ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
МАТЕМАТИЧНИЙ ФАКУЛЬТЕТ
Силабус навчальної дисципліни

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРБЕЗПЕКОЮ

Викладач: *Горелікова Тетяна Олексіївна*
Кафедра: *комп'ютерних наук, І корпус, ауд. 39*
E-mail: *horelikova.t@znu.edu.ua*
Телефон: *(061) 289-12-57*
Інші засоби зв'язку: M*oodle (форум курсу, приватні повідомлення)*

Освітня програма, рівень вищої освіти:		Кібербезпека та захист інформації Бакалавр					
Статус дисципліни:		Обов'язкова					
Кредити ECTS	3	**Навч. рік:**	2026-2027 1 семестр	**Рік навчання**	4	**Тижні**	16
Кількість годин	90	**Кількість змістових модулів**	4	**Лекційні заняття** – 16 год **Лабораторні заняття** – 32 год **Самостійна робота** – 42 год			
Вид контролю:		Залік					
Посилання на курс в Moodle		https://moodle.znu.edu.ua/course/view.php?id=18585					
Консультації: Запис на консультації: особисті повідомлення в Moodle							

ОПИС КУРСУ

Дисципліна присвячена вивченню стратегічних та організаційних засад побудови комплексної системи захисту інформаційної інфраструктури підприємства. У межах курсу здобувачі вищої освіти опановують законодавчу базу та міжнародні регламенти, розглядаючи їх крізь призму формування внутрішніх правил безпеки організації. Значна увага приділяється практичним аспектам захисту операційних систем, перевірці конфігурацій доступу та впровадженню механізмів відстеження подій. Студенти детально вивчають методологію побудови систем управління безпекою на основі міжнародних стандартів та моделей безперервного вдосконалення. Важливе місце в програмі посідає управління ризиками, де розглядаються процеси виявлення цінних ресурсів, оцінки загроз і розрахунку економічної доцільності заходів захисту. Окремий розділ присвячено управлінню кадровими питаннями, навчанню працівників правилам безпечної поведінки та мінімізації ризиків при співпраці з підрядниками. Курс також охоплює питання організації та проведення перевірок стану захищеності, складання звітів про виявлені порушення та оцінки відповідності встановленим вимогам. Завершальним етапом вивчення дисципліни є засвоєння процесів пошуку слабких місць у системах та формування завдань для залучення зовнішніх фахівців з перевірки стійкості до атак. У результаті опанування матеріалу здобувачі набувають навичок розробки керівних документів, оцінювання загрози для бізнесу та здійснення загального контролю безпеки цифрового середовища.

Програмні результати навчання	
ПРН1	Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності
ПРН2	Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки
ПРН3	Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків
ПРН4	Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації
ПРН5	Вирішувати задачі забезпечення безперервності бізнес- процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами
ПРН6	Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів
ПРН7	Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах

ОСНОВНІ НАВЧАЛЬНІ РЕСУРСИ

Презентації лекцій, презентаційні та відео матеріали, завдання та методичні рекомендації до практичних занять і самостійної роботи, методичне забезпечення поточного і підсумкового контроля, основна та додаткова література розміщені на платформі Moodle.

РОЗКЛАД КУРСУ ЗА ТЕМАМИ І КОНТРОЛЬНІ ЗАВДАННЯ

Поточні контрольні заходи

Основними контрольними заходами є завдання практичних занять, завдання самостійних робіт й тести, які виконуються після опанування відповідної теми курсу. Всі поточні контрольні заходи та методичні рекомендації до їх виконання розташовані на платформі Moodle.

Підсумкові контрольні заходи

Індивідуальне завдання. *Розроблення плану управління інформаційною та кібербезпекою для організації, аналіз ризиків, визначення заходів захисту інформаційних активів і підготовка рекомендацій щодо вдосконалення системи управління безпекою (перелік об'єктів та варіантів наведено в завданні). 20 балів. Завдання, вихідні дані та перелік варіантів робіт наведено в завданні на платформі Moodle.*

Підсумковий контроль (залік). *Виконання практичних завдань по варіантам –*
20 балів (проводиться письмово в аудиторії або онлайн на платформі Moodle).

