Київський університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

«ЗАТВЕРДЖУЮ»

Проректор з наукової роботи
_____ Наталія ВІННІКОВА
«_01_» _вересня_ 2022 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ПРИКЛАДНІ АСПЕКТИ МОНІТОРИНГУ ТА АУДИТУ ЗАХИЩЕНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

для аспірантів

спеціальності 125 Кібербезпека

освітнього рівня третього (освітньо-наукового)

освітньо-наукової програми «Інформаційна безпека держави»

Київ – 2022

Розробник:

Соколов Володимир Юрійович, кандидат технічних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики

Викладач:

Соколов Володимир Юрійович, кандидат технічних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики

Робочу програму розглянуто і затверджено на засіданні кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики
Протокол від 01.09.2022 №12

Завідувач кафедри _____ Павло СКЛАДАННИЙ
(підпис)

Робочу програму погоджено з гарантом освітньо-наукової програми «Інформаційна безпека держави»
01.09.2022

Гарант освітньо-наукової програми_____ Наталія КОРШУН
(підпис)

Робочу програму перевірено
01.09.2022

Завідувач аспірантури, докторантури _____ Ілона ТРИГУБ
(підпис)

Пролонговано:

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

1. Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання	
	денна	заочна
Вид дисципліни	вибіркова	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	4/120	
Рік навчання	3	3
Семестр	5,6	5,6
Кількість змістових модулів з розподілом:	4	
Обсяг кредитів	4	4
Обсяг годин, в тому числі:	120	120
Аудиторні	32	16
Модульний контроль	8	–
Самостійна робота	80	104
Семестровий контроль	Залік	

2. Мета та завдання навчальної дисципліни

Мета: формування в аспірантів знань, умінь і навичок з застосування теоретичних основ та організації захисту розподілених інформаційних ресурсів для забезпечення їх безпеки.

Завдання: отримання теоретичних знань та практичних умінь з дослідження теорій і технологій забезпечення безпеки розподілених інформаційних, ресурсів, систем та мереж та набуття наступних компетентностей:

– здатність застосовувати сучасні ІТ технології при створенні захищених розподілених інформаційних систем і захисту інформації в них;

– здатність робити оцінки та знаходити відповідні рішення щодо застосування розподілених інформаційних систем і захисту інформації в них;

– здатність до удосконалення, модернізації та уніфікації розподілених інформаційних систем, засобів і технологій забезпечення безпеки, обробки та перетворення інформації.

У результаті вивчення навчальної дисципліни відповідно до освітньо-наукової програми спеціальності формуються фахові компетентності:

Програмні компетентності	**Код**	**Значення компетентності**
Фахові компетентності (ФК)	**ФК-2**	Здатність застосовувати математичні навички, навички системного аналізу та синтезу для вирішення нагальних проблем в системах інформаційної та/або кібербезпеки і захисту

		інформації
	ФК-7	Здатність до планування і реалізації заходів із захисту інформації на об’єктах критичної інфраструктури, проведення моніторингу, аудиту та відновлення процесів штатного функціонування ІТ систем та мереж після збоїв та відмов разних класів і походження

3. Результати навчання за дисципліною

У результаті вивчення навчальної дисципліни аспірант повинен

знати:

– основні алгоритми, моделі, методи та складні програмні комплекси оцінки характеристик і стану розподілених систем;

– принципи побудови та функціонування розподілених системи управління інформаційною та/або кібербезпекою організації;

– процеси захисту розподілених систем та протоколи коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту;

– сучасні методи проведення наукових і науково-технічних досліджень розподілених систем.

вміти:

– проводити або керувати проведенням наукових і науково-технічних досліджень розподілених систем;

– обґрунтовувати раціональні шляхи щодо захисту інформації, що циркулює в розподілених системах та мережах;

– розробляти та аналізувати проекти розподілених систем, базуючись на стандартизованих технологіях та протоколах передачі даних;

– проектувати та реалізувати розподілених системи відповідно до вимог чинних нормативно-правових документів системи захисту інформації;

– використовувати сучасні техніки для проведення досліджень за напрямом захисту інформації, організації й забезпечення безпеки розподілених систем, а також наукових досліджень вищих рівнів.

