ЗАТВЕРДЖЕНО

Вченою радою
факультету інформаційно-комп'ютерних технологій
28 вересня 2022 р., протокол №2
Голова Вченої ради
_____Тетяна НІКІТЧУК

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
ОК 9 «Розширена мережна та хмарна безпека»

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

Схвалено на засіданні кафедри
комп'ютерної інженерії та кібербезпеки
31 серпня 2022 р., протокол №4
Завідувач кафедри
_____Андрій ЄФІМЕНКО
Гарант освітньо-професійної програми
_____Володимир ВОРОТНІКОВ

Розробники: кандидат технічних наук, завідувач кафедри комп'ютерної інженерії та кібербезпеки Андрій ЄФІМЕНКО,
старший викладач кафедри комп'ютерної інженерії та кібербезпеки Ярослав КРУЧИНСЬКИЙ

Житомир
2022 – 2023 н.р.

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, освітній ступінь</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td>Кількість кредитів 5</td><td>Галузь знань
12 «Інформаційні технології»</td><td colspan="2">нормативна
(нормативна, за вибором)</td></tr>
<tr><td>Модулів – 1</td><td rowspan="5">Спеціальність
125 «Кібербезпека»</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td rowspan="2">Змістових модулів – 6</td><td>1-й</td><td>1-й</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин - 150</td><td>1-й</td><td>1-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="11">Тижневих годин для денної форми навчання:
аудиторних 4
самостійної роботи – 3,5</td><td rowspan="11">Освітній ступінь «магістр»</td><td>32 год.</td><td>4 год.</td></tr>
<tr><td colspan="2">Практичні</td></tr>
<tr><td>–</td><td>–</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>32 год.</td><td>8 год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>86 год.</td><td>138 год.</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2">Вид контролю: 1 семестр – екзамен</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної та індивідуальної роботи становить:

для денної форми навчання – 43 % аудиторних занять, 57 % самостійної та індивідуальної роботи;

для заочної форми навчання − 8 % аудиторних занять, 92 % самостійної та індивідуальної роботи.

2. Мета та завдання навчальної дисципліни

Сучасні технології віртуалізації в поєднанні з IT-інфраструктурою на вимогу широко застосовуються промисловістю для економії капітальних і операційних витрат. Але зовнішні інфраструктури на вимогу викликають нові проблеми безпеки. Дисципліна охоплює вступ до хмарної безпеки, розглядаючи відомі ризики та вразливості та зосереджуючись на надійному архітектурному дизайні для безпечних обчислень. Розглядаються питання управління, аудиту, юридичних питань і дотримання нормативних вимог. Розповідається про методи, які використовуються для розгортання критично важливих механізмів безпеки, пов'язаних із безпечною ізоляцією, безпекою додатків, захистом даних, контролем доступу, конфіденційністю, керуванням ключами, наданням, керуванням ідентифікацією та авторизацією, високою доступністю, керуванням і відповідністю в хмарі. активне середовище.

Завданнями вивчення навчальної дисципліни є:

- Розглядаються снови архітектури хмарних обчислень на основі поточних стандартів, протоколів і найкращих практик, призначених для надання корпоративних IT-служб і бізнес-додатків у хмарі.
- Визначаються відомі загрози, ризики, уразливості та проблеми конфіденційності, пов'язані з IT-сервісами на основі хмари.
- Роглядаються концепції та керівні принципи для розробки та впровадження належних гарантій і контрзаходів для хмарних IT-сервісів.
- Визначаються до розробки хмарних сервісів, які відповідають основним характеристикам хмарної інфраструктури – обчислення на вимогу, спільні ресурси, еластичність і вимірювання використання.
- Надається розуміння галузевих стандартів безпеки, регуляторних мандати, політика аудиту та вимоги відповідності для хмарних інфраструктур.
- Матеріали дисципліни відповідають інструкціям з безпеки в хмарі, встановленим NIST, Cloud Security Alliance та ENISA(European Network and Information Security Agency).

