МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Проректор з навчально-методичної роботи

Каріна НЕМАШКАЛО

РОЗШИРЕНА МЕРЕЖЕВА ТА ХМАРНА БЕЗПЕКА

робоча програма навчальної дисципліни

Галузь знань	***12 Інформаційні технології***
Спеціальність	***125 Кібербезпека***
Освітній рівень	***другий (магістерський)***
Освітня програма	***Кібербезпека***

Статус дисципліни	***обов'язкова***
Мова викладання, навчання та оцінювання	***українська***

Завідувач кафедри
кібербезпеки
та інформаційних технологій *Ольга СТАРКОВА*

Харків
2022

ЗАТВЕРДЖЕНО
на засіданні кафедри *кібербезпеки та інформаційних технологій*
Протокол № 1 від 27.08.2022 р.

Розробник:
Алексієв В. О., д.т.н., проф. кафедри кібербезпеки та інформаційних технологій.

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри

Анотація навчальної дисципліни

Мережева та хмарна безпека є основною складовою побудови IT-інфраструктури будь-якої сучасної організації чи виробництва. Зараз великі корпоративні мережі поєднують, як наявні ресурси IT-підрозділу, так й ресурси, що орендуються як хмарні сервіси (Cloud Computing). Тому актуальною стає розширена мережева та хмарна безпека, що поєднує локальні засоби безпеки й відповідні ресурси та системні рішення захисту у хмарі.

У дисципліні розглядаються питання забезпечення кібербезпеки рівня окремого підприємства чи організації та засоби, які є складовими сервісу хмарних обчислень. Для отримання студентами практичного досвіду передбачено застосування навчальних елементів, що надані за програмою USAID «Кібербезпека критичної інфраструктури України» з напрямку вивчення основ загроз та безпеки у кіберфізичних системах (CPS, cyber-physical systems), Dr. Kemal Akkaya та Yacoub Hanna з Department of Electrical and Computer Engineering, FIU – Florida International University (Кафедра електротехнічної та комп'ютерної техніки Міжнародного університету Флориди), 14.06.2021 – 23.07.2021 р. та Хмарна безпека (Cloud Cyber Security), Dr. Silvia Elaluf-Calderwood з Business School у FIU, 11.07.2022 – 31.08.2022.

Метою викладання дисципліни є формування теоретичних знань та практичних умінь побудови контуру безпеки IT-ресурсів підприємства, компанії чи організації на рівні використання засобів та технологій розширеної мережевої та хмарної безпеки. Сучасний розвиток інформаційних технологій дозволяє підприємствам та компаніям швидко знаходити новітні ринки збуту, отримувати необхідні обчислювальні ресурси для своєї інфраструктури та залучати найсучасніші алгоритми обробки даних, поруч із розвиненим застосуванням ресурсів розподілених сховищ даних. Це має великий вплив на ціну ризику від втрати даних, можливих витрат для бізнесу спровокованих кіберзагрозами та ін. У дисципліні розглядаються особливості забезпечення безпеки починаючи з рівня мережі до залучення ресурсів хмарних технологій.

Результатами вивчення даної дисципліни є придбання навичок з проектування та створення обчислювальної мережі для підприємств та організацій незалежно від їх розміру, з врахуванням адекватних засобів безпеки та побудови ефективної IT-інфраструктури. Також студенти мають розуміти та отримати комплекс практичних навичок щодо пошуку та побудови контуру захисту обчислювальної мережі.

Характеристика навчальної дисципліни

Курс	**1 М**
Семестр	**1**
Кількість кредитів ECTS	**5**
Форма підсумкового контролю	**екзамен**

Структурно-логічна схема вивчення дисципліни

Пререквізити	Постреквізити
Сучасні методи децентралізованого розподілу даних	Основи наукових досліджень та науково-педагогічна діяльність в галузі кібербезпеки

Теорія ризиків в кібербезпеці	Тестування на проникнення та етичний хакінг
	Стандартизація та сертифікація кібернетичної діяльності

Компетентності та результати навчання за дисципліною

Компетентності	Результати навчання
КФ1. 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. КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. КФ4. 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. КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ8. 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. КФ9. Здатність аналізувати, розробляти	РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

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.	
КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури. КФ4. 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. КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ8. 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. КФ9. 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.	РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.	РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо

КФ4. 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. КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ8. 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. КФ9. 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.	попередження та аналізу кіберінцидентів в цілому.
КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ8. 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. КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності	РН13. 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.

функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.	
КФ4. 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.	РН24. Аналізувати, розробляти і супроводжувати інфраструктуру та стек застосунків у безперервному потоці змін Agile DevSecOps.
КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. КФ4. 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. КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ8. 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.	РН26. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби стеганографічного та стеганофонічного 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.

Програма навчальної дисципліни

Змістовий модуль 1. Основи безпеки рівня веб-серверу та хмарного середовища.

Тема 1. *Введення. Розвиток сучасних обчислювальних засобів від комп'ютера до IoT та засобів кіберфізичних систем *.*
Тема 2. *Засоби безпеки рівня корпоративної мережі.*
Тема 3. *Основи хмарних обчислень та архітектурні характеристики **.*
Тема 4. *Дизайн та архітектура безпеки для хмарних обчислень **.*
Тема 5. *Особливості забезпечення безпеки кіберфізичних систем *.*

Змістовий модуль 2. Практика забезпечення безпеки хмарних ресурсів.

Тема 6. *Надійна ізоляція фізичної та логічної інфраструктури **.*
Тема 7. *Захист даних для хмарної інфраструктури та сервісів **.*
Тема 8. *Застосування контролю доступу для служб на основі хмарної інфраструктури **.*
Тема 9. *Моніторинг Аудит і менеджмент **.*
Тема 10. *Перспективи синергічного поєднання засобів безпеки рівня корпоративної мережі та хмарного сервісу.*

* – за матеріалами тренінгу за програмою USAID: Cyber-Physical Systems Security;
** – за матеріалами тренінгу за програмою USAID: Cloud Cyber Security.

Перелік лабораторних та практичних занять, а також питань та завдань до самостійної роботи наведено у таблиці "Рейтинг-план навчальної дисципліни".

Методи навчання та викладання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються проблемні лекції (тема 1, 9), презентації (тема 3, 4), бесіди (тема 7), групові проєкти (тема 9), майстер-класи (тема 5).

Порядок оцінювання результатів навчання

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні, лабораторні та практичні заняття, а також виконання самостійної роботи. Оцінювання сформованих компетентностей у студентів здійснюється за накопичувальною 100-бальною системою. Контрольні заходи включають:

1) поточний контроль, що здійснюється протягом семестру під час проведення лекційних, лабораторних та практичних занять, контрольних робіт та експрес-опитувань і оцінюється сумою набраних балів (максимальна сума – 60 балів; мінімальна сума, що дозволяє студенту складати іспит, – 35 балів);

2) підсумковий/семестровий контроль, що проводиться у формі семестрового екзамену, відповідно до графіку навчального процесу.

Порядок здійснення поточного оцінювання знань студентів.

Оцінювання знань студента під час лекційних, лабораторних та практичних занять проводиться за такими критеріями:

– знати особливості сучасних корпоративних мереж, що будуються на платформі Wondows Server та Linux;

– вміти налагоджувати та застосовувати на практиці засоби безпеки рівня корпоративної мережі;

–знати властивості кіберфізичних систем та засоби забезпечення їх безпеки;

– орієнтуватися у технологіях побудови та супроводження приватної хмари на основі технологій OpenStack, OpenShift та Proxmox VE;

– знати особливості публічних хмарних сервісів Amazon AWS, Microsoft Azure та Google Cloud Platform;

– розуміти особливості побудови гібридної хмари;

– знати 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 доступу, керуванням ідентифікацією та авторизацією, високою доступністю, моніторингом і узгодженістю у активному середовищі хмари;

– вміти надати прогноз щодо перспективи синергічного поєднання засобів безпеки рівня корпоративної мережі та хмарного сервісу.

Підсумковий контроль знань та компетентностей студентів з навчальної дисципліни здійснюється на підставі проведення семестрового екзамену, завданням якого є перевірка розуміння студентом програмного матеріалу в цілому, логіки та взаємозв'язків між окремими розділами, здатності творчого використання накопичених знань, вміння формулювати своє ставлення до певної проблеми навчальної дисципліни тощо.

Лекційні заняття: максимальна кількість балів становить 5 (експрес-опитування).

