МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Чорноморський національний університет імені Петра Могили

Факультет комп'ютерних наук

Кафедра комп'ютерної інженерії

ЗАТВЕРДЖУЮ
Перший проректор
_____ Юрій КОТЛЯР
"__ "_____2023 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Технології захисту інформаційних систем»

Спеціальність 123 Комп'ютерна інженерія
Галузь знань 12 Інформаційні технології
Рівень вищої освіти – третій (доктор філософії)

Розробник	Савінов В. Ю.	_____
Завідувач кафедри спеціальності	Журавська І. М.	_____
Гарант освітньої програми	Чуйко Г. П.	_____
Декан факультету	Бойко А. П.	_____
Начальник НМВ	Шкірчак С. І.	_____

Миколаїв – 2023 рік

Опис навчальної дисципліни

Найменування показника	Характеристика дисципліни	
Найменування дисципліни	Технології захисту інформаційних систем	
Галузь знань	12 Інформаційні технології	
Спеціальність	123 Комп'ютерна інженерія	
Спеціалізація (якщо є)		
Освітня наукова програма	Комп'ютерна інженерія	
Рівень вищої освіти	доктор філософії	
Статус дисципліни	вибіркова	
Курс навчання	2-й	
Навчальний рік	2023−2024	
Номер(и) семестрів	Денна форма	Заочна форма
	4-й	---
Загальна кількість кредитів ЄКТС/годин	3 кред. /90 год.	
Структура дисципліни: – лекції – семінарські заняття (практичні) – годин самостійної роботи здобувачів	Денна форма	Заочна форма
	10 20 60	---
Відсоток аудиторного навантаження	33 %	
Мова викладання	Українська, англійська	
Форма проміжного контролю (якщо є)		
Форма підсумкового контролю	Екзамен	

1. Мета, завдання, компетентності та програмні результати навчання з дисципліни

Мета:

розвинути у PhD-здобувачів здатність розв'язувати комплексні науково-прикладні задачі у сфері комп'ютерної інженерії, що передбачає глибоке переосмислення наявних та створення нових цілісних знань професійної практики, пов'язаної із забезпеченням захисту програмних та інформаційних систем, баз даних.

Для досягнення мети мають вирішуватися такі *завдання*:

- опанування здобувачами понять, методів та засобів захисту інформації від НСД;

- засвоєння здобувачами знань з основ антивірусної діяльності та вмінь їх застосовувати в сучасних кіберсистемах;

- оволодіння принципами побудови алгоритмів інструментів безпеки та їх впровадження;

- формування вмінь здобувачів використовувати сучасні технології захисту у хмарних середовищах;

- розвиток компетенцій використання програмних засобів для вирішення задач захисту інформації;

- формування здатностей здобувачів проектувати та впроваджувати системи зменшення вразливості вебзастосунків.

В результаті вивчення дисципліни здобувач

має знати:

- процеси захищеного зберігання, передачі та доступу до інформації в комп'ютерних системах;
- принципи дослідження безпеки інформаційних процесів і оцінювання рівня їх ефективності;
- принципи розробки алгоритмів роботи інструментів безпеки інформаційних систем та їх впровадження;;

має вміти:

- проєктувати та впроваджувати системи зменшення вразливості інформаційних систем;
- використовувати сучасні технології захисту у хмарних середовищах для отримання наукових результатів, які можуть створювати нові знання у
- комп'ютерній науці та дотичних до неї;
- виконувати оригінальні власні дослідження при використанні програмних та апаратних засобів для вирішення задач захисту інформаційних систем.

Інтегральна компетенція

ІК Здатність продукувати нові ідеї, розв'язувати комплексні проблеми в галузі професійної та/або дослідницько-інноваційної діяльності у сфері комп'ютерної інженерії та комп'ютерних технологій, застосовувати методологію наукової та педагогічної діяльності, а також проводити власне наукове дослідження, результати якого мають наукову новизну, теоретичне та практичне значення на основі модельного представлення та моделювання.

Загальні компетентності:

ЗК02. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК04. Здатність розв'язувати комплексні проблеми у сфері комп'ютерної інженерії на основі системного наукового світогляду та загального культурного кругозору із дотриманням принципів професійної етики та академічної доброчесності.

