Силабус курсу
Безпека хмарних сервісів

Ступінь вищої освіти – бакалавр
Рік навчання: 4
Семестр: 7
Кількість кредитів: 5
Мова викладання: українська

Керівник курсу
Людмила Бабала
Ludmilababala@gmail.com

ПІП
Контактна інформація

Опис дисципліни

Курс поєднує теоретичні знання з практичними навичками через лекції, лабораторні роботи, самостійну роботу та тренінги. Особлива увага приділяється розробці реальних проектів безпеки хмарних середовищ та застосуванню методів OSINT-аналізу для виявлення кіберзагроз.

Мета дисципліни - сформувати у студентів комплексне розуміння сучасних методів та технологій забезпечення кібербезпеки, з особливим акцентом на хмарні технології, методи розвідки відкритих джерел (OSINT) та практичний аналіз державних реєстрів для забезпечення інформаційної безпеки.

Дисципліна спрямована на підготовку фахівців, здатних аналізувати та оцінювати кіберзагрози в хмарному середовищі, впроваджувати ефективні стратегії захисту, проводити OSINT-дослідження та забезпечувати відповідність систем нормативним вимогам у сфері кібербезпеки.

Структура курсу

Години лек/лаб	Тема	Результати навчання	Завдання
3/1	Сучасні загрози в хмарному середовищі	Вивчення типів загроз у хмарному середовищі та методів їх виявлення	Поточне опитування
3/2	Хмарні технології та їх роль у забезпеченні кібербезпеки підприємств	Огляд моделей хмарних послуг та архітектури безпеки в хмарі	Поточне опитування
3/1	Системи виявлення та запобігання вторгнень (IDS/IPS) в хмарних інфраструктурах	Вивчення принципів роботи IDS/IPS у хмарних інфраструктурах	Поточне опитування
3/1	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
3/1	Розвідка відкритих джерел (OSINT) у кібербезпеці	Освоєння методології OSINT та інструментів збору інформації з відкритих джерел	Поточне опитування, тестування
3/2	Аналіз державних електронних реєстрів України	Вивчення методів доступу та аналізу державних реєстрів для задач кібербезпеки	Поточне опитування

Години лек/лаб	Тема	Результати навчання	Завдання
3/1	Реагування на інциденти та управління безпекою в хмарних середовищах	Вивчення процесів виявлення, класифікації та розслідування інцидентів безпеки в хмарному середовищі	Поточне опитування
3/2	Відповідність нормативним вимогам та аудит безпеки хмарних сервісів	Ознайомлення з ключовими стандартами та регуляторними вимогами у сфері кібербезпеки	Поточне опитування
3/1	Практичний аналіз кіберзагроз через державні реєстри та OSINT	Практичне застосування знань для комплексного аналізу кіберзагроз	Поточне опитування

