ЗАТВЕРДЖЕНО

Вченою радою факультету
інформаційно-комп'ютерних
технологій
28 серпня 2024 р., протокол № 8

Голова Вченої ради
_____ Тетяна НІКІТЧУК

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ОК 11 «ХМАРНА БЕЗПЕКА»

для здобувачів вищої освіти освітнього ступеня «магістр»
спеціальності 125 «Кібербезпека та захист інформації»
освітньо-професійна програма «Кібербезпека»
факультет інформаційно-комп'ютерних технологій
кафедра комп'ютерної інженерії та кібербезпеки

Схвалено на засіданні
кафедри комп'ютерної
інженерії та кібербезпеки
26 серпня 2024 р., протокол № 6

Завідувач кафедри
_____ Андрій ЄФІМЕНКО

Гарант освітньо-професійної
програми
_____ Володимир ВОРОТНІКОВ

Розробники: старший викладач кафедри комп'ютерної інженерії та кібербезпеки Вадим МИКОЛАЙЧУК,
кандидат технічних наук, доцент, завідувач кафедри комп'ютерної інженерії та кібербезпеки Андрій ЄФІМЕНКО

Житомир
2024 – 2025 н.р.

Робоча програма навчальної дисципліни «Хмарна безпека» для здобувачів вищої освіти освітнього ступеня «магістр» спеціальності 125 «Кібербезпека та захист інформації» освітньо-професійна програма «Кібербезпека та захист інформації» затверджена Вченою радою факультету інформаційно-комп’ютерних технологій від 28 серпня 2024 р., протокол № 8.

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, спеціальність, освітній ступінь	Характеристика навчальної дисципліни	
		денна форма навчання	заочна форма навчання
Кількість кредитів 3	Галузь знань 12 «Інформаційні технології»	Обов'язкова	
Модулів – 1	125 «Кібербезпека та захист інформації»	Рік підготовки:	
Змістових модулів – 2		1	1
		Семестр	
Загальна кількість годин – 90		1	1
		Лекції	
Тижневих годин для денної форми навчання: аудиторних - 3 самостійної роботи – 2,625	Освітній ступінь «магістр»	16 год.	6 год.
		Лабораторні	
		32 год.	6 год.
		Самостійна робота	
		42 год.	6 год.
		Вид контролю: залік	

Частка аудиторних занять і частка самостійної та індивідуальної роботи у загальному обсязі годин з навчальної дисципліни становить:

для денної форми навчання – 53% аудиторних занять, 47% самостійної та індивідуальної роботи;

для заочної форми навчання − 13% аудиторних занять, 87% самостійної та індивідуальної роботи.

2. Мета та завдання навчальної дисципліни

Метою вивчення навчальної дисципліни є вивчення теоретичних та практичних основ роботи з хмарою AWS, основних концепцій роботи хмар, огляд інфраструктури датацентрів хмарних провайдерів, базові принципи забезпечення хмарної безпеки, огляд роботи віртуальних мереж, обчислювальних сервісів, сервісів для зберігання даних, баз даних для розуміння можливості організації подальшого формування хмарної архітектури відповідно до вимог фреймворків, масштабування та моніторингу, побудови архітектури доступів відповідно до вимог, налаштування безпеки віртуальних мереж, списків доступів, сервісів балансування трафіку, захисту сервісів для зберігання даних, використання та налаштування сервісів логування, налаштування автоматизованого реагування на інциденти. Дисципліна базується на курсах AWS Academy Cloud Foundations та AWS Academy Cloud Security Foundations, що розміщені на платформі AWS Academy.

Завданнями навчальної дисципліни є: розвиток у майбутніх фахівців з кібербезпеки навичок аналізу роботи існуючих хмарних інфраструктур або побудови нових, з врахуванням сучасних стандартів та вимог до забезпечення безпеки хмарних інформаційних систем.

Зміст навчальної дисципліни направлений на формування наступних **компетентностей**, визначених стандартом вищої освіти зі спеціальності 125 «Кібербезпека та захист інформації»:

загальні:

КЗ-1. Здатність до адаптації та дій в новій ситуації.

КЗ-2. Здатність до абстрактного мислення, аналізу і синтезу.

КЗ-3. Здатність проводити дослідження на відповідному рівні.

КЗ-4. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

КЗ-5. Здатність генерувати нові ідеї (креативність).

КЗ-6. Здатність виявляти, ставити та вирішувати проблеми.

КЗ-7. Здатність приймати обґрунтовані рішення.

КЗ-8. Здатність спілкуватися іноземною мовою.

фахові:

КФ-1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.

КФ-2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного

спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.

КФ-3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.

КФ-4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.

КФ-5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ-6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ-7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

КФ-8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ-9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.

КФ-10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.

Отримані знання з навчальної дисципліни стануть складовими наступних **програмних результатів** навчання за спеціальністю 125 «Кібербезпека та захист інформації»:

РН-1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення

бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН-2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

РН-3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

РН-6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

РН-7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН-8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

РН-9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

РН-10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

РН-11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

РН-12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

РН-13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.