Спеціальні компетентності:
СК02. Здатність ініціювати, розробляти і реалізовувати комплексні інноваційні проєкти в комп'ютерній інженерії та дотичні до неї міждисциплінарні проекти.
СК05. Здатність ефективно застосовувати методи аналізу, математичне моделювання, виконувати натурні та обчислювальні експерименти при проведенні наукових досліджень у сфері комп'ютерної інженерії.
СК06. Здатність інтегрувати знання з різних галузей, застосовувати системний підхід та враховувати нетехнічні аспекти при розв'язанні інженерних задач та проведенні досліджень.

Програмні результати навчання:
РН01. Мати передові концептуальні та методологічні знання з комп'ютерної інженерії і на межі предметних галузей, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень на рівні останніх світових досягнень з комп'ютерної інженерії, ІТ-інфраструктур та інформаційних технологій, отримання нових знань та/або здійснення інновацій.
РН02. Планувати і виконувати експериментальні та/або теоретичні дослідження з комп'ютерної інженерії та дотичних міждисциплінарних напрямів з використанням сучасних інструментів та дотриманням норм професійної і академічної етики, критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблем.
РН04. Розробляти та реалізовувати наукові та/або інноваційні інженерні проєкти, які дають можливість переосмислити наявне та створити нове цілісне знання та/або професійну практику і розв'язувати значущі наукові та технологічні проблеми комп'ютерної інженерії з дотриманням норм академічної етики і врахуванням соціальних, економічних, екологічних та правових аспектів.
РН07. Застосовувати загальні принципи та методи математики, інформатики та інших наук, а також сучасні методи та інструменти, цифрові технології та спеціалізоване програмне забезпечення для провадження досліджень у сфері комп'ютерної інженерії.

Об'єкти вивчення та діяльності:
- аналогові та цифрові комп'ютери та комп'ютерні системи, локальні, глобальні комп'ютерні мережі та мережа Інтернет, кіберфізичні системи, Інтернет речей, системи та засоби оброблення великих даних і штучного інтелекту, ІТ-інфраструктури, методи та способи подання, отримання, зберігання, передавання, опрацювання та захисту в них інформації, математичні моделі обчислювальних процесів та технології виконання обчислень, архітектура та організація їх функціонування, інтерфейси та

протоколи взаємодії їх компонентів, методи та технології людино-машинної взаємодії та кооперації, доданої та віртуальної реальності;

- інформаційні процеси, технології, методи, способи, інструментальні засоби та системи для дослідження, проектування, налагодження, виробництва й експлуатації комп'ютерів та комп'ютерних систем і мереж, кіберфізичних систем, Інтернету речей, IT-інфраструктур, розроблення, верифікації та розгортання програмного забезпечення та систем у хмарних та інших середовищах, а також процедури та засоби підтримки та керування життєвим циклом, забезпечення якості, надійності та безпеки.

2. Програма навчальної дисципліни

Денна форма:

№ з/п	Теми	Лекції, годин	Практичні	Самостійна робота
1	Тема 1. Методи та інструменти аналізу вразливостей інформаційних систем (ІС).	2	2	12
2	Тема 2. Політика безпеки при роботі у відкритих мережах в глобальній мережі Інтернет.	2	2	12
3	Тема 3. Використання шаблонів проектування у створенні інструментів безпеки та їх впровадження	2	4	12
4	Тема 4. Конфігурація профілю безпеки ІС на хмарних платформах MsAzure, AWS, GoogleCloud та CloudFlare.	2	8	12
5	Тема 5. Методи та засоби виявлення бот-мереж. Системи захисту від фішингу.	2	4	12
	Всього за дисципліною:	**10**	**20**	**60**

Зміст навчальної дисципліни

2.1. План лекцій

№ з/п	Тема заняття / план
1	**Тема 1. Методи та інструменти аналізу вразливостей інформаційних систем** 1) Nessus: Оцінка вразливостей у UNIX-подібних операційних системах. 2) GFI LANguard: Комерційний сканер мережевих вразливостей під Windows. 3) Retina: Комерційний сканер для оцінки вразливостей. 4) Core Impact: Автоматизований продукт для тестування несанкціонованих проникнень у систему. 5) ISS Internet Scanner: Оцінка вразливостей на рівні застосунків. 6) X-scan: Сканер для дослідження мережевих вразливостей.
2	**Тема 2. Політика безпеки при роботі у відкритих мережах в глобальній мережі Інтернет** 1) Інфраструктура на основі криптографії з відкритими ключами (ІОК). Цифрові сертифікати. Управління цифровими сертифікатами. Компоненти ІОК і їх функції. Центр Сертифікації. Центр Реєстрації. Стандарти PKIX. Стандарти, засновані на ІОК (S/MIME, SSL і TLS, SET, IPSEC). Управління ключами.

