МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки

ТИМОШЕНКО Лідія Миколаївна

Методи оцінювання кібер-ситуаційної обізнаності співробітників об'єкту критичної інфраструктури / Methods for assessing cyber situational awareness of critical infrastructure employees

спеціальність: 125 – Кібербезпека та захист інформації

освітньо-професійна програма –Кібербезпека

Кваліфікаційна робота

Виконала студентка групи КБзм -21
Л.М. Тимошенко

Науковий керівник
д.т.н., професор В.В. Яцків

Кваліфікаційну роботу допущено
до захисту:
«____» _____ ___2025 р.

Завідувач кафедри
_____ В.В.Яцків

ТЕРНОПІЛЬ - 2025

Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки
Освітній ступінь «магістр»
спеціальність: 125 – Кібербезпека та захист інформації
освітньо-професійна програма – Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ В.В.Яцків
«____» _____ 202__ року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТЦІ
ТИМОШЕНКО ЛІДІЇ МИКОЛАЇВНІ

1. Тема кваліфікаційної роботи:
Методи оцінювання кібер-ситуаційної обізнаності співробітників об'єкту критичної інфраструктури / Methods for assessing cyber situational awareness of critical infrastructure employees

керівник роботи д.т.н., професор В.В. Яцків
затверджені наказом по університету від «12» березня 2025 року №242-ст.
2. Строк подання студентом закінченої кваліфікаційної роботи 5 грудня 2025 р.

3. Вихідні дані до кваліфікаційної роботи: завдання на кваліфікаційну роботу студента, наукові статті, технічна література.

4. Основні питання, які потрібно розробити:
– проаналізувати нормативно-правове забезпечення та управління безпекою об'єктів критичної інфраструктури в Україні;
– дослідити можливості тестування як методу оцінювання;
– розробити схему дерева критеріїв і альтернатив та ієрархічну модель оцінки кібер-ситуаційної обізнаності;
– визначити експертні оцінки та довести їх узгодженість;
–розробити програмний застосунок та виконати експериментальне дослідження оцінювання кібер-ситуаційної обізнаності співробітників з аналізом результатів, розробити заходи з підвищення рівня обізнаності та рекомендації по їх впровадженню.

5. Перелік графічного матеріалу у роботі:
– узагальнена схема оргнанізаційної структури ООВА;
– схема алгоритму проведення тестування;
– схема дерева критеріїв і альтернатив;
– схема ієрархічної моделі оцінки кібер-ситуаційної обізнаності.

6. Консультанти розділів кваліфікаційної роботи

	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 12 березня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строки виконання етапів кваліфікаційної роботи	Примітка
1	Аналіз забезпечення інформаційної безпеки об’єктів критичної інфраструктури.	03.2025 р. – 05.2025 р.	
2	Кібер-ситуаційна обізнаність та дослідження методів її оцінювання	06.2025 р. – 08.2025 р.	
3	Розробка програмного застосунку оцінювання кібер-ситуаційної обізнаності	09.2025 р. – 11.2025 р.	

Студентка _____ Тимошенко Л.М.
(підпис)

Керівник роботи _____ д.т.н., професор В.В.Яцків

АНОТАЦІЯ

Тимошенко Л.М. Методи оцінювання кібер-ситуаційної обізнаності співробітників об’єкту критичної інфраструктури. – Рукопис.

Дослідження на здобуття освітнього ступеня «магістр» за спеціальністю 125 «Кібербезпека та захист інформації», освітньо-професійна програма «Кібербезпека». – Західноукраїнський національний університет, Тернопіль, 2025.

Мета кваліфікаційної роботи полягає у покращенні стану захищеності кіберпростору об’єктів критичної інфраструктури та державних адміністрацій шляхом підвищення рівня кібер-ситуаційної обізнаності їх співробітників. Методи дослідження – комп’ютерне тестування, методики оцінювання обізнаності та алгебраїчний підхід, метод аналізу ієрархій.

Результати дослідження. Здійснено аналіз нормативно-правового забезпечення та управління безпекою об’єктів критичної інфраструктури в Україні та існуючого стану захищеності інформаційних ресурсів критично важливої інфраструктури, зокрема, Одеської обласної державної (військової) адміністрації. Дослідження методів оцінювання ситуаційної обізнаності показали, що для оцінювання кібер-ситуаційної обізнаності співробітників державних адміністрацій доцільно використовувати комп’ютерне тестування та метод аналізу ієрархій. Виконано експериментальне дослідження тестування для визначення рівня оцінювання кібер-ситуаційної обізнаності співрбітників в конкретному органі державного управління та проаналізавано одержані результати з наданням відповідних рекоменлацій.

Результати роботи можуть успішно застосовуватися в в органах державного управління України та інших об’єктах критично важливої інфраструктури.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, КРИТИЧНА ІНФРАСТРУКТУРА, КІБЕР-СИТУАЦІЙНА ОБІЗНАНІСТЬ, МЕТОД ТЕСТУВАННЯ, МЕТОД АНАЛІЗУ ІЄРАРХІЙ

ABSTRACT

Tymoshenko L.M. Methods for assessing cyber situational awareness of critical infrastructure employees. – Manuscript.

Research for the degree of "Master" in specialty 125 "Cybersecurity and Information Protection", educational and professional program "Cybersecurity". - Western Ukrainian National University, Ternopil, 2025.

The purpose of the qualification work is to improve the state of cyberspace security of critical infrastructure facilities and state administrations by increasing the level of cyber-situational awareness of their employees. Research methods – computer testing, awareness assessment methods and algebraic approach, hierarchy analysis method.

Research results. An analysis of the regulatory and legal support and security management of critical infrastructure facilities in Ukraine and the current state of security of information resources of critical infrastructure, in particular, the Odessa Regional State (Military) Administration, was carried out. Research on methods for assessing situational awareness showed that it is advisable to use computer testing and the hierarchy analysis method to assess cyber-situational awareness of state administration employees. An experimental testing study was conducted to determine the level of assessment of cyber situational awareness of colleagues in a specific government agency and the results obtained were analyzed.

The results of the work can be successfully applied in government agencies of Ukraine and other critical infrastructure facilities.

Keywords: INFORMATION SECURITY, CRITICAL INFRASTRUCTURE, CYBER SITUATIONAL AWARENESS, TESTING METHOD, HIERARCHY ANALYSIS METHOD

ЗМІСТ

ВСТУП

Поняття «ситуаційна обізнаність» історично походить із військової галузі, де воно активно використовувалося ще за часів Першої світової війни. Однак, із прогресом та поширенням інформаційних технологій, ця концепція вийшла за межі військової справи, отримавши подальший розвиток та глибоку трансформацію в умовах сучасних складних систем. Ситуаційна обізнаність визначається як фундаментальна здатність суб'єкта (користувача, оператора, системи) до оперативного отримання, аналізу та інтеграції інформації щодо актуального стану середовища (або системи, що контролюється). На цій основі, використовуючи накопичені знання, формуються достовірні висновки та приймаються рішення стосовно необхідних дій чи подальшого реагування.

Однією з ключових переваг у сучасній війні рф проти України вважають високу інформаційну обізнаність на полі бою: розуміння розташування противника, його чисельності та рівня боєздатності. Сьогодні Україна презентувала НАТО систему ситуаційної обізнаності Delta, яка надає військовим комплексні дані про дії ворога, сприяє координації сил на місці бою, використовується для планування операцій, взаємодії між підрозділами та забезпечує захищений обмін інформацією.

Перенесення війни в кіберпростір зумовлює зростання кількості практичних розробок і наукових досліджень у сфері кібер-ситуаційної обізнаності (Cyber Situation Awareness, CSA). Це підкреслює важливість вивчення методів оцінювання рівня CSA та загальної інформаційної безпеки систем як у різних галузях державного управління, так і для держави загалом. Комплексний підхід у володінні ситуацією актуальний в різних областях, де є великий обсяг інформаційних потоків і високий ступінь ризику, зокрема, в кібер-просторі.

Актуальність теми кваліфікаційної роботи зумовлена, зокрема, високим рівнем ризиків, що пов'язані з інформаційною безпекою органів державної влади як важливої складової всієї критичної інфраструктури держави[1]. Численні дослідження свідчать, що навіть за наявності якісного програмного й апаратного

захисту найбільшу загрозу інформаційній безпеці становить недостатній рівень обізнаності працівників у цій сфері. Тому питання захисту інформації та підвищення обізнаності персоналу є ключовими для будь-якої державної установи, діяльність якої пов’язана з отриманням, зберіганням і обробкою важливих даних, особливо в умовах повномасштабного вторгнення та посилення кібератак ворога.

Для належного захисту інформації необхідно впроваджувати комплекс заходів, спрямованих на забезпечення її конфіденційності, цілісності та доступності, а також підвищення рівня обізнаності персоналу. Ефективна політика інформаційної безпеки повинна охоплювати використання всіх доступних інструментів та методів захисту.

Забезпечення інформаційної безпеки є одним із ключових пріоритетів у зменшенні ризиків виникнення загроз для інформаційних систем. Величезна кількість досліджень у переважній своїй кількості зосереджується на технологічних аспектах безпеки – зокрема, шифрування, виявлення шкідливого програмного забезпечення чи робота брандмауерів. Однак для багатьох організацій саме людський фактор, а не технології, перетворився на один із найзначніших ризиків. Люди, як і комп’ютери, зберігають, обробляють та передають інформацію, проте захист «людських ресурсів» часто забезпечується недостатньо, що створює додаткові загрози для інформаційної безпеки об’єктів критичної інфраструктури.

Попри значну кількість досліджень, присвячених оцінюванню кіберситуаційної обізнаності та інформаційної безпеки ІТ-систем у різних галузях та сферах, аналогічні роботи майже не зустрічаються щодо органів державного управління, зокрема обласних державних адміністрацій. У цій роботі здійснено порівняльний аналіз факторів впливу на рівень поінформованості як кінцевих користувачів, так і осіб, які ухвалюють рішення в сфері критично важливої інфраструктури (КВІ). Досліджено рівень обізнаності працівників державної адміністрації з питань інформаційної безпеки.

На початку роботи наведено огляд ключових понять, які становлять

теоретичну основу кваліфікаційної роботи, а також методів оцінювання кіберситуаційної обізнаності співробітників. Далі представлено аналіз результатів проведеної оцінки. У завершальній частині сформульовано рекомендації та визначено напрями розробки й впровадження заходів щодо підвищення рівня кіберситуаційної обізнаності працівників держадміністрації.

Мета роботи. Мета кваліфікаційної роботи полягає у покращенні стану захищеності кіберпростору об'єктів критичної інфраструктури та державних адміністрацій шляхом підвищення рівня кібер-ситуаційної обізнаності їх співробітників. Результати цього дослідження можуть використовуватися для встановлення рівня обізнаності співробітників облдержадміністрації, для аналізу змін при впровадженні заходів з кібербезпеки й для порівняння результатів з іншими об'єктами державного управління та критичної інфраструктури.

Для досягнення зазначеної мети поставлено основні **завдання**:

- огляд і аналіз існуючого стану захищеності критично важливої інфраструктури, зокрема, обласної державної адміністрації;
- дослідження методів оцінювання CSA;
- розробка програмного застосунку тестування та моніторинг CSA співробітників;
- розробка заходів підвищення рівня CSA та рекомендацій по їх впровадженню для покращення захищеності інформаційних ресурсів систем різних об'єктів критичної інфраструктури.

Об'єкт дослідження. Рівень кіберситуаційної обізнаності співробітників Одеської обласної (військової) державної адміністрації.

Предмет дослідження. Методи та підходи до оцінювання кіберситуаційної обізнаності працівників Одеської облдержадміністрації.

У дослідженні використано метод аналізу ієрархій, комп'ютерне тестування, методики оцінювання обізнаності та алгебраїчний підхід.

Теоретичну основу становлять праці українських і зарубіжних учених, присвячені застосуванню системного аналізу в управлінських системах, дослідженням у сфері ситуаційної обізнаності, чинні законодавчі документи.

Наукова новизна одержаних результатів.