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
МАТЕМАТИЧНИЙ ФАКУЛЬТЕТ
Силабус навчальної дисципліни

Тиждень і вид заняття	Тема заняття	Контрольні заходи, кількість балів
Змістовий модуль 1. Організаційно-правові засади та системний захист операційних систем		
Тиждень 1 Лекція 1	Стратегічне управління кібербезпекою. Законодавство України, міжнародні стандарти та регламенти.	—
Тиждень 1 Лабораторна робота 1	Встановлення відповідності конфігурацій доступу та привілеїв у Linux вимогам політик безпеки	*Лабораторна робота №1.* Контроль та аудит дотримання політики доступу в операційній системі Linux. (max 3 бали)
Тиждень 2 Лабораторна робота 2	Автоматизація контролю та технічного моніторингу матриці доступу	*Лабораторна робота №2.* Автоматизований збір та аудит конфігурації розмежування доступу й привілеїв. (max 3 бали)
Тиждень 3 Лекція 2	Технічні та організаційні заходи загартування систем. Централізація аудиту подій як інструмент контролю ІБ.	—
Тиждень 3 Лабораторна робота 3	Реалізація політик примусового розмежування доступу.	*Лабораторна робота №3.* Налаштування механізмів примусового контролю доступу та підсистеми. (max 3 бали)
Тиждень 4 Лабораторна робота 4	Провадження корпоративних правил обмеження програмного середовища.	*Лабораторна робота №4.* Реалізація політик обмеження програмного забезпечення та моніторингу подій. (max 3 бали)
Тиждень 4	Розробка корпоративного Стандарту безпечного налаштування та Політики обмеження програмного середовища для операційних систем.	*Самостійна робота №1.* Розробка нормативно-технічного документа. (max 1 бал)
Тиждень 4	Управлінські та регламентні засади системного захисту операційних систем.	*Тест №1.*(max 2 бали)
Змістовий модуль 2. Системи управління інформаційною безпекою (СУІБ) та менеджмент ризиків		
Тиждень 5 Лекція 3	Побудова та впровадження СУІБ за серією стандартів ISO/IEC 27001 / ISO/IEC 27002. Модель безперервного вдосконалення PDCA.	—
Тиждень 5 Практична робота 5	Моделювання контексту організації, визначення мети СУІБ та формування Сфери застосування.	*Практична робота №5.* Проєктування контексту організації та документальне оформлення сфери застосування СУІБ. (max 3 бали)
Тиждень 6 Практична робота 6	Розробка базового комплексу документації СУІБ: Політика інформаційної безпеки, політика прийнятного використання ресурсів.	*Практична робота №6.* Розробка нормативного базису СУІБ. (max 3 бали)
Тиждень 7 Лекція 4	Менеджмент кіберризиків. Методології оцінки та обробки ризиків.	—
Тиждень 7 Практична робота 7	Ідентифікація активів, загроз та вразливостей. Оцінка ймовірності та впливу ризиків.	*Практична робота №7.* Практична ідентифікація активів, загроз та якісна/кількісна оцінка кіберризиків організації (max 3 бали)

Тиждень і вид заняття	**Тема заняття**	**Контрольні заходи, кількість балів**
Тиждень 8 Практична робота 8	Розробка плана обробки ризиків та розрахунок показників ROI/ROSI для заходів захисту.	*Практична робота №8*. Складання Реєстру та Плану обробки ризиків із розрахунком економічної ефективності (ROSI) (max 3 бали)
Тиждень 8	Розробка елементів системи управління інформаційною безпекою (СУІБ): від аналізу контексту організації до Політики класифікації активів.	*Самостійна робота №2*. Практичне проектування управлінської документації СУІБ. (max 1 бал)
Тиждень 8	СУІБ та менеджмент ризиків кібербезпеки	*Тест №2*.(max 2 бали)
Змістовий модуль 3. Управління людським фактором, активами та безпекою ланцюга постачань		
Тиждень 9 Лекція 5	Управління кадровою безпекою та культура кібербезпеки. Програми підвищення обізнаності та протидія соціальній інженерії.	—
Тиждень 9 Практична робота 9	Розробка Програми підвищення обізнаності та сценаріїв тестування персоналу.	*Практична робота №9*. Розробка комплексної програми навчання та оцінки обізнаності персоналу з кібербезпеки. (max 3 бали)
Тиждень 10 Практична робота 10	Формування регламентів кадрової безпеки на етапах найму, трудової діяльності та звільнення співробітників.	*Практична робота №10*. Розробка регламенту HR-безпеки та чек-листів контролю при зміні/звільненні персоналу. (max 3 бали)
Тиждень 11 Лекція 6	Організація управління активами та оцінка ризиків безпеки в ланцюгу постачань.	—
Тиждень 11 Практична робота 11	Побудова Інвентарного реєстру активів організації та розробка Політики класифікації інформації.	*Практична робота №11*. Класифікація інформаційних активів та визначення рольової моделі володіння. (max 3 бали)
Тиждень 12 Практична робота 12	Розробка вимог з кібербезпеки до контрагентів, постачальників та оцінка ризиків третіх сторін.	*Практична робота №12*. Формування регламенту оцінки ризиків підрядників. (max 3 бали)
Тиждень 12	Кадрова безпека, протидія внутрішнім загрозам та оцінка ризиків постачальників	*Самостійна робота №3*. Розробка Політики безпеки ланцюга постачань або Програми протидії внутрішнім загрозам (max 1 бал)
Тиждень 12	Управління кадровою безпекою, активами та ризиками третіх сторін	*Тест №3*.(max 2 бали)
Змістовий модуль 4. Аудит, перевірка та оцінка захищеності		
Тиждень 13 Лекція 7	Аудит інформаційної безпеки. Планування, методологія та проведення внутрішніх/зовнішніх перевірок.	—
Тиждень 13 Практична робота 13	Складання програми та чек-листів аудиту інформаційної безпеки відповідно до Декларації про застосовність.	*Практична робота №13*. Розробка програми та чек-листів аудиту. (max 3 бали)
Тиждень 14 Практична робота 14	Оформлення результатів аудиту: складання протоколів невідповідностей та підготовка підсумкового звіту.	*Практична робота №14*. Оформлення результатів аудиту та звіту про невідповідності. (max 3 бали)