№ з/п	Тема заняття / план
	2) Визначення Інтернет-провайдерства. Апаратні засоби для Інтернет. Протоколи захисту при передачі даних в кабельних та бездротових мережах. 3) Захист інформації в електронних платіжних системах. Забезпечення безпеки електронних платіжних систем на основі смарт-карт і програмно апаратних засобів. 4) Захист інформації при передачі повідомлень. Програма PGP. 5) Підключення до Інтернету Starlink через хмарну інфраструктуру GoogleCloud та підключення SpaceX.
3	**Тема 3. Використання шаблонів проектування у створенні інструментів безпеки та їх впровадження. Методики зменшення вразливості вебзастосунків.** 1) Динамічні сканери безпеки вебзастосунків. 2) Шаблони інструментальної реалізації хешування паролів. 3) Вимоги до інструментів шифрування потоків даних корпоративних організацій. 4) Вебзастосунки збереження паролів користувачів з використанням дешифраторів SHA256. MD5. 5) Конфігурація Apache–сервера.
	Тема 4. Конфігурація профілю безпеки ІС на хмарних платформах MsAzure, AWS, GoogleCloud та CloudFlare. 1) Конфігурація профілю інформаційної безпеки мережі з використанням MsAzure-платформи. Professional Security. HTTPS Request. ASP.net FireWall. 2) Конфігурація профілю інформаційної безпеки мережі з використанням AWS-платформи. Professional Security. HTTPS Request. SQL Injects. 3) Конфігурація профілю інформаційної безпеки для статичних та динамічних HTML-сторінок з використанням платформи GoogleCloud. Professional Security. HTTPS Request. CDN-сервіс у якості FireWall. Використання Google Cloud Platform і Google Earth Engine для NASA. 4) Конфігурація профілю інформаційної безпеки для статичних файлів з використанням платформи CloudFlare. Professional Security. HTTPS Request. AppEngine FireWall. Використання проксі для запобігання визначенню місцезнаходження відвідувача на основі IP-адреси засобами CloudFlare.
	Тема 5. Методи та засоби виявлення бот-мереж. Проектування систем моніторингу антивірусних ухилень. Багатофакторна автентифікація Системи захисту від фішингу. 1) Алгоритми, методи та засоби виявлення бот-мереж в корпоративних мережах. 2) Ідентифікація бот-мереж на основі їх групової активності в DNS-трафіку. 3) Виявлення бот-мереж, які застосовують технології ухилення від виявлення на основі DNS. 4)VPN-тунелювання.

2.2. План практичних занять

№ з/п	Тема заняття / план	Години
1	**Тема 1. Практична робота № 1. Пошук та ліквідація вразливостей вебсерверів** 1) Виконати сканування серверу (ЗА ВАРІАНТАМИ) на наявність вразливості «Poodle» за допомогою nmap. 2) Описати ключі, використані в команді. 3) Відключити у власному браузері SSLv3	2
2	**Тема 2. Практична робота № 2. Програмний засіб криптографічного захисту PGP Desktop для виконання операцій шифрування і цифрового підпису повідомлень.** 1) встановити PGP Desktop; 2) створити пару ключів; 3) ввести ключову фразу (пароль) для захисту таємного ключа; 4) опублікувати відкритий ключ в PGP на Global Directory Server АБО експортувати відкритий ключ на знімний носій (USB-flash) АБО скопіювати його в текстовий файл; 5) отримати файл з розширенням .asc від своїх резидентів та виконати для нього команду Import; 6) зашифрувати і/або засвідчити повідомлення Вашим цифровим підписом та відправити респонденту; 7) розшифрування отримане повідомлення від респондента та/або перевірити справжність ЕЦП відправника	2
3	**Тема 3. Практична робота № 3. Розробка дешифратора SHA256** 1) Побудування алгоритму. 2) Перевірка цілісності та доступності відновленої інформації. 3) Порівняння хеш-функцій.	2
4	**Тема 3. Практична робота № 4. Розробка дешифратора MD5.** 1) Побудування алгоритму. 2) Вирівнювання потоків даних. 3) Перевірка цілісності та доступності відновленої інформації.	2
5	**Тема 4. Практична робота № 5. Конфігурація профілю інформаційної безпеки мережі з використанням MsAzure платформи.** 1) Professional Security. 2) HTTPS Request. 3) ASP.net FireWall.	2
6	**Тема 4. Практична робота № 6. Конфігурація профілю інформаційної безпеки мережі з використанням AWS-платформи.** 1) Professional Security. 2) HTTPS Request. 3) SQL Injects.	2
7	**Тема 4. Практична робота № 7. Конфігурація профілю інформаційної безпеки мережі з використанням GoogleCloud CDN платформи.** 1) Professional Security. 2) HTTPS Request. 3) AppEngine FireWall.	2
8	**Тема 4. Практична робота № 8. Конфігурація профілю інформаційної безпеки мережі з використанням CloudFlare платформи.** 1) Professional Security.	2