Лабораторні заняття та практичні: максимальна кількість балів становить 55 (виконання лабораторних робіт – 20, виконання практичних робіт – 25, контрольні роботи – 10), а мінімальна – 25.

Самостійна робота: складається з часу, який здобувач витрачає на підготовку до виконання лабораторних робіт та на підготовку до екзамену з дисципліни, в технологічній карті бали на цій вид робіт не виділені.

Підсумковий контроль: проводиться з урахуванням іспиту.

Екзаменаційний білет охоплює програму дисципліни і передбачає визначення рівня знань та ступеня опанування студентами компетентностей.

Кожен екзаменаційний білет складається із 3 практичних ситуацій (одне стереотипне, одне діагностичне та одне евристичне завдання), які передбачають вирішення типових професійних завдань фахівця на робочому місці та дозволяють діагностувати рівень теоретичної підготовки студента і рівень його компетентності з навчальної дисципліни. Оцінювання кожного завдання екзаменаційного білету наступне: перше завдання – це 10 тестових завдань закритої форми, виконання його оцінюється 20 балами; друге завдання – присвячене розробленню структурної схеми побудови контуру безпеки корпоративної мережі компанії, виконання його оцінюється 10 балами; третє завдання – рішення евристичного завдання щодо планування розгортання контуру безпеки рівня хмарного сервісу, виконання його оцінюється 10 балами. Результат семестрового екзамену оцінюється в балах (максимальна кількість – 40 балів, мінімальна кількість, що зараховується, – 25 балів) і проставляється у відповідній графі екзаменаційної "Відомості обліку успішності".

Студента слід вважати атестованим, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60. Мінімально можлива кількість балів за поточний і модульний контроль упродовж семестру – 35 та мінімально можлива кількість балів, набраних на екзамені, – 25.

Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час екзамену, та балів, отриманих під час поточного контролю за накопичувальною системою. Сумарний результат у балах за семестр складає: "60 і більше балів – зараховано", "59 і менше балів – не зараховано" та заноситься у залікову "Відомість обліку успішності" навчальної дисципліни.

Рейтинг-план навчальної дисципліни

Тема	**Форми та види навчання**	**Форми оцінювання**	**Max бал**
Т	***Аудиторна робота***		

Тема 1	Лекція	Проблемна лекція *"Введення. Розвиток сучасних обчислювальних засобів від комп'ютера до IoT та засобів кіберфізичних систем. "*		
Тема 2				
	Лекція	Лекція *"Засоби безпеки рівня корпоративної мережі."*.		
	Лабораторне заняття	Практична робота №1 *"Основи безпеки у корпоративних мережах. Безпека даних." за матеріалами тренінгу за програмою USAID: Cloud Cyber Security*.		
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 3	***Аудиторна робота***			
	Лекція	Лекція *"Основи хмарних обчислень та архітектурні характеристики"*.		
	Лабораторне заняття	Практична робота №1. Продовження.	Захист практичної роботи №1	10
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 4	***Аудиторна робота***			
	Лекція	Лекція *" Дизайн та архітектура безпеки для хмарних обчислень."*		
	Лабораторне заняття	Лабораторна робота №1. "Огляд особливостей побудови мережи корпоративного рівня та мереж підприємства із залученням		

		компонентів кіберфізичних систем" (Executing Modbus Protocol – за матеріалами тренінгу за програмою USAID).		

	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 5	***Аудиторна робота***			
	Лекція	Лекція *" Особливості забезпечення безпеки кіберфізичних систем."*	Контрольна робота	5
	Лабораторне заняття	Лабораторна робота №1. Продовження.	Захист практичної роботи №1	10
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		

Тема 6	***Аудиторна робота***			
	Лекція	Лекція *" Надійна ізоляція фізичної та логічної інфраструктури."*		
	Лабораторне заняття	Лабораторна робота №2 *"Захист протоколу обміну даними у кіберфізичної системі." (Modbus-TLS Demo – за матеріалами тренінгу за програмою USAID).*		
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		

Тема 7	***Аудиторна робота***			
	Лекція	Лекція *" Захист даних для хмарної інфраструктури та сервісів."*		
	Лабораторне заняття	Лабораторна робота №2. Продовження.	Захист лабораторної роботи №2	10
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 8	***Аудиторна робота***			
	Лекція	Лекція *" Застосування контролю доступу для служб на основі хмарної інфраструктури."*	Експрес-опитування	5
	Лабораторне заняття	Практична робота №2. "Застосування засобів безпеки у хмарі." за матеріалами тренінгу за програмою USAID: Cloud Cyber Security.		
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		

Тема 9	***Аудиторна робота***			
	Лекція	Лекція *" Моніторинг Аудит і менеджмент."*	Контрольна робота	5
	Лабораторне заняття	Практична робота №2. Продовження.		
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт.		

