МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій

Затверджую
Декан факультету комп'ютерних інформаційних технологій
_____ Ігор ЯКИМЕНКО
"30" 08 2024р.

Затверджую
Проректор з науково-педагогічної роботи
_____ Віктор ОСТРОВЕРХОВ
"30" 08 2024 р.

РОБОЧА ПРОГРАМА

з дисципліни

«Системи та технології кібербезпеки»

Ступінь вищої освіти – перший (бакалаврський)
Галузь знань: 12 Інформаційні технології
Спеціальність: 125 Кібезбезпека
Освітньо-професійна програма «Кібезбезпека»

Кафедра кібербезпеки

Форма навчання	Курс	Семестр	Лекції	Лабор	ІРС	Тре-нінг	СРС	Разом	Залік
Денна	4	7	26	12	2	6	104	150	7

Тернопіль – ЗУНУ - 2024

Робочу програму склала к.е.н., доц.кафедри кібербезпеки Людмила БАБАЛА

Робоча програма затверджена на засіданні кафедри кібербезпеки, протокол № 1 від 26.08.2024 р.

Завідувач кафедри кібербезпеки проф. Василь ЯЦКІВ

Розглянуто та схвалено групою забезпечення спеціальності Кібербезпека та захист інформації, протокол № 1 від 30.08.2024 р.

Керівнник ГЗС проф. Василь ЯЦКІВ

Гарант ОПП проф. Михайло КАСЯНЧУК

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Системи та технології кібербезпеки»

1. Опис дисципліни «Системи та технології кібербезпеки»

Дисципліна – Системи та технології кібербезпеки	Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень	Характеристика навчальної дисципліни
Кількість кредитів ECTS 5	**Галузь знань –** 12 «Інформаційні технології»	Вибіркова дисципліна, мова навчання - *українська*
Кількість залікових модулів - 3	**Спеціальність –** 125 «Кібербезпека»	*Денна:* Рік підготовки:4 Семестр – 1
Кількість змістових модулів - 2	Ступінь вищої освіти – бакалавр	*Денна:* лекції – 24 год.; лабор.- 16 год
Загальна кількість годин - - 150		Самостійна робота: 102 *год.,* Тренінг – 6 год. Індивідуальна робота : 2*год.*
Тижневих годин: 10 год., з них аудиторних – 3 год		Вид підсумкового контролю – *залік*

2. Мета й завдання вивчення дисципліни «Системи та технології кібербезпеки**»**

2.1. Мета вивчення дисципліни:

Метою викладання дисципліни "Системи та технології кібербезпеки" є формування у студентів комплексного розуміння сучасних методів та технологій забезпечення кібербезпеки, з особливим акцентом на хмарні технології та розробку безпечних додатків, включаючи використання платформи Glide.app.

2.2. Завдання вивчення дисципліни:

В результаті вивчення курсу "Системи та технології кібербезпеки" студенти повинні:

знати:

- Основні концепції кібербезпеки та типи сучасних кіберзагроз;
- Принципи роботи та архітектуру хмарних технологій з точки зору безпеки;
- Методи виявлення та запобігання вторгненням у хмарних середовищах;
- Концепції управління ідентифікацією та доступом у хмарних сервісах;
- Основи криптографії та методи шифрування даних у хмарних сховищах;
- Принципи безпечної розробки мобільних додатків, зокрема з використанням Glide.app;
- Методології тестування на проникнення та аналізу вразливостей хмарних систем;
- Процеси реагування на інциденти та управління безпекою в хмарному середовищі;

- Ключові нормативні вимоги та стандарти у сфері кібербезпеки;
- Можливості створення no-code додатків для моніторингу кібербезпеки

вміти:

- Аналізувати та оцінювати кіберзагрози в сучасному цифровому середовищі
- Налаштовувати та управляти системами виявлення та запобігання вторгнень у хмарних інфраструктурах
- Впроваджувати ефективні стратегії управління ідентифікацією та доступом
- Застосовувати методи шифрування та управління ключами для захисту даних у хмарі
- Розробляти безпечні мобільні додатки з використанням Glide.app
- Проводити аналіз вразливостей та тестування на проникнення в хмарних системах
- Розробляти та впроваджувати плани реагування на інциденти кібербезпеки
- Забезпечувати відповідність хмарних сервісів нормативним вимогам та проводити аудит безпеки
- Створювати захищені no-code додатки для моніторингу кібербезпеки за допомогою Glide.app.

