



Міжнародний гуманітарний університет
Факультет кібербезпеки, програмної інженерії та комп'ютерних наук
Комп'ютерної інженерії та інноваційних технологій

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Галузь знань	12 Інформаційні технології
Спеціальність	122 Комп'ютерні науки
Назва освітньої програми	Комп'ютерні науки
Рівень вищої освіти	перший (бакалаврський)

Розробники і викладачі	Контактний тел.	E-mail
професор кафедри комп'ютерної інженерії та інноваційних технологій, доктор технічних наук, професор Радівілова Тамара Анатоліївна	+380951609153	tamara.radivilova@gmail.com

Дисципліна «Захист інформації в інформаційно-комунікаційних системах» є обов'язковим компонентом освітньої програми «Комп'ютерні науки» для здобуття освітнього рівня «бакалавр» й спрямована на формування знань і навичок із захисту інформації в інформаційно-комунікаційних системах, включаючи криптографічні методи, мережеву безпеку, організаційні заходи та сучасні технології кіберзахисту.

МЕТА ДИСЦИПЛІНИ. Метою дисципліни є забезпечення здобувачів знаннями з питань захисту інформації у інформаційно-комунікаційних системах від порушення її конфіденційності, цілісності та доступності з урахуванням сучасного стану та перспективних напрямів розвитку криптографії та стеганографії, а також набуття практичних навичок застосування криптографічних, технічних, організаційних та мережевих методів захисту інформації під час її передавання, оброблення та зберігання.

ПРЕРЕКВІЗИТИ. Передумовами вивчення дисципліни є знання і вміння, отримані здобуачем при вивченні навчальних дисциплін бакалаврської підготовки. Дисципліна базується на основних положеннях дисциплін: «Вища математика», «Дискретна математика», «Теорія інформації та кодування», «Комп'ютерні мережі».

ПОСТРЕКВІЗИТИ. Зміст дисципліни узгоджено з освітньо-професійною програмою підготовки фахівців з комп'ютерних наук та забезпечує необхідну теоретичну й практичну базу для подальшого вивчення дисциплін бакалаврської підготовки, практики та написання кваліфікаційної роботи.

2. ОЧІКУВАНІ КОМПЕТЕНТНОСТІ, ЯКІ ПЛАНУЄТЬСЯ СФОРМУВАТИ ТА ДОСЯГНЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ

Інтегральна компетентність

Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі комп'ютерних наук або у процесі навчання, що передбачає застосування теорій та методів інформаційних технологій і характеризується комплексністю та невизначеністю умов.

Загальні компетентності (ЗК)

ЗК6. Здатність вчитися й оволодівати сучасними знаннями.

ЗК7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК11. Здатність приймати обґрунтовані рішення.

ЗК14. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

Спеціальні компетентності (СК)

СК1. Здатність до математичного формулювання та досліджування неперервних та дискретних математичних моделей, обґрунтовування вибору методів і підходів для розв'язування теоретичних і прикладних задач у галузі комп'ютерних наук, аналізу та інтерпретування.

СК14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.

СК17. Здатність проєктувати та керувати інформаційно-комунікаційними системами, забезпечувати розробку та супровід програмного забезпечення.

Програмні результати навчання (ПРН)

ПР1. Застосовувати знання основних форм і законів абстрактно-логічного мислення, основ методології наукового пізнання, форм і методів вилучення, аналізу, обробки та синтезу інформації в предметній області комп'ютерних наук.

ПР13. Володіти мовами системного програмування та методами розробки програм, що взаємодіють з компонентами комп'ютерних систем, знати мережні технології, архітектури комп'ютерних мереж, мати практичні навички технології адміністрування комп'ютерних мереж та їх програмного забезпечення.

ПР16. Розуміти концепцію інформаційної безпеки, принципи безпечного проєктування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.

ПР18. Здійснювати проєктування та керування інформаційно-комунікаційними системами, забезпечувати розробку та супровід програмного забезпечення.

