



## Силабус курсу СИСТЕМИ ТА ТЕХНОЛОГІЇ КІБЕРБЕЗПЕКИ

Ступінь вищої освіти – бакалавр

Рік навчання: 4

Семестр: 7

Кількість кредитів: 5

Мова викладання: українська

### Керівник курсу

ПП

Людмила Бабала

Контактна інформація

Ludaduma7@gmail.com

### Опис дисципліни

Курс поєднує теоретичні знання з практичними навичками через лекції, лабораторні роботи, самостійну роботу та тренінги. Особлива увага приділяється розробці реальних проектів, таких як створення безпечних NO-CODE додатків для моніторингу кібербезпеки.

Мета дисципліни "Системи та технології кібербезпеки" - сформувати у студентів комплексне розуміння сучасних методів та технологій забезпечення кібербезпеки, з особливим акцентом на хмарні технології та розробку безпечних додатків, включаючи використання платформи Glide.app.

Дисципліна спрямована на підготовку фахівців, здатних аналізувати та оцінювати кіберзагрози, впроваджувати ефективні стратегії захисту, розробляти безпечні додатки та забезпечувати відповідність систем нормативним вимогам у сфері кібербезпеки.

### Структура курсу

Години лек/пр	Тема	Результати навчання	Завдання
2/1	Основи кібербезпеки та сучасні загрози в хмарному середовищі.	Вивчення базових концепцій, типів сучасних кіберзагроз та методів захисту інформації.	Поточне опитування
3/2	Хмарні технології та їх роль у забезпеченні кібербезпеки підприємств	Огляд моделей хмарних послуг, архітектури безпеки в хмарі та стратегій мінімізації ризиків.	Поточне опитування
2/1	Системи виявлення та запобігання вторгнень (IDS/IPS) в хмарних інфраструктурах	Вивчення принципів роботи IDS/IPS у хмарних інфраструктурах.	Поточне опитування
2/2	Управління ідентифікацією та доступом (IAM) у хмарних середовищах	Освоєння методів автентифікації, авторизації та управління привілеями у хмарних середовищах.	Поточне опитування
3/2	Шифрування даних та управління ключами в хмарних сховищах	Вивчення методів шифрування та управління ключами в хмарних сховищах.	Поточне опитування
2/1	Безпека мобільних додатків: розробка захищених застосунків з використанням Glide.app	Розробка безпечних мобільних додатків: Практичне застосування принципів безпечної розробки з використанням платформи Glide.app.	Поточне опитування, тестування

2/1	Аналіз вразливостей та тестування на проникнення в хмарних системах	Освоєння методологій та інструментів для оцінки безпеки хмарних ресурсів.	Поточне опитування
3/2	Реагування на інциденти та управління безпекою в хмарних середовищах	Вивчення процесів виявлення, класифікації та розслідування інцидентів безпеки в хмарному середовищі	Поточне опитування
2/2	Відповідність нормативним вимогам та аудит безпеки хмарних сервісів	Ознайомлення з ключовими стандартами та регуляторними вимогами у сфері кібербезпеки.	Поточне опитування
3/2	Створення захищених NO-CODE додатків для моніторингу кібербезпеки за допомогою Glide.app	Практичне застосування знань для розробки захищених додатків для моніторингу кібербезпеки за допомогою Glide.app.	Поточне опитування

### Рекомендовані джерела інформації

1. Stallings, W., & Brown, L. (2022). Computer Security: Principles and Practice (4th ed.). Pearson.
2. Sullivan, N. (2022). Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Wiley.
3. Vacca, J. R. (2021). Cloud Computing Security: Foundations and Challenges. CRC Press.
4. Conklin, W. A., White, G., Williams, D., Davis, R. L., & Cothren, C. (2021). CompTIA Security+ All-in-One Exam Guide, Sixth Edition (Exam SY0-601). McGraw Hill.
5. Fowler, S. (2019). Production-Ready Microservices: Building Standardized Systems Across an Engineering Organization. O'Reilly Media.
6. Basta, A., & Halton, W. (2019). Computer Security and Penetration Testing (3rd ed.). Cengage Learning.
7. Yoon, H. J. (2020). Cybersecurity in the Digital Age: Tools, Techniques & Best Practices. Business Expert Press.
8. Diogenes, Y., & DMITRENKO, M. (2019). Cybersecurity – Azure Security: Get to grips with building and maintaining cloud security solutions for your Azure environment. Packt Publishing.
9. <https://docs.glideapps.com/>
10. <https://www.udemy.com/course/build-no-code-apps-with-glide/>
11. Winden, M. (2021). "The Definitive No-Code Revolution Guide." Self-published.
12. <https://www.youtube.com/c/GlideApps>
13. <https://techcrunch.com/search/glide>

### Політика оцінювання

**Політика щодо дедлайнів та перескладання:** Для виконання індивідуальних завдань і проведення контрольних заходів встановлюються конкретні терміни. Перескладання модулів відбувається з дозволу дирекції факультету за наявності поважних причин (наприклад, лікарняний).

**Політика щодо академічної доброчесності:** Використання друкованих і електронних джерел інформації під час контрольних заходів заборонено.

**Політика щодо відвідування:** Відвідування занять є обов'язковим компонентом оцінювання. За об'єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування) навчання може відбуватись в онлайн формі за погодженням із керівником курсу.

### Оцінювання

Модуль 1	Модуль 2	Модуль 3
----------	----------	----------

40%	40%	5%	15%
Поточне оцінювання	Модульний контроль	Тренінги	Самостійна робота
Оцінка за даний модуль визначається як середнє арифметичне за виконання та захист лабораторних робіт №1-6.	Складається із письмової роботи, яка містить 2 теоретичні запитання (по 30 балів - max 60 балів) та 10 тестів (по 4 бали - max 40 балів).	Оцінюється виконання індивідуального завдання тренінгу (виконання роботи - 60 балів, захист роботи - 40 балів)	Оцінюється якість розробки, відповідність потребам підприємства, повнота реалізації функціоналу (виконання роботи - 60 балів, захист роботи - 40 балів)

Шкала оцінювання:

ECTS	Бали	Зміст
A	90–100	відмінно
B	85–89	добре
C	75-84	добре
D	65-74	задовільно
E	60-64	достатньо
FX	35-59	незадовільно з можливістю повторного складання
F	1-34	незадовільно з обов'язковим повторним курсом