Рекомендовані джерела інформації

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. Дата оновлення: 28.12.2023. URL: https://zakon.rada.gov.ua/laws/show/2163-19
2. Про затвердження Стратегії кібербезпеки України : Указ Президента України від 26.08.2021 № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013
3. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу : НД ТЗІ 1.1-003-99. Київ: ДССЗЗІ України, 1999. 62 с.
4. Системи управління якістю. Вимоги: ДСТУ Архипов А. Є., Архипова Н. І. Кібербезпека критичних інфраструктур: теорія і практика: навчальний посібник. Київ:
5. НАУ, 2020. 284 с.
6. Бабала Л. В., Бойчук А. В. Інформаційна система підтримки управлінської діяльності підприємства. ISO 9001:2015. Київ: ДП «УкрНДНЦ», 2016. 22 с.
7. Оцінювання економічної ефективності проектних рішень у будівництві: ДСТУ-Н Б А.3.1-23:2013. Київ: Мінрегіон України, 2014. 16 с.
6. Modern problems of science, education and society: Proceedings of the 8th International scientific and practical conference. Kyiv: SPC «Sci-conf.com.ua», 2023. С. 228-232.
7. Грищук Р. В., Данилюк В. А. Основи кібербезпеки: навчальний посібник. Житомир: ЖНАЕУ, 2021. 544 с.
8. Ковальчук О., Бабала Л., Іваницький Р. Інтелектуальна модель виявлення асоціативних правил у базах даних кримінальних правопорушень. Herald of Khmelnytskyi National University. Technical sciences. 2025. Vol. 03-27. DOI: 10.31891/2307-5732-2025-349-27.
9. Корченко О. Г., Казмірчук С. В. Системи виявлення вторгнень : навчальний посібник. Київ: КПІ ім. Ігоря Сікорського, 2022. 312 с.
10. Лахно В. А., Касаткіна Н. В. Захист інформації в комп'ютерних системах і мережах : навчальний посібник. Суми : СумДПУ імені А. С. Макаренка, 2021. 268 с.
11. Бабала Л. В., Данилюк І. В. Проектування та реалізація комп'ютеризованої системи контролю дотримання вимог безпеки. The 7th International scientific and practical conference "Perspectives of contemporary science: theory and practice" (August 19-21, 2024). Lviv: SPC «Sci-conf.com.ua», 2024. С. 183-186.
12. Basta, A., & Halton, W. Computer Security and Penetration Testing. 3rd ed. Boston: Cengage Learning, 2019. 576 p.
13. Bazzell, M. Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information. 8th ed. North Charleston: Intel Techniques, 2021. 784 p.
14. Brown, A. K. Investment Evaluation Methods for Smart Manufacturing. London: Springer-Verlag, 2023. 356 p.
15. Chen, L., Patel, K., Mueller, S. Cost-Benefit Analysis in Manufacturing Automation. International Journal of Production Economics. 2024. Vol. 267. P. 108-125.
16. Conklin, W. A., White, G., Williams, D., Davis, R. L., & Cothren, C. CompTIA Security+ All-in-One Exam Guide, Sixth Edition (Exam SY0-601). 6th ed. New York: McGraw Hill, 2021. 896 p.
17. Diogenes, Y., & Dmitrenko, M. Cybersecurity – Azure Security: Get to grips with building and

maintaining cloud security solutions for your Azure environment. Birmingham: Packt Publishing, 2019. 456 p.
18. Stallings, W., & Brown, L. Computer Security: Principles and Practice. 4th ed. London: Pearson, 2022. 912 p.
19. Sullivan, N. Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Hoboken: Wiley, 2022. 528 p.
20. Vacca, J. R. Cloud Computing Security: Foundations and Challenges. Boca Raton: CRC Press, 2021. 584 p.
21. Yoon, H. J. Cybersecurity in the Digital Age: Tools, Techniques & Best Practices. New York: Business Expert Press, 2020. 298 p.
22. CERT-UA: офіційний веб-сайт. URL: https://cert.gov.ua
23. Державна служба спеціального зв'язку та захисту інформації України: офіційний веб-сайт. URL: https://cip.gov.ua
24. Державна служба статистики України: офіційний веб-сайт. URL: http://www.ukrstat.gov.ua
25. Міністерство економіки України: офіційний веб-сайт. URL: https://www.me.gov.ua
26. Національний банк України: офіційний веб-сайт. URL: https://bank.gov.ua
27. NIST Cybersecurity Framework: офіційний веб-сайт. URL: https://nist.gov/cyberframework
28. OWASP (Open Web Application Security Project): офіційний веб-сайт. URL: https://owasp.org
29. Shodan Search Engine : веб-сервіс. URL: https://shodan.io

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

Підсумковий бал (за 100-бальною шкалою) з дисципліни "Безпека хмарних сервісів" 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
Загальна оцінка за лабораторні роботи розраховується як середнє арифметичне з виконання 6 лабораторних робіт.	1. Теоретичні питання: 2 пита-ння по 30 балів - max 60 балів. 2. Тестові питання:10 тестів - max 40 балів.	Оцінюється виконання індивідуального завдання тренінгу (виконання роботи - max 60 балів, захист роботи - max 40 балів)	Оцінюється якість розробки, відповідність потребам підприємства, повнота реалізації функціоналу. (виконання роботи - max 60 балів, захист роботи - max 40 балів)

Виконання лабораторних робіт:

90-100 балів (Відмінно) - здобувач самостійно, без помилок, виконав усі кроки лабораторної роботи, правильно задокументував етапи та вільно оперує поняттями та принципами хмарної безпеки, управління ідентифікацією та доступом, а також методами OSINT-аналізу.