РН-14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.

РН-15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.

РН-17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об’єктивно оцінювати результати навчання.

Під час вивчення навчальної дисципліни здобувачі вищої освіти зможуть отримати додатково наступні Soft skills:

- *комунікативні навички*: письмове, вербальне й невербальне спілкування; уміння грамотно спілкуватися по e-mail; вести дискусію і відстоювати свою позицію; навички працювати в команді;
- *уміння виступати привселюдно*: навички, необхідні для виступів на публіці; навички проведення презентації;
- *керування часом:* уміння справлятися із завданнями вчасно;
- *гнучкість і адаптивність:* гнучкість, адаптивність і здатність змінюватися; уміння аналізувати ситуацію, орієнтування на вирішення проблеми;
- *лідерські якості*: уміння спокійно працювати в напруженому середовищі; уміння ухвалювати рішення; уміння ставити мету, планувати діяльність;
- *особисті якості:* креативне й критичне мислення; етичність, чесність, терпіння, повага до оточуючих.

3. Програма навчальної дисципліни

Модуль 1

Змістовий модуль 1. Принципи роботи AWS та ключові сервіси.

Тема 1. Особливості хмарних технологій, служб та концепцій. (КЗ-1, КЗ-2, КЗ-3, КЗ-4, КЗ-5, КЗ-6, КЗ-7, КЗ-8, КФ-1, КФ-2, КФ-3, КФ-4, КФ-5, КФ-6, КФ-7, КФ-8, КФ-9, КФ-10, РН-1, РН-2, РН-3, РН-6, РН-7, РН-8, РН-9, РН-10, РН-11, РН-12, РН-13, РН-14, РН-15. РН-17)

Концепція хмарних технологій. Переваги хмарних технологій. Вступ до Amazon Web Services (AWS). Міграція до AWS з використанням AWS Cloud Adoption Framework.

Тема 2. Інструменти та принципи аналізу витрат в AWS. Огляд принципу роботи інфраструктури сервісів AWS. Основи хмарної безпеки в AWS. (КЗ-1, КЗ-2, КЗ-3, КЗ-4, КЗ-5, КЗ-6, КЗ-7, КЗ-8, КФ-1, КФ-2, КФ-3, КФ-4, КФ-5, КФ-6, КФ-7, КФ-8, КФ-9, КФ-10, РН-1, РН-2, РН-3, РН-6, РН-7, РН-8, РН-9, РН-10, РН-11, РН-12, РН-13, РН-14, РН-15. РН-17)

Основи ціноутворення сервісів в AWS. Total Cost of Ownership. AWS Organizations. Білінг в AWS та управління витратами. Підтримка. Огляд глобальної інфраструктури AWS. Сервіси та категорії сервісів AWS. Модель розподіленої відповідальності. AWS Identity та доступи в AWS (IAM). Захист облікових записів AWS. Захист даних в AWS. Забезпечення інфраструктури до вимог стандартів законів, стандартів індустрії та відповідності фреймворкам.

Тема 3. Сервіси для роботи з віртуальними мережами, обчислювальні сервіси, сервіси зберігання даних, сервіси баз даних. (КЗ-1, КЗ-2, КЗ-3, КЗ-4, КЗ-5, КЗ-6, КЗ-7, КЗ-8, КФ-1, КФ-2, КФ-3, КФ-4, КФ-5, КФ-6, КФ-7, КФ-8, КФ-9, КФ-10, РН-1, РН-2, РН-3, РН-6, РН-7, РН-8, РН-9, РН-10, РН-11, РН-12, РН-13, РН-14, РН-15. РН-17)

Основи комп’ютерних мереж. Amazon VPC: побудова та забезпечення безпеки. Amazon Route 53. Amazon CloudFront. Огляд обчислювальних сервісів в AWS. Amazon EC2. Сервіси для роботи з контейнерами. AWS Lambda. AWS Elastic Beanstalk. Amazon EBS. Amazon S3. Amazon EFS. Amazon S3 Glacier. Amazon RDS. Amazon DynamoDB. Amazon Redshift. Amazon Aurora.

Тема 4. Хмарна архітектура, масштабування та моніторинг. (КЗ-1, КЗ-2, КЗ-3, КЗ-4, КЗ-5, КЗ-6, КЗ-7, КЗ-8, КФ-1, КФ-2, КФ-3, КФ-4, КФ-5, КФ-6, КФ-7, КФ-8, КФ-9, КФ-10, РН-1, РН-2, РН-3, РН-6, РН-7, РН-8, РН-9, РН-10, РН-11, РН-12, РН-13, РН-14, РН-15. РН-17)

AWS Well-Architected Framework. Надійність та доступність сервісів AWS. AWS Trusted Advisor. Amazon ELB. Amazon CloudWatch. Amazon EC2 Auto Scaling.

