Силабус освітнього компонента
Програма навчальної дисципліни

Організаційне забезпечення захисту інформації

Шифр та назва спеціальності
К4 – Управління інформаційною безпекою

Інститут
ННІ комп`ютерних наук та інформаційних технологій (320

Спеціалізація
-

Кафедра
Кібербезпеки (328)

Освітня програма
Управління інформаційною безпекою

Тип дисципліни
Вибіркова

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна

Семестр
7

Мова викладання
Українська

Викладачі, розробники

КОРОЛЬ Ольга Григорівна
olha.korol@khpi.edu.ua
Кандидат технічних наук, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 175, з яких 19 навчальних посібників, 74 статті у закордонних виданнях та фахових виданнях України, 18 патентів на корисну модель, 9 у наукометричній базі Scopus, гарант освітньо-професійної програми «Кібербезпека» другого (магістерського) рівня вищої освіти. 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

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: «Вступ до спеціальності. Ознайомча практика», «Організаційне

забезпечення захисту інформації», «Безпека в DevOps», «Організація та безпека баз даних», «Управління IT-проєктами та їх безпека» у студентів бакалавріату.
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Організаційне забезпечення захисту інформації" є вибірковою навчальною дисципліною. Дисципліна призначена для набуття теоретичних знань з захисту інформації та практичних навичок з організації забезпечення захисту інформації. Студенти вивчають основні напрямки, принципи та умови організаційного захисту; основні підходи, вимоги, методи та засоби.

Мета та цілі дисципліни

Формування теоретичних знань щодо проведення аналізу і оцінки загроз інформаційній безпеці об'єкта, оцінки збитків внаслідок протиправного розкриття інформації обмеженого доступу, організації і забезпечення режиму таємності, підбору, розподілу і роботи з кадрами.

Формат занять

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

Компетентності

ЗК3. Здатність до абстрактного мислення, аналізу та синтезу.
ЗК4. Здатність спілкуватися державною мовою як усно, так і письмово.
ЗК5. Здатність спілкуватися іноземною мовою.
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.
СК6. Здатність використовувати іноземну мову для отримання додаткових знань і умінь з питань управління інформаційною безпекою, взаємодіяти з іноземними партнерами.
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.
РН4. Вільно спілкуватися державною мовою.

РН5. Вільно спілкуватися іноземною мовою у межах потреби своєї професійної діяльності.
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.
РН17. Вміти розв'язувати задачі управління інфораційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.
РН18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.
РН19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах.
РН20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
РН21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.
РН22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.

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)

Антивірусний захист інформації , Комплексні системи захисту інформації, знання механізмів роботи з MS Word, MS Excel.

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. Завдання організаційного забезпечення захисту інформації. Аналіз і оцінка загроз інформаційної безпеки об'єкта. Роль організаційних заходів в створенні надійного механізму захисту інформації. Завдання, які вирішуються на організаційному рівні для забезпечення безпеки функціонування інформації. Класифікація загроз щодо інформаційної безпеки за базовими ознаками. Три основних види загроз.	2
Тема 2. Оцінка збитків внаслідок протиправного розкриття інформації обмеженого доступу і заходи щодо його локалізації. Перелік інформації з обмеженим доступом: державна, комерційна, банківська, професійна, службова таємниці, персональні дані і інтелектуальна власність. Огляд способів несанкціонованого доступу. Умови, що сприяють неправомірному володінню конфіденційною інформацією. Показник критерію ступеня відсутності або наявності завданої об'єкту матеріальної та моральної шкоди. Параметри вартості ризику від настання події.	2
Тема 3. Служба безпеки об'єкта. Основні завдання служби безпеки. Принципи системи безпеки підприємства. Функції служби захисту інформації підприємства. Перелік підрозділів служби безпеки об'єкта обробки інформації або підприємства і їх функції.	2
Тема 4. Підбір, розподіл і робота з кадрами. Етапи процедури відбору персоналу. Перевірка персоналу на благонадійність. Процес перевірки керівних кадрів. Укладання контрактів та угод про секретності. Особливості звільнення співробітників, які володіють конфіденційною інформацією. Підбір, розподіл і робота з кадрами служби безпеки. Дотримання трудової дисципліни і законності, зміцнення фізичного розвитку, здоров'я, підвищення культури. Соціальний захист персоналу служби безпеки.	2
Тема 5. Організація і забезпечення режиму таємності. Особливості режиму секретності. Порядок організації режиму секретності. Закриті роботи режиму секретності. Документи, які регламентують роботу підрозділів із захисту державної таємниці. Права працівників підрозділів із захисту державної таємниці. Основні завдання постійно діючих технічних комісій. Структура і зміст переліку відомостей, що становлять конфіденційну інформацію підприємства. Порядок допуску співробітників до відомостей, що становлять комерційну таємницю. Життєвий цикл документів, які містять комерційну таємницю.	2
Тема 6. Організація пропускного, внутрішньо об'єктового і протипожежного режиму. Заходи, які регламентує пропускний режим. Встановлення відповідальності за забезпечення пропускного режиму і збереження матеріальних цінностей у структурних підрозділах. Документація з пропускного режиму. Заходи внутрішньо об'єктового режиму. Забезпечення протипожежного режиму.	2
Тема 7. Захист інформації при аваріях та інших екстремальних ситуаціях. Особливості інформаційного впливу в екстремальних умовах. Превентивні заходи. Питання, які вирішуються і документуються при складанні попереджувального плану дій. Перелік відомостей плану дій.	2