та досягти наступних програмних результатів навчання:

– вирішувати задачі, впровадження, супроводу та управління розподілених системами захисту;

– забезпечувати процеси захисту розподілених систем шляхом встановлення та коректної експлуатації програмних га програмно-апаратних комплексів засобів захисту;

– здійснювати захист ресурсів і процесів в розподілених системах на основі моделей безпеки та встановлених режимів їх безпечного функціонування;

– забезпечувати процеси захисту розподілених систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту, виконувати розробку експлуатаційної документації на КЗЗ.

Програмні результати навчання:

Код	Значення програмного результату
ПРН-4	забезпечувати неперервність бізнес процесів на базі системи управління інформаційною та/або кібербезиекою, згідно вітчизняних та міжнародних вимог і стандартів; здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій, вміти застосовувати їх як в побуті, так і в професійній діяльності; проводити або керувати проведенням наукових і науково- технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та/або кібербезпеки ОІД; обґрунтовувати раціональні шляхи щодо захисту інформації на ОІД та інформації, що циркулює в ІТ системах та мережах; використовувати сучасні техніки для проведення досліджень за напрямом захисту інформації, організації й забезпечення безпеки мережевої інфраструктури об’єктів інформаційної діяльності, а також наукових досліджень вищих рівнів.
ПРН-7	- вирішувати задачі центрального і децентралізованого адміністрування доступом до ІР і процесів в ІКС та реалізовувати заходи з протидії отриманню несанкціонованого доступу до них; - володіти науково-організаційними основами проведення аудиту безпеки ІКС, а також науковими методам та практичними навичками щодо створення систем моніторингу безпеки в ІТ системах та мережах

4. Структура навчальної дисципліни

Тематичний план для денної форми навчання

Назви змістових модулів і тем	Усього	Розподіл годин між видами робіт			
		Аудиторна			Самостійна
		Лекції	Практичні	Лабораторні	
Змістовий модуль І. Класи захищених інформаційно-комунікаційних систем і вразливостей					
Тема 1. Класи захищених інформаційно-комунікаційних систем і вразливостей	28	4	3	1	20
Модульний контроль	2				
Разом	**30**	**4**	**3**	**1**	**20**
Змістовий модуль ІІ. Децентралізовані моделі P2P і атакуючі P2P системи					
Тема 2. Децентралізовані моделі P2P і атакуючі P2P системи	28	3	4	1	20
Модульний контроль	2				
Разом	**30**	**3**	**4**	**1**	**20**
Змістовий модуль ІІІ. Скоординована кластеризація ресурсів					
Тема 3. Скоординована кластеризація ресурсів	28	4	3	1	20
Модульний контроль	2				
Разом	**30**	**4**	**3**	**1**	**20**
Змістовий модуль ІV. Координаційні класи та напади					
Тема 4. Координаційні класи та напади	28	3	4	1	20
Модульний контроль 4	2				
Разом	**30**	**3**	**4**	**1**	**20**
Усього	**120**	**14**	**14**	**4**	**80**

Тематичний план для заочної форми навчання

Назви змістових модулів і тем	Усього	Розподіл годин між видами робіт			
		Аудиторна			Самостійна
		Лекції	Практичні	Лабораторні	
Змістовий модуль І. Класи захищених інформаційно-комунікаційних систем і вразливостей					
Тема 1. Класи захищених інформаційно-комунікаційних систем і вразливостей	30	2	2	–	26
Разом	**30**	**2**	**2**	–	**26**
Змістовий модуль ІІ. Децентралізовані моделі P2P і атакуючі P2P системи					
Тема 2. Децентралізовані моделі P2P і атакуючі P2P системи	30	2	2	–	26
Разом	**30**	**2**	**2**	–	**26**
Змістовий модуль ІІІ. Скоординована кластеризація ресурсів					
Тема 3. Скоординована кластеризація ресурсів	30	2	2	–	26
Разом за змістовим модулем	**30**	**2**	**2**	–	**26**
Змістовий модуль IV. Координаційні класи та напади					
Тема 4. Координаційні класи та напади	30	2	–	2	26
Разом	**30**	**2**	–	**2**	**26**
Усього	**120**	**8**	**6**	**2**	**104**

5. Програма навчальної дисципліни

ЗМІСТОВИЙ МОДУЛЬ І. Класи захищених інформаційно-комунікаційних систем і вразливостей

Тема 1. Класи захищених інформаційно-комунікаційних систем і вразливостей

Класи розподілених систем. Класи вразливостей і загроз. Контроль доступу/допуску та керування ідентифікаторами. Транспортування даних. Служби управління ресурсами та координація. Безпека даних.