3. ОБСЯГ ТА ОЗНАКИ КУРСУ

Загалом		Вид заняття (денне відділення / заочне відділення)				Ознаки курсу		
ЄКТС	годин	Лекційні заняття	Лабораторні заняття	Практичні заняття	Самостійна робота	Курс, (рік навчання)	Семестр	Обов'язкова / вибіркова
5	150	26/ 12	-	40/8	84 / 130	4	7	Обов'язкова

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин									
	денна форма					Заочна форма				
	Усього	у тому числі				Усього	у тому числі			
		Лекції	Лабор	Практ	Сам. роб.		Лекції	Лабор	Практ	Сам. роб.
Тема 1. Основи інформаційної безпеки в інформаційно-комунікаційних системах. Актуальність проблеми захисту інформації, основні принципи та об'єкти захисту в інфокомунікаційних системах. Нормативно-правове забезпечення захисту інформації в інформаційно-комунікаційних системах. Моделі загроз і порушників у інформаційно-комунікаційних системах мережах.	30	4		10	16	30	4		2	24
Тема 2. Криптографічні механізми захисту інформації. Основні поняття криптографічного захисту інформації. Класичні методи шифрування. Симетричні криптографічні алгоритми. Алгоритми шифрування на базі мережі Фейстеля. Сучасні стандарти шифрування, що побудовані на SP-мережі. Системи ідентифікації та автентифікації. Електронний цифровий підпис. Основи стеганографічного захисту інформації. Сумісне використання стеганографічного та криптографічного захисту інформації.	40	6		10	24	40	2		2	36
Тема 3. Технічні засоби та протоколи захисту інформації в інформаційно-комунікаційних системах. Протоколи безпеки мережевих комунікацій. Захист мережевої інфраструктури. Інтеграція інтелектуального відеоспостереження в системи безпеки. Безпека безпроводових і мобільних мереж.	40	8		10	22	40	4		2	34

Тема 4. Управління безпекою інформаційно-комунікаційних систем. Управління ризиками в інформаційно-комунікаційних системах. Моніторинг, виявлення та реагування на інциденти. Аудит та тестування безпеки інформаційно-комунікаційних систем. Комплексні підходи до побудови систем інформаційної безпеки. Перспективи та сучасні тенденції захисту інформації в інформаційно-комунікаційних системах та мережах	40	8		10	22	40	2		2	36
Усього годин	150	26		40	84	150	12		8	130
ПІДСУМКОВИЙ КОНТРОЛЬ – ЕКЗАМЕН										

5. ТЕХНІЧНЕ Й ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ / ОБЛАДНАННЯ

Студенти отримують теми та питання курсу, основну і додаткову літературу, рекомендації, завдання та оцінки за їх виконання як традиційним шляхом, так і з використанням університетської платформи он-лайн навчання на базі Moodle. Окрім того, практичні навички у пошуку та аналізу інформації за курсом, з оформлення індивідуальних завдань, тощо, студенти отримують, користуючись університетськими комп'ютерними класами та бібліотекою.

6. САМОСТІЙНА РОБОТА

До самостійної роботи студентів щодо вивчення дисципліни «Захист інформації в інформаційно-комунікаційних системах» включаються:

1. Знайомство з науковою та навчальною літературою відповідно зазначених у програмі тем.
2. Опрацювання теоретичного матеріалу, здобутого під час семестру.
3. Виконання практичних, лабораторних та індивідуальних завдань, сформованих викладачем.
4. Консультації з викладачем протягом семестру.
5. Самостійне опрацювання окремих питань навчальної дисципліни.
6. Підготовка та виконання індивідуальних завдань.
7. Підготовка до підсумкового контролю знань.

