МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

СИЛАБУС ВИБІРКОВОГО ОСВІТНЬОГО КОМПОНЕНТУ

«ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ. ХМАРНІ ТЕХНОЛОГІЇ»

Мова навчання – ***українська***

Шифр та найменування галузі знань ***«Інформаційні технології»***

Код та найменування спеціальності ***№ F3 «Комп'ютерні науки»***

Освітньо-професійна програма ***Інформаційні технології проектування***

Ступінь вищої освіти ***магістр***

Затверджено на засіданні

Методичної Ради зі спеціальності ***F3 «Комп'ютерні науки»***
« » 202 р. протокол № .

Реєстраційний номер в навчальному відділі НЦООП

_____

1. Загальна інформація

Кафедра: Інформаційних технологій та кібербезпеки

Викладач: **Антонова Альфія Раісівна,** доцент, к.т.н., доцент кафедри інформаційних технологій та кібербезпеки

Контакти:

Профайл http://www.kit.onaft.edu.ua/lecturer/3

allaantonova62@gmail.com

048-720-41-22

Освітній компонент викладається на *1* курсі у *1* семестрі

Кількість: кредитів - 5, годин – 150

Аудиторні заняття, годин:	всього	лекції	лабораторні	практичні
денна	66	32	34	-
заочна	10	6	4	-
Самостійна робота, годин	Денна – 84			Заочна – 140

Розклад занять

2. Анотація освітнього компоненту

Освітній компонент (ОК) «ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ. ХМАРНІ ТЕХНОЛОГІЇ»

Предметом вивчення навчальної дисципліни «Технології захисту інформації. Хмарні технології» є вивчення способів адміністрування і управління безпекою, аналізу та налагодженню системи безпеки, автоматизації задач налагодження системи безпеки, оцінки безпеки інформаційних технологій, розробки політики інформаційної безпеки та створенню безпечного зовнішнього середовища за стандартом. Відомо, що інформація, створювана, збережена і оброблювана засобами обчислювальної техніки, стала визначати дії більшої частини людей і технічних систем. В той же час, також різко зросли можливості свідомого нанесення шкоди, зниження ефективності її функціонування (відмови та порушення працездатності програмних і технічних засобів; навмисні загрози).

Особлива увага буде приділена, окрім природних способів виявлення і своєчасного усунення зазначених вище причин (шкоди), також і спеціальним способам захисту інформації від порушень працездатності систем. Особливо, від загроз реалізація яких виконується при постійній участі людини та після розробки відповідних комп'ютерних програм без безпосередньої участі людини.

3. Мета освітнього компоненту

Мета освітнього компоненту – формування теоретичних знань та практичних умінь побудови контуру безпеки ІТ-ресурсів підприємства, компанії чи організації на рівні засобів та технологій розширеної мережевої та хмарної безпеки.

4. Компетентності та програмні результати навчання

У результаті вивчення освітнього компоненту «ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ. ХМАРНІ ТЕХНОЛОГІЇ» здобувач вищої освіти отримує наступні програмні компетентності та програмні результати навчання, які визначені в Стандарті вищої освіти зі спеціальності № F3 «КОМП'ЮТЕРНІ НАУКИ» та освітньо-професійній програмі «ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ПРОЕКТУВАННЯ» підготовки магістрів.

Курс забезпечує набуття таких компетентностей: ЗК 2, ЗК 3, ЗК 4, ЗК 7 ФК 2 та програмних результатів навчання: ПРН 3, ПРН 4, ПРН 5, ПРН 8, ПРН 10, ПРН 13, ПРН 15,

ПРН 18, ПРН 20, ПРН 25, ПРН 27, ПРН 30, ПРН 34, ПРН 36, ПРН 39, ПРН 43, ПРН 45, ПРН 48, ПРН 52, ПРН 54.

Після завершення цього курсу ви повинні вміти робити наступне:

• Визначати переваги безпеки та обов'язки використання хмари Amazon Web Services (AWS).

• Використовувати функції керування ідентифікацією та доступом AWS.

• Описувати, як захистити мережевий доступ до ресурсів AWS.

• Пояснювати доступні методи шифрування даних у стані спокою та даних у дорозі.

• Визначати, які служби AWS можна використовувати для моніторингу та реагування на інциденти.