Змістовий модуль 2. Ключові принципи, сервіси та інструменти захисту інфраструктури, що використовує AWS.

Тема 5. Основні поняття безпеки в AWS. Доступ до хмарних ресурсів в AWS. (КЗ-1, КЗ-2, КЗ-3, КЗ-4, КЗ-5, КЗ-6, КЗ-7, КЗ-8, КФ-1, КФ-2, КФ-3, КФ-4, КФ-5, КФ-6, КФ-7, КФ-8, КФ-9, КФ-10, РН-1, РН-2, РН-3, РН-6, РН-7, РН-8, РН-9, РН-10, РН-11, РН-12, РН-13, РН-14, РН-15. РН-17)

Особливості побудови безпечної архітектури в хмарі. Побудова архітектури безпеки. Модель розподіленої відповідальності. Основи IAM. Аутентифікація та авторизація з IAM. AWS Organizations.

Тема 6. Захист інфраструктури в AWS. Захист даних додатків, що використовують AWS. (КЗ-1, КЗ-2, КЗ-3, КЗ-4, КЗ-5, КЗ-6, КЗ-7, КЗ-8, КФ-1, КФ-2, КФ-3, КФ-4, КФ-5, КФ-6, КФ-7, КФ-8, КФ-9, КФ-10, РН-1, РН-2, РН-3, РН-6, РН-7, РН-8, РН-9, РН-10, РН-11, РН-12, РН-13, РН-14, РН-15. РН-17)

Структура трирівневих додатків. Використання VPC. Налаштування публічних та приватних підмереж та інтернет протоколів. AWS Security groups. AWS network ACLs. AWS load balancers. Захист обчислювальних ресурсів. Захист даних at rest. Сервіси для захисту Amazon S3. Захист даних at transit. Інші служби захисту даних в AWS.

Тема 7. Логування та моніторинг. (КЗ-1, КЗ-2, КЗ-3, КЗ-4, КЗ-5, КЗ-6, КЗ-7, КЗ-8, КФ-1, КФ-2, КФ-3, КФ-4, КФ-5, КФ-6, КФ-7, КФ-8, КФ-9, КФ-10, РН-1, РН-2, РН-3, РН-6, РН-7, РН-8, РН-9, РН-10, РН-11, РН-12, РН-13, РН-14, РН-15. РН-17)

Вступ до логування та моніторингу в AWS, їх важливість. Зберігання логів в AWS. Сервіси в AWS з вбудованими механізмами логування. Моніторинг та звітування. Кращі практики впровадженні моніторингу та логування.

Тема 8. Реагування та управління інцидентами. (КЗ-1, КЗ-2, КЗ-3, КЗ-4, КЗ-5, КЗ-6, КЗ-7, КЗ-8, КФ-1, КФ-2, КФ-3, КФ-4, КФ-5, КФ-6, КФ-7, КФ-8, КФ-9, КФ-10, РН-1, РН-2, РН-3, РН-6, РН-7, РН-8, РН-9, РН-10, РН-11, РН-12, РН-13, РН-14, РН-15. РН-17)

Вступ до формування звітів та керування інцидентами. Сервіси AWS, що забезпечують виявлення та розпізнавання загроз. Послуги AWS, які підтримують фазу вирішення та відновлення. Кращі практики для управління інцидентами.

4. Структура (тематичний план) навчальної дисципліни

Змістові модулі і теми	Кількість годин							
	денна форма				заочна форма			
	усього	лекції	практичні (лабораторні)	самостійна робота	усього	лекції	практичні (лабораторні)	самостійна робота
Модуль 1								
Змістовий модуль 1. Назва								
Тема 1. Особливості хмарних технологій, служб та концепцій	11,25	2	4	5,25	11,25	0,75	0,75	9,75
Тема 2. Інструменти та принципи аналізу витрат в AWS. Огляд прицнипу роботи інфраструктури сервісів AWS. Основи хмарної безпеки в AWS	11,25	2	4	5,25	11,25	0,75	0,75	9,75
Тема 3. Сервіси для роботи з віртуальними мережами, обчислювальні сервіси, сервіси зберігання даних, сервіси баз даних	11,25	2	4	5,25	11,25	0,75	0,75	9,75
Тема 4. Хмарна архітектура, масштабування та моніторинг	11,25	2	4	5,25	11,25	0,75	0,75	9,75
Разом за змістовий модуль 1	45	8	16	21	45	3	3	39
Змістовий модуль 2. Ключові принципи, сервіси та інструменти захисту інфраструктури, що використовує AWS.								
Тема 5. Основні поняття безпеки в AWS. Доступ до хмарних ресурсів в AWS	11,5	2	4	5,25	11,25	0,75	0,75	9,75
Тема 6. Захист інфрастуктури в AWS. Захист даних додатків, що використовують AWS	11,5	2	4	5,25	11,25	0,75	0,75	9,75
Тема 7. Логування та моніторинг	11,5	2	4	5,25	11,25	0,75	0,75	9,75
Тема 8. Реагування та управління інцидентами	11,5	2	4	5,25	11,25	0,75	0,75	9,75
Разом за змістовий модуль 2	45	8	16	21	45	3	3	39
ВСЬОГО	**90**	**16**	**32**	**42**	**90**	**6**	**6**	**78**