Тематика та питання до самостійної підготовки та індивідуальних завдань

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
	Тема 1. Основи інформаційної безпеки в інформаційно-комунікаційних системах. Аналіз загроз інформації при передачі по каналах зв'язку. Методи захисту інформації в каналах зв'язку. Поняття інформаційної безпеки у інформаційно-комунікаційних систем. Ключові принципи захисту:	16	24

	конфіденційність, цілісність, доступність. Типові загрози та вразливості у мережах зв'язку. Об'єкти захисту, класифікація засобів захисту. Роль політик безпеки. Поняття загрози та порушника: визначення, класифікація, приклади. Взаємозв'язок між моделями загроз і порушників. Практичне застосування моделей загроз та порушників, використання у проектуванні політик безпеки та систем захисту інфокомунікаційних мереж. Законодавча база України у сфері інформаційної безпеки та захисту інформації. Міжнародні нормативні документи та стандарти (ISO/IEC 27000-series, рекомендації ITU, директиви ЄС).		
	Тема 2. Криптографічні механізми захисту інформації. Призначення криптографічного захисту. Архітектура інформаційно-комунікаційних систем та точки вразливості. Принципи побудови систем захисту інформації. Схема побудови складного шифру. Особливості та призначення симетричних криптосистем. Дослідження алгоритму шифрування DES. Режими роботи та недоліки. Методи підвищення криптостійкості криптосистеми. Алгоритм 3-DES. Криптосистема IDEA. Схема SP-мережі. Реалізація SP-мережі в криптосистемах AES та ДСТУ 7624:2014 «Калина». Прості методи автентифікації за паролем. Біометричні методи автентифікації. Класифікація асиметричних криптосистем за призначенням. Метод генерування та розподілення ключів Діффі-Хеллмана. Процедури генерування асиметричної пари ключів та система шифрування RSA. Процедура шифрування в криптосистемі Ель-Гамала. Біометрико-криптографічні перетворення при підтвердженні справжності користувача. Багатофакторна автентифікація. Методи побудови схем електронного підпису. Процедура створення підпису в алгоритмі RSA. Різновиди ЕП.	24	36
	Тема 3. Технічні засоби та протоколи захисту інформації в інформаційно-комунікаційних системах. Призначення протоколів безпеки (SSL/TLS, IPsec, SSH, HTTPS, Kerberos, S/MIME та PGP). Загрози та методи захисту мережевої інфраструктури. Типові загрози (перехоплення трафіку, атаки «людина посередині» (MITM), підроблені точки доступу, IMSI-catchers, шкідливі мобільні додатки). Методи захисту Wi-Fi мереж (WPA2/WPA3, сегментація мережі, контроль доступу). Поняття, структура, типи політик. політики Zero Trust, адаптивні політики безпеки, інтеграція з хмарними сервісами.	22	34
	Тема 4. Управління безпекою інформаційно-комунікаційних систем. Методологія управління ризиками. Управління ризиками інформаційної безпеки (ISO/IEC 27005). NIST Risk Management Framework. Методики OCTAVE, FAIR. Засоби захисту (IDS/IPS, SIEM, криптографічні рішення). Принципи безперервного моніторингу. Використання SIEM-систем (Security Information and Event Management). Системи IDS/IPS (Intrusion Detection/Prevention Systems). План реагування на інциденти (Incident Response Plan). Методології аудиту (ISO/IEC 27001, COBIT, NIST). рекомендації з безпеки (ISO/IEC 27002). OWASP Testing Guide для веб-додатків. Рекомендації CERT щодо тестування та аудиту. Принципи побудови системи. Принцип «захист у глибину» (defense in depth). Значення інформаційної безпеки в умовах цифрової трансформації. Тенденції розвитку технологій захисту. Використання штучного інтелекту та машинного навчання для виявлення аномалій. Автоматизація реагування на інциденти (SOAR-платформи). Інтеграція кібербезпеки у всі бізнес-процеси. Використання квантових технологій для криптографії майбутнього.	22	36
	Всього	84	130

7. ВИДИ ТА МЕТОДИ КОНТРОЛЮ

Види контролю	Складові оцінювання	
	Для екзамену	Для заліку
поточний контроль , який здійснюється у ході: проведення практичних (лабораторних) занять, виконання самостійної роботи, індивідуальних завдань, дослідна робота здобувача тощо.	50%	100%
підсумковий контроль	50%	

Методи діагностики знань (контролю)	фронтальне опитування; наукова доповідь, реферати, усне повідомлення, індивідуальне опитування; робота у групах; ділова гра, розв'язання ситуаційних завдань, кейсів, практичних завдань, екзамен
--	---