1. Вперше запропоновано модель і програмний застосунок для оцінювання ситуаційної обізнаності співробітників об'єктів критичної інфраструктури на основі методів комп'ютерного тестування та аналізу ієрархій. Це дозволило обґрунтувати доцільність застосування запропонованих підходів і заходів для підвищення рівня захищеності інформаційних ресурсів таких об'єктів

2. Подальшого розвитку набули модель ситуаційної обізнаності Ендслі та метод аналізу ієрархій у сфері кіберзахисту, що дало змогу реалізувати моніторинг кіберситуаційної обізнаності – надзвичайно важливий інструмент для системи державної безпеки в умовах постійних інформаційних атак з боку ворога та воєнного стану.

Практичне значення отриманих результатів. Практична значущість роботи полягає в обґрунтуванні необхідності оцінювання кіберситуаційної обізнаності співробітників об'єктів критичної інфраструктури та в розробці програмного забезпечення для такого оцінювання. Отримані результати можуть бути використані для подальшого дослідження питань, пов'язаних із формуванням заходів з інформаційної безпеки об'єктів критичної інфраструктури та підвищенням рівня кібер-ситуаційної обізнаності співробітників.

Дослідження з тематики даної кваліфікаційної роботи магістра розпочато під час роботи над виконанням Проєкту «Кібербезпека критично важливої інфраструктури України» (від Агентства США з міжнародного розвитку в рамках проєкту USAID/ Кібербезпека) [1].

Публікації та апробація КР. Основні положення та результати апробовані на конференціях "Кібербезпека та компютерно-інтегровані технології", «Інформаційна безпека та інформаційні технології», «Стан, досягнення і перспективи інформаційних систем і технологій», науково-практичному симпозіумі «Захист інформації», опубліковані у збірниках матеріалів [2-7] та фаховому журналі «Інформатика та математичні методи в моделюванні» [8,9].

1 АНАЛІЗ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1 Загальна характеристика інформаційної безпеки

Зміст поняття інформаційної безпеки охоплює два основні аспекти:

– власне інформаційну безпеку як стан захищеності кіберпростору;

– діяльність із забезпечення захисту інформації, яка полягає у запобіганні витокам конфіденційних даних та недопущенні несанкціонованого доступу.

Марущак А.І. визначає інформаційну безпеку підприємства, організації чи установи як цілеспрямовану діяльність посадових осіб із використанням законних заходів і засобів, спрямовану на досягнення такого рівня захищеності інформаційного та кіберсередовища, який забезпечує стабільне функціонування та динамічний розвиток організації [10].

Інший підхід до визначення інформаційної безпеки, запропонований Литвинюком А.А., базується на виділенні системних параметрів та функціонального блоку. За його визначенням: "Інформаційна безпека – це захищеність інформації та відповідної інфраструктури від навмисних або випадкових впливів природного чи штучного походження, які можуть завдати неприйнятних збитків суб'єктам інформаційних відносин" [11]. При цьому системними параметрами є сама інформація та інфраструктура, що є по суті забезпечувальною системою – від обслуговуючого персоналу до електропостачання. Функціональний блок включає ті загрози і можливі збитки для інформаційної системи, які не можна ігнорувати через порушення стану інформаційної безпеки.

Уникнути всіх можливих збитків неможливо, і, до того ж, немає економічно обґрунтованого способу захисту, коли витрати на засоби і заходи безпеки не перевищують очікуваний розмір збитків. Тому необхідно приймати певні компроміси і захищатися лише від тих загроз, допуск яких неприпустимий, що робить поріг неприйнятності матеріально визначеним [8]. Отже, метою захисту інформації є зменшення можливих збитків до прийнятного рівня.

Оскільки захист інформації є процесом забезпечення інформаційної безпеки, ключовими факторами цього процесу виступають загроза та ризик. Загрозу визначають як потенційну причину (подію, порушення, інцидент), здатну знизити рівень інформаційної безпеки системи та спричинити негативні наслідки або збитки для системи чи організації.

Ризик – це можливий збиток, тобто поєднання ймовірності реалізації загроз і шкоди від них. При цьому оцінка загрози і ризику проводиться не абстрактно, а стосовно конкретного об’єкта захисту. У менеджменті бізнес-процесів замість терміна "ресурс" часто використовують синонім – "актив", під яким розуміють усе, що є цінністним для системи або організації.

Приклади таких активів – це інформаційне та програмне забезпечення, мережеве та апаратне обладнання, інформаційні системи, персонал, окремі співробітники та імідж організації. Таким чином, активами вважаються всі об’єкти, що потребують захисту шляхом застосування процесів інформаційної безпеки.

Загрози інформаційній безпеці класифікують за кількома критеріями:

– за причинами виникнення: техногенні або природні, навмисні або випадкові;

– за розташуванням джерела небезпеки: зовнішні або внутрішні;

– за компрометованою підсистемою чи її сегментом: мережеві, криптографічні тощо;

– за етапом життєвого циклу системи: реалізаційні, експлуатаційні;

– за результуючим ефектом: порушення конфіденційності, цілісності або доступності.

Залежно від виду загрози інформаційну безпеку розглядають як:

– забезпечення стану захищеності особи, громади, суспільства та держави від впливу шкідливої інформації;

– захист інформаційних прав і свобод кожної людини;

– забезпечення захищеності інформації, інформаційних ресурсів та інформаційних систем від несанкціонованого впливу сторонніх осіб.

Основні поняття щодо інформаційної безпеки та її складові зображено на рисунку 1.1 [11].

Рисунок 1.1 – Складові інформаційної безпекии

Об'єкти інформаційної безпеки складають:

– свідомість та психологію особи;

– інформаційні системи різноманітного рівня й призначення.

Суб'єктами інформаційної безпеки є:

– держава, яка реалізує функції через відповідні органи;

– громадяни;

– суспільні та інші організації та об'єднання, що мають повноваження щодо забезпечення інформаційної безпеки відповідно до законодавства [12].

Провідним предметом інформаційної безпеки виступає інформація в автоматизованих комп'ютерних системах, у тому числі в телекомунікаціях, зокрема в інтернеті.

Усі інтереси суб'єктів, співвідносні до використання інформаційної інфраструктури, можна поділити на такі категорії [11] (рисунок 1.2):

- забезпечення конфіденційності й цілісності інформаційних ресурсів та підтримуючої їх інфраструктури;
- забезпечення достовірності, доступності, автентичності й підзвітності.

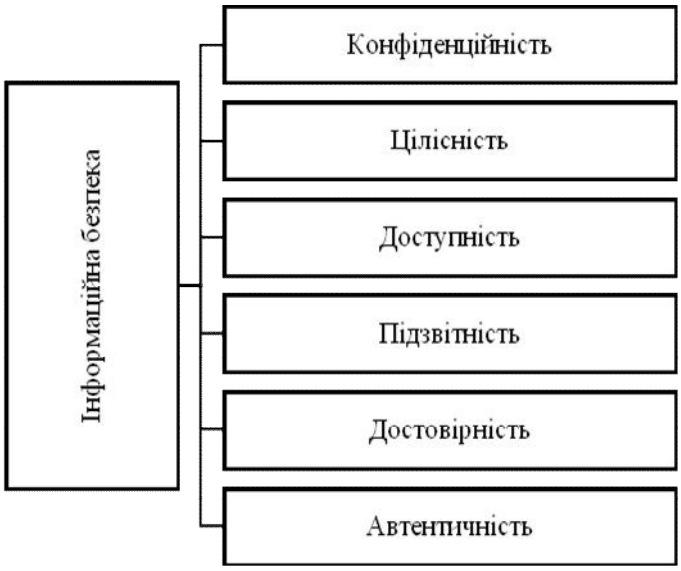

Рисунок 1.2 – Категорії інформаційної безпеки

Конфіденційність – це стан інформації, коли доступ до неї мають лише ті суб’єкти, які мають на це право.

Цілісність означає запобігання несанкціонованій модифікації інформації [9].

Доступність характеризується як запобігання постійному або тимчасовому приховуванню інформації від користувачів із правами доступу.

Достовірність інформації – відповідність інформації передбаченій поведінці або очікуваному результату.

Категорія підзвітність передбачає ідентифікацію суб’єкта доступу та реєстрацію його дій.

Автентичність (справжність) гарантує, що суб’єкт або ресурс відповідають заявленій ідентичності.

Основні завдання забезпечення інформаційної безпеки включають:

– виявлення та оцінювання джерел загроз інформаційній та кібербезпеці;

– розробку державної політики у сфері інформаційної та кібербезпеки, комплексу заходів і засобів для її реалізації;

– створення нормативно-правової бази для забезпечення інформаційної безпеки;

– координацію діяльності органів державної влади, установ та організацій у реалізації політики інформаційної безпеки;

– формування системи забезпечення інформаційної та кібербезпеки, удосконалення організаційного забезпечення, методів та засобів запобігання інцидентам та ліквідації наслідків порушень безпеки;

– забезпечення участі держави у створенні та використанні глобальних інформаційних мереж і систем [12].

Забезпечення інформаційної безпеки та захист інформації повинні мати системний характер: організаційні, апаратні, програмні та фізичні засоби захисту мають застосовуватися під єдиним управлінням одночасно.

1.2 Нормативно-правове забезпечення та управління безпекою об'єктів критичної інфраструктури в Україні

Розглянемо етапи формування термінології щодо критичної інфраструктури (КІ), відзначивши, що правотворча й наукова активність у цій сфері постійно зростає, про це свідчить значний масив нових досліджень.

У низці нормативно-правових актів відносно давно запропоновано офіційні визначення цього терміна. Так, у Постанові КМ України «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави» від 23 серпня 2016 року № 563 критична інфраструктура визначена як «Сукупність об'єктів інфраструктури держави, які є найбільш важливими для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу чи руйнування яких може мати вплив на національну безпеку й оборону, природне середовище, призвести до значних фінансових збитків і людських жертв» [12].

У розпорядженні КМ України від 6 грудня 2017 року № 1009-р це ж поняття сформульовано як «Сукупність об'єктів, які є стратегічно важливими для економіки й безпеки держави, суспільства, населення та порушення функціонування яких може завдати шкоди життєво важливим національним інтересам України» [13].

Про поняття «критична інфраструктура» йдеться також в Указі Президента

України «Про рішення Ради національної безпеки та оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» від 26 травня 2015 року № 287/2015. У документі серед загроз національній безпеці визначено й загрози критичній інфраструктурі, зокрема: «критична зношеність основних фондів об'єктів інфраструктури України та недостатній рівень їх фізичного захисту; недостатній рівень захищеності критичної інфраструктури від терористичних посягань і диверсій; неефективне управління безпекою критичної інфраструктури та систем життєзабезпечення» [14].

Питання щодо того, які саме об'єкти відносять до критичної інфраструктури, має широкий спектр відповідей. Відомий дослідник у цій сфері, Д. Бірюков, визначає критичну інфраструктуру як «сукупність об'єктів, технологій, державних і наукових структур, порушення регламентної діяльності яких впливає на економічну, соціально-політичну, військову та екологічну безпеку» [15].

Усі дослідники погоджуються, що нині захист критичної інфраструктури України – це комплекс заходів нормативно-правового, організаційного та технологічного характеру, спрямованих на забезпечення її безпеки та стійкості [16].

Проаналізувавши різні дефініції, С. Теленик узагальнює, що поняття критичної інфраструктури ґрунтується на таких складових:

– загальне визначення критичної інфраструктури як сукупності об'єктів;

– ознаки, за якими ці об'єкти належать до критичних;

– потенційні впливи на об'єкти критичної інфраструктури та їх наслідки;

– державні й суспільні інтереси та відносини, яким може бути завдано шкоди [14].

До об'єктів критичної інформаційної інфраструктури слід відносити автоматизовані системи управління державних органів, установ, підприємств і суб'єктів господарювання у сферах охорони здоров'я, освіти і науки, транспорту, зв'язку, енергетики, банківського сектору, промисловості тощо [17].

У Порядку формування переліку об’єктів критичної інформаційної інфраструктури (постанова КМУ від 09.10.2020 № 943) визначено, що до переліку включаються всі об’єкти інформаційної інфраструктури (автоматизовані, інформаційні, телекомунікаційні, інформаційно-телекомунікаційні системи та АСУ ТП), що експлуатуються на об’єкті критичної інфраструктури [18]. У Законі України «Про основні засади кібербезпеки України» [19] для позначення відповідних відносин застосовується термін «об’єкт критичної інформаційної інфраструктури».