5. Теми практичних (лабораторних) занять

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
Модуль 1			
Змістовий модуль 1. Принципи роботи AWS та ключові сервіси.			
1	Ознайомлення з платформою AWS Academy. AWS Identity and Access Management (IAM).	4	0,75
2	Ознайомлення з основними поняттями хмар. Інструменти для аналізу витрат в AWS. Огляд інфраструктури AWS. AWS Cloud Security. Побудова VPC та запуск веб-серверу. Вступ до EC2 та розгортання.	4	0,75
3	Розгортання AWS Lambda. Розгортання AWS Elastic Beanstalk. Робота з AWS EBS. Розгортання AWS S3, AWS S3 Glacier.	4	0,75
4	Розгортання серверу БД. Розгортання Amazon DynamoDB, Amazon Redshift, Amazon Aurora. Масштабування інфраструктури в AWS.	4	0,75
Змістовий модуль 2. Ключові принципи, сервіси та інструменти захисту інфраструктури, що використовує AWS.			
5…	Використання Resource-based policies для Amazon S3	4	0,75
6	Покращення безпеки Amazon VPC з Amazon Security Groups. Шифрування даних at rest з використанням AWS KMS.	4	0,75
7	Моніторинг та сповіщення про інциденти з CloudTrail та CloudWatch	4	0,75
8	Автоматизація управління інцидентами з AWS Config та AWS Lambda	4	0,75
	РАЗОМ	**32**	**6**

6. Завдання для самостійної роботи

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
Модуль 1			
Змістовий модуль 1. Принципи роботи AWS та ключові сервіси.			
1	Ознайомлення з IaaS, Pass, SaaS; shared responsibility model. Знайомство з Public, Private, Hybrid cloud.	3	4
2	Особливості роботи з обчислювальними сервісами, хмарними мережами, сервісами зберігання даних, PaaS рішеннями для баз даних.	7	10
3	Amazon WAF.	14	25
Змістовий модуль 2. Ключові принципи, сервіси та інструменти захисту інфраструктури, що використовує AWS			
4	IAM для сервісів AWS.	3	6
5	Шифрування at rest, at transition.	3	4
6	ClotudTrail та CloudWatch. Автоматизація інцидентів.	26	32
	РАЗОМ	**42**	**78**

7. Індивідуальні самостійні завдання

Індивідуальні самостійні завдання базуються на проходженні курсів AWS Academy Cloud Foundations та AWS Academy Cloud Security Foundations, які розміщені на платформі AWS Academy; проходження курсів Ultimate AWS Certified Cloud Practitioner CLF-C02 та Ultimate AWS Certified Security Specialty SCS-C02 на платформі Udemy; виконання та захисті лабораторних робіт.

8. Методи навчання

Під час викладання навчальної дисципліни використовуються наступні методи навчання.

Результат навчання	Методи навчання
РН-1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	– Вербальні методи (лекція, пояснення) – Наочні методи (спостереження, демонстрація, ілюстрація) – Практичні методи (проведення дослідів, експериментів, виконання різних видів вправ, практичних завдань, кейсів) – Ситуаційний метод – Дискусійний метод – Методи самостійної роботи (анотування опрацьованого матеріалу, вирішення задач, проведення розрахунків,

Результат навчання	Методи навчання
	написання есе, підготовка доповідей, написання наукових статей)
РН-2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах	– Вербальні методи (лекція, пояснення) – Наочні методи (спостереження, демонстрація, ілюстрація) – Практичні методи (проведення дослідів, експериментів, виконання різних видів вправ, практичних завдань, кейсів) – Дискусійний метод – Ситуаційний метод – Методи самостійної роботи (анотування опрацьованого матеріалу, вирішення задач, проведення розрахунків, написання есе, підготовка доповідей, написання наукових статей)
РН-3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.	– Вербальні методи (лекція, пояснення) – Наочні методи (спостереження, демонстрація, ілюстрація) – Практичні методи (проведення дослідів, експериментів, виконання різних видів вправ, практичних завдань, кейсів) – Дискусійний метод – Ситуаційний метод Методи самостійної роботи (анотування опрацьованого матеріалу, вирішення задач, проведення розрахунків, написання есе, підготовка доповідей, написання наукових статей)
РН-6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	– Вербальні методи (лекція, пояснення) – Наочні методи (спостереження, демонстрація, ілюстрація) – Практичні методи (проведення дослідів, експериментів, виконання різних видів вправ, практичних завдань, кейсів) – Дискусійний метод – Ситуаційний метод Методи самостійної роботи (анотування опрацьованого матеріалу, вирішення задач, проведення розрахунків, написання есе, підготовка доповідей, написання наукових статей)
РН-7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	– Вербальні методи (лекція, пояснення) – Наочні методи (спостереження, демонстрація, ілюстрація) – Практичні методи (проведення дослідів, експериментів, виконання різних видів вправ, практичних завдань, кейсів)

