МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД

“УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ”

кафедра твердотільної електроніки та інформаційної безпеки

«ЗАТВЕРДЖУЮ»
Декан фізичного факультету
_____ /Лазур В.Ю./
«30» червня 2023 року

Робоча програма навчальної дисципліни
БЕЗПЕКА ХМАРНИХ ТЕХНОЛОГІЙ ТА РОЗПОДІЛЕНИХ ОБЧИСЛЕНЬ

Рівень вищої освіти	другий (магістерський) рівень вищої освіти
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека та захист інформації
Освітня програма	Безпека інформаційних і комунікаційних систем
Статус дисципліни	Обов’язова
Мова навчання	Українська

Ужгород 2023

Робоча програма навчальної дисципліни «**Безпека хмарних технологій та розподілених обчислень**» для здобувачів вищої освіти галузі знань **12 Інформаційні технології** спеціальності **125 Кібербезпека та захист інформації** освітньої програми **Безпека інформаційних і комунікаційних систем.**

Розробник: доктор технічних наук, старший науковий співробітник Давиденко А.М.

Робочу програму розглянуто та затверджено на засіданні кафедри твердотільної електроніки та інформаційної безпеки
протокол № 9 від « 15 » червня 2023 р.

Завідувач кафедри _____ Різак В.М.

Схвалено науково-методичною комісією фізичного факультету
протокол № 10 від « 28 » червня 2023 р.
Голова науково-методичної комісії _____ Карбованець М. І.

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Найменування показників	**Розподіл годин за навчальним планом**
	Денна форма навчання
Кількість кредитів ЄКТС – **4**	Рік підготовки:
Загальна кількість годин - **120**	**1**
Кількість модулів – **2**	Семестр:
Тижневих годин для денної форми навчання:	**2**
	Лекції:
аудиторних – **3**	**24**
	Практичні (семінарські):
самостійної роботи студента – **4**	**24**
Вид підсумкового контролю: **іспит**	Лабораторні:
Форма підсумкового контролю: **усна**	Самостійна робота:
	72

2. МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Безпека хмарних технологій та розподілених обчислень»

Мета курсу – надання студентам цілісної системи знань з використання сучасних технологій "хмарних" обчислень, які є розвитком IT- послуг доставки, що передбачає шлях до оптимізації використання, і швидкого розгортання ресурсів через системи і рішення, які є більш ефективними і масштабованими на основі найважливіших методів обробки інформації; формування у студента алгоритмічного мислення та розуміння логіки процесів; навичок побудови хмарних сховищ даних з використанням об'єктно-орієнтованих технологій, що є основою для фахівця в галузі «Безпеки інформаційних і комунікаційних систем».

Завдання дисципліни «Безпека хмарних технологій та розподілених обчислень» – навчити використовувати набуті знання з "хмарних" технологій, методів "хмарних" обчислень та надійного зберігання даних у "хмарних" сховищах; основ функціонування комп'ютерних систем (КС) та їх побудови; правил та методів захисту програмного забезпечення даних у КС; виявити задатки і розвити творчі здібності студентів з основних напрямків, закономірностей, змісту і форм наукової творчості, методів планування, організації і керування науковою творчістю, роботи наукових колективів, сучасних

теоретичних і експериментальних методів пошуку нових наукових рішень, принципів патентного пошуку, патентування, винахідницької і раціоналізаторської роботи, написання наукових робіт.

Фокус навчальної дисципліни: зміст та матеріал навчальної дисципліни стосується аналізу теоретико-методологічних основ безпеки хмарних технологій та розподілених обчислень як галузі наукових знань, які орієнтують студента на актуальні питання сьогоднішнього стану хмарних технологій, в рамках яких можлива подальша професійна та наукова кар'єра у галузі кібербезпеки.

Місце дисципліни в структурі освітньо-наукової програми: курс відноситься до дисциплін циклу професійної підготовки, за результатами яких здобувачі здають іспит та виконують навчальний процес по спеціальності 125 Кібербезпека та захист інформації.