5. Інформаційний обсяг освітнього компоненту

5.1 Перелік лекційних завдань

Тема	Зміст теми	Кількість годин	
		денна	заочна
Змістовний модуль 1. ОСНОВИ БЕЗПЕКИ РІВНЯ ВЕБ-СЕРВЕРУ			
1	Введення. Основні терміни та визначення	2	1
2	Особливості сучасних корпоративних мереж	4	-
3	Засоби безпеки рівня корпоративної мережі	4	-
4	Атаки масового призначення	4	1
5	Тестування ризиків у функції «запам'ятати мене». Тестування брутфорс автентифікації. Тестування незахищеної captcha	4	1
Змістовний модуль 2. ПРАКТИКА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ВЕБ-РЕСУРСІВ			
6	Хмарні середовища: можливості, переваги та ризики. Стратегія розвитку хмари.	2	1
7	Публічні хмарні сервіси Amazon AWS, Microsoft Azure та Google Cloud Platform.	4	1
8	Засоби безпеки рівня хмарного сервісу. Безпека в хмарі AWS. Принципи проектування безпеки. Модель розподіленої відповідальності	2	-
9	Принципи управління хмарними інфраструктурами. Мережеві аспекти хмарних технологій. Використання груп безпеки AWS. Використання списків управління доступом мережі AWS. Використання балансувальників навантаження AWS.	2	-
10	Особливості розробки програмного забезпечення для хмарних інформаційних систем.	2	-
11	Перспективи синергічного поєднання засобів безпеки рівня корпоративної мережі та хмарного сервісу.	2	1
Разом за ОК:		**32**	6

5.2 Перелік практичних/лабораторних робіт

№ з/п	Назва практичної/лабораторної роботи	Кількість годин	
		денна	заочна
1	Використання AWS Management Console	4	1
2	Використання політик на основі ресурсів для захисту сегмента S3	6	1
3	Захист ресурсів VPC за допомогою груп безпеки	6	-
4	Шифрування даних у спокої за допомогою AWS KMS	6	1

5	Моніторинг і сповіщення за допомогою CloudTrail і CloudWatch	6	-
6	Усунення інциденту за допомогою AWS Config і Lambda	6	1
Всього за ОК:		**34**	4

6. **Система оцінювання та вимоги**

Контроль успішності навчання здобувача проводиться у формах вхідного, поточного і підсумкового контролів.

Вхідний контроль якості навчання здійснюється на початку курсу проведенням перевірки залишкових знань здобувачів за ОК, що забезпечують вивчення даного освітнього компоненту (діагностика первинних знань здобувачів).

Формами поточного контролю є:

- *тестування знань здобувачів з певних тем або з певних окремих питань ОК;*
- *виконання і захист лабораторних робіт;*
- *усне опитування;*
- *тощо.*

Підсумковий контроль – ***залік.***

Нарахування балів:

Вид роботи, що підлягає контролю	Максимальна кількість оціночних балів
Змістовний модуль 1. ОСНОВИ ПАРАЛЕЛЬНИХ ОБЧИСЛЕНЬ	
Лекційний курс*	8
Лабораторні роботи*	8
Самостійна робота*	8
Тестування*	8
Виконання індивідуального завдання	3
Всього за змістовний модуль 1	**35**
Змістовний модуль 2. ОСНОВИ РОБОТИ З MPI	
Лекційний курс*	8
Лабораторні роботи*	8
Самостійна робота*	8
Тестування*	8
Виконання індивідуального завдання	3
Всього за змістовний модуль 2	**35**
Екзамен	**30,0**
Всього	**100,0**

*Є можливість визнання результатів неформальної освіти відповідно до п.2 Положення про порядок перезарахування результатів навчання (навчальних дисциплін) в Одеському національному технологічному університеті.

Критерії оцінювання програмних результатів навчання здобувачів

Підсумковий контроль – екзамен

27-30 балів	якщо здобувач демонструє повні й глибокі знання навчального матеріалу, достовірний рівень розвитку умінь і навичок, правильне й обґрунтоване формулювання практичних висновків, уміння приймати необхідні рішення в різних нестандартних ситуаціях, вільне володіння науковими термінами, високу комунікативну культуру	відмінно
23-26 балів	якщо здобувач виявляє дещо обмежені знання навчального матеріалу, допускає окремі несуттєві помилки й неточності	дуже добре
18-22 бали	якщо здобувач засвоїв основний навчальний матеріал, володіє необхідними уміннями та навичками для вирішення стандартних завдань, проте при цьому допускає неточності, не виявляє самостійності суджень, демонструє недоліки комунікативної культури	задовільно
0-17 балів	якщо здобувач не володіє необхідними знаннями, уміннями й навичками, науковими термінами, демонструє низький рівень комунікативної культури	незадовільно

Лабораторні роботи (приклад оцінювання однієї роботи)