Результат навчання	Методи навчання
	– Дискусійний метод – Ситуаційний метод – Методи самостійної роботи (анотування опрацьованого матеріалу, вирішення задач, проведення розрахунків, написання есе, підготовка доповідей, написання наукових статей)
РН-8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.	– Вербальні методи (лекція, пояснення) – Наочні методи (спостереження, демонстрація, ілюстрація) – Практичні методи (проведення дослідів, експериментів, виконання різних видів вправ, практичних завдань, кейсів) – Дискусійний метод – Ситуаційний метод Методи самостійної роботи (анотування опрацьованого матеріалу, вирішення задач, проведення розрахунків, написання есе, підготовка доповідей, написання наукових статей)
РН-9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.	– Вербальні методи (лекція, пояснення) – Наочні методи (спостереження, демонстрація, ілюстрація) – Практичні методи (проведення дослідів, експериментів, виконання різних видів вправ, практичних завдань, кейсів) – Дискусійний метод – Ситуаційний метод – Методи самостійної роботи (анотування опрацьованого матеріалу, вирішення задач, проведення розрахунків, написання есе, підготовка доповідей, написання наукових статей)
РН-10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.	– Вербальні методи (лекція, пояснення) – Наочні методи (спостереження, демонстрація, ілюстрація) – Практичні методи (проведення дослідів, експериментів, виконання різних видів вправ, практичних завдань, кейсів) – Дискусійний метод – Ситуаційний метод – Методи самостійної роботи (анотування опрацьованого матеріалу, вирішення задач, проведення розрахунків, написання есе, підготовка доповідей, написання наукових статей)
РН-11. Аналізувати, контролювати та	– Вербальні методи (лекція, пояснення)

Результат навчання	Методи навчання
забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	– Наочні методи (спостереження, демонстрація, ілюстрація) – Практичні методи (проведення дослідів, експериментів, виконання різних видів вправ, практичних завдань, кейсів) – Дискусійний метод – Ситуаційний метод – Методи самостійної роботи (анотування опрацьованого матеріалу, вирішення задач, проведення розрахунків, написання есе, підготовка доповідей, написання наукових статей)
РН-12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.	– Вербальні методи (лекція, пояснення) – Наочні методи (спостереження, демонстрація, ілюстрація) – Практичні методи (проведення дослідів, експериментів, виконання різних видів вправ, практичних завдань, кейсів) – Дискусійний метод – Ситуаційний метод – Методи самостійної роботи (анотування опрацьованого матеріалу, вирішення задач, проведення розрахунків, написання есе, підготовка доповідей, написання наукових статей)
РН-13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку	– Вербальні методи (лекція, пояснення) – Наочні методи (спостереження, демонстрація, ілюстрація) – Практичні методи (проведення дослідів, експериментів, виконання різних видів вправ, практичних завдань, кейсів) – Дискусійний метод – Ситуаційний метод – Методи самостійної роботи (анотування опрацьованого матеріалу, вирішення задач, проведення розрахунків, написання есе, підготовка доповідей, написання наукових статей)
РН-14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.	– Вербальні методи (лекція, пояснення) – Наочні методи (спостереження, демонстрація, ілюстрація) – Практичні методи (проведення дослідів, експериментів, виконання різних видів вправ, практичних завдань, кейсів) – Дискусійний метод – Ситуаційний метод – Методи самостійної роботи (анотування

Результат навчання	Методи навчання
	опрацьованого матеріалу, вирішення задач, проведення розрахунків, написання есе, підготовка доповідей, написання наукових статей)
РН-15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб	– Вербальні методи (лекція, пояснення) – Наочні методи (спостереження, демонстрація, ілюстрація) – Дискусійний метод – Ситуаційний метод
РН-17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об’єктивно оцінювати результати навчання.	– Наочні методи (спостереження, демонстрація, ілюстрація) – Практичні методи (проведення дослідів, експериментів, виконання різних видів вправ, практичних завдань, кейсів) – Методи самостійної роботи (анотування опрацьованого матеріалу, вирішення задач, проведення розрахунків, написання есе, підготовка доповідей, написання наукових статей)

9. Методи контролю

Перевірка досягнення результатів навчання здійснюється з використанням наступних методів.