Відповідно до освітньої програми Безпека інформаційних і комунікаційних систем для другого (магістерського) рівня спеціальності 125 Кібербезпека та захист інформації, вивчення дисципліни сприяє формуванню у здобувачів другого рівня вищої освіти таких компетентностей:

Інтегральна: Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.

*Загальні компетентності**:***

1. Здатність застосовувати знання у практичних ситуаціях (КЗ-1).
2. Здатність проводити дослідження на відповідному рівні (КЗ-2).
3. Здатність до абстрактного мислення, аналізу та синтезу (КЗ-3).
4. Здатність оцінювати та забезпечувати якість виконуваних робіт(КЗ-4).
5. Здатність діяти соціально відповідально та громадсько свідомо (КЗ-5).

Фахові компетенції (ФК)

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. (КФ1)

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 (КФ2).

3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури (КФ3).

4. 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 (КФ5).

5. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації (КФ6).

А відповідно до професійного стандарту «Фахівець сфери захисту інформації» вивчення дисципліни сприяє формуванню у здобувачів другого рівня вищої освіти таких компетентностей:

Загальні компетентності (ЗК)

ЗК.01. Здатність діяти соціально відповідально та громадсько свідомо.

ЗК.02. Здатність застосовувати знання у практичних ситуаціях, розв'язувати завдання/задачі та практичні проблеми у професійній діяльності.

ЗК.05. Здатність до адаптації та дії в новій ситуації.

ЗК.07. Здатність спілкуватися рідною мовою як усно, так і письмово, спілкуватися іноземною (переважно англійською) на рівні, що забезпечує ефективну професійну діяльність.

Професійні компетентності (за трудовою дією або групою трудових дій) згідно професійного стандарту «Фахівець сфери захисту інформації»

Д1. Здатність аналізувати, інтегрувати і використовувати кращі світові практики, стандарти при розробці нормативних документів системи технічного та криптографічного захисту інформації.

Д2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування щодо систем технічного та криптографічного захисту інформації.

Е1. Здатність здійснювати технічне керівництво фахівцями структурних підрозділів підприємства (організації), до функцій яких входять питання захисту інформації та кібербезпеки.

Е2. Здатність взаємодіяти із керівництвом і фахівцями технологічних та інших підрозділів підприємства/організації з технологічних та інших питань, пов'язаних із забезпеченням захисту інформації та кіберзахисту.

Е3. Здатність взаємодіяти із зовнішніми партнерами в межах визначених повноважень.

3. ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Відповідно до освітньо-професійної програми «Безпека інформаційних і комунікаційних систем» для другого (магістерського) рівня спеціальності 125 Кібербезпека та захист інформації**,** вивчення навчальної дисципліни повинно забезпечити досягнення здобувачами вищої освіти таких програмних результатів навчання (РН)**:**

Програмні результати навчання	
Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах	РН 2
Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки	РН 4
Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.	РН 5
Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	РН 6
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 7

Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.	РН 8
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 11
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 12
Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.	РН 22
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.	РН 23
Володіти методиками аналізу, синтезу, оптимізації та прогнозування якості процесів функціонування інформаційних процесів та технологій в розподілених інформаційно- комунікаційних системах.	РН 24

Очікувані результати навчання, які повинні бути досягнуті здобувачами освіти після опанування навчальної дисципліни «Безпека хмарних технологій та розподілених обчислень»:

1. Демонструє вміння інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах (РН 2).

2. Демонструє здатність застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки (РН 4).

3. Знає та розуміє проблеми кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення (РН 5).

4. Володіє методикою аналіза та оцінювання захищеністі систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення (РН 6).

5. Демонструє здатність 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 7).

6. Демонструє вміння досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури (РН 8).

7. Має навички аналізу, контролю та забезпечення ефективного функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації (РН 11).

8. Демонструє вміння 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 12).

9. Освоїв методологію планування та виконання експериментальних і теоретичних досліджень, висування і перевірки гіпотез, вибору для цього придатних методів та інструментів, виконання статистичної обробки даних, оцінювання достовірності результатів досліджень, аргументування висновків (РН 22).

10. Має навички в обґрунтованні вибору 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 (РН 23).