Уперше на небезпеку знищення або пошкодження об’єктів критичної інфраструктури було звернено увагу у рішенні РНБО України від 01.03.2014 «Про невідкладні заходи щодо забезпечення національної безпеки, суверенітету і територіальної цілісності України» [20]. Важливість захисту критичної інфраструктури визначена у Стратегії національної безпеки України та низці рішень РНБО 2016–2017 рр. Значний поступ у нормативно-правовому регулюванні було зроблено після ухвалення Стратегії кібербезпеки України [21], Закону України «Про основні засади забезпечення кібербезпеки України» [19] та Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави [12].

Проблеми правового забезпечення кібербезпеки критичної інформаційної інфраструктури України досліджували О. Баранов, П. Гарасим, К. Бєляков, С. Божок, І. Діордіца, В. Ліпкан, Н. Коваленко, Б. Кормич, І. Кушнір, О. Малашко, Ю. Максименко, М. Микитюк, Л. Сопільник, М. Стрельбіцький, О. Тихомиров, О. Юдін та інші. Хоча їх роботи мають значну теоретичну та практичну цінність, у наукових і навчально-методичних джерелах зберігається низка дискусійних положень щодо правового забезпечення кібербезпеки критичної інформаційної інфраструктури.

Сучасні виклики та пріоритетні завдання сектору безпеки у сфері захисту критичної інфраструктури висвітлено в працях О. Суходолі [22]. Проблеми забезпечення інформаційної безпеки об’єктів критичної інфраструктури досліджували С. Гончар, Г. Леоненко, О. Юдін [23].

Питання управління безпекою та критичною інфраструктурою розробляли Д. Бірюков, Д. Бобро, Г. Ситник, А. Семенченко, О. Суходоля, В. Лядовська, С. Кондратов, С. Кулінська, В. Куйбіда, О. Насвіт та інші.

Базовим документом, який регламентує бачення і принципи формування Державної служби захисту критичної інфраструктури (ДСЗКІ), є Концепція створення державної системи захисту критичної інфраструктури, затверджена розпорядженням КМУкраїни від 6 грудня 2017 року № 1009-р. Окрім цього, важливим є проєкт Закону України «Про критичну інфраструктуру та її захист», який визначає основні підходи до державної політики у цій сфері. У ньому зазначено, що метою державної політики є забезпечення безперебійного та стійкого функціонування об'єктів КІ, запобігання несанкціонованому втручанню, прогнозування та відвернення кризових ситуацій, а також підвищення рівня безпеки та стійкості інфраструктурних об'єктів [24].

Україна за роки незалежності зробила суттєвий прогрес у сфері захисту КІ, зокрема, щодо адміністративно-правового регулювання. Важливою віхою стало ухвалення Концепції (основ державної політики) національної безпеки України [25], що стала фундаментом для подальших нормативно-правових актів у сфері національної безпеки. Пізніше з'явилися наукові праці, що підкреслювали важливість питань безпеки, включно із захистом об'єктів КІ [9, 26-30].

У подальші роки були ухвалені Конституція України, Закон «Про національну безпеку України», послання Президента, а також Закон України «Про основи національної безпеки України» (2003 р.) [31, 32], який замінив Концепцію 1997 року. У ньому було уточнено перелік сфер, що потребують захисту, зокрема інформаційну, енергетичну, екологічну, науково-технологічну тощо.

Важливим документом стала Стратегія національної безпеки України 2015 року, у якій уперше окремо визначено загрози безпеці критичної інфраструктури [31]. Ухвалено нову редакцію Закону України «Про національну безпеку України» 21 червня 2018 року № 2469-VIII, у якому значну увагу приділено питанням захисту критичної інфраструктури. Пізніше підготовлено проєкт Закону України «Про критичну інфраструктуру та її захист», покликаний сформувати

необхідну нормативно-правову базу у відповідній сфері [32, 33].

Закон України «Про критичну інфраструктуру» в його останній редакції № 3931-IX від 22.08.2024 – це ключовий нормативний акт, що створює національну систему захисту об’єктів, які забезпечують життєдіяльність держави (енергетика, транспорт, фінанси, ІТ, охорона здоров'я тощо), визначаючи операторів КІ, їх відповідальність, принципи державно-приватного партнерства та механізми реагування на загрози для забезпечення стійкості цих об'єктів до кібератак, диверсій та інших інцидентів, що важливо в умовах гібридної війни.

Згідно Закону, «об’єкти критичної інфраструктури – об’єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам» [34]. В Законі визначено оператори КІ як юридичні або фізичні особи, які управляють об’єктами КІ, несуть відповідальність за їх захист та функціонування, включаючи кібербезпеку, дано поняття Національна системи захисту КІ, принципи та Інструменти захисту, зокрема, впровадження паспортів безпеки, визначення відповідальних осіб, створення механізмів обміну інформацією. І лише у 2025 році затверджено Методики та Критерії і показники оцінки стану захищеності об’єктів КІ наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України, а саме 14 січня 2025 року [35].

Отже, нормативно-правове забезпечення критично важливої інфраструктури в Україні удосконалюється та розвивається управління безпекою об’єктів критичної інфраструктури.

1.3 Одеська обласна державна адміністрація як елемент критично важливої інфраструктури України

Одеська обласна державна (військова) адміністрація (ОВА) може бути віднесена до критично важливої інфраструктури України, адже саме її функціонування має стратегічне значення для забезпечення життєдіяльності,

безпеки та обороноздатності Одеського регіону, збої в її роботі можуть призвести до надзвичайних ситуацій та негативного впливу на економіку, енергетику та соціальну сферу.

ОВА координує роботу всіх галузей в області, включно з енергетикою, транспортом, охороною здоров'я, зв'язком та комунальним господарством [36]. В умовах військового стану ОВА відіграє ключову роль у координації оборонних заходів та забезпеченні стійкості регіону.

Одещина – це стратегічний південний форпост України з найбільшим портом у місті Одеса, важливими транспортними вузлами, зокрема, порти Південний, Чорноморськ, Рені, промисловістю, енергетикою та логістикою, критично важливим агросектором. Вона забезпечує експорт/імпорт, життєдіяльність регіону та держави, а також оборону й логістику для ЗСУ, особливо у контексті повномасштабної війни та "зернової" ініціативи, тому її стабільна робота – запорука економічної та безпекової стійкості України.

Необхідно ще раз наголосити на важливому геополітичному значенні Одещини через розташування біля Чорного моря, близько Молдови та Румунії, а також через статус ключового логістичного хабу. Це робить Одеську область стратегічно важливою для безпеки держави.

Одеська ОВА координує роботу всіх служб (медичних, соціальних, комунальних), що забезпечують життєдіяльність мільйонів мешканців регіону [37]. В умовах війни, робота Одеської ОВА та інфраструктури є життєво необхідною для стабільного функціонування економіки та забезпечення обороноздатності України.

Українське законодавство визначає об'єкти критичної інфраструктури як підприємства та установи, що є стратегічно важливими, і ОВА підпадає під ці критерії. Закон України «Про критичну інфраструктуру» та підзаконні акти, які визначають порядок віднесення об'єктів до критично важливих та їх категоризацію за рівнем критичності. Таким чином, ОВА є не просто адміністративним органом, а ключовим елементом системи забезпечення життєдіяльності та безпеки в регіоні, що автоматично відносить її до об'єктів

критичної інфраструктури.

Одеська обласна державна (військова) адміністрація як кожна державна адміністрація є місцевим органом виконавчої влади і належить до системи органів виконавчої влади України. В межах своїх повноважень державна адміністрація кожного рівня здійснює виконавчу владу на відповідній адміністративно-територіальній одиниці та громаді, а також реалізує делеговані повноваження, надані відповідною радою.

Для виконання своїх функцій в держадміністрації створено аппарат, департаменти, сектори та інші структурні підрозділи (рисунок 1.3) [39].

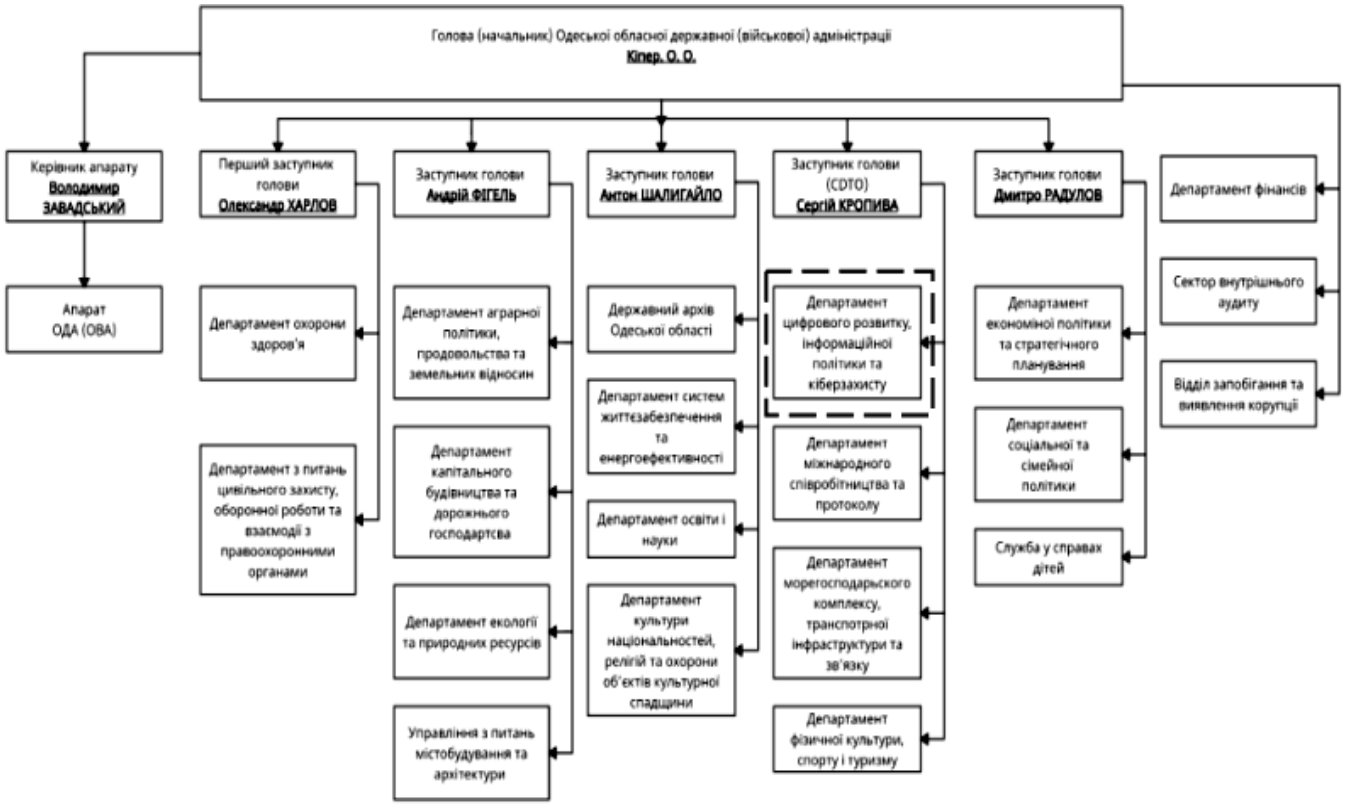

Рисунок 1.3 – Оргструктура Одеської ОВА

Місцеві держадміністрації забезпечують на своїй території виконання Конституції України, законів держави, актів Президента, Кабінету Міністрів та інших органів виконавчої влади; законність і правопорядок, дотримання прав та свобод громадян; підготовку, затвердження та виконання місцевих бюджетів; реалізацію загальнодержавних та регіональних програм соціально-економічного

розвитку, охорони довкілля та інших передбачених програм; звітність щодо виконання програм і бюджетів; взаємодію з різними органами місцевого самоврядування; здійснення інших повноважень, наданих державою або делегованих радами [36].