№ з/п	Тема заняття / план	Години
	2) HTTPS Request. 3) CDN-сервіс у якості FireWall.	
9	**Тема 5. Практична робота № 9. Виявлення ботнетів.** 1) Створити віртуальну мережу за допомогою середовища на віртуальних машинах Windows, що виступають бот-клієнтами. В якості ботів було використати такі типи: *roB****, OpenDataUa, MedicalCorps_bot. 2) Запустити програму для аналізу ботнет-трафіку (наприклад, Spybot - Search & Destroy Free) у двох режимах: – тільки ботнет-трафік – ботнет-трафік разом зі звичайним. 3) Виявити всі канали командного та керуючого трафіку (C&C) ботнета	2
10	**Захист робіт**	2
	Разом	**20**

2.3. Забезпечення освітнього процесу

Практичні роботи з дисципліни проводяться у комп'ютерних класах із доступом до глобальної мережі Інтернет та можливістю адміністрування наданих комп'ютерних систем для встановлення віртуальних машин.

Описи завдань розміщено у системі дистанційного навчання Moodle для PhD-програми.

3. Підсумковий контроль

1. Методи та інструменти аналізу вразливостей інформаційних систем.
2. Nessus: Оцінка вразливостей у UNIX-подібних операційних системах.
3. GFI LANguard: Комерційний сканер мережевих вразливостей під Windows.
4. Retina: Комерційний сканер для оцінки вразливостей.
5. Core Impact: Автоматизований продукт для тестування несанкціонованих проникнень у систему.
6. ISS Internet Scanner: Оцінка вразливостей на рівні застосунків.
7. X-scan: Сканер для дослідження мережевих вразливостей.
8. Політика безпеки при роботі у відкритих мережах в глобальній мережі Інтернет
9. Інфраструктура на основі криптографії з відкритими ключами (ІОК). Цифрові сертифікати. Управління цифровими сертифікатами. Компоненти ІОК і їх функції. Центр Сертифікації. Центр Реєстрації. Стандарти PKIX. Стандарти, засновані на ІОК (S/MIME, SSL і TLS, SET, IPSEC). Управління ключами.

10. Визначення Інтернет-провайдерства. Апаратні засоби для Інтернет. Протоколи захисту при передачі даних в кабельних та бездротових мережах.

11. Захист інформації в електронних платіжних системах. Забезпечення безпеки електронних платіжних систем на основі смарт-карт і програмно апаратних засобів.

12. Захист інформації при передачі повідомлень. Програма PGP.

13. Підключення до Інтернету Starlink через хмарну інфраструктуру GoogleCloud та підключення SpaceX.

14. Використання шаблонів проектування у створенні інструментів безпеки та їх впровадження. Методики зменшення вразливості вебзастосунків.

15. Динамічні сканери безпеки вебзастосунків.

16. Шаблони інструментальної реалізації хешування паролів.

17. Вимоги до інструментів шифрування потоків даних корпоративних організацій.

18. Вебзастосунки збереження паролів користувачів з використанням дешифраторів SHA256. MD5.

19. Конфігурація Apache-сервера.

20. Порівняння засобів безпеки ІС на хмарних платформах MsAzure, AWS, GoogleCloud та CloudFlare.

21. Конфігурація профілю інформаційної безпеки мережі з використанням MsAzure-платформи. Professional Security. HTTPS Request. ASP.net FireWall.