8. ОЦІНЮВАННЯ ЗДОБУВАЧІВ ВИЩОЇ ТА ФАХОВОЇ ПЕРДВИЩОЇ ОСВІТИ ЗА НАВЧАЛЬНУ ДИСЦИПЛІНУ У МІЖНАРОДНОМУ ГУМАНІТАРНОМУ УНІВЕРСИТЕТІ (поточний контроль, підсумковий контроль, загальний результат оцінювання)

ЕКЗАМЕН

<i>Поточний контроль</i>			
Види роботи	Планові терміни виконання	Форми контролю та звітності	Максимальний відсоток оцінювання
Систематичність і активність роботи на практичних (лабораторних) заняттях			
1.1. Підготовка до практичних (лабораторних) занять	Відповідно до робочої програми та розкладу занять	Перевірка обсягу та якості засвоєного матеріалу під час практичних (лабораторних) занять	30
Виконання завдань для самостійного опрацювання			
1.2. Індивідуальне тестування, завдання, підготовка реферату (есе) за заданою тематикою	Відповідно до робочої програми та розкладу занять	Розгляд відповідного матеріалу під час аудиторних занять або ІКР ¹ , перевірка конспектів навчальних текстів тощо	10
Виконання індивідуальних завдань, дослідна робота здобувача			
1.3. Інші види індивідуальних завдань, в т.ч. підготовка наукових публікацій, участь у	Відповідно до робочої програми та	Обговорення результатів проведеної роботи під час аудиторних занять, наукових конференцій та	10

¹ Індивідуально-консультативна робота викладача зі здобувачами

роботі круглих столів, конференцій тощо.	розкладу занять	круглих столів.	
Разом балів за поточний контроль			50
Підсумковий контроль екзамен			50
Загальний результат оцінювання			100

Поточний контроль знань здобувачів освіти при формі контролю **екзамен** (максимум 50 балів) оцінюється за шкалою («2», «3», «4», «5»), з обов'язковим переведенням балів за кожний вид роботи таким чином:

- за підготовку до аудиторних занять (максимум 30 балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості практичних (лабораторних) занять, для переведу балів за підготовку до аудиторних занять середньоарифметична оцінка множиться на коефіцієнт 6;
- за виконання завдань для самостійного опрацювання (тестування, завдання, підготовка реферату (есе) за заданою тематикою) (максимум 10 балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості програмного матеріалу, що виноситься на самостійне вивчення, для переведу зазначених балів середньоарифметична оцінка множиться на коефіцієнт 2;
- за інші види індивідуальних завдань, в т.ч. підготовку наукових публікацій, участь у роботі круглих столів, конференцій тощо (максимум 10- балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості інших видів індивідуальних завдань, для переведу балів за підготовку до аудиторних занять середньоарифметична оцінка множиться на коефіцієнт 2.

КРИТЕРІЇ ОЦІНЮВАННЯ ЗА ПОТОЧНИЙ КОНТРОЛЬ

- «2»- виставляється за неправильну відповідь (письмову роботу), яка не відповідає змісту теми та свідчить про нерозуміння її основних положень;
- «3» -виставляється за відповідь (письмову роботу), яка відповідає змісту теми, але є неповною і неточною у визначенні понять, свідчить про неповне розуміння основних положень навчального матеріалу, свідчить про те, що знання студента мають фрагментарний, поверховий характер;
- «4» - оцінюється правильна і обґрунтована відповідь (письмова робота), з якої видно, що студент знає й розуміє теоретичний матеріал в обсязі навчальної теми, володіє необхідними навичками, не допускає суттєвих помилок.
- «5» - оцінюється повна, правильна, ґрунтовна відповідь (письмова робота) на запитання теми, що передбачає логічність і послідовність викладу матеріалу, володіння термінологією, показує вміння повно й глибоко використовувати теоретичні знання в практичній площині.