Ключові слова: розподілені системи, вразлисовті, загрози, безпека даних.

Література:

1. C. Cachin, R. Guerraoui, and L. Rodrigues, Introduction to Reliable and Secure Distrbuted Programming. Springer, 2011.

2. H. Bos, The Cyber Security Body of Knowledge. University of Bristol, 2021, ch. Operating Systems & Virtualisation, version 1.0.1. [Online]. Available: https://www.cybok.org/

3. M. Steen and A. Tannenbaum, Distributed Systems. Prentice Hall, 2017.

4. D. Gollmann, The Cyber Security Body of Knowledge. University of Bristol, 2021, ch. Authentication, Authorisation & Accountability, version 1.0.2. [Online]. Available: https://www.cybok.org/

5. C. Rossow and S. Jha, The Cyber Security Body of Knowledge. University of Bristol, 2021, ch. Network Security, version 2.0. [Online]. Available: https://www.cybok.org/

6. W. Lee, The Cyber Security Body of Knowledge. University of Bristol, 2021, ch. Malware & Attack Technology, version 1.0.1. [Online]. Available: https://www.cybok.org/

ЗМІСТОВИЙ МОДУЛЬ ІІ. Децентралізовані моделі P2P і атакуючі P2P системи

Тема 2. Децентралізовані моделі P2P і атакуючі P2P системи

Неструктуровані, структуровані, гібридні і ієрархічні протоколи P2P. Типи атак. Напади та їх пом’якшення.

Ключові слова: протокол P2P, атака, напад.

Література:

1. C. Esposito and M. Ciampi, “On security in publish/subscribe services: A survey,” IEEE Communication Surveys and Tutorials, vol. 17, no. 2, 2015.

2. A. Uzunov, “A survey of security solutions for distributed publish/subscribe systems,” Computers and Security, vol. 61, pp. 94–129, 2016.

3. G. Urdaneta, G. Pierre, and M. V. Steen, “A survey of DHT security techniques,” ACM Comput. Surv., vol. 43, no. 2, pp. 8:1–8:49, 2011.

ЗМІСТОВИЙ МОДУЛЬ ІІІ. Скоординована кластеризація ресурсів

Тема 3. Скоординована кластеризація ресурсів

Стилі координації систем. Надійне та безпечне групове спілкування. Координаційні властивості. Схема керування та координації реплікації: основа пом'якшення атак.

Ключові слова: координація систем, групове спілкування, пом’якшення атак.

Література:

1. C. Cachin, R. Guerraoui, and L. Rodrigues, Introduction to Reliable and Secure

Distrbuted Programming. Springer, 2011.
2. D. Gollmann, The Cyber Security Body of Knowledge. University of Bristol, 2021, ch. Authentication, Authorisation & Accountability, version 1.0.2. [Online]. Available: https://www.cybok.org/.
3. D. Sgandurra and E. Lupu, “Evolution of attacks, threat models, and solutions for virtualized systems,” ACM Computing Surveys, vol. 48, no. 3, pp. 46:1–46:38, Feb. 2016. [Online]. Available: http://doi.acm.org/10.1145/2856126
4. M. Vukolic, “Quorum systems: Applications to storage & consensus,” Morgan Claypool, 2012.
5. P. Viotti and M. Vukolic, “Consistency in non-transactional distributed storage systems,” ACM Computing Surveys, vol. 49, no. 1, 2016.
6. A. Lakshman and P. Malik, “Cassandra: a decentralized structured storage system,” ACM SIGOPS Operating Systems Review, vol. 44, no. 2, pp. 35–40, 2010.
7. D. Ongaro and J. Ousterhout, “In search of an understandable consensus algorithm,” in USENIX Annual Technical Conference (USENIX ATC), 2014, pp. 305–319.

ЗМІСТОВИЙ МОДУЛЬ IV. Координаційні класи та напади

Тема 4. Координаційні класи та напади

Клас координації ресурсів: розгляд інфраструктури і програм.

Ключові слова: ресурс, координація системи, інформаційна інфраструктура.