Тиждень і вид заняття	**Тема заняття**	**Контрольні заходи, кількість балів**
Тиждень 15 Лекція 8	Організація процесів управління вразливостями, проведення аудиту захищеності та замовлення послуг	—
Тиждень 15 Практична робота 15	Розробка регламенту моніторингу вразливостей, оцінка ризиків пріоритезація оновлень.	*Практична робота №15.* Розробка регламенту управління вразливостями та оцінка ризиків. (max 3 бали)
Тиждень 16 Практична робота 16	Формування технічного завдання на проведення зовнішнього аудиту захищеності.	Практична робота №16. Формування ТЗ на проведення аудиту захищеності. (max 3 бали)
Тиждень 16	Аналіз та розв'язання комплексного управлінського кейсу з оцінки захищеності та комплаєнсу організації	*Самостійна робота №4.* Розв'язання комплексного управлінського кейсу. (max 1 бал)
Тиждень 16	Аудит, комплаєнс та оцінка захищеності інформаційних систем.	*Тест №4.*(max 2 бали)

Шкала оцінювання: національна та ECTS

За шкалою ECTS	За шкалою університету	За національною шкалою	
		Екзамен	Залік
A	90 – 100 (відмінно)	5 (відмінно)	Зараховано
B	85 – 89 (дуже добре)	4 (добре)	
C	75 – 84 (добре)		
D	70 – 74 (задовільно)	3 (задовільно)	
E	60 – 69 (достатньо)		
FX	35 – 59 (незадовільно – з можливістю повторного складання)	2 (незадовільно)	Не зараховано
F	1 – 34 (незадовільно – з обов'язковим повторним курсом)		

СПИСОК ДЖЕРЕЛ

Основна література

1. Луценко В.М., Прогонов Д.О. Методи та засоби технічного захисту інформації: навч. посібник. – Київ: КПІ ім. Ігоря Сікорського, 2021. – 289 с.
2. Гребенюк А.М., Рибальченко Л.В. Основи управління інформаційною безпекою: навч. посібник – Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. –144 с.
3. Гур'єв В.І., Мехед Д.Б., Ткач Ю.М., Фірсова І.В. Інформаційна безпека держави: навч. посібник. – Ніжин: ТПК «Орхідея», 2018. – 166 с.
4. Шелест, М.Є., Корченко, О.Г., Іванченко, Є.В., Ткач, Ю.М. , Казмірчук, С.В. Менеджмент інформаційної безпеки: навчальний посібник для студентів спеціальності 125" Кібербезпека".Ніжин : ФОП Лук'яненко В.В. ТПК «Орхідея»,2019. – 408 с
5. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с.

Інформаційні ресурси та нормативно-правове забезпечення

6. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України. URL: https://zakon.rada.gov.ua/laws/show/v0365500-11.
7. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).