11. Володіє методиками аналізу, синтезу, оптимізації та прогнозування якості процесів функціонування інформаційних процесів та технологій в розподілених інформаційно-комунікаційних системах (РН 24).

4. ЗАСОБИ ДІАГНОСТИКИ ТА КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Засобами оцінювання та методами демонстрування результатів навчання з навчальної дисципліни є: **оцінювання домашніх і самостійних завдань та контрольних робіт; оцінювання завдань, виконаних студентами під час практичних занять, іспит.**

Контрольні заходи включають такі ***форми контролю та критерії оцінювання результатів навчання:*** поточний, модульний та підсумковий контроль.

Поточний контроль– оцінювання рівня знань, умінь і навичок здобувачів, що здійснюється в ході навчального процесу проведенням усного опитування, контрольної роботи, тестування, домашнього завдання тощо.

Результатом *модульного контролю* є модульна бальна оцінка, за якою підбивається підсумок роботи студентів впродовж модуля у відповідності до кредитно-трансферної системи оцінювання знань.

Підсумковий семестровий контроль проводиться у формі іспиту в обсязі навчального матеріалу, що визначений навчальною програмою, та в терміни, встановлені графіком навчального процесу. При семестровому контролі отримані здобувачем згідно кредитно-трансферної системи оцінювання знань переводяться в оцінки за національною шкалою та за шкалою ЄКТС.

Комплексний показник успішності здобувача другого рівня вищої освіти, його обізнаності в предметі, що вивчається, характеризує якість його знань, систематичність, творчість, активність та самостійність. Максимальна сума балів за всі види робіт (контрольні, самостійне вивчення, практичні (семінарські) заняття) з даного курсу становить 100 балів.

Розподіл балів, які отримують здобувачі вищої освіти (модуль 1)

Поточне оцінювання та самостійна робота						**Модульна контрольна робота**	**Сума**
Т1	Т2	Т3	Т4	Т5	Т6	20	**60**
6	6	6	6	8	8		

Розподіл балів, які отримують здобувачі вищої освіти (модуль 2)

Поточне оцінювання та самостійна робота						Модульна контрольна робота	Сума
Т1	Т2	Т3	Т4	Т5	Т6	20	**60**
6	6	6	6	8	8		

Оцінювання окремих видів навчальної роботи з дисципліни

Вид діяльності здобувача вищої освіти	Модуль 1		Модуль 2	
	Кількість	Максимальна кількість балів (сумарна)	Кількість	Максимальна кількість балів (сумарна)
Практичні заняття	6	40	6	40
Разом		**40**		**40**

Критерії оцінювання модульної контрольної роботи

Завдання для **модульної контрольної роботи** складається з 4 питань, кожне з яких оцінюється максимально у 5 балів. При оцінюванні кожного завдання контрольної роботив раховується обсяг і правильність виконаних завдань: оцінка "відмінно" ставиться за правильне виконання всіх завдань; оцінка "добре" ставиться за виконання 75 % усіх завдань; оцінка "задовільно" ставиться, якщо правильно виконано більше 50% запропонованих завдань; оцінка "незадовільно" ставиться, якщо завдань виконано менше від 50 %.. Неявка на модульну контрольну роботу – 0 балів.

Критерії оцінювання підсумкового семестрового контролю

Усі завдання, передбачені програмою, мають бути виконані у встановлені терміни. Якщо студент/ка був/ла відсутній на заняттях, він/вона мають можливість відпрацювати навчальні питання та завдання під час самостійної підготовки та обов'язково звітують про опанування навчального матеріалу викладачу. Студенти, які пропустили більше 30% з тих занять, де було передбачено оцінювання, не відзвітували за індивідуальну та самостійну роботу, до семестрового контролю не допускаються. У разі коли студент/ка не виконав/ла умови допуску до складання семестрового контролю, завчасно, але не пізніше трьох робочих днів до складання семестрового контролю, рішенням кафедри йому/їй встановлюється індивідуальний термін ліквідації заборгованості. Якщо заборгованість неліквідована у визначений кафедрою термін, то студент/ка вважається таким/ою, що не виконав/ла вимоги робочої програми навчальної дисципліни і у відомості обліку успішності йому/їй виставляється оцінка «незараховано» за національною шкалою і FX – за шкалою ЄКТС. При повній відсутності позитивних поточних оцінок, за визначені звітності, і не ліквідації заборгованості у визначений кафедрою термін, студенту курс з навчальної дисципліни не зараховується і в графі "підсумкова оцінка", йому виставляється оцінка "недопущений" за національною шкалою і F за шкалою ЄКТС. У такому випадку студенту/ці йому пропонується пройти повний курс повторно. У разі відмови його/її відраховують з університету.