Література:

1. H. Bos, The Cyber Security Body of Knowledge. University of Bristol, 2021, ch. Operating Systems & Virtualisation, version 1.0.1. [Online]. Available: https://www.cybok.org/
2. D. Gollmann, The Cyber Security Body of Knowledge. University of Bristol, 2021, ch. Authentication, Authorisation & Accountability, version 1.0.2. [Online]. Available: https://www.cybok.org/
3. D. Sgandurra and E. Lupu, “Evolution of attacks, threat models, and solutions for virtualized systems,” ACM Computing Surveys, vol. 48, no. 3, pp. 46:1–46:38, Feb. 2016. [Online]. Available: http://doi.acm.org/10.1145/2856126
4. P. Manadhata and J. Wing, “An attack surface metric,” IEEE Trans Software Engineering, vol. 37, no. 3, pp. 371–386, May 2011.
5. G. Hogben and M. Dekker, “Survey and analysis of security parameters in cloud SLAs across the european public sector,” European Network and Information Security Agency, Tech. Rep., 2014.
6. Joint Task Force Transformation Initiative, “Security and privacy controls for federal information systems and organizations,” National Institute of Standards and Technology, Tech. Rep. Special Publication 800-53, Revision 4, 2014.
7. A. Bessani et al, “Secure storage in a cloud-of-clouds,” ACM Eurosys, pp. 31–46, 2011.
8. E. Androulaki et al, “Hyperledger fabric: A distributed operating system for permissioned bockchains,” ACM Eurosys, 2018.
9. A. Gencer, S. Basu, I. Eyal, R. van Renesse, and E. Sirer, “Decentralization in Bitcoin and Ethereum networks,” Financial Cryptography and Data Security Conference, 2018.

6. Контроль навчальних досягнень

6.1. Система оцінювання навчальних досягнень аспірантів денної форми навчання

№ з/п	Вид діяльності аспіранта	Макс. кільк. балів заодиницю	Модуль 1		Модуль 2		Модуль 3		Модуль 4	
			Кільк.один.	Макс. кільк. балів	Кільк.один.	Макс. кільк. балів	Кільк.один.	Макс. кільк. балів	Кільк.один.	Макс. кільк. балів
1	Відвідування лекцій	1	3	3	3	3	3	3	3	3
2	Відвідування практичних занять	1	3	3	3	3	3	3	3	3
3	Відвідування лабораторних занять	1	1	1	1	1	1	1	1	1
4	Робота на практичних заняттях	5	3	15	3	15	3	15	3	15
5	Робота на лабораторних заняттях	10	1	10	1	10	1	10	1	10
4	Виконання завдань для самостійної роботи	5	3	15	3	15	3	15	3	15
5	Виконання модульної контрольної роботи	25	1	25	1	25	1	25	1	25
6	Макс. кількість балів за видами поточного контролю			**72**		**72**		**72**		**72**
7	Максимальна кількість балів:	**288**								
8	Розрахунок коефіцієнта Бал max / Сума балів max	**100/288=0,35**								

Система оцінювання навчальних досягнень аспірантів заочної форми навчання

№ з/п	Вид діяльності аспіранта	Макс. кільк. балів заодиницю	Модуль 1		Модуль 2		Модуль 3		Модуль 4	
			Кільк.один.	Макс. кільк. балів	Кільк.один.	Макс. кільк. балів	Кільк.од.	Макс. кільк. балів	Кільк.один.	Макс. кільк. балів
1	Відвідування лекцій	1	1	1	1	1	1	1	1	1
2	Відвідування практичних занять	1	1	1	1	1	1	1	–	–
3	Відвідування лабораторних занять	1	–	–	–	–	–	–	1	1
4	Робота на практичних заняттях	5	1	5	1	5	1	5	–	–
5	Робота на лабораторних заняттях	10	–	–	–	–	–	–	1	10
4	Виконання завдань для самостійної роботи	5	6	30	6	30	6	30	6	30
6	Макс. кількість балів за видами поточного контролю			**37**		**37**		**37**		**42**
7	Максимальна кількість балів:	**153**								
9	Розрахунок коефіцієнта Бал max / Сума балів max	**100/153=0,65**								

Умовою зарахування кожного змістовного модулю та отримання аспірантом заліку є здобуття не менше 35% балів (Бал min / Бал max = 35:100=0,35) за результатами всіх видів означених діяльностей в кожному змістовному модулі.