РЕГУЛЯЦІЇ І ПОЛІТИКИ КУРСУ[1]

Відвідування занять. Регуляція пропусків.
Інтерактивний характер курсу передбачає обов'язкове відвідування практичних занять. Аспіранти, які за певних обставин не можуть відвідувати практичні заняття регулярно, мусять впродовж тижня узгодити із викладачем графік індивідуального відпрацювання пропущених занять. Окремі пропущенні завдання мають бути відпрацьовані на найближчій консультації впродовж тижня після пропуску. Відпрацювання занять здійснюється шляхом виконання індивідуального письмового завдання. Аспіранти, які станом на початок екзаменаційної сесії мають понад 70% невідпрацьованих пропущених занять, до сесії не допускаються.

Політика академічної доброчесності
Усі письмові роботи, що виконуються аспірантами під час проходження курсу, перевіряються на наявність плагіату за допомогою спеціалізованого програмного забезпечення UniCheck. Відповідно до чинних правових норм, плагіатом вважатиметься: копіювання чужої наукової роботи чи декількох робіт та оприлюднення результату під своїм іменем; створення суміші власного та запозиченого тексту без належного цитування джерел; рерайт (перефразування чужої праці без згадування автора оригінального тексту). Будь-яка ідея, думка чи речення, ілюстрація чи фото, яке ви запозичуєте, має супроводжуватися посиланням на першоджерело. Приклади оформлення цитувань див. на платформі Moodle: https://cutt.ly/1I4Q8Me.
Виконавці індивідуальних завдань обов'язково додають до текстів своїх робіт власноруч підписану Декларацію академічної доброчесності (див. посилання у Додатку до силабусу).
Роботи, в яких виявлено ознаки плагіату, до розгляду не приймаються і відхиляються без права перескладання. Якщо ви не впевнені, чи підпадають зроблені вами запозичення під визначення плагіату, будь ласка, проконсультуйтеся з викладачем.
Висока академічна культура та європейські стандарти якості освіти, яких дотримуються в ЗНУ, вимагають від дослідників відповідального ставлення до вибору джерел. Посилання на такі ресурси, як Wikipedia, бази даних рефератів та письмових робіт (Studopedia.org та подібні) є неприпустимим. Рекомендовані бази даних для пошуку джерел: електронні ресурси Національної бібліотеки ім. Вернадського: http://www.nbuv.gov.ua; *наукометрична база Scopus: https://www.scopus.com; наукометрична база Web of Science: https://apps.webofknowledge.com*

Використання комп'ютерів/телефонів на занятті
Використання мобільних телефонів, планшетів та інших гаджетів під час лекційних та практичних занять дозволяється виключно у навчальних цілях (для уточнення певних даних, перевірки правопису, отримання довідкової інформації тощо). Будь ласка, не забувайте активувати режим «без звуку» до початку заняття.

Комунікація
Базовою платформою для комунікації викладача з аспірантами є платформа Moodle. Важливі повідомлення загального характеру регулярно розміщуються викладачем на форумі курсу. Для персональних запитів використовується сервіс приватних повідомлень. Відповіді на запити аспірантів подаються викладачем впродовж трьох робочих днів. Для оперативного отримання повідомлень про оцінки та нову інформацію, розміщену на платформі Moodle, будь ласка, переконайтеся, що адреса електронної пошти, зазначена у вашому профайлі на Moodle, є актуальною, та регулярно перевіряйте папку «Спам». Якщо за технічних причин доступ до Moodle є неможливим або ваше питання потребує термінового розгляду, направте електронного листа на пошту або у зазначені меседжери викладача. У листі обов'язково вкажіть ваше прізвище, ім'я та курс.

---

[1] Тут зазначається все, що важливо для курсу: наприклад, умови допуску до лабораторій, реактивів і т.д. Викладач сам вирішує, що треба знати студенту для успішного проходження курсу!

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
МАТЕМАТИЧНИЙ ФАКУЛЬТЕТ
Силабус навчальної дисципліни

ДОДАТОК ДО СИЛАБУСУ ЗНУ

АКАДЕМІЧНА ДОБРОЧЕСНІСТЬ. Аспіранти і викладачі Запорізького національного університету несуть персональну відповідальність за дотримання принципів академічної доброчесності, затверджених ***Кодексом академічної доброчесності ЗНУ*****:** https://tinyurl.com/ya6yk4ad. *Декларація академічної доброчесності здобувача вищої освіти* (додається в обов'язковому порядку до письмових кваліфікаційних робіт, виконаних здобувачем, та засвідчується особистим підписом): https://tinyurl.com/y6wzzlu3.