Деякі державні органи створюють власні регіональні представництва, взаємодія яких здійснюється на основі співпраці з обласною військовою держадміністрацією (ОВА). Це такі органи, зокрема, як Відділ Держгеокадастру в Одеській області, Відділ статистики, Державна податткова інспекція Головного управління ДФС в Одеській області, Відділ обслуговування громадян, Сервісний центр Пенсійного фонду України в Одеській області, Прокуратура, Головне управління Національної поліції в Одеській області, Відділ СБУ.

Департаменти облдержадміністрації здійснюють керівництво окремими галузями управління та відповідають за їх розвиток. Вони підзвітні та підконтрольні голові державної адміністрації, а також органам виконавчої влади вищого рівня. Кожен відділ має визначені функції та завдання.

Розгляд питань у державній адміністрації, що належать до її компетенції, зокрема щодо делегованих радою повноважень, проводиться головою адміністрації, його заступниками, керівником апарату, апаратом адміністрації, службами, комісіями, а також дорадчими, консультативними та іншими допоміжними органами, утвореними головою державної адміністрації.

Діяльність державної адміністрації та її структурних підрозділів є відкритою і прозорою, за винятком розгляду питань, що містять державну таємницю або конфіденційну інформацію, яка є власністю держави [39].

Обласна державна адміністрація інформує громадськість про свою діяльність, залучає громадян до проведення перевірок, підготовки та розгляду питань, що належать до її компетенції.

Формування планів роботи державної адміністрації здійснюється керівником апарату та відділом організаційної роботи апарату за пропозиціями структурних підрозділів, погодженими із заступниками голови відповідно до розподілу обов’язків. Плани роботи адміністрації включають заходи, спрямовані

на виконання законів України, актів Верховної Ради та Президента України, Кабінету Міністрів та органів виконавчої влади вищого рівня, доручень Президента і Прем'єр-міністра, реалізацію державних, обласних і районних програм соціально-економічного та культурного розвитку, а також здійснення інших визначених законами та делегованих обласною радою повноважень із реалізації державної політики.

Апарат обласної державної адміністрації у мирний час виконує відповідно до покладених на нього завдань планування та координацію роботи всіх структурних підрозділів адміністрації; ведення документації; підготовку та проведення нарад, зібрань, колегій та інших заходів. Апарат ОДА здійснює взаємодію зі засобами масмедіа, взаємодію від імені адміністрації з представницькими органами, зокрема щодо госпобслуговування. Апарат ОДА відповідальний за проведення прес-конференцій та організацію прийому громадян, контролює виконання як своїх, так і вищих державних рішень; контролює роботу зі скаргами та пропозиціями громадян; здійснює матеріально-технічне, кадрове, юридичне, інформаційне та фінансове забезпечення діяльності адміністрації [40]. В умовах воєнного стану з 24 лютого 2024 року всі основні фінкції незалежно від поточної ситуації апарат облдержадміністрації продовжує виконувати незмінно.

У процесі виконання своїх завдань апарат державної адміністрації взаємодіє зі структурними підрозділами адміністрації (див. рис. 1.3), територіальними органами центральних органів виконавчої влади, виконавчими апаратами міських та районних рад, виконавчими комітетами сільських і селищних рад [36].

Надання доручень працівникам апарату здійснюється головою державної адміністрації та керівником апарату; інші посадові особи адміністрації можуть видавати доручення тільки і завжди за погодженням із керівництвом.

Важливе місце органах державного управління займає автоматизація документообігу як складова широкого впровадження комп'ютерних інформаційних технологій у період інформаційної доби [41, 42]. Ключовим аспектом комп'ютеризації є створення системи «e-government», що передбачає:

– впровадження автоматизованих систем широкого призначення;

– створення веб-представництв органів урядування в інтернеті;

– поліпшення зв’язку між органами влади та громадянами.

Тому питання взаємодії адміністрації з кіберпростором та кіберзахисту інфраструктури сьогодні неймовірно актуальні.

Одеська обласна державна (військова) адміністрація – це тимчасовий орган державної влади**,** який є місцевим органом виконавчої влади, що діє замість Обласної державної адміністрації (ОВА) в умовах воєнного стану, забезпечуючи безпеку, оборону та життєдіяльність регіону. Вона виконує функції як ОВА, так і місцевого самоврядування, координуючи дії з військовим командуванням. Підпорядковується Президенту України та Генеральному штабу Збройних Сил України (у мирний час – Кабміну) [43].

Під час воєнного стану собливе значення Одеська ОВА має в підтримці обороноздатності регіону, зокрема, мобілізація усіх ресурсів, взаємодія з підрозділами та командуванням ЗСУ, Ради нацбезпеки і оборони та Нацгвардії України [2-3]. Основні задачі ОВА при цьому - це забезпечення безперебійного і стабільного функціонування об’єктів критичної інфраструктури області, до яких відносять порти, Укрзалізницю, медичні установи, енергетичну інфраструктуру, навчальні заклади, операторів зв’язку. Отже, ОВА в умовах сьогодення критично важливий стратегічний центр управління та захисту регіону.

У даному розділі роботи проаналізовано забезпечення інформаційної безпеки у сфері критичної інфраструктури України, зокрема, детально висвітлено термінологію з інформаційної безпеки, нормативно-правового забезпечення захисту критичної інфраструктури, наведено оргструктуру Одеської ОВА.

У результаті поставлено основні завдання на наступні розділи роботи:

- дослідження методів оцінювання CSA;
- розробка програмного засобу оцінювання рівня CSA співробітників;
- розробка рекомендацій по впровадженню заходів для підвищення рівня захищеності інформаційних ресурсів державної адміністрації.

2 КІБЕР-СИТУАЦІЙНА ОБІЗНАНІСТЬ ТА ДОСЛІДЖЕННЯ МЕТОДІВ ЇЇ ОЦІНЮВАННЯ

2.1 Кібер-ситуаційна обізнаність

Сучасний стрімкий розвиток інформаційних технологій суттєво змінює світовий порядок. Кіберпростір, будучи відкритим і вільним, розширює можливості людей, сприяє розвитку суспільства, глобального ринку ідей, наукових досліджень та інновацій, стимулює ефективність державного управління та активну участь громадян у вирішенні локальних і національних питань. Це забезпечує прозорість діяльності органів влади та сприяє запобіганню корупційним проявам.

Разом із цими перевагами, розвиток комп'ютерних технологій породжує нові, раніше невідомі загрози національній та міжнародній безпеці. Зокрема, окрім випадкових інцидентів природного походження, зростає кількість і потужність цілеспрямованих кібератак, що здійснюються окремими державами, групами чи особами [44].

Російська федерація, здійснивши широкомасштабне воєнне вторгнення в Україну, також веде активні дії в інформаційному просторі[45]. Це проявляється у незаконному зборі, використанні, поширенні та знищенні персональних даних, а також у здійсненні кібероперацій, крадіжок та шахрайства в інтернеті. Ці дії підтверджують транснаціональний характер кіберзлочинності, яка здатна завдавати значної шкоди інтересам суспільства, держави та міжнародної безпеки.

Забезпечення безпечного, стабільного та надійного кіберпростору можливе через підвищення цифрової грамотності громадян, формування культури безпеки в кіберпросторі, набуття комплексних знань і навичок для реалізації цілей кібербезпеки, а також шляхом впровадження державних та громадських проєктів, спрямованих на підвищення обізнаності суспільства щодо потенційних кіберзагроз і методів їхнього протидії.

Вимоги до кіберзахисту державних електронних інформаційних ресурсів, інформаційної інфраструктури та об'єктів критичної інфраструктури, до яких

належать органи держуправління, визначені законодавством і стандартами [46, 47]. Вони передбачають особливі вимоги до кібер-ситуаційної обізнаності співробітників державних органів щодо інформаційної та кібербезпеки шляхом проведення навчальних заходів, тренінгів та інших освітніх програм.

Сучасне поняття «ситуаційна обізнаність» означає здатність людей та техніки збирати інформацію про поточний стан системи або середовища і на основі цих даних формувати висновки щодо необхідних дій для уникнення помилок у майбутньому [4]. Завдання системи ситуаційної обізнаності полягає у забезпеченні автономного прийняття рішень інтелектуальною системою в умовах динамічного середовища.

Ситуаційна обізнаність забезпечує цілісне та конкретне уявлення про загрози і вразливості, дозволяючи організаціям своєчасно виявляти, обробляти та аналізувати інформацію в режимі реального часу. Вона також дає змогу точно оцінювати безпекову позицію підприємства та середовище загроз, що сприяє визначенню поточного й прогнозованого рівня ризику та ступеня захисту.

CSA(Cyber Situation Awareness) означає безпосереднє знання корисної, надлишкової та іншої релевантної інформації щодо діяльності в кіберпросторі, яке формується в результаті поєднання розвідувальної та оперативної діяльності у кіберпросторі та суміжних сферах [48].

Особливу увагу приділяють людині як найслабшій ланці кібербезпеки. Ситуаційна обізнаність дозволяє мінімізувати ймовірність людських помилок і зменшити заподіяні ними збитки. Фактично, вона стає ключовим елементом практик Infosec, оскільки забезпечує створення внутрішніх каналів обміну інформацією про загрози, що дозволяє попереджати ключових співробітників про потенційні загрози та сценарії атак.

Ситуаційна обізнаність надає організаціям змогу усвідомлювати поточний стан їхнього середовища та кіберпростору загалом. Отримана інформація сприяє групам реагування на інциденти у прийнятті обґрунтованих рішень щодо оптимальних заходів захисту від потенційних загроз та атак зловмисників або щодо реагування на них.

Кібер-ситуаційну обізнаність визначають як здатність аналітиків безпеки та осіб, які приймають рішення [49-51]:

– візуалізувати та оцінювати поточний стан IT-інфраструктури та захисну позицію IT-середовища;

– визначати ключові складові інфраструктури для виконання критичних функцій, ідентифікувати джерела та ключові показники шкідливої активності;

– прогнозувати можливі дії противника, здатні пошкодити найважливіші елементи IT-інфраструктури;

У моделі М.Ендслі виділяють три рівні ситуаційної обізнаності: сприйняття, розуміння та прогнозування (рисунок 2.1) [7]. Згодом, з урахуванням людського фактора та застосування поняття ситуаційної обізнаності у кіберпросторі, Б. Макгінесс [51] та С. Онвубіка і Т. Оуенс в [52] запропонували додатковий п’ятий рівень ситуаційної обізнаності – дію.

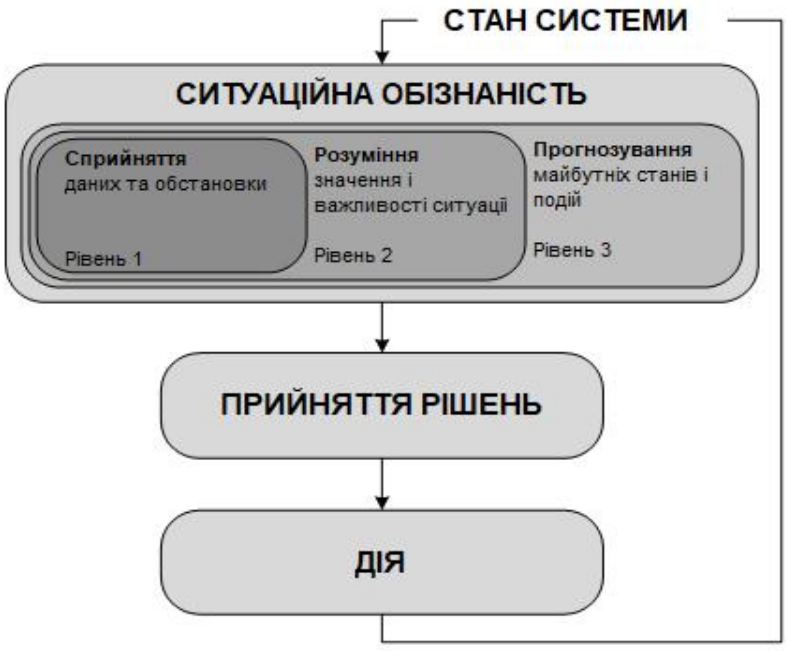

Рисунок 2.1 – Схема моделі Ендслі [7]

Рівень 1 – «Сприйняття даних та обставин». На цьому рівні аналітики інформаційної безпеки ідентифікують потенційно уразливі елементи системи захисту інформації. Це передбачає використання індивідуальних та незалежних

інструментів для моніторингу мережевої інфраструктури. Інформація про стан, атрибути та динаміку відповідних загроз як з внутрішнього, так і із зовнішнього середовища, дозволяє структурувати дані в значущі подання, що служать основою для наступних рівнів: розуміння, прогнозування та прийняття рішень.