6.2. Завдання для самостійної роботи та критерії її оцінювання

Самостійна робота є видом позааудиторної індивідуальної діяльності аспіранта, результати якої використовуються у процесі вивчення програмового матеріалу навчальної дисципліни та містить результати дослідницького пошуку, відображає певний рівень його навчальної компетентності. В межах кожної теми аспіранти, використовуючи рекомендовану літературу, повинні самостійно опрацювати джерела за запропонованою тематикою. Завдання для самостійної роботи подаються письмово. Кожна робота оцінюється від 1-5 балів

Завдання для самостійної роботи аспірантів денної форми навчання

№ з/п	Назва теми
Змістовий модуль 1. Класи захищених інформаційно-комунікаційних систем і вразливостей	
1	Класи розподілених систем
2	Служби управління ресурсами та координація
Змістовий модуль 2. Децентралізовані моделі P2P і атакуючі P2P системи	
3	Неструктуровані протоколи P2P
4	Ієрархічні протоколи P2P
Змістовий модуль 3. Скоординована кластеризація ресурсів	
5	Стилі координації систем
6	Схема керування та координації реплікації: основа пом'якшення атак
Змістовий модуль 4. Координаційні класи та напади	
7	Клас координації ресурсів – розгляд інфраструктури
8	Клас координації послуг – розгляд програм

Завдання для самостійної роботи аспірантів заочної форми навчання

№ з/п	Назва теми
Змістовий модуль 1. Класи захищених інформаційно-комунікаційних систем і вразливостей	
1	Класи розподілених систем
2	Класи вразливостей і загроз
3	Контроль доступу/допуску та керування ідентифікаторами
4	Транспортування даних
5	Служби управління ресурсами та координація
6	Безпека даних
Змістовий модуль 2. Децентралізовані моделі P2P і атакуючі P2P системи	
7	Неструктуровані протоколи P2P
8	Структуровані протоколи P2P
9	Гібридні протоколи P2P
10	Ієрархічні протоколи P2P
11	Типи атак
12	Напади та їх пом’якшення
Змістовий модуль 3. Скоординована кластеризація ресурсів	

13	Стилі координації систем
14	Надійне та безпечне групове спілкування
15	Координаційні властивості
16	Схема керування та координації реплікації: основа пом'якшення атак
Змістовий модуль 4. Координаційні класи та напади	
17	Клас координації ресурсів – розгляд інфраструктури
18	Клас координації послуг – розгляд програм

Критерії оцінювання самостійної роботи аспіранта

№ п/п	Критерії оцінювання роботи	Максимальна кількість балів за кожним критерієм
1	Критичний аналіз суті та змісту першоджерел. Виклад фактів, ідей, результатів досліджень в логічній послідовності. Аналіз сучасного стану дослідження проблеми, розгляд тенденцій подальшого розвитку даного питання.	2
2	Доказовість висновків, обґрунтованість власної позиції, пропозиції щодо розв’язання проблеми, визначення перспектив дослідження	2
3	Дотримання вимог щодо технічного оформлення	1
	Разом	5

6.3. Форми проведення модульного контролю та критерії оцінювання

Оцінка за кожний змістовий модуль включає бали за поточну роботу аспіранта на практичних заняттях, за виконання домашніх завдань, за модульну контрольну роботу. Модульний контроль знань аспіранта здійснюється після завершення вивчення навчального матеріалу модуля. Форма проведення – комп’ютерний тест, що складається з 20 питань закритої та відкритої форм. Модульна контрольна робота оцінюється у 25 балів. Критерії оцінювання модульного контролю наведено у таблиці.

Критерії оцінювання модульного контролю

Сума балів	Значення оцінки
22-25	аспірант виявив повне знання програмного матеріалу, успішно виконує передбачені програмою завдання, засвоїв основну літературу рекомендовану програмою, виявив систематичний характер знань з дисципліни і здатний до самостійного доповнення
13-21	аспірант виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та майбутньої роботи за професією, вміє виконувати завдання, передбачені програмою, знайомий з основною рекомендованою літературою
0-13	аспірант, що виявив часткове знання основного програмового матеріалу, не завжди вміє виконувати завдання, передбачені програмою, знайомий лише частково з основною рекомендованою літературою.

6.4 Форми проведення семестрового контролю та критерії оцінювання

Семестровий контроль знань аспірантів здійснюється після завершення вивчення навчального матеріалу дисципліни у формі заліку. Підсумкова семестрова (залікова) рейтингова оцінка аспіранта є сумою підсумкових фактичних оцінок аспіранта за змістовими модулями.