1,5 – 2,0 балів	*Лабораторна відпрацьована та вчасно захищена, надані повні обґрунтовані відповіді*	відмінно
1,0 - 1,4 балів	*Лабораторна відпрацьована та вчасно захищена, при відповіді допущені неточності*	дуже добре
0,75 – 0,9 балів	*Лабораторна відпрацьована, відповіді неповні, допущені помилки*	добре
0,4 – 0,7 балів	*Лабораторна відпрацьована, відповіді незадовільні, допущені грубі помилки*	достатньо
0-0,3 балів	*Лабораторна не відпрацьована або дані незадовільні відповіді*	незадовільно

Тестування (приклад оцінювання)

9,0-10,0	*90 - 100 % правильних відповідей*	відмінно
7,4 -8,9	*74 – 89% правильних відповідей*	дуже добре
6,0 – 7,3	*60 – 73% правильних відповідей*	добре
3,5 – 5,9	*35 – 59 % правильних відповідей*	достатньо
0 – 3,4	*0-35 % правильних відповідей*	незадовільно

7. Засоби діагностики успішності навчання

Методи навчання, які використовуються у процесі проведення занять, а також самостійних робіт за ОК:

Лекційні заняття*: Словесні методи: розповідь, пояснення, бесіда, дискусія; Наочні: ілюстрація, спостереження, демонстрація; пояснювально- демонстративний метод, проблемний виклад.*

Лабораторні заняття: *виконання лабораторних дослідів з наступних захистом результатів досліджень.*

Самостійна робота*: робота з навчально-методичними матеріалами, робота зі статистично-аналітичними звітами, складання планової та звітної документації, науково-*

дослідна робота студентів (методи пізнання, аналогій, оцінка, ілюстрація тощо), складання скетчів за темами лекцій, реферування, конспектування)

8. Інформаційні ресурси

Базові (основні):

1. Cyber Security. Simply. Make it Happen. : Monograph / edit. Abolhassan. – Springer International Publishing, 2017. – ISBN 978- 3- 319-46528-9 (print) ; 978-3-319-46529-6 (online). 127 p
2. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163
3. Державна служба спеціального зв'язку та захисту інформації України./ www.dsszzi.gov.ua
4. Cybersecurity Fundamentals/ ISACA/ www/isaca/org/cyber? Cybersecurity Funamentals Study Guide/ 2003.- 156 p.
5. Cyber-Physical Security : Monograph / edit. Clark. – Springer International Publishing, 2017. – ISBN 978-3-319-32822-5 (print) ; 978-3-319-32824-9 (online). 299 p.
6. Cloud computing / N. B. Ruparelia. – Cambridge; London: The MIT Press, 2016. – 260 c. – (The MIT Press essential knowledge series)
7. Cloud computing for science and engineering / I. Foster, D. B. Gannon. – Cambridge; London: The MIT Press, 2017. – 372 c. – (Scientific and engineering computation)
8. Data analysis in the cloud: models, techniques and applications / D. Talia, P. Trunfio, F. Marozzo. – Amsterdam [etc.]: Elsevier, 2016. – 138 c. – (Computer science: reviews andtrends) - ISBN 978-0-12- 802881

Додаткові:

1. AWS Security Incident Response Guide, 2020. - 65 p. [Electronic resource]. – Access mode: https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-responseguide/welcome.html?did=wp_card&trk=wp_card
2. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2020 . – 678 с.

9. Політика освітнього компоненту

Політика всіх освітніх компонент в ОНТУ є уніфікованою та визначена з урахуванням законодавства України, Корпоративному кодексу ОНТУ */ГІПЕРПОСИЛАННЯ*, Кодексу академічної доброчесності ОНТУ*/ГІПЕРПОСИЛАННЯ*, Положення про організацію освітнього процесу ОНТУ*/ГІПЕРПОСИЛАННЯ*, Положення про порядок перезарахування результатів навчання (навчальних дисциплін) в ОНТУ*/ГІПЕРПОСИЛАННЯ*, вимог ISO 9001:2015*/ГІПЕРПОСИЛАННЯ* та роботодавців (*/ГІПЕРПОСИЛАННЯ НА СТОРІНКУ НА Ф-ТІ*)

Викладач /ПІДПИСАНО/ Альфія АНТОНОВА

Розглянуто та затверджено на засіданні кафедри_____

Протокол від «____»_____202 р. № ___

Завідувач кафедри /ПІДПИСАНО/ Павло ЛОМОВЦЕВ

ПОГОДЖЕНО:

Гарант ОП *ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ПРОЕКТУВАННЯ*
доцент, каф. інформаційних
технологій та кібербезпеки /ПІДПИСАНО/ Павло ЛОМОВЦЕВ