КРИТЕРІЇ ОЦІНЮВАННЯ ПІДСУМКОВОГО КОНТРОЛЮ ЗНАНЬ ЗДОБУВАЧІВ ЗА ІСПИТ (максимум 50 балів)

Рівень знань оцінюється:

- від 40 до 50 балів - студент виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки;
- 30 до 40 балів - студент володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді;
- 20 - 30 балів - студент відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, з допомогою викладача може аналізувати навчальний матеріал, але дає недостатньо обґрунтовані, невичерпні відповіді, допускає помилки.
- 10 - 20 балів - володіє навчальним матеріалом на середньому рівні, допускає помилки, серед яких є значна кількість суттєвих;
- 0 10 балів - володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні, на всі запитання дає необґрунтовані, невичерпні відповіді, допускає помилки.

9. КРИТЕРІЇ ЗАГАЛЬНИХ РЕЗУЛЬТАТІВ ОЦІНЮВАННЯ ЗНАНЬ ЗДОБУВАЧІВ (для екзамену / заліку)

Рівень знань оцінюється:

- «відмінно» / «зараховано» А - від 90 до 100 балів. Студент виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки. Був присутній на лекціях та семінарських заняттях, під час яких давав вичерпні, обґрунтовані, теоретично і практично правильні відповіді, має конспект з виконаними завданнями до самостійної роботи, презентував реферат (есе) за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;
- «добре» / «зараховано» В - від 82 до 89 балів. Студент володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді. Був присутній на лекціях та семінарських заняттях, має конспект з виконаними завданнями до самостійної роботи, презентував реферат (есе) за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;
- «добре» / «зараховано» С - від 74 до 81 балів. Студент відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, з допомогою викладача може аналізувати навчальний матеріал, але дає недостатньо обґрунтовані, невичерпні відповіді, допускає помилки. При цьому враховується наявність конспекту з виконаними завданнями до самостійної роботи, реферату та активність у науково-дослідній роботі;
- «задовільно» / «зараховано» D - від 64 до 73 балів. Студент був присутній не на всіх лекціях та семінарських заняттях, володіє навчальним матеріалом на середньому рівні, допускає помилки, серед яких є значна кількість суттєвих. При цьому враховується наявність конспекту з виконаними завданнями до самостійної роботи, рефератів (есе);
- «задовільно» / «зараховано» E - від 60 до 63 балів. Студент був присутній не на всіх лекціях та семінарських заняттях, володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні, на всі запитання дає необґрунтовані, невичерпні відповіді, допускає помилки, має неповний конспект з завданнями до самостійної роботи.
- «незадовільно з можливістю повторного складання» / «не зараховано» FX – від 35 до 59 балів. Студент володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу.
- «незадовільно з обов'язковим повторним вивченням дисципліни» / «не зараховано» F – від 0 до 34 балів. Студент не володіє

навчальним матеріалом.

ТАБЛИЦЯ ВІДПОВІДНОСТІ ЗАГАЛЬНИХ РЕЗУЛЬТАТІВ ОЦІНЮВАННЯ ЗНАНЬ ЗА РІЗНИМИ ШКАЛАМИ

100-бальною шкалою	Шкала за ECTS	За національною шкалою	
		екзамен	залік
90-100	A	Відмінно	Зараховано
82-89	B	Добре	
74-81	C		
64-73	D	Задовільно	
60-63	E		
35-59	FX	Незадовільно	Не зараховано
1-34	F		

10. ДОТРИМАННЯ ВИМОГ АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ

Викладання та засвоєння навчальної дисципліни передбачає неухильне дотримання вимог академічної доброчесності, яка регулюється Законом України “Про освіту” (Відомості Верховної Ради (ВВР), 2014, № 37-38, ст.2004), «Методичними рекомендаціями для закладів вищої освіти з підтримки принципів академічної доброчесності» (Лист МОН № 1/9-650 від 23.10.18 року), іншими нормативними документами. Зокрема, основні засади дотримання академічної доброчесності визначено у «Положенні про академічну доброчесність у Міжнародному гуманітарному університеті», «Кодексі академічної доброчесності Міжнародного гуманітарного університету» та «Інструкції щодо процедури технічної перевірки на наявність текстових запозичень (академічного плагіату)», затверджені наказом МГУ від 03.05.2024 р., № 708а.