6.5. Оцінювання освітніх досягнень аспірантів за системою ECTS

Рейтингова оцінка	Оцінка за стобальною шкалою	Значення оцінки
A	90–100 балів	Відмінно – відмінний рівень знань (умінь) в межах обов'язкового матеріалу з можливими незначними недоліками
B	82–89 балів	Дуже добре – достатньо високий рівень знань (умінь) в межах обов'язкового матеріалу без суттєвих (грубих) помилок
C	75–81 балів	Добре – в цілому добрий рівень знань (умінь) з незначною кількістю помилок
D	69–74 балів	Задовільно – посередній рівень знань (умінь) із значною кількістю недоліків, достатній для подальшого навчання або професійної діяльності
E	60–68 балів	Достатньо – мінімально можливий допустимий рівень знань (умінь)
FX	35–59 балів	Незадовільно з можливістю повторного складання – незадовільний рівень знань, з можливістю повторного перескладання за умови належного самостійного доопрацювання
F	1–34 балів	Незадовільно з обов'язковим повторним вивченням – досить низький рівень знань (умінь), що вимагає повторного вивчення дисципліни

7. Рекомендовані джерела:

Основні (базові):

1. C. Cachin, R. Guerraoui, and L. Rodrigues, Introduction to Reliable and Secure Distrbuted Programming. Springer, 2011.
2. M. Steen and A. Tannenbaum, Distributed Systems. Prentice Hall, 2017.
3. C. Esposito and M. Ciampi, “On security in publish/subscribe services: A survey,” IEEE Communication Surveys and Tutorials, vol. 17, no. 2, 2015.
4. A. Uzunov, “A survey of security solutions for distributed publish/subscribe systems,” Computers and Security, vol. 61, pp. 94–129, 2016.
5. G. Urdaneta, G. Pierre, and M. V. Steen, “A survey of DHT security techniques,” ACM Comput. Surv., vol. 43, no. 2, pp. 8:1–8:49, 2011.
6. D. Sgandurra and E. Lupu, “Evolution of attacks, threat models, and solutions for virtualized systems,” ACM Computing Surveys, vol. 48, no. 3, pp. 46:1–46:38, Feb. 2016. [Online]. Available: http://doi.acm.org/10.1145/2856126
7. M. Vukolic, “Quorum systems: Applications to storage & consensus,” Morgan Claypool, 2012.
8. P. Viotti and M. Vukolic, “Consistency in non-transactional distributed storage systems,” ACM Computing Surveys, vol. 49, no. 1, 2016.
9. A. Lakshman and P. Malik, “Cassandra: a decentralized structured storage system,” ACM SIGOPS Operating Systems Review, vol. 44, no. 2, pp. 35–40, 2010.
10. D. Ongaro and J. Ousterhout, “In search of an understandable consensus algorithm,” in USENIX Annual Technical Conference (USENIX ATC), 2014, pp. 305–319.
11. P. Manadhata and J. Wing, “An attack surface metric,” IEEE Trans Software Engineering, vol. 37, no. 3, pp. 371–386, May 2011.
12. G. Hogben and M. Dekker, “Survey and analysis of security parameters in cloud SLAs across the european public sector,” European Network and Information Security Agency, Tech. Rep., 2014.
13. Joint Task Force Transformation Initiative, “Security and privacy controls for federal information systems and organizations,” National Institute of Standards and Technology, Tech. Rep. Special Publication 800-53, Revision 4, 2014.
14. A. Bessani et al, “Secure storage in a cloud-of-clouds,” ACM Eurosys, pp. 31–46, 2011.
15. E. Androulaki et al, “Hyperledger fabric: A distributed operating system for permissioned bockchains,” ACM Eurosys, 2018.
16. A. Gencer, S. Basu, I. Eyal, R. van Renesse, and E. Sirer, “Decentralization in Bitcoin and Ethereum networks,” Financial Cryptography and Data Security Conference, 2018.

Додаткові ресурси:

1. H. Bos, The Cyber Security Body of Knowledge. University of Bristol, 2021, ch. Operating Systems & Virtualisation, version 1.0.1. [Online]. Available: https://www.cybok.org/
2. D. Gollmann, The Cyber Security Body of Knowledge. University of Bristol, 2021, ch. Authentication, Authorisation & Accountability, version 1.0.2. [Online].

Available: https://www.cybok.org/
3. C. Rossow and S. Jha, The Cyber Security Body of Knowledge. University of Bristol, 2021, ch. Network Security, version 2.0. [Online]. Available: https://www.cybok.org/
4. W. Lee, The Cyber Security Body of Knowledge. University of Bristol, 2021, ch. Malware & Attack Technology, version 1.0.1. [Online]. Available: https://www.cybok.org/