3. Програма дисципліни " Системи та технології кібербезпеки "

Змістовий модуль 1 – Основи кібербезпеки та захист даних у хмарних середовищах

Тема 1. Основи кібербезпеки та сучасні загрози в хмарному середовищі

- Поняття кібербезпеки та її важливість
- Типи кіберзагроз (віруси, фішинг, ransomware тощо)
- Вектори атак та методи їх виявлення у хмарному середовищі
- Базові принципи захисту інформації у хмарному середовищі
- Роль людського фактору в кібербезпеці

Тема 2. Хмарні технології та їх роль у забезпеченні кібербезпеки підприємств

- Огляд моделей хмарних послуг (IaaS, PaaS, SaaS)
- Переваги та ризики використання хмарних технологій
- Архітектура безпеки в хмарі
- Розподіл відповідальності між провайдером та клієнтом
- Стратегії мінімізації ризиків у хмарному середовищі

Тема 3. Системи виявлення та запобігання вторгнень (IDS/IPS) в хмарних інфраструктурах

- Принципи роботи IDS/IPS
- Особливості впровадження IDS/IPS у хмарному середовищі
- Аналіз мережевого трафіку та виявлення аномалій
- Налаштування та управління правилами IDS/IPS
- Інтеграція з іншими системами безпеки

Тема 4. Управління ідентифікацією та доступом (IAM) у хмарних середовищах

- Концепції IAM у хмарних сервісах
- Методи автентифікації та авторизації
- Управління привілеями та ролями
- Федеративний доступ та Single Sign-On (SSO)
- Моніторинг та аудит доступу

Тема 5. Шифрування даних та управління ключами в хмарних сховищах

- Основи криптографії у хмарних середовищах
- Шифрування даних у стані спокою та під час передачі
- Управління життєвим циклом ключів
- Технології захисту ключів (HSM, KMS)
- Відповідність регуляторним вимогам щодо шифрування

Змістовий модуль 2 – Розробка, безпека та управління хмарними додатками

Тема 6. Безпека мобільних додатків: розробка захищених застосунків з використанням Glide.app

- Огляд платформи Glide.app та її можливостей
- Принципи безпечної розробки мобільних додатків
- Реалізація механізмів автентифікації та авторизації в Glide.app
- Захист даних користувачів у додатках Glide
- Тестування безпеки додатків, створених на Glide.app

Тема 7. Аналіз вразливостей та тестування на проникнення в хмарних системах

- Методології тестування на проникнення
- Специфіка аналізу вразливостей у хмарних середовищах
- Інструменти для сканування та оцінки безпеки хмарних ресурсів
- Автоматизація процесів виявлення вразливостей
- Розробка та впровадження плану усунення виявлених вразливостей

Тема 8. Реагування на інциденти та управління безпекою в хмарних середовищах

- Створення плану реагування на інциденти для хмарних систем
- Виявлення та класифікація інцидентів безпеки
- Процеси розслідування та аналізу інцидентів у хмарі
- Інструменти та платформи для управління безпекою в хмарі

Тема 9. Відповідність нормативним вимогам та аудит безпеки хмарних сервісів

- Огляд ключових стандартів та регуляторних вимог (GDPR, HIPAA, PCI DSS)
- Проведення аудиту безпеки хмарних сервісів
- Управління ризиками та відповідністю
- Документування та звітність з питань безпеки
- Співпраця з хмарними провайдерами щодо відповідності вимогам

Тема 10. Створення захищених NO-CODE додатків для моніторингу кібербезпеки за допомогою Glide.app

- Огляд можливостей Glide.app для створення інструментів моніторингу
- Проектування інтерфейсу додатку для відстеження показників безпеки
- Інтеграція з джерелами даних про кібербезпеку
- Налаштування сповіщень та звітності в додатку
- Забезпечення безпеки самого додатку для моніторингу

4. Структура залікового кредиту дисципліни "Системи та технології кібербезпеки"