Рівень 2 – «Розуміння ситуації». На цьому рівні аналітики кібербезпеки здійснюють агрегування, аналіз, узагальнення та зіставлення отриманих даних про загрози та інциденти в інформаційній системі. Саме розуміння забезпечує формування сценарію поточної ситуації, яку реалізують шляхом оцінки значущості доказів втручань та загроз, які підлягають моніторингу.

Рівень 3 – «Прогнозування майбутнього». Експерти з інформаційної безпеки на цьому рівні прогнозують потенційні події – методи та типи атак на інформаційну систему. Точність прогнозів підвищується за рахунок застосування сучасних систем моніторингу та технологій, здатних виявляти закономірності виникнення майбутніх подій та станів. Зокрема, використання систем раннього попередження атак дозволяє вдосконалити планування та впровадити профілактичні заходи для запобігання можливим інцидентам.

Рівні 4 та 5 – «Прийняття рішень» та «Дія». На п’ятому рівні рекомендують та реалізують адекватні контрзаходи, спрямовані на зменшення або усунення ризиків, пов’язаних із роботою інформаційних систем. Саме дія передбачає оперативне реагування та забезпечення ефективного контролю для підтримки інформаційної безпеки [52].

Модель інформаційної безпеки як формальне вираження політики безпеки передбачає вибір та обґрунтування базових принципів архітектури захищених комп’ютерних систем. Вони визначають механізми реалізації засобів та методів захисту інформації, ґрунтуючись на аналізі інформаційних потоків у системі.

Експертами відзначено, що більшість органів державного управління мають низький рівень захищеності інформаційних систем. Сучасна діяльність організацій потребує зберігання та обробки великих обсягів інформації, що стає можливим завдяки зниженню вартості обчислювальної потужності, збільшенню пропускної здатності мереж та розвитку систем зберігання даних. Разом із цим

зростають ризики витоку інформації, посилюється тиск регулюючих органів та підвищуються очікування зацікавлених сторін щодо безпеки інформації.

Ці тенденції підтверджуються результатами досліджень, які свідчать про недостатню обізнаність органів державного управління щодо стану інформаційної безпеки у власному середовищі. Зокрема, під час засідання постійної комісії з питань бюджету, фінансів та соціально-економічного розвитку директором Департаменту внутрішньої та інформаційної політики Одеської обласної державної адміністрації у доповіді про виконання Програми розвитку інформаційного забезпечення органів держуправління Одеського регіону на 2021–2025 роки підсумовано [40], що приблизно третина органів самоврядування мали негативний досвід втрат чи крадіжок інформації.

Співробітники органів державного управління повинні підтримувати високий рівень обізнаності щодо інформації, необхідної для функціонування їхньої організації. Усвідомлення загроз IT-безпеки дозволяє уникнути потенційних втрат інформаційних ресурсів. Для оцінки рівня розуміння та ефективності діяльності співробітників керівництву доцільно проводити вимірювання обізнаності про інформаційну безпеку. Результати такого вимірювання слугуватимуть базою для визначення того, чи відповідає обізнаність співробітників очікуванням організації.

Органи державного управління оперують великими обсягами інформації та володіють значними обчислювальними потужностями. Вони також забезпечують відносно відкритий доступ до своїх інформаційних ресурсів для громадськості. Поєднання цих факторів робить державні установи вразливими до кібератак [54]. Проблеми безпеки та конфіденційності інформаційних систем у сфері державного управління залишаються актуальними навіть при наявності сучасних стандартів безпеки, передових методів управління інформаційними системами та технічного забезпечення.

Разом із цим, лише частина організацій забезпечує прийнятні заходи безпеки інформаційних систем і проводить належну підготовку співробітників щодо підвищення CSA. Фактично більшість фахівців із безпеки інформаційних

систем зосереджують увагу на технічних аспектах захисту – таких як брандмауери, маршрутизатори чи програмне забезпечення для виявлення вторгнень – і відповідних рішеннях. Водночас соціяльно-організаційні аспекти, зокрема ризики, пов’язані з недостатньою обізнаністю кінцевих користувачів інформаційних систем, зазвичай залишаються поза увагою.

2.2 Можливості тестування як методу оцінювання кібер-ситуаційної обізнаності співробітників

Перш ніж розглядати особливості оцінювання рівня CSA, доцільно з’ясувати сутність поняття «оцінювання». Ефективне та змістовне оцінювання співробітників можливо лише за умови застосування об’єктивних методів і методик, розроблених на їх основі, які орієнтовані на досягнення конкретних цілей, вирішення завдань та забезпечення результативності процесу.

У системах оцінювання співробітників державної обладміністрації можна застосовувати різні методи та методики з певними техніками (рисунок 2.2).

Рисунок 2.2 – Схема оцінювання

Під методом оцінювання персоналу розуміють сукупність визначених теоретико-методологічних підходів оцінки якостей, поведінки та ефективності роботи співробітника. Вибір конкретного методу оцінки залежить від

характеристик цієї системи [5].

Під технікою оцінювання розуміють спосіб збору, зберігання та аналізу інформації, що слугує підставою для встановлення оцінки. Техніку визначають за відповідними інструкціями, які передбачають використання певних інструментів для збору, зберігання та аналізу інформації.

Залежно від виконання конкретних функцій оцінки в обласній держадміністрації виділяють три основні види: попереднє, поточне й підсумкове оцінювання.

Попередня оцінка містить діагностичні задачі, її проводять перед початком вивчення стану обізнаності. Його мета – визначити початковий рівень CSA, фактичні знання, вміння та навички, пов’язані з комп’ютерною грамотністю. Попередня діагностика дозволяє визначити приріст знань та навичок співробітника протягом період часу.

Поточне оцінювання – це систематична перевірка та оцінювання результатів роботи співробітника за окремими темами або напрямами.

Підсумкове оцінювання – це комплексна перевірка перед закінченням курсу з кібербезпеки з перевіркою отриманих результатів із усіх ключових напрямів навчання.

Для діагностики знань співробітників розробляють спеціальні методи, використовують різні форми та методи оцінювання знань:

- письмова перевірка знань чи письмова робота;
- усна перевірки знань чи усне опитування;
- перевірки практичної роботи з комп'ютером;
- ігрові методи (гейміфікація) оцінювання;
- самооцінювання;
- тестування;
- інтерв'ю.

Для оцінювання CSA співробітників держадміністрації у роботі застосовано метод тестування як дослідження, що здійснюється шляхом діагностування знань, вмінь та навичок на основі виконання стандартизованих завдань. Тести ефективно

використовуються на всіх етапах процесу навчання та дозволяють здійснювати попередній, поточний та підсумковий контроль рівня співробітників щодо різних аспектів конкретної ситуації.

Систематична перевірка знань сприяє не лише ефективному засвоєнню нових відомостей, а й формує свідоме ставлення до роботи, дисциплінованість, працьовитість та цілеспрямованість. Крім того, вона активізує увагу та розвиває аналітичні здібності.

Використання тестового контролю забезпечує рівні умови перевірки для всіх співробітників, що підвищує об’єктивність оцінювання знань.

Система комп'ютерного тестування є зручною для оцінювання знань співробітників, оскільки вона дозволяє уникнути витрат робочого часу на усні відповіді та оперативно реагувати на різні ситуації. Доцільно організовувати централізований збір і обробку одержаних результатів при наявності в організації інтернету.

Розрізняють такі традиційні типи тестових завдань:

– вписування або введення правильної відповіді з клавіатури;
– вибір відповіді з набору заданих варіантів (одного або кількох);
– встановлення відповідності між елементами;
– визначення правильної послідовності;
– вибір фрагмента з графічної ілюстрації.

Практика тестового оцінювання реально свідчить, що ключовим етапом є підготовка тестів. Кожне запитання має бути змістовним і структурованим відповідно до мети оцінювання.

Спираючись на принципи комп’ютерного тестування, розроблено пробні тестові завдання для оцінювання CSA співробітників Одеської обласної державної адміністрації. Запропоновано 30 питань з інформаційної та кібербезпеки. Деякі відповіді працівників вказують на високий рівень обізнаності та правильні методи забезпечення безпеки, тоді як інші демонструють недостатню обізнаність, ненавмисну недбалу поведінку чи проведення діяльності з підвищеним ризиком.

Комп’ютерне тестування володіє такими перевагами порівняно з традиційно визнаними формами контролю [55]:

– швидке отримаання результатів та звільнення співробітників, що організовують оцінювання, від рутинного оброблення результатів;

– індивідуалізація самого процесу;

– психологічний комфорт співробітників;

– підвищення об’єктивності оцінки рівня знань;

– за потреби конфіденційність тестування;

– більший інтерес порівняно з традиційними формами опитування;

– можливість використання технічних засобів;

– оперативність;

– виключення впливу зовнішніх факторів, таких як настрій або рівень кваліфікації;

– універсальність та охоплення всих стадій робочого процесу;

– контроль за великим обсягом процесу;

– зменшення часу на оцінювання приблизно на 50% порівняно з традиційним опитуванням.

Результати тестування дозволяють виявити слабкі місця у підготовці співробітників та визначити пріоритети для подальшого навчання і підвищення CSA. На основі отриманих даних можна розробити рекомендації щодо вдосконалення заходів безпеки та формування культури кібербезпеки у державній адміністрації.

Цей тест для оцінки обізнаності співробітників у сфері безпеки розроблено з метою з’ясувати, як працівники реагують на конкретні ситуації та питання, пов’язані з інформаційною безпекою та загрозами кібербезпеці.

Кожній відповіді присвоєно одне з трьох значень CSA: обізнаність, необізнаність або невизначеність.

На рисунку 2.3 зображено схему алгоритму проведення опитування згідно розроблених тестових завдань.

Зразок тестових завдань, складених у даній роботі, наведено на рисунку 2.4.

Рисунок 2.3 – Схема алгоритму проведення опитування

У роботі [56] запропоновано оцінювання рівня культури інформаційної безпеки організації шляхом визначення рівня саме культури з врахуванням персональних показників співробітників, актуальних ризиків та нормативних вимог до ведення безпечної діяльності, а не їх обізнаності.

3. Чи зв'язуетесь ви із адміністратором безпеки в разі злому або зараження комп'ютера?
А) Так, я повідомляю про злом або зараження робочого ПК
Б) Ні, я вирішую проблему злому або зараження робочого ПК самостійно
В) Я не знаю, з ким зв'язатися в разі злому або зараження комп'ютера

4. Ви коли-небудь знаходили вірус або троян на вашому комп'ютері на роботі?
А) Так, мій комп'ютер був заражений раніше
Б) Ні, мій комп'ютер ніколи не був заражений
В) Я не знаю, що таке вірус або троян

5. Ви проводите періодичну перевірку комп'ютеру за допомогою антивірусу для профілактики злому або зараження?
А) Так, проводжу.
Б) Ні, не проводжу.
В) Я не знаю, як проводити перевірку.

6. Чи користуетесь ви парольним захистом на вашому робочому комп'ютері?
А) Так, користуюсь
Б) Ні, не користуюсь
В) Я не знаю, як встановити парольний захист.

7. Ви коли-небудь давали свій пароль з роботи комусь іншому?
А) Так
Б) Ні
В) Я не маю паролю.

8. Якщо ви форматуєте жорсткий диск або стираєте файли на ньому, вся інформація про нього назавжди втрачається?
А) Правильне твердження
Б) Хибне твердження
В) Я не впевнений

Рисунок 2.4 – Зразок тесту для оцінювання CSA співробітників

2.3 Використання методу аналізу ієрархії

У рамках даного дослідження для знаходження експертних оцінок використано метод аналізу ієрархій та його практичне застосування.