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

КЗ-1. Здатність застосовувати знання у практичних ситуаціях.

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-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.

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

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-4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

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-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-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-16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.

РН-19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.

РН-20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.

РН-21. Використовувати методи натурного, фізичного і комп’ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

РН-23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

3. Програма навчальної дисципліни

Модуль 1

ЗМІСТОВНИЙ МОДУЛЬ I. ОСНОВИ ХМАРНИХ ОБЧИСЛЕНЬ І АРХІТЕКТУРНІ ХАРАКТЕРИСТИКИ

Вступ до хмарних технологій. Сфери застосування хмарних технологій. Поняття хмарних обчислень. Архітектурний і технологічний вплив хмарних обчислень. Моделі розгортання хмарних систем. Сфери контролю в хмарній системі: Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS). Ролі хмарних обчислень. Ризики та проблеми безпеки.

ЗМІСТОВНИЙ МОДУЛЬ II. ДИЗАЙН ТА АРХІТЕКТУРА БЕЗПЕКИ ДЛЯ ХМАРНИХ ОБЧИСЛЕНЬ

Керівні принципи розробки безпеки для хмарних обчислень: безпечна ізоляція, комплексний захист даних, наскрізний контроль доступу, моніторинг і аудит. Огляд інструкцій CSA, NIST і ENISA щодо безпеки в хмарі. Загальні вектори атак та загрози.

ЗМІСТОВНИЙ МОДУЛЬ III. БЕЗПЕЧНА ІЗОЛЯЦІЯ ФІЗИЧНОЇ ТА ЛОГІЧНОЇ ІНФРАСТРУКТУРИ

Визначення поняття ізоляції. Обчислення, мережа та зберігання. Поширені вектори атак і загрози. Стратегії безпечної ізоляції: мультиоренда, стратегії віртуалізації, стратегії сегментації мережі між орендарями, стратегії ізоляції сховищ.

ЗМІСТОВНИЙ МОДУЛЬ IV. ЗАХИСТ ДАНИХ ДЛЯ ХМАРНОЇ ІНФРАСТРУКТУРИ ТА СЕРВІСІВ

Життєвий цикл інформації на основі хмарної системи. Захист даних для конфіденційності та цілісності. Загальні вектори атак і загрози. Шифрування, редагування даних, керування ключами, забезпечення видалення даних. Процедури збереження, видалення та архівація даних орендарів. Стратегії захисту даних.

ЗМІСТОВНИЙ МОДУЛЬ V. ЗАСТОСУВАННЯ КОНТРОЛЮ ДОСТУПУ ДЛЯ СЛУЖБ НА ОСНОВІ ХМАРНОЇ ІНФРАСТРУКТУРИ

Визначення вимог до контролю доступу до хмарної інфраструктури. Визначення найпоширеніших векторів атак і загрози. Застосування стратегій контролю доступу: обчислення, мережа та зберігання. Автентифікація та авторизація. Контроль доступу на основі ролей, багатофакторна автентифікація. Параметри керування доступом до хосту, сховища та мереж. Зміцнення та мінімізація ОС, забезпечення віддаленого доступу, перевірене та вимірюване завантаження. Брандмауери, IDS, IPS і honeypots.

ЗМІСТОВНИЙ МОДУЛЬ VI. МОНІТОРИНГ, АУДИТ І УПРАВЛІННЯ

Проактивний моніторинг діяльності, реагування на інциденти. Моніторинг несанкціонованого доступу, зловмисного трафіку, зловживання системними привілеями, виявлення вторгнень, подій і сповіщень. Аудит – створення записів, звітування та управління. Журнали аудиту захисту від втручання. Якість послуг. Безпечне управління. Керування користувачами. Управління ідентифікацією. Інформація про безпеку та управління подіями

