Силабус освітнього компонента
Програма навчальної дисципліни

Організаційне забезпечення захисту інформації

Шифр та назва спеціальності
F5 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій (320

Спеціалізація
-

Кафедра
Кібербезпеки (328)

Освітня програма
Кібербезпека

Тип дисципліни
Вибіркова

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна, заочна

Семестр
7

Мова викладання
Українська, англійська

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: «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" охоплює комплекс заходів, що регламентують виробничу діяльність та взаємодію співробітників для захисту конфіденційної інформації від внутрішніх і зовнішніх загроз.

Мета та цілі дисципліни

Формування теоретичних знань щодо нормативно-правової бази, процедур безпеки, роль персоналу та організаційно-технічні методи для забезпечення конфіденційності, цілісності та доступності інформації.

Формат занять

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

Компетентності

ЗК1. Здатність застосовувати знання у практичних ситуаціях.
ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.
ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово.
ЗК6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації
СК2. Здатність використовувати інформаційні технологій, сучасні методи і моделей кібербезпеки та систем захисту інформації.
СК4. Здатність забезпечувати захист інформації в інформаційних системах згідно встановленої політики кібербезпеки та захисту інформації.

Результати навчання

РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.
РН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.
РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.
РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.
РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення та передачі сигналів тощо, принципи, методи і поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.
РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
РН10. Вміти використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.
РН12. Застосовувати методи захисту інформації в інформаційних системах згідно встановленої політики інформаційної безпеки.
РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних та програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних систем та\або інфраструктури організації в цілому.

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)

Захист об´єктів критичної інфраструктури, Інформаційна безпека держави, Правове регулювання кібербезпеки.

Особливості дисципліни, методи та технології навчання

Лекції проводяться інтерактивно з використанням мультимедійних технологій. Застосовуються активні форми проведення занять: лекція, лекційне опитування, практичні заняття, співбесіда, консультація. На заняттях використовується компетентністний підхід до навчання, акцентується увага на застосуванні он-лайн курсу з розгляду сучасних питань у галузі кібербезпеки.

Програма навчальної дисципліни

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Правові та нормативні основи. 1. Вивчення законодавства та нормативних актів, що регулюють захист інформації 2. Вивчення кращих практик з міжнародних стандартів організації захист інформації	2
Тема 2. Організаційні заходи. 1. Розробка та впровадження правил, що регламентують роботу співробітників 2. Процедури доступу та взаємодії з інформаційними системами	2
Тема 3. Управління персоналом. 1. Відбір персоналу, який має доступ до конфіденційної інформації 2. Навчання персоналу, який має доступ до конфіденційної інформації 3. Контроль за персоналом, який має доступ до конфіденційної інформації	4
Тема 4. Процедури безпеки. 1. Розробка процедур для запобігання несанкціонованого доступу, витоку або пошкодження даних 2. Реалізація процедур для запобігання несанкціонованого доступу, витоку або пошкодження даних	4
Тема 5. Забезпечення інформаційної безпеки. 1. Комплексне управління системою захисту інформації для протидії загрозам 2. Управління захистом від людського фактору та шлідливого програмного забезпечення	2
Тема 6. Кризове управління. 1. Планування дій у надзвичайних ситуаціях 2. Планування дій, пов'язаних із порушенням безпеки інформації	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Аналіз нормативно-правової бази. 1. Огляд та порівняльний аналіз ключових законодавчих актів України щодо захисту інформації. 2. Огляд та порівняльний аналіз та міжнародних стандартів щодо захисту інформації.	3	1
Тема 2. Інвентаризація та класифікація активів 1. Складання переліку інформаційних активів (сервери, дані, ПЗ) для вибраної організації. 2. Визначення власників активів та їхня класифікація за ступенем конфіденційності, цілісності та доступності.	3	1
Тема 3. Оцінка ризиків. 1. Проведення якісної або кількісної оцінки ризиків для 3-5 визначених інформаційних активів. 2. Ідентифікація загроз та вразливостей. 3. Розрахунок рівня ризику.	3	1
Тема 4. Розробка політики безпеки. 1. Складання проекту "Загальної політики інформаційної безпеки" організації. 2. Визначення її структури, цілей та сфер застосування.	3	1
Тема 5. Політика управління доступом. 1. Розробка політики управління доступом (фізичним та логічним). 2. Визначення правил Role-Based Access Control (RBAC) для типових посад (адміністратор, менеджер, рядовий співробітник).	3	1
Тема 6. Політика паролів та автентифікації. 1. Складання політики керування паролями (вимоги до складності, терміну дії, правил зміни) 2. Складання рекомендацій щодо використання багатофакторної аутентифікації (MFA).	3	1
Тема 7. Реагування на інформаційні інциденти. 1. Розробка процедури (Плану) реагування на типовий інцидент безпеки. 2. Визначення етапів: виявлення, локалізація, усунення, відновлення.	3	1
Тема 8. План безперервності бізнесу (BCP). 1. Складання плану забезпечення безперервності бізнесу 2. Складання плану відновлення після катастроф для критичної бізнес-функції. 3. Визначення RTO (Recovery Time Objective) та RPO (Recovery Point Objective).	3	1
Тема 9. Організація фізичного захисту 1. Розробка схеми фізичного захисту критичного об'єкта. 2. Обґрунтування вибору засобів контролю доступу (шлагбауми, СКУД, відеоспостереження).	4	1
Тема 10. Програма навчання персоналу 1. Розробка структури навчальної програми для співробітників з питань інформаційної безпеки.	4	1

2. Розробка змісту навчальної програми для співробітників з питань інформаційної безпеки.		
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 10$

Контрольні роботи

За наявності

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Основи та аналіз ризиків	2
Тема 2. Розробка політик та документації	2
Тема 3. Процедури та планування захисту	2
Загалом	$\sum_{i=1}^{m} b_i=6$

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. Огляд ключових законодавчих актів України 1. Закон України "Про захист інформації в інформаційно-комунікаційних системах"	7
Тема 2. Огляд Міжнародних Стандартів 1. Загальний регламент про захист даних (GDPR, ЄС)	7
Тема 3. Складання переліку та класифікації інформаційних активів використаємо приклад IT-компанії 1. Інвентаризація інформаційних активів 2. Класифікація активів (за критеріями CIA) 3. Визначення категорій даних	7
Тема 4. Якісна оцінка ризиків 1. Методологія оцінки 2. Аналіз та розрахунок ризиків	7
Тема 5. Складання політики управління доступом 1. Загальні положення та цілі політики 2. Управління фізичним доступом 3. Управління логічним доступом	7
Тема 6. Проєкт політики керування паролями та автентифікації для організації, що відповідає сучасним стандартам безпеки **1.** Вимоги до складності паролів 2. Термін дії та правила зміни паролів 3. Зберігання та використання паролі 4. Використання багатофакторної автентифікації	9
Тема 7. Процедура реагування на інформаційні інциденти **1.** Виявлення та реєстрація 2. Локалізація та ізоляція	7

Тема 8. Складання плану забезпечення безперервності бізнесу та плану відновлення після катастроф 1. Аналіз впливу на бізнес та ключові метрики 2. План відновлення після катастроф	7
Тема 9. Проєкт організації фізичного захисту критичного об'єкта є необхідною частиною організаційного захисту 1. Схема багаторівневого фізичного захисту 2. Обґрунтування вибору засобів контролю доступу 3. Підтримка та Тестування	7
Тема 10. Програма навчання персоналу з інформаційної безпеки 1. Вступний інструктаж 2. Регулярне навчання	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
0,6	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** Сергій ЄВСЕЄВ