ОСВІТНІЙ ПРОЦЕС ТА ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ОСВІТИ. Перевірка набутих аспірантами знань, навичок та вмінь (атестації, заліки, іспити та інші форми контролю) є невід'ємною складовою системи забезпечення якості освіти і проводиться відповідно до *Положення про організацію та методику проведення поточного та підсумкового семестрового контролю навчання студентів ЗНУ*: https://tinyurl.com/y9tve4lk**.**

ПОВТОРНЕ ВИВЧЕННЯ ДИСЦИПЛІН, ВІДРАХУВАННЯ. Наявність академічної заборгованості до 6 навчальних дисциплін (в тому числі проходження практики чи виконання курсової роботи) за результатами однієї екзаменаційної сесії є підставою для надання аспіранту права на повторне вивчення зазначених навчальних дисциплін. Порядок повторного вивчення визначається *Положенням про порядок повторного вивчення навчальних дисциплін та повторного навчання у ЗНУ*: https://tinyurl.com/y9pkmmp5. Підстави та процедури відрахування аспірантів, у тому числі за невиконання навчального плану, регламентуються *Положенням про порядок переведення, відрахування та поновлення студентів у ЗНУ*: https://tinyurl.com/ycds57la.

НЕФОРМАЛЬНА ОСВІТА. Порядок зарахування результатів навчання, підтверджених сертифікатами, свідоцтвами, іншими документами, здобутими поза основним місцем навчання, регулюється *Положенням про порядок визнання результатів навчання, отриманих у неформальній освіті*: https://tinyurl.com/y8gbt4xs.

ВИРІШЕННЯ КОНФЛІКТІВ. Порядок і процедури врегулювання конфліктів, пов'язаних із корупційними діями, зіткненням інтересів, різними формами дискримінації, сексуальними домаганнями, міжособистісними стосунками та іншими ситуаціями, що можуть виникнути під час навчання, регламентуються *Положенням про порядок і процедури вирішення конфліктних ситуацій у ЗНУ*: https://tinyurl.com/ycyfws9v. Конфліктні ситуації, що виникають у сфері стипендіального забезпечення здобувачів вищої освіти, вирішуються стипендіальними комісіями факультетів, коледжів та університету в межах їх повноважень, відповідно до: *Положення про порядок призначення і виплати академічних стипендій у ЗНУ*: https://tinyurl.com/yd6bq6p9; *Положення про призначення та виплату соціальних стипендій у ЗНУ*: https://tinyurl.com/y9r5dpwh.

ЗАПОБІГАННЯ КОРУПЦІЇ. Уповноважена особа з питань запобігання та виявлення корупції (Воронков В. В., 1 корп., 29 каб., тел. +38 (061) 289-14-18).

ПСИХОЛОГІЧНА ДОПОМОГА. Телефон довіри практичного психолога (061)228-15-84 (щоденно з 9 до 21).

РІВНІ МОЖЛИВОСТІ ТА ІНКЛЮЗИВНЕ ОСВІТНЄ СЕРЕДОВИЩЕ. Центральні входи усіх навчальних корпусів ЗНУ обладнані пандусами для забезпечення доступу осіб з інвалідністю та інших маломобільних груп населення. Допомога для здійснення входу у разі потреби надається черговими охоронцями навчальних корпусів. Якщо вам потрібна спеціалізована допомога, будь-ласка, зателефонуйте (061) 228-75-11 (начальник охорони). Порядок супроводу (надання допомоги) осіб з інвалідністю та інших маломобільних груп населення у ЗНУ: https://tinyurl.com/ydhcsagx.

РЕСУРСИ ДЛЯ НАВЧАННЯ. Наукова бібліотека: http://library.znu.edu.ua. Графік роботи абонементів: понеділок – п`ятниця з 08.00 до 17.00; субота з 09.00 до 15.00.

ЕЛЕКТРОННЕ ЗАБЕЗПЕЧЕННЯ НАВЧАННЯ (MOODLE): HTTPS://MOODLE.ZNU.EDU.UA
Якщо забули пароль/логін, направте листа з темою «Забув пароль/логін» за адресами:
· для аспірантів ЗНУ - moodle.znu@gmail.com, Савченко Тетяна Володимирівна
У листі вкажіть: прізвище, ім'я, по-батькові українською мовою; шифр групи; електронну адресу.
Якщо ви вказували електронну адресу в профілі системи Moodle ЗНУ, то використовуйте посилання для відновлення паролю https://moodle.znu.edu.ua/mod/page/view.php?id=133015.

Центр інтенсивного вивчення іноземних мов: http://sites.znu.edu.ua/child-advance/
Центр німецької мови, партнер Гете-інституту: https://www.znu.edu.ua/ukr/edu/ocznu/nim
Школа Конфуція (вивчення китайської мови): http://sites.znu.edu.ua/confucius.