4. Структура (тематичний план) навчальної дисципліни

Змістовні модулі	Кількість годин			
	Всього	Лекції	Лабораторні	Самостійна робота
2	3	4	5	6
Модуль 1				
ЗМІСТОВНИЙ МОДУЛЬ 1 ОСНОВИ ХМАРНИХ ОБЧИСЛЕНЬ І АРХІТЕКТУРНІ ХАРАКТЕРИСТИКИ	22	4	4	14
ЗМІСТОВНИЙ МОДУЛЬ 2. ДИЗАЙН ТА АРХІТЕКТУРА БЕЗПЕКИ ДЛЯ ХМАРНИХ ОБЧИСЛЕНЬ	22	4	4	14
ЗМІСТОВНИЙ МОДУЛЬ 3 БЕЗПЕЧНА ІЗОЛЯЦІЯ ФІЗИЧНОЇ ТА ЛОГІЧНОЇ ІНФРАСТРУКТУРИ	22	4	4	14
ЗМІСТОВНИЙ МОДУЛЬ 4 ЗАХИСТ ДАНИХ ДЛЯ ХМАРНОЇ ІНФРАСТРУКТУРИ ТА ПОСЛУГ	22	4	4	14
ЗМІСТОВНИЙ МОДУЛЬ 5 ЗАСТОСУВАННЯ КОНТРОЛЮ ДОСТУПУ ДЛЯ СЛУЖБ НА ОСНОВІ ХМАРНОЇ ІНФРАСТРУКТУРИ	30	8	8	14
ЗМІСТОВНИЙ МОДУЛЬ 6 МОНІТОРИНГ, АУДИТ І УПРАВЛІННЯ	32	8	8	16
ВСЬОГО	150	32	32	86

5. Завдання для самостійної роботи

Відпрацювання матеріалу навчальних курсу The Cloud Security course (Certificate of Cloud Security Knowledge training developed by Cloud Security Alliance) (проходження онлайн навчання, виконання тестових контрольних робіт, виконання тестових проміжних оцінювань).

7. Індивідуальні завдання

Не передбачені.

8. Методи навчання

На лекційних заняттях: розповідь, пояснення, демонстрація, бесіда, дискусія. На лабораторних заняттях: пояснення, виконання модельного прикладу, виконання індивідуального варіанту завдання. Самостійна робота студента: реферати, повідомлення, науково-пошукові, дослідницькі проекти, виконання он-лайн курсів.

За джерелами знань використовуються такі методи навчання: словесні – розповідь, пояснення, лекція, інструктаж; наочні – демонстрація, ілюстрація; практичні – лабораторна робота, практична робота, вправи. За характером логіки пізнання використовуються такі методи: аналітичний, синтетичний, аналітико-синтетичний, індуктивний, дедуктивний. За рівнем самостійної розумової діяльності використовуються методи: проблемний, частково-пошуковий, дослідницький.

9. Методи контролю

Контрольні заходи включають поточний та підсумковий модульний контроль в тому числі у вигляді комп'ютерних тестів, виконання практичних завдань.

Поточний контроль здійснюється під час проведення лабораторних занять для перевірки рівня підготовки студента до виконання конкретного завдання. Форма проведення поточного контролю: усне опитування, вирішення ситуаційних задач, тестовий контроль, виконання практичного завдання. Оцінюється вхідний, проміжний, кінцевий рівень знань студента.

Підсумковий контроль проводиться у вигляді комп'ютерних тестів. Детальний розподіл балів наводиться у рейтинг-листі дисципліни.

Шкала оцінювання

За шкалою	Екзамен	Залік	Бали
A	Відмінно	Зараховано	90-100
B	Добре	Зараховано	82-89
C			74-81
D	Задовільно	Зараховано	64-73
E			60-63
FX	Незадовільно	Не зараховано	35-59
F		Не зараховано	0-34

12. Інформаційні ресурси мережі Інтернет

1. Навчальний курс Cloud Security 1.01 [Електронний ресурс] – Режим доступу: www.netacad.com.
2. Security Guidance for Critical Areas of Focus in Cloud Computing v4.0 [Електронний ресурс] – Режим доступу: https://cloudsecurityalliance.org/artifacts/security-guidance-v4/