Тема 8. Забезпечення захисту інформації при здійсненні міжнародного науково-технічного та економічного співробітництва. Канали поширення конфіденційної інформації.	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Шаблони документів. Ознайомлення з призначенням шаблонів, створення та використання стандартних форм документів для забезпечення єдиного стилю та структурованості.	3	-
Тема 2. Створення конструкційної сітки документа складної структури. Вивчення способів організації складних документів за допомогою таблиць, розділів, колонок та логічної структури.	3	0,1
Тема 3. Використання колонтитулів під час створення бланків документів. Практика оформлення верхніх та нижніх колонтитулів для нумерації сторінок, заголовків та службової інформації.	3	0,1
Тема 4. Використання стилів у електронних документах. Впровадження стилів для уніфікованого форматування тексту, заголовків, списків та інших елементів документа.	3	0,1
Тема 5. Основи створення документів з обчислюваними реквізитами. Використання формул, полів і автоматичних обчислень для динамічного заповнення реквізитів документа.	3	0,1
Тема 6. Автоматизація створення та розсилання однотипних документів. Робота з механізмами масових розсилок, злиття документів та автоматизації повторюваних процесів.	3	0,1
Тема 7. Створення переліків відомостей інформації з обмеженим доступом. Формування списків та таблиць конфіденційних даних із зазначенням рівнів доступу та обмежень.	3	0,1
Тема 8. Складання та оформлення організаційно-розпорядчих документів. Практичне створення наказів, розпоряджень та службових листів із дотриманням вимог нормативних документів.	3	-
Тема 9. Ведення документів, що містять інформацію з грифом. Формування справ. Організація роботи з документами з грифом «таємно», ведення справ, класифікація та зберігання.	4	0,1
Тема 10. Відбирання та передавання документів на знищення Процедури відбору застарілих документів, контроль їх утилізації та дотримання правил конфіденційності при знищенні.	4	0,1

Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 0{,}8$

Контрольні роботи

За наявності

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Організаційне забезпечення захисту інформації та аналіз загроз. Перевірка знань студентів щодо завдань організаційного рівня захисту інформації, класифікації загроз та їх впливу на безпеку об'єкта. Включає аналіз основних видів загроз інформаційній безпеці, оцінку ризиків та роль організаційних заходів у створенні надійного механізму захисту.	0,1
Тема 2. Оцінка збитків і заходи захисту інформації обмеженого доступу. Перевірка знань студентів щодо видів інформації з обмеженим доступом, методів несанкціонованого доступу та оцінки можливих збитків. Включає аналіз умов, що сприяють неправомірному володінню конфіденційною інформацією, розрахунок вартості ризику та заходів щодо локалізації потенційних загроз.	0,1
Загалом	$\sum_{i=1}^{m} b_i$=0,2

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу, підготовка до лабораторних занять, контрольних робіт та екзамену.

