



Силабус освітнього компонента Програма навчальної дисципліни



Організація документообігу з обмеженим доступом

Шифр та назва спеціальності

257 – Управління інформаційною безпекою

Інститут

ННІ комп'ютерних наук та інформаційних технологій (320)

Освітня програма

Управління інформаційною безпекою

Кафедра

Кібербезпеки (328)

Рівень освіти

Бакалавр

Тип дисципліни

Спеціальна (фахова), Обов'язкова

Семестр

5

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](#)



КОРОЛЬ Ольга Григорівна

olha.korol@khpi.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 "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 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-4. Здатність спілкуватися державною мовою як усно, так і письмово.

КЗ-8. Здатність до соціальної взаємодії, співробітництва, розв'язання конфліктів у сфері професійної діяльності, лідерства і командної роботи.

ФК-2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.

ФК-4. Здатність прогнозувати реалізації управлінських рішень щодо захисту інформації.

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-5. Вільно спілкуватися іноземною мовою у межах потреби своєї професійної діяльності.

ПРН-6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки

ПРН-10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.

ПРН-13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах.

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

ПРН-17. Вміти розв'язувати задачі управління інформаційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.

ПРН-18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.

ПРН-19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-комунікаційних системах.

ПРН-21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.

ПРН-22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.

Обсяг дисципліни

Загальний обсяг дисципліни 150 год. (5 кредитів ECTS): лекції – 32 год., лабораторні роботи – 32 год., самостійна робота – 86 год.

Передумови вивчення дисципліни (пререквізити)

Інформаційна безпека держави, Правове регулювання кібербезпеки, 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

Теми лекційних занять

Тема 1. Загальнотеоретичні засади правового регулювання інформації з обмеженим доступом.

Поняття інформації та її ознаки. Інформація з обмеженим доступом у доктрині та праві. Загальна характеристика видів інформації з обмеженим доступом.

Тема 2. Поняття та правовий зміст персональних даних як об'єкта правової охорони в Україні.

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.

Тема 3. Сучасні тенденції використання інформації з обмеженим доступом в установах.

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.

Тема 4. Особливості поводження з інформацією з обмеженим доступом в процесі підприємницької діяльності.

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

Тема 5. Основи технічного захисту інформації в сучасних інформаційних системах.

Класи завдань з технічного захисту інформації в інформаційних системах. Захист інформації від витоку технічними каналами. Захист інформації від несанкціонованого доступу.

Тема 6. Захист електронної інформації.

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 7. Ведення документів, що містять конфіденційну інформацію із грифом “Для службового користування”.

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

Тема 8. Організація роботи з секретними документами.

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.

Тема 9. Юридична відповідальність у сфері обігу інформації з обмеженим доступом.

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.

Тема 10. Документ і документаційне забезпечення управління в Україні.

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.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Організаційна робота із захисту інформації з обмеженим доступом в країнах НАТО і ЄС.

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

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

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. 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/Шуайбов 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

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

Роман КОРОЛЬОВ