Особа, що приймає рішення(ОПР) при визначенні експертних оцінок часто спирається лише на інтуїтивні уявлення, що впливає на якість та характер прийнятих рішень.

Математичним інструментом системного підходу до складних проблем прийняття рішень є метод аналізу ієрархій (МАІ) [57], широко визнаний науковцями. МАІ не гарантує "правильного" рішення, але дозволяє обрати варіант, що найкращим чином узгоджується з розумінням суті проблеми та вимогами до її вирішення. Метод аналізу ієрархій запропоновано американським математиком Томасом Сааті.

В основі MAI використано порівняння обраних альтернатив (рисунок 2.5). Суть цього методу полягає у представленні експертами певної проблеми за допомогою ієрархії критеріїв та підпорядкованих критеріям альтернатив [6].

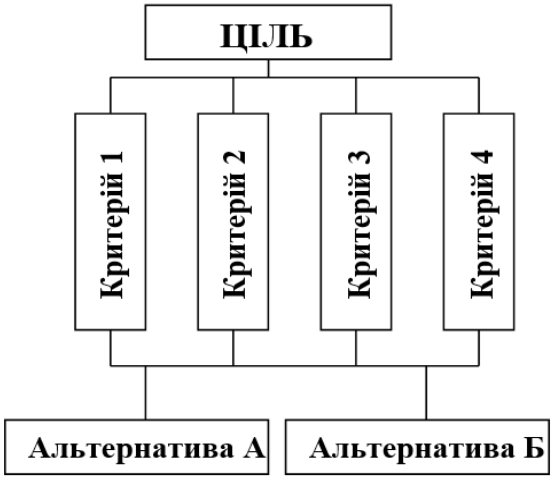

Рисунок 2.5 – Дерево критеріїв та альтернатив за Сааті

Етапи застосування методу для подальшої їх реалізації подані нижче .

1. Постановка завдання та визначення мети.

2. Визначення основних критеріїв та підпорядкованих альтернатив.

3. Побудова ієрархії: дерево від мети через критерії до альтернатив.

4. Побудова матриці парних порівнянь критеріїв за цілями та альтернатив за критеріями.

5. Застосування визначеного способу аналізу одержаних матриць.

6. Визначення ваги кожної альтернативи за системою ієрархії.

Необхідність формування декількох критеріїв визначається оцінкою рівня обізнаності. Застосування багатокритеріального підходу для оцінювання загроз кібербезпеці зумовлене отриманням найточніших результатів дослідження. Даний підхід експертного оцінювання застосований для аналізу CSA співробітників обласної державної адміністрації.

При оцінці CSA виникає проблема визначення поведінки в ситуаціях, що можуть завдати найбільшої шкоди. Для її вирішення необхідно виявити

найвідповідніші варіанти відповідей і проранжувати їх щодо визначених критеріїв оцінки.

У випадку, заявленому у даній роботі, ієрархічну модель системи кібербезпеки розглядають як цілеспрямовану інформаційно-управлінську структуру з урахуванням ієрархічних рівнів організації. На першому рівні – кібер-ситуаційна обізнаність, на другому – основні на наш погляд сфери кіберзахисту, а на останньому рівні ієрархії – конкретні рівні кіберобізнаності [4]. У даній роботі виділені наступні сфери кіберзахисту і відповідні критерії їх оцінки, враховуючи експертні судження та певний практичний досвід.

Обрано такі критерії (сфери кіберзахисту):

- соціальна інженерія (а);
- управління доступом (б);
- загрози від вірусів, троянів, ransomware (в);
- захист від шкідливого програмного забезпечення (г);
- фізична безпека (д);
- безпечне використання службових комп'ютерів, планшетів, телефонів(е);
- безпечна робота з інформацією (є);
- безпека хмарних сховищ (ж);
- реагування на інциденти (з);
- політика інформаційної безпеки установи (и).

Функції управління в моделі розподілено між підпорядкованими рівнями, а організація системи загалом підпорядкована головній меті – забезпеченню визначеного рівня кібербезпеки. При цьому важатимемо, що елементи кожного рівня незалежні. Крім того, ієрархія будуватиметься від верхнього рівня вниз.

Для відповідей (альтернатив) скористаємось засобами моделі AIU (Awareness, Ignorance, Uncertainty) – обізнаність, необізнаність, невизначеність.

Ієрархічна модель оцінки CSA співробітників може бути представлена наступним чином: верхній рівень моделі відповідає загальній кібер-ситуаційній обізнаності, середній рівень – охоплює основні сфери кіберзахисту, а нижній рівень – деталізує конкретні рівні обізнаності співробітників.

Така структура дозволяє системно оцінювати знання, навички та поведінку персоналу в умовах кіберзагроз та забезпечує ефективне ранжування варіантів дій відповідно до критеріїв безпеки (рисунок 2.6).

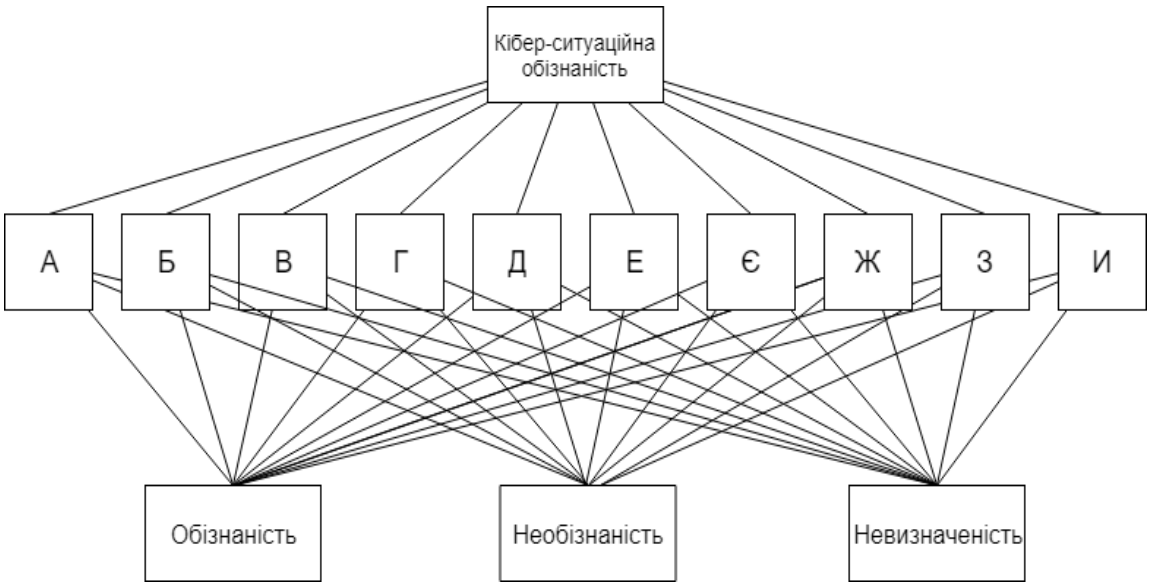

Рисунок 2.6 – Ієрархічна модель оцінки CSA

Модель є спрощеною – залежно від завдання можна було б додавати більше елементів та рівнів. Вона відображає наше розуміння проблеми CSA співробітників державної адміністрації.

Після побудови ієрархічної моделі згідно MAI приступають до визначення вагів критеріїв. У загальному випадку оцінювання експерта визначають так: нехай задано деяку множину $A=\{A_h\}$, $h=(1,k)$, це альтернативи, що мають бути порівнянними з деякою визначеною множиною C_n критеріїв для обчислення відносних коефіцієнтів значущості w_h.

Причому ці коефіцієнти мають обов'язково задовольняти умову такого рівняння нормування $\sum w_h=1$ [58]. Далі елементи з множини альтернатив $A=\{A_h\}$, де $h=(1,k)$ необхідно порівняти попарно експертами-аналітиками з множини E_I для того, щоб одержати вектор парних порівнянь $D=\{d_{ij}\}$, $i,j=(1,k)$.

Таким чином, отримаємо квадратну матрицю парних порівнянь, що є наслідком парних порівнянь елементів множини альтернатив (таблиця 2.1).

Таблиця 2.1 – Парні порівняння

	A_1	A_2	A_3	…	A_n
A_1	$\frac{w_1}{w_1}$	$\frac{w_1}{w_2}$	$\frac{w_1}{w_3}$	…	$\frac{w_1}{w_n}$
A_2	$\frac{w_2}{w_1}$	$\frac{w_2}{w_2}$	$\frac{w_2}{w_3}$	…	$\frac{w_1}{w_n}$
A_3	$\frac{w_3}{w_1}$	$\frac{w_3}{w_2}$	$\frac{w_3}{w_3}$	…	$\frac{w_3}{w_n}$
…	…	…	…	…	…
A_n	$\frac{w_n}{w_1}$	$\frac{w_n}{w_2}$	$\frac{w_n}{w_3}$	…	$\frac{w_n}{w_n}$

На основі експертних оцінок були сформовані матриці попарних порівнянь критеріїв та альтернатив за визначеними критеріями, що дозволило встановити їх пріоритети. Порівняння здійснювалися за шкалою пріоритетів, запропонованою самим Томасом Сааті (від 1 до 9) [59].

Причому матриця може містити вектори – лише один рядок або один стовпець. Квадратна матриця характеризується однаковою кількістю рядків і стовпців та має додаткові корисні властивості, зокрема власні вектори і власні значення. Використання саме таких обчислень дозволяє кількісно визначати порівняльну важливість факторів або результатів у певній проблемній ситуації. Фактори з найбільшими величинами важливості отримують пріоритетну увагу та вагу під час вирішення проблеми або розробці плану дій.

Із врахуванням різнорідності критеріїв оцінки експертами-аналітиками виставляться за шкалою відносної важливості. Ось приклад, при порівнянні відносних ваг критеріїв оцінки, коли дано критерій A з вагою W_A і критерій $Б$ з вагою $W_Б$, тоді відношення критерію A до $Б$ заносять у матрицю W_A / $W_Б$. Зворотну величину $W_Б$, / W_A заносять в цю матрицю як відношення критерію $Б$ до критерію A [24] (таблиця 2.2).

Таблиця 2.2 – Шкала пріоритетів [59]

Ступінь важливості	Визначення	Коментар
1	Порівнянна важливість	Обидва критерії вносять рівнозначний внесок
3	Деяке переважання значущості одного критерію над іншим	Досвід і знання дають малу перевагу одному критерію перед іншим, але судження не є достатньо переконливі
5	Значна перевага одного критерію над іншим	Є вірогідні дані чи логічні міркування для відображення переваги одного з критеріїв
7	Дуже велика очевидна перевага	Переконливі дані про перевагу одного з критеріїв. Перевагу видно практично
9	Абсолютна перевага	Явні свідчення про перевагу одного критерію перед іншим, вони надзвичайно переконливі
2,4,6,8	Проміжні значення між переліченими ступенями шкали	Ситуації, у якій необхідне компромісне рішення між рівнями
Зворотні величини значень	При протилежному порівнянні обирають зворотнє значення	У випадках зазначення узгодженості при утворенні матриці, отриманні *N* значень

Відповідно до узгодження порівнюють відносну важливість елементів ліворуч від діагоналі матриці щодо елементів над діагоналлю (див. табл. 2.1). Якщо елемент ліворуч від діагоналі важливіший за елемент над діагоналлю, у матрицю заносять ціле датнє число від 1 до 9; в протилежному випадку використовують зворотнє значення (дріб). Важливість елемента порівняно з самим собою дорівнює 1, тому діагональ матриці заповнена одиницями. Симетричні клітинки заповнюються оберненими значеннями: якщо елемент *А* вважають «злегка більш важливим» за елемент *Б* (3 на шкалі), то елемент *Б* «злегка менш важливий» за елемент *А* (1/3 на шкалі).

Для отримання колективних оцінок у процесі обробки експертної інформації застосовуватимемо алгебраїчний метод.