Опрацювання теоретичного матеріалу

Теми самостійного вивчення	Кількість годин
Тема 1. Методи внутрішнього аудиту інформаційної безпеки. Вивчення підходів до перевірки ефективності заходів захисту інформації та відповідності внутрішнім політикам.	7
Тема 2. Психологічні аспекти безпеки інформації. Вивчення поведінки персоналу, соціальної інженерії та методів зниження ризику людського фактору.	7
Тема 3. Криптографічні методи захисту інформації. Основи шифрування, цифрові підписи та їх застосування на організаційному рівні.	7
Тема 4. Управління ризиками інформаційної безпеки. Методи оцінки та управління ризиками, моделі і методики зниження можливих збитків..	7
Тема 5. Політики безпеки та стандарти ISO/IEC 27000. Вивчення міжнародних стандартів безпеки інформації та розробка корпоративних політик захисту.	7
Тема 6. Аудит і контроль доступу до інформаційних ресурсів. Методи управління доступом, ведення журналів доступу та контроль дотримання політик безпеки.	7
Тема 7. Соціальна інженерія та методи протидії. Аналіз загроз соціальної інженерії, навчання персоналу та впровадження превентивних заходів.	7

Тема 8. Інформаційна безпека у мобільних та хмарних системах. Особливості організаційних заходів безпеки при використанні мобільних пристроїв та хмарних сервісів.	7
Тема 9. Ведення журналів інцидентів і реагування на порушення безпеки. Практика фіксації інцидентів, класифікація подій та розробка планів реагування.	8
Тема 10. Захист персональних даних та GDPR. Організаційні заходи для захисту персональних даних відповідно до міжнародних стандартів та законодавства.	8
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. Про інформацію: Закон України від 2 жовтня 1992 року № 2657-XII. Поточна редакція від 27.07.2023.
URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
2. Про науково-технічну інформацію: Закони України від 25 червня 1993 року № 3322-XII . Поточна редакція від 19.04.2014.
URL: https://zakon.rada.gov.ua/laws/show/3322-12#Text
3. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. Поточна редакція від 01.01.2024.
URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
4. Про державну таємницю: Закон України від 21.01.1994 № 3855-XII // ВВР України. Поточна редакція від 01.01.2024.
URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text.
5. Про захист персональних даних: Закон України від 09.02.2010 №2297–VI // ВВР України. Поточна редакція від 27.10.2022.
URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.
6. Захист інформації в автоматизованих системах управління : навчальний посібник / Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 226с. URL: https://moodle.znu.edu.ua/pluginfile.php/1142772/mod_resource/content/1/Zahyst_informacii_ASU.PDF
7. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518. Поточна редакція від 07.09.2022.
URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text
8. Комплексні системи захисту інформації : навчальний посібник / [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця : ВНТУ, 2018. – 118 с.
URL: https://pdf.lib.vntu.edu.ua/books/IRVC/Yaremchuk_2018_118.pdf

9. Логінова Н. І. Правовий захист інформації : навчальний посібник / Н. І. Логінова, Р. Р. Дробожур. – Одеса : Фенікс, 2015. – 264 с.
URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/6dbd7fae-06f3-4afd-b2f7-871688668ea0/content
10. Остапов С. Е. Технологія захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
URL: http://kist.ntu.edu.ua/textPhD/tzi.pdf

Додаткова література

1. Бурячок В.Л., Толюпа С.В., Семко В.В. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: посібник. Київ. ДУТ-КНУ, 2016. 178 с.
https://duikt.edu.ua/uploads/p_303_92597962.pdf
2. Яремчук Ю. Є. Дослідження комбінаційних характеристик вітчизняних радіо непрозорих тканин М1, М2 та М3 / Ю. Є. Яремчук, В. С. Катаєв, В. В. Сінюгін // Реєстрація, зберігання та обробка даних. – 2015. – Том 17. №3 – С. 56-65.
http://nbuv.gov.ua/UJRN/rzod_2015_17_3_8
3. Яремчук Ю. Є. Дослідження характеристик вітчизняних радіо непрозорих тканин Н1, Н2 та Н3 при різних комбінаціях їхнього застосування / Ю. Є. Яремчук, В. С. Катаєв, М. Ю. Гижко, П. В. Павловський // Реєстрація, зберігання та обробка даних. – 2016. – Том 18, № 1. – С. 42-51.
https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/34773/93691.pdf?sequence=2&isAllowed=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:

$$О = П \cdot k_1 + К \cdot k_2 + І \cdot k_3 + Пк \cdot k_4$$

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, *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 ЄВСЕЄВ
	30.08.2025		**Гарант ОП** Роман КОРОЛЬОВ