Іспит отримує студент/ка, що виявив/ла знання основного програмового матеріалу в обсязі, необхідному для подальшого навчання та майбутньої роботи за професією, вміє виконувати завдання, передбачені програмою, ознайомлений/на з рекомендованою літературою. Підсумкова оцінка розраховується за накопичувальною системою. При цьому максимальна кількість балів встановлюється наступним чином: за змістовий модуль №1 – 100 балів; за змістовий модуль №2 – 100 балів.

При виставленні оцінки враховуються результати навчальної роботи здобувача протягом семестру.

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	ОцінкаECTS	Оцінка за національною шкалою	
		Екзамен та диференційований залік	Залік
90 – 100	**A**	відмінно	Зараховано
82-89	**B**	добре	
74-81	**C**		
64-73	**D**	задовільно	
60-63	**E**		
35-59	**FX**	незадовільно з можливістю повторного складання	Не зараховано
0-34	**F**	незадовільно з обов’язковим повторним вивченням дисципліни	

За бажанням студента результуюча підсумкова екзаменаційна оцінка може бути визначена як інтегрована оцінка засвоєння всіх тем дисципліни і кількісно дорівнює середньому арифметичному балів, отриманих за кожний модуль.

Результати підсумкового контролю знань заносяться до екзаменаційної відомості.

Дотримання академічної доброчесності

Під час навчання учасники освітнього процесу зобов'язані дотримуватися академічної доброчесності: етичних принципів та визначених законом правил (https://vumonline.ua/course/academic-integrity-at-the-university/), якими мають керуватися учасники освітнього процесу з метою забезпечення довіри до результатів навчання та/або наукових (творчих) досягнень.

Дотримання академічної доброчесності науково-педагогічним складом передбачає: посилання на джерела інформації у разі використання ідей, тверджень, відомостей; надання достовірної інформації про результати досліджень та власну педагогічну (науково-педагогічну, творчу) діяльність.

Дотримання академічної доброчесності здобувачами освіти передбачає: самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання; посилання на джерела інформації у разі використання ідей, тверджень, відомостей; надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності.

За порушення академічної доброчесності здобувачі освіти можуть бути притягнені до такої академічної відповідальності як: повторне проходження оцінювання (підсумковий модульний контроль, підготовка індивідуального завдання за іншою темою тощо).

Перевірка індивідуальних робіт здобувачів на наявність академічного плагіату проводиться викладачем або спеціально призначеним для цього працівником УжНУ за допомогою програмного продукту, що використовується в УжНУ з визначення рівня унікальності роботи.

5. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

5.1. Зміст навчальної дисципліни

Модуль 1. ЗАБЕЗПЕЧЕННЯ НАДІЙНОГО ЗБЕРЕЖЕННЯ ДАНИХ ЗА РАХУНОК ВИКОРИСТАННЯ "ХМАРНИХ" ТЕХНОЛОГІЙ.

Тема 1. **Місце дисципліни в системі підготовки професіонала із організації інформаційної безпеки.**

Причини виникнення "хмарних" технологій і "хмарних" сховищ даних. Основні фактори появи "хмарних" сховищ, набори Web-додатків для роботи з документами, файлові сховища, конкуренція між поштовими сервісами, online-сховища.

Тема 2. **Основні поняття і визначення хмарних технологій.**

Хмарне сховище, Хмарні обчислення, Хмарна інфраструктура.