Одним із найефективніших способів вирішення цієї задачі є обчислення середнього геометричного. Для цього елементи кожного рядка перемножуються,

після чого здобувається корінь ступеню n, тут n – кількість елементів. Далі цей стовпик чисел нормалізують шляхом ділення кожного числа на суму всіх чисел. Альтернативний підхід передбачає нормалізацію елементів кожного стовпця матриці, а потім усереднення значень по рядках. Це дозволяє знайти порядок пріоритетів кожного елемента та конкретне значення його пріоритету.

Компонента власного вектора першого рядку матриці попарних порівнянь дорівнює [59]:

$$\sqrt[4]{\left(\frac{w_1}{w_1}\right)\times\left(\frac{w_1}{w_2}\right)\times\left(\frac{w_1}{w_3}\right)\times\left(\frac{w_1}{w_4}\right)}. \qquad (2.1)$$

Після визначення компонент власного вектора для всіх n рядків стає можливим їх подальше використання у розрахунках. Для цього обчислюється вектор пріоритетів – головний власний вектор матриці, який після нормалізації перетворюється на вектор пріоритетів (таблиця 2.3).

Таблиця 2.3 – Обчислення вектору пріоритетів [57]

Матриця парних порівнянь					Обчислення власного вектора		Нормалізація результату для вектора пріоритетів
	A_1	A_2	A_3	A_4		Знайти суму стовпців й нормалізувати	
A_1	$\frac{w_1}{w_1}$	$\frac{w_1}{w_2}$	$\frac{w_1}{w_3}$	$\frac{w_1}{w_4}$	$\sqrt[4]{\left(\frac{w_1}{w_1}\right)\times\left(\frac{w_1}{w_2}\right)\times\left(\frac{w_1}{w_3}\right)\times\left(\frac{w_1}{w_4}\right)}=a$		$\frac{a}{сума}=x_1$
A_2	$\frac{w_2}{w_1}$	$\frac{w_2}{w_2}$	$\frac{w_2}{w_3}$	$\frac{w_2}{w_4}$	$\sqrt[4]{\left(\frac{w_2}{w_1}\right)\times\left(\frac{w_2}{w_2}\right)\times\left(\frac{w_2}{w_3}\right)\times\left(\frac{w_2}{w_4}\right)}=b$		$\frac{b}{сума}=x_2$
A_3	$\frac{w_3}{w_1}$	$\frac{w_3}{w_2}$	$\frac{w_3}{w_3}$	$\frac{w_3}{w_4}$	$\sqrt[4]{\left(\frac{w_3}{w_1}\right)\times\left(\frac{w_3}{w_2}\right)\times\left(\frac{w_3}{w_3}\right)\times\left(\frac{w_3}{w_4}\right)}=c$		$\frac{c}{сума}=x_3$
A_4	$\frac{w_4}{w_1}$	$\frac{w_4}{w_2}$	$\frac{w_4}{w_3}$	$\frac{w_4}{w_4}$	$\sqrt[4]{\left(\frac{w_4}{w_1}\right)\times\left(\frac{w_4}{w_2}\right)\times\left(\frac{w_4}{w_3}\right)\times\left(\frac{w_4}{w_4}\right)}=d$		$\frac{d}{сума}=x_4$

Множення матриці парних порівнянь критеріїв та альтернатив за цими критеріями на вектор пріоритетів проводять так (2.2) :

$$\begin{pmatrix} \frac{w_1}{w_1} & \frac{w_1}{w_2} & \frac{w_1}{w_3} & \frac{w_1}{w_4} \\ \frac{w_2}{w_1} & \frac{w_2}{w_2} & \frac{w_2}{w_3} & \frac{w_2}{w_4} \\ \frac{w_3}{w_1} & \frac{w_3}{w_2} & \frac{w_3}{w_3} & \frac{w_3}{w_4} \\ \frac{w_4}{w_1} & \frac{w_4}{w_2} & \frac{w_4}{w_3} & \frac{w_4}{w_4} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{matrix} \frac{w_1}{w_1} \cdot x_1 + \frac{w_1}{w_2} \cdot x_2 + \frac{w_1}{w_3} \cdot x_3 + \frac{w_1}{w_4} \cdot x_4 = Y_1; \\ \frac{w_2}{w_1} \cdot x_1 + \frac{w_2}{w_2} \cdot x_2 + \frac{w_2}{w_3} \cdot x_3 + \frac{w_2}{w_4} \cdot x_4 = Y_2; \\ \frac{w_3}{w_1} \cdot x_1 + \frac{w_3}{w_2} \cdot x_2 + \frac{w_3}{w_3} \cdot x_3 + \frac{w_3}{w_4} \cdot x_4 = Y_3; \\ \frac{w_4}{w_1} \cdot x_1 + \frac{w_4}{w_2} \cdot x_2 + \frac{w_4}{w_3} \cdot x_3 + \frac{w_4}{w_4} \cdot x_4 = Y_4. \end{matrix} \quad (2.2)$$

З матрицею даного вигляду одержуємо, що справді елементи x_1 , x_2 , x_3 *та* x_4 є відповідно відносні коефіцієнти значущості w_1, w_2, w_3 та w_4.

Виходячи з відношення w_1/w_2 і визначаємо кожен компонент власного вектора.

Важливо зауважити, що в одержаній матриці суджень відсутнє відношення виду w_1/w_2, тут є лиш цілі числа чи ж їх обернені величини зі шкали. Дана матриця в загальному випадку не є узгодженою. Алгебраїчна задача у випадку узгодженості полягає у розв'язанні рівняння $Aw = w_n$, а завдання із оберненосиметричними судженнями – у розв'язанні рівняння $A'w' = \lambda_{max} w'; A' = (a)$, де λ – це найбільше власне значення матриці суджень A [5].

Матриця порівняння критеріїв – експертна матриця пріоритетності розміром 10x10 наведена у таблиці 2.4 .

Після одержання матриць порівняння та парних суджень далі потрібно визначити оцінки альтернатив. На наступному кроці виконаємо порівняння заданих альтернатив за визначеними критеріями.

У таблиці 2.5 подано матрицю порівняння за одним з критеріїв – «Фізична безпека». Аналогічно проведено оцінку альтернатив за кожним із решти критеріїв та побудовано відповідні матриці порівнянь критеріїв та матриці порівняння альтернатив за визначеними критеріями.

Таблиця 2.4 – Порівняння критеріїв

	а	**б**	**в**	**г**	**д**	**е**	**є**	**ж**	**з**	**и**
а	1	2	1/7	1/5	1/6	1/5	1/5	1/2	5	1/5
б	1/2	1	3	1	1/5	3	1	1	5	1
в	7	1/3	1	1	1/5	1	1	1/6	1/3	1/7
г	5	1	1	1	1/5	1/5	1/3	1/4	3	1/6
д	6	5	5	5	1	1	5	1	6	2
е	5	1/3	1	5	1	1	3	1/3	5	1/3
є	5	1	1	3	1/5	1/3	1	1	5	1
ж	2	1	6	4	1	3	1	1	5	1
з	1/5	1/5	3	1/3	1/6	1/5	1/5	1/5	1	1/4
и	5	1	7	6	1/2	3	1	1	4	1

Таблиця 2.5 – Порівняння альтернатив за критерієм «Фізична безпека»

«Фізична безпека»	Обізнаність	Необізнаність	Невизначеність
Обізнаність	1	7	5
Необізнаність	1/7	1	1/3
Невизначеність	1/5	3	1

Зокрема, побудовано відповідні матриці порівнянь соціальної інженерії; управління доступом; загрози від вірусів, троянів, ransomware; захисту від шкідливого програмного забезпечення; безпечне використання службових комп'ютерів, планшетів, телефонів; безпечна робота з інформацією; безпеки хмарних сховищ, реагування на інциденти, політики інформаційної безпеки установи, використання особистих пристроїв.

Наступним кроком методу аналізу ієрархій є саме аналіз одержаних матриць. Отже, знаходимо суму елементів кожного стовпця за формулою (2.3):

$$S_j = a_{1j} + a_{2j} + \cdots + a_{nj} . \quad (2.3)$$

На наступному кроці виконують ділення кожного елемента матриці на суму елементів відповідного стовпця за формулою (2.4):

$$A_{ij} = \frac{a_{ij}}{s_j}. \quad (2.4)$$

Після цього формують проміжну матрицю, де обчислюють середнє значення для кожного рядочка. Саме одержаний стовпчик і задає ваги критеріїв та альтернатив процесу.

Матрицю ваги альтернатив та матрицю ваги критеріїв, наведені у таблицях 2.6 та 2.7, формують на основі отриманих з обчислень даних.

Таблиця 2.6 – Ваги альтернатив

Кібер-ситуаційна обізнаність	Обізнаність	Необізнаність	Невизначеність
Обізнаність	0,74	0,63	0,78
Необізнаність	0,11	0,09	0,05
Невизначеність	0,14	0,26	0,15

Таблиця 2.7 – Ваги параметрів за Сааті

Критерій	Вага
Соціальна інженерія	0,22
Управління доступом	0,14
Загрози від вірусів, троянів, ransomware	0,05
Захист від шкідливого програмного забезпечення	0,05
Фізична безпека	0,05
Безпечне використання службових комп'ютерів, планшетів, телефонів	0,11
Безпечна робота з інформацією	0,09
Безпека хмарних сховищ	0,10
Реагування на інциденти	0,15
Політика інформаційної безпеки установи	0,03

Таким чином, у результаті застосування методу аналізу ієрархій визначено у дослідженні експертну оцінку CSA (таблиця 2.8).

Таблиця 2.8 – Оцінка CSA

Кібер-ситуаційна обізнаність	Середнє
Обізнаність	0,71
Необізнаність	0,09
Невизначеність	0,19

Метод аналізу ієрархій дозволяє перевіряти узгодженість експертних оцінок, тобто чисел у матрицях попарних порівнянь. Для цього знаходять дві взаємопов'язані характеристики, перша з яких – індекс узгодженості (I_y). Його знаходять з формули:

$$I_y = \frac{\lambda_{max} - n}{n-1}, \qquad (2.5)$$

де: n – порядок матриці,

λ_{max} –найбільше власне число матриці.

Також для перевірки узгодженості експертних оцінок використовують відношення узгодженості (B_y) (2.6):

$$B_y = \frac{I_y}{M(I_y)}, \qquad (2.6)$$

де: $M(I_y)$ – середнє значення індексу узгодженості матриці парних порівнянь (таблиця 2.9).

Таблиця 2.9 – Індекс узгодженості матриці

n	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
$\mathbf{P_n}$	0	0	0.59	0.91	1.13	1.25	1.33	1.42	1.46	1.49

Узгодженість експертних оцінок CSA співробітників для критерію «фізичний захист» зображено на рисунку 2.7.

Фізичний захист	Обізнаність	Необізнаність	Невизначеність
Обізнаність	1	7	5
Необізнаність	1/7	1	1/3
Невизначеність	1/5	3	1

$\lambda_{max} = 3{,}06$.

$I_y = 0{,}03$

$B_y = 0{,}052$ – матриця узгоджена.

Рисунок 2.7 – Узгодженість оцінок CSA

Аналогічно перевірено узгодженості експертних оцінок CSA співробітників для кожного з обраних критеріїв. Відомо [57], що позитивна обернено-симетрична матриця узгоджена тоді і лише тоді, коли порядок матриці та її найбільше власне максимальне число свівпадають (тобто $n = \lambda_{max}$). В неузгоджених обернено-симетричних матрицях $\lambda_{max} \neq n$, і практично $\lambda_{max} > n$ а отже $I_y > 0$ та $B_y > 0$. На практиці ж вважають, що, якщо $B_y \leq 0{,}1$, то можна бути задоволеним ступенем узгодженості матриці. У нашому випадку для критерію «фізичний захист» отримали значення $\lambda_{max} = 3.06$, $I_y = 0.03$, $B_y = 0.052$. Отже, матриця є узгодженою і маємо експертну оцінку рівня CSA співробітників.

У цьому розділі розглянуто поняття CSA та вимоги до розробки тестових завдань. За допомогою методу аналізу ієрархій (MAI) одержано такі матриці – порівняння обраних із сфери кібербезпеки критеріїв, порівняння заданих альтернатив за обраним критерієм, а також визначено ваги альтернатив і критеріїв. На основі цих даних отримано експертну оцінку рівня CSA співробітників. Знайдено найбільше власне число матриці парних порівнянь, індекс узгодженості, відношення узгодженості. Отже, експертні оцінки узгоджені.