Результат навчання	Методи контролю
РН-1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	– Усне опитування, участь у дискусії, відповіді на проблемні запитання – Перевірка виконання домашніх завдань, практичних завдань, вправ, кейсів – Перевірка виконання та захист лабораторних робіт – Експрес-тестування – Самооцінювання та взаємооцінювання – Залік
РН-2. Інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах	– Усне опитування, участь у дискусії, відповіді на проблемні запитання – Перевірка виконання домашніх завдань, практичних завдань, вправ, кейсів – Перевірка виконання та захист лабораторних робіт – Експрес-тестування – Самооцінювання та взаємооцінювання – Залік
РН-3. Провадити дослідницьку та/або	– Усне опитування, участь у дискусії, відповіді

Результат навчання	Методи контролю
інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.	на проблемні запитання – Перевірка виконання домашніх завдань, практичних завдань, вправ, кейсів – Перевірка виконання та захист лабораторних робіт – Експрес-тестування – Самооцінювання та взаємооцінювання – Залік
РН-6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	– Усне опитування, участь у дискусії, відповіді на проблемні запитання – Перевірка виконання домашніх завдань, практичних завдань, вправ, кейсів – Перевірка виконання та захист лабораторних робіт – Експрес-тестування – Самооцінювання та взаємооцінювання – Залік
РН-7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв’язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	– Усне опитування, участь у дискусії, відповіді на проблемні запитання – Перевірка виконання домашніх завдань, практичних завдань, вправ, кейсів – Перевірка виконання та захист лабораторних робіт – Експрес-тестування – Самооцінювання та взаємооцінювання – Залік
РН-8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.	– Усне опитування, участь у дискусії, відповіді на проблемні запитання – Перевірка виконання домашніх завдань, практичних завдань, вправ, кейсів – Перевірка виконання та захист лабораторних робіт – Експрес-тестування – Самооцінювання та взаємооцінювання – Залік
РН-9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.	– Усне опитування, участь у дискусії, відповіді на проблемні запитання – Перевірка виконання домашніх завдань, практичних завдань, вправ, кейсів – Перевірка виконання та захист лабораторних робіт – Експрес-тестування – Самооцінювання та взаємооцінювання – Залік
РН-10. Забезпечувати безперервність бізнес/операційних процесів, а також	– Усне опитування, участь у дискусії, відповіді на проблемні запитання

Результат навчання	Методи контролю
виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.	– Перевірка виконання домашніх завдань, практичних завдань, вправ, кейсів – Перевірка виконання та захист лабораторних робіт – Експрес-тестування – Самооцінювання та взаємооцінювання – Залік
РН-11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	– Усне опитування, участь у дискусії, відповіді на проблемні запитання – Перевірка виконання домашніх завдань, практичних завдань, вправ, кейсів – Перевірка виконання та захист лабораторних робіт – Експрес-тестування – Самооцінювання та взаємооцінювання – Залік
РН-12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.	– Усне опитування, участь у дискусії, відповіді на проблемні запитання – Перевірка виконання домашніх завдань, практичних завдань, вправ, кейсів – Перевірка виконання та захист лабораторних робіт – Експрес-тестування – Самооцінювання та взаємооцінювання – Залік
РН-13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку	– Усне опитування, участь у дискусії, відповіді на проблемні запитання – Перевірка виконання домашніх завдань, практичних завдань, вправ, кейсів – Перевірка виконання та захист лабораторних робіт – Експрес-тестування – Самооцінювання та взаємооцінювання – Залік
РН-14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.	– Усне опитування, участь у дискусії, відповіді на проблемні запитання – Перевірка виконання домашніх завдань, практичних завдань, вправ, кейсів – Перевірка виконання та захист лабораторних робіт – Експрес-тестування – Самооцінювання та взаємооцінювання – Залік
РН-15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також	– Усне опитування, участь у дискусії, відповіді на проблемні запитання

Результат навчання	Методи контролю
знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб	– Перевірка виконання домашніх завдань, практичних завдань, вправ, кейсів – Перевірка виконання та захист лабораторних робіт – Експрес-тестування – Самооцінювання та взаємооцінювання – Залік
РН-17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об’єктивно оцінювати результати навчання.	– Усне опитування, участь у дискусії, відповіді на проблемні запитання – Перевірка виконання домашніх завдань, практичних завдань, вправ, кейсів – Перевірка виконання та захист лабораторних робіт – Експрес-тестування – Самооцінювання та взаємооцінювання – Залік

[1] Програмні результати навчання, які формуються під час вивчення дисципліни, зазначаються лише для обов’язкових навчальних дисциплін.

10. Оцінювання результатів навчання здобувачів вищої освіти

Оцінювання результатів навчання здобувачів вищої освіти з навчальної дисципліни здійснюється відповідно до Положення про оцінювання результатів навчання здобувачів вищої освіти у Державному університеті «Житомирська політехніка» та розподілу балів, що наведений нижче.

Система оцінювання результатів навчання здобувачів вищої освіти з навчальної дисципліни включає поточний та підсумковий контроль.

Поточний контроль проводиться для оцінювання рівня засвоєння знань, формування умінь і навичок здобувачів вищої освіти впродовж вивчення ними матеріалу модуля (змістових модулів) навчальної дисципліни. Поточний контроль здійснюється під час проведення навчальних занять.