22. Конфігурація профілю інформаційної безпеки мережі з використанням AWS-платформи. Professional Security. HTTPS Request. SQL Injects.

23. Конфігурація профілю інформаційної безпеки для статичних та динамічних HTML-сторінок з використанням платформи GoogleCloud. Professional Security. HTTPS Request. CDN-сервіс у якості FireWall. Використання Google Cloud Platform і Google Earth Engine для NASA.

24. Конфігурація профілю інформаційної безпеки для статичних файлів з використанням платформи CloudFlare. Professional Security. HTTPS Request. AppEngine FireWall. Використання проксі для запобігання визначенню місцезнаходження відвідувача на основі IP-адреси засобами CloudFlare.

25. Методи та засоби виявлення бот-мереж. Проектування систем моніторингу антивірусних ухилень.

26. Багатофакторна автентифікація Системи захисту від фішингу.

27. Алгоритми, методи та засоби виявлення бот-мереж в корпоративних мережах.

28. Ідентифікація бот-мереж на основі їх групової активності в DNS-трафіку.

29. Виявлення бот-мереж, які застосовують технології ухилення від виявлення на основі DNS.

30. VPN-тунелювання.

4. Критерії оцінювання та засоби діагностики результатів навчання

№ з/п	Вид діяльності (завдання)	Максимальна кількість балів
1	Індивідуальні самостійні завдання	15
2	Практичні завдання виконані на парі (9 робіт · 5 балів)	45
3	Екзамен	40
	Всього	**100**

Критерії оцінювання завдань
для досягнення максимальної кількості балів

Перевірка отриманих знань та навичок здобувачами відбувається шляхом проведення усного опитування на практичних заняттях та виконання самостійних домашніх завдань (індивідуальне завдання).

Поточна рейтингова оцінка складається з балів, які здобувач отримує протягом засвоєння даної дисципліни, виконання та захисту домашніх завдань, виступів на практичних заняттях. Якщо здобувач успішно (з позитивними за національною шкалою оцінками) виконав передбачені в даній дисципліні всі види навчальної роботи, то він допускається до екзамену.

Протягом семестру здобувач виконує три види завдань: Практичні роботи; Індивідуальні самостійні завдання; Захист робіт (презентація роботи у вигляді доповіді).

Оцінювання практичних робіт

Максимальний бал (100 % від максимального балу) виставляється за роботу, виконану вчасно та у відповідності до робочого завдання, якщо отримані правильні результати, охайно виконаний звіт, правильно сформульовані висновки до роботи, на захисті продемонстровано розуміння усіх результатів та етапів їх отримання, вільне володіння теоретичним підґрунтям роботи;

Робота оцінюється у 50 % від максимального балу, якщо работа виконана невчасно та/або наявні недоліки при виконанні роботи, отриманих результатах, оформленні звіту, зроблених висновках та при захисті роботи;

Робота оцінюється у 25 % від максимального балу, якщо робота виконана самостійно, повністю у відповідності до робочого завдання та власноручно виконаний звіт, але виконана невчасно та/або не захищена;

Робота оцінюється у 0 балів, якщо виконана несамостійно, не відповідає завданню (варіанту), виконана невчасно.

Оцінювання індивідуальних самостійних завдань

Якщо при виконанні здобувачем допускаються незначні неточності, то кількість балів зменшуються на 5 %. Якщо при виконанні здобувачем

допускаються значні неточності, але принципи не викривлено то на 10 %, якщо помилки суттєві, то бали зменшуються на 20 %.

Оцінювання підсумкового контролю навчання (екзамен)

Оцінювання роботи здобувачів оцінюється у 100 балів. Сорок балів здобувач отримує за умов якісного складання екзамену. Якщо проходження підсумкового контролю оцінується на «добре» або «задовільно», це відповідає 15 балам і 10 балам. Розподіл максимальної кількості балів по питанням здійснюється рівномірно – 20 балів за кожне питання.

Білети для підсумкового контролю:

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Чорноморський національний університет імені Петра Могили
Факультет комп'ютерних наук
Кафедра комп'ютерної інженерії
Спеціальність 123 «Комп'ютерна інженерія»
Дисципліна «Технології захисту інформаційних систем»
Білет № 0

1. Захист інформації при передачі повідомлень. Програма PGP.
2. Конфігурація профілю інформаційної безпеки мережі з використанням MsAzure платформи.

