витоку інформації та методи їх блокування.

8

Аналіз каналів витоку (акустичних, електромагнітних, оптичних), методи виявлення та захисту.

Тема 4. Система роботи з документами з грифом «Для службового користування». Порядок приймання, обліку, зберігання та знищення документів, що містять конфіденційну інформацію.	9
Тема 5. Особливості організації секретного діловодства. Правила класифікації, реєстрації та обліку секретних документів. Обладнання приміщень та вимоги до персоналу.	9
Тема 6. Юридична відповідальність у сфері обігу інформації з обмеженим доступом. Види правопорушень, що виникають у сфері захисту інформації, та види юридичної відповідальності (кримінальна, адміністративна, цивільна, дисциплінарна).	9
Тема 7. Документування управлінської інформації в державних установах України. Нормативно-правова база ведення діловодства, стандартизація управлінських документів, сучасні тенденції цифрового документообігу.	9
Загальна кількість годин	60

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. Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту інформації. Посібник для курсантів ВНЗ МВС України. – К.: Вид. Національної академії внутріш. справ, 2012. – 104 с.

<https://nni1.naiu.kiev.ua/files/KIT/posibnuk%20tzi.pdf>

2. Організація захисту інформації з обмеженим доступом: навч. посіб./А.М.Гуз, І.П.Касперський, С.О.Князєв та ін. – К. Нац. акад., СБУ, 2018. – 252 с.

<http://za.inf.ua/bo/oziod18.pdf>

3. Організаційна робота із захисту інформації в інформаційно- комунікаційних системах (практикум). Навчально-методичний посібник для самостійної роботи студента з курсу за вибором/Шуаїбов О. К. - Ужгород, ДВНЗ «УжНУ», «Говерла». 2011. – 98 с.

<https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/20031/1/MET-ORG-ROB-ZACH-INF-11.pdf>

4. Практичний посібник для організації електронного документообігу та контролю доступу до конфіденційних даних. "Document and Records Management" – Waddington, P.

<https://www.osa.tas.gov.au/wp-content/uploads/2023/08/Advice-54-Records-Management-Toolkit-for-LG-Fact-Sheet-1-Mail-Processing.pdf>

5. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements URL:

<https://www.iso.org/ru/contents/data/standard/08/28/82875.html>

Додаткова література

6. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. Дата оновлення: 27.10.2022. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>.
7. Про державну таємницю: Закон України від 21.01.1994 № 3855-XII. Дата оновлення: 01.01.2024. URL: <https://zakon.rada.gov.ua/laws/show/3855-12#Text>
8. ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення. URL: <https://tzi.com.ua/downloads/DSTU%203396.0-96.pdf>.
9. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements URL: <https://www.iso.org/ru/contents/data/standard/08/28/82875.html>
10. ДСТУ ISO/IEC 15408-1:2023 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 1. Вступ та загальна модель (ISO/IEC 15408-1:2022, IDT).
https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104382
11. ДСТУ ISO/IEC 15408-2:2023 Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 2. Функційні компоненти безпеки (ISO/IEC 15408-2:2022, IDT).
https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104383
12. ДСТУ ISO/IEC 15408-3:2023 Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 3. (ISO/IEC 15408-3:2022, IDT).
https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104388
13. Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію: Постанова Кабінету Міністрів України від 19 жовтня 2016 р. № 736. Дата оновлення: 25.08.2023. URL: <https://zakon.rada.gov.ua/laws/show/736-2016-%D0%BF#Text>

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 (П, К, 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 СВСЕЄВ

30.08.2025



Гарант ОП
Роман КОРОЛЬОВ