Відповідно до ст.42 Закону України “Про освіту” академічна доброчесність - це сукупність етичних принципів та визначених законом правил, якими мають керуватися учасники освітнього процесу під час навчання, викладання та провадження наукової (творчої) діяльності з метою забезпечення довіри до результатів навчання та/або наукових (творчих) досягнень.

Дотримання академічної доброчесності передбачає:

- самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей);
- посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;
- дотримання норм законодавства про авторське право і суміжні права;
- надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

11. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Криптографічний захист інформації: Навч. посіб./ Йона Л.Г., Онацький О.В., Белова Ю.В. - Одеса: ДУІТЗ, 2023. – 250 с.
2. Жилін А. В., Шаповал О. М., Успенський О. А. Технології захисту інформації в інформаційно-телекомунікаційних системах: навчальний посібник. Київ: КПП ім. Ігоря Сікорського, 2020.
3. Остапов С. Е., Євсєєв С. П., Король О. Г. Кібербезпека: сучасні технології захисту: навчальний посібник. Львів: Новий Світ-2000, 2020.
4. Andress J. The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. – 3rd ed. – Amsterdam : Elsevier, 2020. – 240 p.
5. Комплекс навчально-методичного забезпечення навчальної дисципліни "Захист систем електронної комерції та мультисервісних систем", освітньо-кваліфікаційний рівень бакалавр для спеціальності 125 - Кібербезпека [Електронний ресурс] : освітня програма підготовки "Управління інформаційною безпекою" / ХНУРЕ ; розроб. Т.А. Радівілова. – Харків, 2019. – 397 с.
5. Stallings W. Effective Cybersecurity: A Guide to Using Best Practices and Standards. – Boston : Addison-Wesley, 2018. – 336 p.
6. ДСТУ ISO/IEC 27001:2023. Інформаційна безпека, кібербезпека та захист приватності. Системи управління інформаційною безпекою. Вимоги. – Київ : ДП «УкрНДНЦ», 2023.
7. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. – Geneva : ISO, 2022.

Допоміжна

8. Андерсон Р. Дж. Інженерія безпеки: посібник для створення захищених систем. Пер. з англ. Київ: Логос, 2010.
9. Mulesa, O., Horvat, P., Radivilova, T., Sabadosh, V., Baranovskyi, O., & Duran, S. (2023). Design of mechanisms for ensuring the execution of tasks in project planning . Eastern-European Journal of Enterprise Technologies, 2(4 (122), 16–22.
10. Lyudmyla Kirichenko, Tamara Radivilova, Oksana Pichugina, Larysa Chala, Danyil Khandak. Trend Detection in Short Time Series Using Discrete Wavelet Transform. Proceedings of the IX International Scientific Conference "Information Technology and Implementation" (IT&I-2022). Kyiv, Ukraine, November 30 - December 02, 2022. Vol.3347, pp.159-168.
11. Lyudmyla Kirichenko, Tamara Radivilova, Juliia Stepanenko. Applying Recurrence Plots to Classify Time Series. Proceedings of the 5th International Conference on Computational Linguistics and Intelligent Systems (COLINS 2021). Volume I: Main Conference, Lviv, Ukraine, April 22-23, 2021. Vol.2870. pp. 1770-1780.
12. Radivilova, T., Kirichenko, L., Tawalbeh, M., & Ilkov, A. (2021). Виявлення аномалій в телекомунікаційному трафіку статистичними методами. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка, 3(11), 2021, 183-194.

Інформаційні ресурси

- 1 Національна бібліотека України ім. В.І. Вернадського. URL: <http://www.nbuv.gov.ua>.
- 2 Портал кіберполіції України. URL: <https://cyberpolice.gov.ua/>
- 3 ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Женева: International Organization for Standardization, 2022. Режим доступу: <https://www.iso.org/standard/27001>