75-89 балів (Добре) - здобувач виконав завдання лабораторної роботи, але з кількома дрібними помилками, які не вплинули на кінцевий результат (наприклад, неточна послідовність дій), виникали питання під час роботи.
60-74 балів (Задовільно) - здобувач виконав завдання, але з суттєвими помилками, наприклад, не з першого разу. Розуміння поставлених у лабораторній роботі завдань є поверхневим.
1-59 балів (Незадовільно) - здобувач не зміг виконати завдання або результати були повністю невірними. Не продемонстрував базових навичок роботи з хмарними платформами, IDS/IPS системами або OSINT-інструментами.

Оцінювання модульного контролю:

90-100 балів (Відмінно) - здобувач демонструє повне і глибоке знання теоретичного матеріалу, а також практичних аспектів, вільно оперує поняттями та принципами безпеки хмарних сервісів та методів OSINT. Здатний не просто відповідати на тестові запитання, а й аналізувати складні ситуації, знаходити неочевидні рішення, аргументовано висловлювати власну позицію. Виявляє ініціативу в опануванні матеріалу, що виходить за межі навчальної програми.
75-89 балів (Добре) - здобувач має ґрунтовні знання з усіх основних розділів дисципліни. Демонструє вміння застосовувати теоретичні знання, що обговорюються на занятті, бере участь у обговореннях, відповідає на запитання викладача.
60-74 балів (Задовільно) - здобувач володіє мінімально необхідним обсягом знань. Відповіді переважно на тестові запитання, можуть містити неточності, може плутатися в термінах і поняттях. Не виявляє ініціативи в опрацюванні матеріалу, а лише відтворює інформацію, отриману на лекціях.
1-59 балів (Незадовільно) - здобувач не володіє або володіє лише фрагментарними знаннями з дисципліни. Відповіді переважно неправильні, що свідчить про повну відсутність розуміння матеріалу.

Тренінг:

90-100 балів (Відмінно) - здобувач самостійно, без помилок, виконав усі етапи завдання, правильно задокументував усі етапи роботи, та вільно оперує поняттями та принципами кібербезпеки хмарних середовищ та OSINT-методології.
75-89 балів (Добре) - здобувач виконав завдання, але з кількома дрібними помилками, які не вплинули на кінцевий результат (наприклад, неточна послідовність дій), виникали питання під час роботи.
60-74 балів (Задовільно) - здобувач виконав завдання, але з суттєвими помилками, наприклад, не з первого разу. Розуміння поставлених у тренінгу завдань є поверхневим.
1-59 балів (Незадовільно) - здобувач не зміг виконати завдання або результати були повністю невірними. Не продемонстрував базових навичок роботи з хмарними технологіями безпеки або OSINT-платформами.

Самостійна робота:

90–100 балів (Відмінно) - доповідь охоплює всі ключові аспекти обраної теми, демонструючи глибоке розуміння предмета. Дослідження містить не лише опис, але й глибокий аналіз, порівняння різних підходів та методів, а також обґрунтовані висновки. Використані сучасні та актуальні джерела інформації, що свідчить про обізнаність здобувач а з останніми тенденціями у сфері безпеки хмарних сервісів та OSINT-аналітиці. Здобувач вільно володіє матеріалом, виступає впевнено та відповідає на всі запитання.
75–89 балів (Добре) - доповідь розкриває основні питання теми, але може бути менш деталізованою. В роботі є аналітичні елементи, але вони можуть бути не достатньо глибокими. Використані джерела інформації є релевантними, але можуть бути не найновішими. Здобувач демонструє знання матеріалу, але може мати незначні труднощі з відповідями на додаткові питання.
60–74 балів (Задовільно) - доповідь охоплює лише основні аспекти теми. Можуть бути пропущені важливі деталі. Робота має описовий характер, аналіз та висновки є поверхневими. Здобувач не завжди впевнено відповідає на запитання. Виступ може бути нечітким.
1–59 балів (Незадовільно) - зміст доповіді не відповідає темі або є компіляцією застарілих даних. Робота є прямим копіюванням без самостійного опрацювання.

Шкала оцінювання

За шкалою ЗУНУ	За національною шкалою	За шкалою ECTS
90–100	**відмінно**	**A (відмінно)**
85–89	**добре**	**B (дуже добре)**
75–84		**C (добре)**
65–74	**задовільно**	**D (задовільно)**
60–64		**E (достатньо)**
35–59	**незадовільно**	**FX (незадовільно з можливістю повторного складання)**
1–34		**F (незадовільно з обов'язковим повторним курсом)**

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