		Виконання лабораторних завдань		
Тема 10	***Аудиторна робота***			
	Лекція	Лекція *"Перспективи синергічного поєднання засобів безпеки рівня корпоративної мережі та хмарного сервісу."*		
	Лабораторне заняття	Практична робота №2. Продовження.	Захист практичної роботи №2	15
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до екзамену		
Екзамен				40

Рекомендована література

Основна

1. 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.

2. Юрчишин, В. Я. Хмарні та Грід-технології: конспект лекцій [Електронний ресурс] : навчальний посібник для студентів спеціальності 121 «Інженерія програмного забезпечення» (освітня програма «Програмне забезпечення комп'ютерних та інформаційно-пошукових систем») / В. Я. Юрчишин ; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 5,93 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2019. – 263 с. – Режим доступу: https://ela.kpi.ua/handle/123456789/29960

3. OWASP Web Security Testing Guide. [Electronic resource]. –Access mode : https://owasp.org/www-project-web-security-testing-guide/

Додаткова

4. Гаркуша І.М. Конспект лекцій з дисципліни "Операційні системи" для студентів галузі знань 12 "Інформаційні технології" спеціальності 126 "Інформаційні системи та технології". – Д.: НТУ «ДП», 2020. – 73 с. – Режим доступу: https://it.nmu.org.ua/ua/scientific_method_materials/textbooks.php

5. Управління інформаційною безпекою. Конспект лекцій [Електронний ресурс] : навчальний посібник для студентів спеціальності 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського ; уклад.: С. О. Носок, О. М. Фаль, В. М. Ткач. – Електронні текстові дані (1 файл: 1,11 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 258 с. – Режим доступу: https://ela.kpi.ua/handle/123456789/43377

6. Олещенко, Л. М. Технології оброблення великих даних. Конспект лекцій [Електронний ресурс] : навчальний посібник для студентів спеціальності 121 «Інженерія програмного забезпечення» (освітня програма «Інженерія програмного забезпечення мультимедійних та інформаційно-пошукових систем») / Л. М. Олещенко ; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 5,55 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 227 с. – Режим доступу: https://ela.kpi.ua/handle/123456789/42206

7. Proxmox VE Admin Guide for 6.x, 2020. – 462 p. [Electronic resource]. –Access mode: https://www.proxmox.com/en/downloads/item/proxmox-ve-admin-guide-for-6-x

8. AWS Security Incident Response Guide, 2020. - 65 p. [Electronic resource]. –Access mode: https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/welcome.html? did=wp_card&trk=wp_card

Інформаційні ресурси

9. Azure network security overview, 2022 [Electronic resource]. –Access mode: https://docs.microsoft.com/en-us/azure/security/fundamentals/network-overview

10. Implement network segmentation patterns on Azure, 2021 [Electronic resource]. –Access mode: https://docs.microsoft.com/en-us/azure/architecture/framework/security/design-network-segmentation

11. Secure and govern workloads with network-level segmentation [Electronic resource]. –Access mode: https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/network-level-segmentation

12. Windows N-tier application on Azure [Electronic resource]. –Access mode: https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/n-tier/n-tier-sql-server

13. How to create and deploy an Azure Cloud Service (classic), 2021 [Electronic resource]. –Access mode: https://docs.microsoft.com/en-us/azure/cloud-services/cloud-services-how-to-create-deploy-portal

14. Installation and Setup. Google Cloud project. [Electronic resource]. –Access mode: https://cloud.google.com/deployment-manager/docs/step-by-step-guide/installation-and-setup

15. Configuring Oracle Cloud as the Service Provider. [Electronic resource]. –Access mode: https://docs.oracle.com/en/cloud/get-started/subscriptions-cloud/csimg/configuring-oracle-cloud-service-provider.html

16. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною "Розширена мережева та хмарна безпека" https://pns.hneu.edu.ua/.