Підсумковий контроль проводиться для підсумкового оцінювання результатів навчання здобувачів вищої освіти з навчальної дисципліни. Підсумковий контроль здійснюється після завершення вивчення навчальної дисципліни або наприкінці семестру. Підсумковий контроль проводиться у формі заліку. Процедура складання заліку визначена у Положенні про організацію освітнього процесу у Державному університеті «Житомирська політехніка».

Розподіл балів з навчальної дисципліни

Види робіт здобувача вищої освіти	Кількість балів за семестр	
	денна форма	заочна форма
Виконання завдань поточного контролю	100	100

Види робіт здобувача вищої освіти	Кількість балів за семестр	
	денна форма	заочна форма
Підсумкова семестрова оцінка	**100**	**100**

Розподіл балів за виконання завдань поточного контролю

Види робіт здобувача вищої освіти	Кількість балів за семестр	
	денна форма	заочна форма
Виконання завдань під час навчальних занять	60	30
Виконання та захист індивідуальних самостійних завдань[2]	40	70
Виконання науково-дослідної роботи та інших видів робіт (**додаткові – заохочувальні бали**)[3]: 1. Участь у студентських предметних олімпіадах, Всеукраїнському конкурсі студентських наукових робіт, грантах, науково-дослідних проектах 2. Підготовка наукових статей, тез доповідей наукових конференцій 3. Інші види робіт (наводиться перелік інших видів робіт)		
Разом за виконання завдань поточного контролю	**100**	**100**

Розподіл балів за виконання завдань під час навчальних занять

Види робіт здобувача вищої освіти	Кількість балів за семестр	
	денна форма	заочна форма
Виконання та захист лабораторних робіт	60	60
Проходження курсів AWS Academy Cloud Foundations та AWS Academy Cloud Security Foundations	30	30
Проходження курсів Udemy	10	10
Разом за виконання завдань під час навчальних занять	**100**	**100**

З метою застосування цілих чисел для оцінювання результатів роботи здобувачів під час навчальних занять може використовуватися 100-бальна шкала оцінювання щодо кожного окремо виду робіт. Розрахунок загальної кількості балів, які здобувач може набрати за результатами роботи під час навчальних занять протягом семестру, проводиться за формулою:

$$Р_{НЗ} = \sum(Р_i \times ВК_i) \times К_{НЗ}, \quad (1)$$

де $Р_{НЗ}$ – загальна кількість балів, набраних здобувачем за виконання завдань під час навчальних занять за семестр;

$Р_i$ – кількість набраних здобувачем балів за семестр за виконання і-го виду робіт під час навчальних занять (за 100-бальною шкалою);

$ВК_i$ – ваговий коефіцієнт за виконання і-го виду робіт під час навчальних занять. Значення вагових коефіцієнтів розраховуються шляхом ділення кількості балів, яка передбачена за виконання окремого виду робіт під час навчальних занять, на сумарну кількість балів за виконання усіх видів робіт під час навчальних занять за семестр;

$К_{НЗ}$ – коригувальний коефіцієнт, який визначається шляхом ділення кількості балів, що передбачена за виконання завдань під час навчальних занять за семестр, на 100 балів.

Якщо здобувач вищої освіти набрав за поточний контроль 60 балів або більше, він може погодити дану оцінку в електронному кабінеті і вона стане семестровою оцінкою за вивчення навчальної дисципліни.

Якщо здобувач вищої освіти під час вивчення навчальної дисципліни набрав 60 балів або більше і бажає покращити свій результат успішності, він проходить процедуру підсумкового контролю у формі заліку. За складання заліку здобувач вищої освіти може набрати 100 балів. Семестрова оцінка з навчальної дисципліни формується за результатами підсумкового контролю.

Здобувач вищої освіти допускається до процедури підсумкового контролю у формі заліку, якщо за виконання завдань поточного контролю набрав 50 балів або більше.

Якщо здобувач вищої освіти за результатами поточного контролю набрав 35–49 балів, він отримує право за власною заявою опанувати окремі теми (змістові модулі) навчальної дисципліни понад обсяги, встановлені навчальним планом освітньої програми. Вивчення окремих складових навчальної дисципліни понад обсяги, встановлені навчальним планом освітньої програми, здійснюється у вільний від занять здобувача вищої освіти час.

Якщо здобувач вищої освіти за результатами поточного контролю набрав від 0 до 34 балів (включно), він вважається таким, що не виконав вимоги робочої програми навчальної дисципліни та має академічну заборгованість. Здобувач вищої освіти отримує право за власною заявою опанувати навчальну дисципліну у наступному семестрі понад обсяги, встановлені навчальним планом освітньої програми.