		Кількість годин				
	Лекції	Лабор. заняття	Індивід робота	Тренінг	Самос-тійна робота	Контр. заходи
Змістовий модуль 1 – Основи кібербезпеки та захист даних у хмарних середовищах						
Тема 1. Основи кібербезпеки та сучасні загрози в хмарному середовищі	2	1	1	3	10	поточне опит.
Тема 2. Хмарні технології та їх роль у забезпеченні кібербезпеки підприємств	3	2			11	поточне опит.
Тема 3. Системи виявлення та запобігання вторгнень (IDS/IPS) в хмарних інфраструктурах	2	1			10	поточне опит.
Тема 4. Управління ідентифікацією та доступом (IAM) у хмарних середовищах	2	2			11	поточне опит.
Тема 5. Шифрування даних та управління ключами в хмарних сховищах	2	1			10	Модуль-ний контр
Змістовий модуль 2 – Розробка, безпека та управління хмарними додатками						
Тема 6. Безпека мобільних додатків: розробка захищених застосунків з використанням Glide.app	3	2	1	3	10	поточне опит.
Тема 7. Аналіз вразливостей та тестування на проникнення в хмарних системах	2	1			10	поточне опит.
Тема 8. Реагування на інциденти та управління безпекою в хмарних середовищах	3	2			10	поточне опит.
Тема 9. Відповідність нормативним вимогам та аудит безпеки хмарних сервісів	2	2			10	поточне опит.
Тема 10. Створення захищених NO-CODE додатків для моніторингу кібербезпеки за допомогою Glide.app	3	2			10	Модуль-ний контр
Разом	**24**	**16**	**2**	**6**	**102**	

5. Тематика лабораторних занять

Лабораторне заняття 1: Аналіз та оцінка ризиків у хмарному середовищі

- Проведення аналізу потенційних загроз для конкретного хмарного сценарію
- Оцінка вразливостей та їх потенційного впливу
- Розробка стратегії мінімізації ризиків

Лабораторне заняття 2: Налаштування та тестування IDS/IPS у хмарній інфраструктурі

- Встановлення та конфігурація IDS/IPS у хмарному середовищі
- Створення та налаштування правил виявлення
- Проведення симуляції атак та аналіз ефективності системи

Лабораторне заняття 3: Управління ідентифікацією та доступом у хмарі

- Налаштування IAM-політик у хмарному сервісі
- Впровадження багатофакторної автентифікації
- Створення та управління ролями з різними рівнями доступу

Лабораторне заняття 4: Розробка безпечного мобільного додатку з використанням Glide.app

- Створення прототипу мобільного додатку на Glide.app
- Імплементація механізмів автентифікації та авторизації
- Тестування безпеки створеного додатку

Лабораторне заняття 5: Проведення тестування на проникнення в хмарному середовищі

- Планування та підготовка до тестування на проникнення
- Використання інструментів для сканування вразливостей
- Аналіз результатів та розробка рекомендацій щодо усунення виявлених вразливостей

Лабораторне заняття 6: Створення NO-CODE додатку для моніторингу кібербезпеки на Glide.app

- Проєктування інтерфейсу додатку для відстеження показників безпеки
- Налаштування інтеграції з джерелами даних про кібербезпеку
- Імплементація системи сповіщень та генерації звітів

6. Самостійна робота

Самостійна робота "Розробка безпечних NO-CODE додатків для моніторингу кібербезпеки з використанням Glide.app"

Мета роботи: Розробити безпечний NO-CODE додаток для моніторингу кібербезпеки з використанням платформи Glide.app, орієнтований на потреби конкретного підприємства.

Завдання:

1. Кожен студент обирає реальне або вигадане підприємство для розробки додатку.
2. На основі специфіки обраного підприємства, студент розробляє додаток, який включає:
   - Проектування інтерфейсу додатку для відстеження показників безпеки
   - Інтеграцію з релевантними джерелами даних про кібербезпеку
   - Налаштування системи сповіщень та звітності
   - Забезпечення безпеки самого додатку для моніторингу

3. Студент повинен підготувати звіт, який містить:
- Опис обраного підприємства та його потреб у сфері кібербезпеки
- Детальний опис розробленого додатку, включаючи скріншоти інтерфейсу
- Пояснення вибору конкретних показників для моніторингу
- Опис реалізованих механізмів інтеграції, сповіщень та безпеки
- Інструкцію з використання додатку
- Аналіз потенційних обмежень та пропозиції щодо подальшого вдосконалення

Роботу необхідно здати викладачу у вигляді письмового звіту та презентації розробленого додатку. Захист роботи відбувається у формі усної презентації з демонстрацією функціоналу додатку.

7. Організація та проведення тренінгу з дисципліни Системи та технології кібербезпеки

"Комплексна безпека хмарних технологій та розробка захищених NO-CODE додатків"

Цей тренінг охоплює ключові аспекти безпеки хмарних середовищ та створення захищених додатків без кодування, поєднуючи теоретичні знання з практичними навичками. Учасники отримають досвід роботи з різноманітними інструментами та методологіями, від аналізу ризиків до розробки мобільних додатків з урахуванням вимог безпеки.