Тема 3. **Типи хмар.**

Приватна хмара, публічна хмара, громадська хмара, гібридна хмара, сервер, сервер (програма), клієнт, база даних, система управління базами даних (СКБД), Web-сервер, Web-додаток - клієнт-серверне ПЗ.

Тема 4. **Поняття "хмарного" сховища даних.**

Переваги і недоліки "хмарних" сховищ даних на основі "хмарних" технологій. Модель online - сховища на численних розподілених в мережі серверах. Внутрішня структура серверів клієнта.

Тема 5**. Зберігання та обробка даних «хмари».**

Порядок розташування серверів зберігання даних, їх програмне забезпечення, уразливості.

Тема 6**. Проблеми безпеки хмарних обчислень.**

Методи захисту хмар. Консолідація і віртуалізація IT-інфраструктури. Елементи консолідації - сервер, системи зберігання, додатки.

Модуль 2. ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ БЕЗДРОТОВИХ, МОБІЛЬНИХ ТА ХМАРНИХ ТЕХНОЛОГІЙ.

Тема 1. Базові типи консолідації.

Логічний тип консолідації: гомогенна консолідація, гетерогенна консолідація (Exchange Server і SQL Server). Віртуалізація ресурсів фізичного сервера.

Тема 2. Види хмарних обчислень.

Сервіс-надають (Everything as a service) технології: "Інфраструктура як сервіс" ("Infrastructure as a Service" або "IaaS"), "Платформа як сервіс" ("Platform as a Service", "PaaS"), "Програмне забезпечення як сервіс "(" Software as a Service "або" SaaS "). SaaS - модель розгортання програми.

Тема 3. Загрози для хмарних обчислень.

Труднощі при переміщенні звичайних серверів в обчислювальний хмара. Вимоги до безпеки хмарних обчислень. Розмежування контролю доступу та забезпечення прозорості змін на системному рівні. Динамічність віртуальних машин.

Тема 4. Уразливості віртуальних середовищ.

Загроза віддаленого злому або зараження зловмисним ПЗ. Захист бездіяльних віртуальних машин (визначення доступу до сховища образів віртуальних машин). Захист периметра і розмежування мережі (визначення загального рівня захищеності, розмежування сегментів з різними рівнями довіри в хмарі).

Тема 5. Атаки на хмари: програмне забезпечення.

Традиційні атаки на ПЗ (уразливості операційних систем, модульних компонентів, мережевих протоколів). Функціональні атаки на елементи хмари. Атаки на клієнта (Cross Site Scripting, «викрадення» паролів, перехоплення веб-сесій, «людина посередині»). Атаки

на гипервизор. Атаки на системи управління. Способи захисту в області безпеки хмар (Cloud Security Alliance).

Тема 6. Способи захисту від загроз безпеки в хмарних обчисленнях.

Збереження даних (шифрування), захист даних при передачі (AES, TLS, IPsec), аутентифікація (токени і сертифікати), ізоляція користувачів (технології VPN (Virtual Private Network), VLAN (Virtual Local Area Network) і VPLS (Virtual Private LAN Service).

5.2. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин					
	Форма навчання - денна:					
	Усього	у тому числі				
		лекції	практичні (семінарські)	Практичні (лабораторні)	індивідуальна робота	Самостійна робота
Модуль 1						
Тема 1. **Місце дисципліни в системі підготовки професіонала із організації інформаційної безпеки.**	9	2		1		6
Тема 2. **Основні поняття і визначення хмарних технологій.**	9	2		1		6
Тема 3. **Типи хмар.**	10	2		2		6
Тема 4. **Поняття "хмарного" сховища даних.**	10	2		2		6
Тема 5. **Зберігання та обробка даних «хмари».**	10	2		2		6
Тема 6. **Проблеми безпеки хмарних обчислень.**	10	2		2		6
Модульна контрольна робота	2			2		
Разом за І модуль	60	12		12		36
Модуль 2						
Тема 1. **Базові типи консолідації.**	10	2		2		6