Процедура надання додаткових освітніх послуг здобувачу вищої освіти з метою вивчення навчального матеріалу дисципліни понад обсяги, встановлені навчальним планом освітньої програми, визначена у Положенні про надання додаткових освітніх послуг здобувачам вищої освіти в Державному університеті «Житомирська політехніка».

Визнання результатів навчання, набутих у неформальній та/або інформальній освіті

Визнання результатів навчання, набутих у неформальній та/або інформальній освіті в рамках окремих тем навчальної дисципліни, здійснюється викладачем за

зверненням здобувача вищої освіти та представленням документів, які підтверджують результати навчання (сертифікати, свідоцтва, скріншоти тощо). Рішення про визнання та оцінка за відповідну частину освітнього компонента приймається викладачем за результатами співбесіди зі здобувачем вищої освіти.

Визнання результатів навчання, набутих у неформальній та/або інформальній освіті в рамках цілого освітнього компонента, здійснюється за процедурою, яка визначена у Положенні про організацію освітнього процесу у Державному університеті «Житомирська політехніка».

Шкала оцінювання

Шкала ЄКТС	Національна шкала	100-бальна шкала
A	Зараховано	90-100
B	Зараховано	82-89
C		74-81
D	Зараховано	64-73
E		60-63
FX	Не зараховано	35-59
F	Не зараховано	0-34

11. Глосарій[1]

№ з/п	Термін державною мовою	Відповідник англійською мовою
1	Інфраструктура як послуга	Infrastructure as a service (IaaS)
2	Платформа як послуга	Platform as a service (PaaS)
3	Програма як послуга	Software as a service (SaaS)
4	Оркестрація	Orchestration
5	Публічна хмара	Public cloud
6	Приватна хмара	Private cloud
7	Об’єктне сховище	Object storage
8	Гібридна хмара	Hybrid cloud
9	Інфраструктура як код	Infrastructure as Code (IaC)
10	Віртуальна приватна хмара	Virtual Private Cloud (VPC)
11	Система керування ідентичністю й доступом	Identity and Access Management (IAM)
12	Безперервна інтеграція/безперервне розгортання	Continuous Integration/Continuous Deployment (CI/CD)
13	Балансування навантаження	Load Balancing
14	Керування ідентифікацією та доступом	Identity and Access Management (IAM)
15	Шифрування даних	Data Encryption
16	Управління ключами	Key Management
17	Безпека на основі ролей	Role-based Access Control (RBAC)

№ з/п	Термін державною мовою	Відповідник англійською мовою
18	Балансування навантаження	Load Balancing
19	Керування ідентифікацією та доступом	Identity and Access Management (IAM)
20	Шифрування даних	Data Encryption
21	Відмова в обслуговуванні	Denial of Service (DoS)
22	Розподілена відмова в обслуговуванні	Distributed Denial of Service (DDoS)
23	Управління ключами	Key Management
24	Безпека на основі ролей	Role-based Access Control (RBAC)
25	Балансування навантаження	Load Balancing
26	Керування ідентифікацією та доступом	Identity and Access Management (IAM)
27	Шифрування даних	Data Encryption
28	Інтерфейс командного рядка	Command-Line Interface (CLI)
29	Інтерфейс програмування застосунків	Application Programming Interface (API)
30	Передача репрезентативного стану	Representational State Transfer (REST)
31	Проєкт з безпеки веб-додатків	Open Web Application Security Project (OWASP)

12. Рекомендована література

Основна література

Основна література з навчальної дисципліни має бути за останні 5 років.

1. Heartin Kanikathottu. AWS Security Cookbook: Practical solutions for managing security policies, monitoring, auditing, and compliance with AWS. 2020, – 440p.
2. Dylan Shields. AWS Security. 2022, – 312p.
3. Albert Anthony. Aws: Security Best Practices on AWS.
4. John Culkin, Mike Zazon. AWS Cookbook: Recipes for Success on AWS. 2021, – 358p.
5. Jonathan Helmus, AWS Penetration Testing: Beginner's guide to hacking AWS with tools such as Kali Linux, Metasploit, and Nmap. 2020, – 330p.

Допоміжна література

1. Ben Piper, David Clinton. AWS Certified Cloud Practitioner Study Guide With 500 Practice Test Questions: Foundational (CLF-C02) Exam. 2023, – 320p.
2. Marcello Zillo Neto, Gustovo A.A. Santana, Fernando Sapata, Mauricio Munoz, Alexandre M.S.P. Moraes, Thiago Morais, Dario Lucas Goldfarb. AWS Certified Security Study Guide: Specialty (SCS-C01) Exam. 2021, – 496p.

13. Інформаційні ресурси в Інтернеті

1. AWS Academy [Електронний ресурс] – Режим доступу до ресурсу: https://awsacademy.instructure.com/.
2. AWS Documentation [Електронний ресурс] – Режим доступу до ресурсу: https://docs.aws.amazon.com/.
3. AWS Training and Certification [Електронний ресурс] – Режим доступу до ресурсу: https://aws.amazon.com/training/.