Канд. техн. наук, доц._____ В. Ю. Савінов Зав. кафедрою_____
"____"_____ 202_р. "____"_____ 202_р.

5. Рекомендовані джерела інформації

Основні

1. Neil I. CompTIA Security+: SY0-601 Certification Guide: Complete Coverage of the New CompTIA Security+ (SY0-601) Exam to Help You Pass on the First Attempt. Packt Publ., 2020. 550 p. URL: https://www.google.com.ua/books/edition/CompTIA_Security+_SY0_601_Certification/fEUREAAAQBAJ?hl=en&gbpv=1.

2. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 2.5-004-99 (зі Змінами № 806-2012). URL: http://www.dut.edu.ua/ua/lib/3/category/919/view/1032 .

3. Остапов С. Е., Євсеєв С. П., Король О. Г. Технології захисту інформації. Львів : Новий світ-2000, 2020. 678 с.

4. Посібник з належної практики захисту критичної інфраструктури (План безпеки). Національний центр захисту критичної інфраструктури, 2021. 46 с. URL: https://cip.gov.ua/ua/news/perelik-dokumentiv-mizhnarodnikh-organizacii-u-sferi-zakhistu-kritichnoyi-infrastrukturi

5. Про захист персональних даних. Закон України від 1 червня 2010 року № 2297-VI (зі змінами від 29.07.2022 № 2494-IX). URL: https://zakon.rada.gov.ua/laws/show/2297-17.

6. Про Стратегію кібербезпеки України. РНБО; Рішення від 27.01.2016. Введено в дію Указом Президента України від 15 березня 2016 року № 96/2016 URL: https://zakon.rada.gov.ua/laws/show/n0003525-16

Додаткові

7. Журавська І. М., Обухова К. О. Особливості реалізації та оцінка криптостійкості шифру Rabbit. Комп'ютерно-інтегровані технології: освіта, наука, виробництво / Луцьк. нац. техн. ун-т. 2020. № 41. С. 159–164. DOI: 10.36910/6775-2524-0560-2020-41-25.

8. Колодяжний К. О., Журавська І. М. Розробка захищеної інформаційної системи для сфери охорони здоров'я. Могилянські Могилянські читання – 2022 : тези доп. XXV Всеукр. наук.-метод. конф. Миколаїв, 7–11 листоп. 2022 р. Миколаїв : Чорном. нац. ун-т ім. Петра Могили, 2022. С. 31–33.ня – 2022 : тези доп. XXV Всеукр. наук.-метод. конф. Миколаїв, 7–11 листоп. 2022 р. Миколаїв : Чорном. нац. ун-т ім. Петра Могили, 2022. С. 31–33.

9. Про Державну службу спеціального зв'язку та захисту інформації України. Закон України від 23 лютого 2006 року № 3475-IV (зі змінами від 23.08.2023 № 3343-IX). URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text.

10. Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.2017 № 2163-VIII (зі змінами від 28.07.2022 № 2470-IX). URL: https://zakon.rada.gov.ua/laws/show/2163-19

11. Про захист інформації в інформаційно-комунікаційних системах. Закон України від 05.07.1994 № 80/94-ВР (зі змінами від 01.12.2022 № 2801-IX). URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.

12. Про електронні документи та електронний документообіг. Закон України від 22 травня 2003 року № 851-IV. URL: https://zakon.rada.gov.ua/laws/show/851-15.

13. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури. Постанова Кабінету Міністрів України від 19.06.2019 № 518 (зі змінами від 02.09.2022 № 991). URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF.

14. Про затвердження Порядку надання послуг конфіденційного зв'язку органам державної влади та органам місцевого самоврядування, державним підприємствам, установам та організаціям. Постанова Кабінету Міністрів України 11.10.2002 № 1519 (зі змінами від 22.07.2022 № 820). URL: https://zakon3.rada.gov.ua/laws/show/1519-2002-%D0%BF.

15. Burlachenko I., Zhuravska I., Davydenko Y., Savinov V. Vulnerabilities analysis and defense based on MAS method in fast dynamic wireless networks. Proc. of the 2018 IEEE 4th Intern. Symposium on Wireless Systems within the Internat. Conf. on Intelligent Data Acquisition and Advanced Computing Syst. (IDAACS-SWS 2018), 2018. P. 98–102, No. 8525692.