Тема 2. **Види хмарних обчислень.**	10	2		2		6
Тема 3. **Загрози для хмарних обчислень.**	8	2				6
Тема 4. **Уразливості віртуальних середовищ.**	10	2		2		6
Тема 5. **Атаки на хмари: програмне забезпечення.**	10	2		2		6
Тема 6. **Способи захисту від загроз безпеки в хмарних обчисленнях.**	10	2		2		6
Модульна контрольна робота	2			2		
Разом за ІІ модуль	60	12		12		36
Разом за 2 семестр	120	24		24		72

5.3. Теми практичних (семінарських) занять

№ з/п	Назва теми	Кількість годин
1	**Основи моніторингу та спеціалізованих структур керування безпекою**	2
2	**Дослідження бездротових технологій та їх протоколів**	2
3	**Вивчення основних мережевих протоколів та принципів їх роботи.**	2
4	**Аналіз та дослідження загроз та вразливостей мобільних додатків та мобільних пристроїв**	2
5	**Основи побудови бездротової мережі на основі різних пристроїв та технологій.**	2
6	**Модульна контрольна робота**	2
7	**Аналіз та дослідження загроз та вразливостей WiFi-мереж.**	2
8	**Аналіз та дослідження побудови хмарної інфраструктури.**	2

9	**Аналіз та дослідження документування подій у мережі, автоматизація записів.**	2
10	**Аналіз та дослідження моделей обслуговування у хмарних технологіях.**	2
11	**Аналіз та дослідження систем реагування на інциденти інформаційної безпеки.**	2
12	**Модульна контрольна робота**	2
	Разом	24

5.4. Самостійна робота

Самостійна робота магістра є одним із засобів оволодіння навчальним матеріалом у час, вільний від обов'язкових навчальних занять, і є невід'ємною складовою процесу вивчення цієї дисципліни. Основними напрямками самостійної роботи магістрів з навчальної дисципліни «Безпека хмарних технологій та розподілених обчислень» є опрацювання рекомендованої літератури, а також вивчення окремих питань, винесених на самостійне опрацювання.

№	Назва роботи	Кількість годин
1	Проробка лекційного матеріалу.	24
2	Підготовка до практичних занять	24
3	Проробка питань програми, які не викладались на лекціях	24
	Разом	**72**

6. ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ВИКОРИСТАННЯ ЯКИХ ПЕРЕДБАЧАЄ НАВЧАЛЬНА ДИСЦИПЛІНА

При вивчення навчальної дисципліни використовуються наступні методи навчання:

– пояснювально-ілюстративний метод;

– метод проблемного викладу;

– репродуктивний метод;

– дослідницький метод.

Реалізація цих методів здійснюється при проведенні лекцій, демонстрацій, самостійному вирішенні задач, роботі з навчальною літературою, аналізі та вирішенні задач з аудиту інформаційної безпеки.

У процесі вивчення дисципліни використовується система інформаційних ресурсів: дидактичні, програмні, інтернет-мережа, бібліографічні, бібліотечні. Серед них нормативно-правова база (закони, постанови, положення, накази): сайти Міністерства освіти і науки України, інтернет-ресурси, періодичні видання, наукові праці професорсько-викладацького складу, тези та матеріали наукових конференцій.

Наочні засоби: мультимедійні презентації у програмі Microsoft Office Power Point; відеоматеріали з каналу Youtube; зразки друкованих медіа джерел, схематизованих навчально-методичних матеріалів і довідкових статей; роздавальні матеріали – табличні й схематичні основи, інфографіка тощо.

Технічні засоби: лекційний курс передбачає використання технічних засобів навчання, комп'ютерних проекторів.

Для дистанційного навчання використовується Moodle (e-learn.uzhnu.edu.ua) та Google Meet.

7. РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основна література

1. K. Valli Madhavi ,et al, Cloud Computing : Security Measures Threats and Counter International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278- 5841, Vol 1, Issue 4, September 2012.
2. The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology [Електронний ресурс] / NIST Computer Security Division, Information Technology Laboratory. Електрон.дані. – Gaithersburg: National Institute of Standards and Technology. – 2011. – Режим доступу: World Wide Web. – URL: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
3. B. Grobauer, T. Walloschek and E. Stöcker, IEEE Security and Privacy, vol. 99, "Understanding Cloud Computing Vulnerabilities,", 2010.
4. Boniface M. Platform-as-a-Service Architecture for Real-Time Quality of Service Management in Clouds / M. Boniface // 5th International Conference on Internet and Web Applications and Services (ICIW (Barcelona, Spain: IEEE, 2010), P. 155–160.
5. Kevin Hamlen. (2010). Security Issues for cloud computing. International Journal of Information Security and Privacy. 4 (2), p12-15.
6. Бабак В.П., Корченко О.Г. Інформаційна безпека та сучасні мережеві технології: Англо-українсько-російський словник термінів . – К.: НАУ, 2003. – 670с.
7. Юдін О.І. Захист інформації в мережах передачі даних // О.І. Юдін, О.Г. Корченко, Г.Ф. Конахович – К.: Вид-во ТОВ «НВП» Інтерсервіс», 2009. – 716 с.

Допоміжна література

1. Зінченко О.В., Іщеряков С.М., Прокопов С.В., Сєрих С.О., Василенко В.В. Хмарні технології. – Навчальний посібник. – К: ФОП Гуляєва В.М., 2020. – 74 с.
2. Соколов В. Ю. Безпека безпроводових і мобільних мереж : Навчальний посібник / В. Ю. Соколов, В. Л. Бурячок, М. М. Таджділні / ред. перекл. О. П. Райтер. — 2 вид., доп. — К. : КУБГ, 2019. — 130 с.
3. Raghuram Yeluri, Enrique Castro-Leon. Building the Infrastructure for Cloud Security: A Solutions View. Apress, 2014 p. - 244 p.
4. Huseni Saboowala, Muhammad Abid, Sudhir Modali. Designing Networks and Services for the Cloud: Delivering business-grade cloud applications and services. Cisco Press, 2013. - 336 p.

Інформаційні ресурси в мережі Інтернет

1. НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИЕТ [Електронний ресурс] – Режим доступу: http://bit.nau.edu.ua/ru/publications/one/audit_ta_upravlinnya_incidentami_informacijno_bezpeki
2. ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ [Електронний ресурс] – Режим доступу: http://213.160.139.43/uploads/l_2048_32915773.pdf
3. АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ [Електронний ресурс] – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=81998&cat_id=3883

Онлайн середовища:

– Prometheus (http://courses.prometheus.org.ua/);

– студія онлайн освіти (https://courses.ed-era.com/);

Додаткові ресурси

1. http://it.ridne.net – Журнал "Інформаційні технології. Аналітичні матеріали"

2. https://nus.org.ua - Нова українська школа
3. https://www.ranok.com.ua - Видавництво «Ранок»
4. https://vseosvita.ua – Всеосвіта

Використання програмного забезпечення

1. http://e-learning.lnu.edu.ua/mod/url/view.php?id=22521 – TuxMathScrabble
2. https://www.mousealphabet.com/ua/ – Mouse alphabet
3. http://teach-inf.at.ua – Програмне забезпечення

Ресурси для розробки відео і презентацій

1. https://educat.at.ua
2. https://prezi.com/3fxjrclfi2r6/presentation/ – Онлайн сервіс створення презентацій (prezi) Використання Веб-технологій для розробки дидактичних матеріалів, інтерактивних вправ, контрольних і тестових робіт, відео-матеріалів, книг для читання, збереження власних напрацювань.

Корисні Інтернет ресурси.

1. https://www.armoredpenguin.com/crossword/ – Середовище для створення кросвордів
2. https://learningapps.org – Створення вправ
3. https://worditout.com – Створення хмар
4. https://jamboard.google.com – Jamboard
5. https://uk.wikipedia.org/wiki – Wiki сервіс
6. https://wordart.com – WordArt
7. http://disted.edu.vn.ua/media/bp/html/etusivu.htm – Онляндія
8. https://www.blogger.com – Блогер (для створення блогів)
9. https://www.google.com – Форми (для створення опитування)
10. https://go.playposit.com – Play posit