Мета тренінгу:

Забезпечити учасників комплексними теоретичними знаннями та практичними навичками в галузі безпеки хмарних технологій та розробки захищених NO-CODE додатків, підготувавши їх до ефективного управління ризиками та створення безпечних рішень у сучасному цифровому середовищі.

Перелік задач для тренінгу:

1. Розробіть додаток для моніторингу спроб несанкціонованого доступу до корпоративної мережі. Інтегруйте його з журналами безпеки та налаштуйте сповіщення про підозрілу активність.
2. Створіть додаток для відстеження вразливостей у програмному забезпеченні компанії. Реалізуйте функціонал для категоризації вразливостей за рівнем критичності та статусом усунення.
3. Розробіть дашборд для візуалізації ключових показників ефективності (KPI) кібербезпеки організації. Включіть графіки та діаграми для наочного представлення даних.
4. Створіть додаток для управління інцидентами безпеки. Реалізуйте функціонал для реєстрації інцидентів, призначення відповідальних та відстеження статусу вирішення.
5. Розробіть систему для моніторингу фішингових атак. Інтегруйте її з джерелами даних про підозрілі email-и та реалізуйте механізм сповіщень для команди безпеки.
6. Створіть додаток для відстеження дотримання політик безпеки співробітниками компанії. Включіть функціонал для проведення опитувань та відстеження навчання з питань кібербезпеки.
7. Розробіть інструмент для моніторингу безпеки хмарної інфраструктури. Реалізуйте інтеграцію з API хмарних провайдерів для отримання даних про стан безпеки.

8. Створіть додаток для управління доступом до корпоративних ресурсів. Реалізуйте функціонал для запиту, схвалення та відкликання прав доступу.
9. Розробіть систему для відстеження та аналізу аномалій у мережевому трафіку. Реалізуйте візуалізацію аномалій та механізм сповіщень про підозрілу активність.
10. Створіть додаток для управління оновленнями безпеки в організації. Включіть функціонал для відстеження статусу оновлень на різних пристроях та системах.

Ці завдання дозволять студентам отримати практичний досвід створення безпечних NO-CODE додатків для різних аспектів моніторингу кібербезпеки з використанням платформи Glide.app.

Порядок проведення тренінгу:

Вступна частина проводиться з метою ознайомлення студентів із запропонованими завданнями тренінгу.

Організаційна частина полягає у створенні робочого настрою у колективі студентів.

Практична частина реалізується шляхом виконання одного вибраного завдання тренінгу.

Підведення підсумків. Обговорення результатів виконаних завдань. Обмін думками з питань, що виносились на тренінг.

8. Методи навчання.

У навчальному процесі застосовуються: лекції, в тому числі з використання мультимедійного проектора та інших ТЗН; лабораторні роботи, індивідуальні заняття; самостійна робота студентів, робота в Інтернет.

9. Засоби оцінювання та методи демонстрування результатів навчання

- У процесі вивчення дисципліни «Системи та технології кібербезпеки» використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:
- поточне опитування;
- модульне тестування та опитування;
- оцінювання лабораторних робіт;
- оцінювання тренінгів;
- оцінювання результатів самостійної роботи;

10. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100-бальною шкалою) з дисципліни "Системи та технології кібербезпеки" визначається як середньозважена величина, в залежності від питомої ваги кожної складової залікового кредиту:

Модуль 1		**Модуль 2**	**Модуль 3**
40%	40%	5%	15%
Поточне оцінювання	Модульний контроль	Тренінги	Самостійна робота
- Складається з 6 лабораторних робіт. Загальна оцінка за лабораторні роботи розраховується як середнє арифметичне.	- Складається із письмової роботи, яка містить 2 теоритичні запитання та 10 тестів. Загальна оцінка розраховується 60 балів за теоретичні запитання та 40 балів за тести.	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)

10. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

№	Найменування	Номер теми
1.	Проектор	1-10
2.	Персональний комп’ютер	1-10
3.	Електронний варіант лекцій	1-10
4.	Методичні вказівки до виконання лабораторних робіт (електронний варіант)	1-10
3.	Хмарна платформа (наприклад, AWS, Azure або Google Cloud)	1-10
4	Програмне середовище Glide.app	1-10

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