Наступним кроком є розробка програмного застосунку для оцінювання CSA, а також визначення заходів і рекомендацій щодо його впровадження.

3 РЕАЛІЗАЦІЯ ПРОГРАМНОГО ЗАСТОСУНКУ ОЦІНЮВАННЯ КІБЕР-СИТУАЦІЙНОЇ ОБІЗНАНОСТІ

3.1 Обгрунтування вибіру програмних засобів реалізації

Для реалізації оцінювання CSA було обґрунтовано використання декількох програмних засобів, одним із яких є мова програмування Python.

Python використовують як інтерпретовану мову скриптів різного призначення. Вона має синтаксис, наближений до псевдокоду, що дозволяє зменшити обсяг коду та спрощує опис завдань. Початок створення мови припадає на кінець 1980их років, а реалізував ідеї Гвідо ван Россум [60]. Елегантний та структурований синтаксис Python сприяє ефективній командній роботі над програмним кодом.

Розглянемо основні переваги мови Python та порівняємо її з іншими сучасними мовами програмування. При виборі мови програмування важливо враховувати такі критерії:

− простота у вивченні;

− зрозумілість коду;

− висока швидкість розробки;

− сучасність;

− інтерактивність.

Python – високорівнева мова програмування, що використовується по всьому світу як у навчанні, так і в промислових проектах, і останнім часом набуває дедалі більшої популярності серед розробників.

Природно виникає питання – чому Python настільки популярний і чому саме його варто використовувати. Для багатьох головною перевагою є легкість читання коду, який зазвичай компактніший, ніж на інших мовах програмування. На різних форумах Python описують як «правильний вибір», оскільки код на ньому легше читається, містить лише необхідні інструкції та економить фахівцю час на розв’язання задач.

Обсяг програмного коду на Python зазвичай становить лише третину або

навіть п’яту частину еквівалентного коду на C++ або Java, що зменшує час на введення, налагодження та супровід програми. Значною перевагою є також обов’язкове використання відступів, що привчає писати акуратний код.

Для запуску програми на Python не потрібна проміжна компіляція і зв’язування, як у C або C++: інтерпретатор виконують код негайно, дозволяючи працювати в інтерактивному режимі і швидко отримувати результати змін.

Крім того, Python оснащений потужними вбудованими інструментами. Стандартна бібліотека надає дуже багато можливостей, а розширення, наприклад NumPy, забезпечує об’єкти масивів, доступ до математичних бібліотек і підтримку паралельних обчислень, створення анімацій та тривимірних об’єктів та багато іншого.

Сучасність мови підтверджується її використанням відомими компаніями:

- компанія Google широко використовує Python у своїй пошуковій системі і оплачує працю автора Python;
- служба колективного використання відеоматеріалів YouTube в значній частині реалізована на Python;
- популярний застосунок BitTorrent для обміну файлами написаний на Python;
- такі компанії, зокрема, як Intel, Hewlett-Packard використовують Python для тестування програм;
- і NSA використовує Python для шифрування та аналізу розвідданих.

Python є однією восьми найпопулярніших мов програмування за версією TIOBE PCI та займає третє місце за популярністю, не враховуючи, звісно, C-подібні мови [61].

Окрім Python реалізації програмного застосунку використаний табличний процесор MS Excel з наведених нижче причин.

Електронні таблиці або табличні процесори – це програмні засоби, які моделюють на екрані двовимірну таблицю, що складається з рядків і стовпців. Одним із найпопулярніших застосунків є MS Excel із пакета MS Office. Основне призначення Excel полягає у вирішенні різноманітних розрахункових задач, вхідні

дані для яких подають у вигляді таблиць. Використання цього інструменту значно спрощує рутинну роботу користувачів.

Особливістю електронних таблиць є можливість застосовувати формули для встановлення зв'язків між контентом комірок. Причому за цими формулами розрахунки виконуються автоматично, а зміна значення будь-якої комірки призводе відразу до перерахунку всіх пов'язаних з нею комірок і, відповідно, до оновлення таблиці відповідно до змінених даних. Основні фактори, які слід враховувати при виборі електронних таблиць:

– виконання складних однотипних розрахунків над великими обсягами даних;
– автоматизація підсумкових обчислень;
– розв'язання задач шляхом підбору значень необхідних параметрів;
– пошук оптимальних параметрів та розв'язання оптимізаційних задач;
– підготовка табличних документів;
– статистичний аналіз результатів експериментів;
– побудова різноманітних діаграм за вказаними даними;
– створення та робота з базами даних.

Отже, застосування електронних таблиць значно спрощує обробку даних і дає змогу отримувати необхідні результати без програмування. У комбінації з мовами програмування табличний процесор MS Excel перетворюється на універсальний інструмент, здатний ефективно розв'язувати практично будь-які завдання незалежно від їхньої складності.

Тому для реалізації поставлених у даній роботі завдань обрано поєднання MS Excel з Python.

3.2 Розробка програмного застосунку тестування та моніторинг кібер-ситуаційної обізнаності

Відповідно до завдання потрібно розробити програму для оцінювання CSA співробітників, яка після проходження тесту виводитиме результати на екран. Для

зручності аналізу відповідей корисно відстежувати кожну відповідь тестованого та зберігати журнал відповідей у текстовий файл на жорсткому диску.

Програмий застосунок реалізовано з графічним інтерфейсом користувача в обгрунтовано обраному середовищі Python.

Основні функції застосунку:

− запит ідентифікаційного номеру, дати проходження оцінювання та департамент співробітника;

− вивід питання з бази даних опитування;

− обробка відповіді співробітника;

− аналіз відповідей співробітниківз розрахунком їх підсумкових балів;

− протоколювання відповідей та їх збереження у базу даних;

− вивід цінки тестування для персоналу та департаменту.

Також програмний застосунок додатково надає такі функції – авторизація співробітника шляхом введення його ID, визначення дати тестування та зазначення департаменту співробітника. При розробці застосунку спроєктовано спеціальну форму авторизації персоналу. Для зручного вводу даних про співробітника було розміщено на формі введення полів вводу даних користувача (рисунок 3.1).

Для проведення тестування на екрані запрограмовані такі кнопки – «Почати тест», «Побудувати графік за ID», «Знайти середнє за відділом».

У процесі обирання одного із запропонованих варіантів на екран виводяться такі фоми:

– запитання для початку проходження опитування у залежності від департаменту /відділу співробітника (кнопка «Почати тест»);

– графічне зображення індивідуальних результатів тестування співробітника у залежності від введеного для цього значення ID («Побудувати графік по ID»);

– усередний результат опитування за департаментом/відділом адміністрації у залежності від вибору назви підрозділу (кнопка «Знайти середнє за відділом»).

```
def begin():
    global e1
    global e2
    global e3
    l1= Label(root, bg='white', fg='black', width=100, height=1, wraplength=900)
    l1['text']="Введіть ваш id:"
    l1.config(font=("Courier", 18))
    l1.pack()

    e1=Entry(root, width=50)
    e1.pack()

    l2= Label(root, bg='white', fg='black', width=100, height=1, wraplength=900)
    l2['text']="Дата опитування:"
    l2.config(font=("Courier", 18))
    l2.pack()

    e2=Entry(root, width=50)
    e2.insert(0,datetime.today().strftime('%Y-%m-%d'))
    e2.pack()

    l3= Label(root, bg='white', fg='black', width=100, height=1, wraplength=900)
    l3['text']="Відділ апарату:"
    l3.config(font=("Courier", 18))
    l3.pack()
```

Рисунок 3.1 – Об’єкти форми введення

У застосунку для відображення питань та введення відповідей користувача передбачена окрема форма (рисунок 3.2). Програма отримує список питань, варіанти відповідей, бали та рекомендації з бази даних, якою в цьому випадку є таблиця MS Excel.

Питання	Відповіді	Вага відповіді	Рекомендації
1. На території районної державної адміністрації є охорона?	А) Так, у нас є служба безпеки районної державної адміністрації.	0,72	
	Б) Ні, у нас немає служби безпеки районної державної адміністрації	0,08	Рекомендація: Якщо служба безпеки на території районної державної адміністрації дійсно існує, користувач може бути високим ризиком для організації, тому що він насправді дезінформованим. Якщо служби безпеки дійсно не існує на території районної державної адміністрації, варто створити її.)
	В) Я не знаю	0,2	Рекомендація: Користувач не проінформований і представляє ризик з очевидних причин.
2. Чи є у вашому кабінеті/службовому приміщенні система сигналізації?	А) Так, є	0,72	
	Б) Ні, немає	0,08	Рекомендація: У службових приміщеннях органів державного управління повинні стояти системи сигналізації для обмеження незаконного доступу до кабінету
	В) Я не знаю, чи має бути у моєму кабінету система сигналізації	0,2	Рекомендація: У службових приміщеннях органів державного управління повинні стояти системи сигналізації для обмеження незаконного доступу до кабінету. Якщо співробітник не знає, отже він не ознайомлений із політикою безпеки.

Рисунок 3.2 – Фрагмент бази даних опитування

При розробці екранної форми передбачено таку організацію бази запитань, щоб кожне питання передбачало вибір лише одного з трьох запропонованих варіантів відповіді. Тестовий варіант проведення опитування на початковому етапі не повинен містити запитань із множинним вибором або запитань без правильної відповіді, а також питань, що потребують введення текстової відповіді.

З урахуванням вищевикладених умов розроблено послідовність роботи з програмним застосунком.

1. Запуск екранної форми авторизації співробітника.

2. Виконання наступних дій при виборі кнопки «Почати тестування»:

- генерація переліку запитань з бази диних;
- формування набору з конкатенації ID співробітника, дати тестування та департаменту/відділу;
- обнулення числа отриманих балів;
- приховуваннння форми авторизації співробітника,
- вивід форми з тестовими запитаннями;
- відображення на екрані одного запитання та можливих варіантів відповідей;
- очікування вибору варіанту відповіді та натискання на нього.

3. Виконання наступних дій при виборі кнопки варіанту відповіді:

– аналіз обраного варіанту відповіді із знаходенням відповідного балу та збільшенням результату на отриманий бал оцінювання;

– збереження протоколу поточного опитування та обраного варіанту відповіді співробітника;

– вивід на екран відповідної результату рекомендації;

– збільшення номера запитання на 1 у разі, якщо номер поточного питання менше загальної кількості питань тестування;

– виведення наступного запитання на екранну форму;

– перехід роботи до початку етапу 3.

4. Виконання наступних дій після порівняння номера поточного питання із

загальною кількістю питань у базі даних:

– підрахунок загальної оцінки на основі одержаних балів;

– вивід на екран повідомлення з оцінкою тесту та відповідними рекомендаціями;

– збереження результатів оцінювання співробітника в базу результатів.

5. Закриття форми опитування шляхом натискання "хрестика".

6. Кінець роботи.

Для формування результатів конкретного співробітника у вигляді графіку необхідно обрати кнопку «Побудувати графік по ID», і графік зміни результатів зображатиметься в іншій екранній формі. При виборі кнопки «Побудувати графік за ID» саме з форми авторизації програма звертатиметься до бази даних і після знаходження результатів певного співробітника формуватиме їх у графічному вигляді, який буде зображено в іншій екранній формі.

При виборі кнопки «Знайти середнє за відділом» на формі авторизації співробітника застосунок звертатиметься за запитом даних до бази про тестування для обраного відділу та дати, та обчислюватиме середнє арифметичне, яке відображатиме одержаний результат вже на іншій формі.

Програмний за стосунок опитування та набір тестових завдань за обраними сферами кібербезпеки, та й сам перелік цих напрямів за розпорядженням керівництва департаменту цифрового розвитку, інформаційної політики та кіберзахисту Одеської ОВА (див. схему на рисунку 1.3) через звернення до адміністратора бази даних тестування чи керівництва обласної державної адміністрації та оцінювання можна змінити шляхом внесення змін до файлу таблиці MS Excel.

Послідовність виконання дій для внесення змін до бази даних опитування наведена далі.

1. Завантаження таблиці MS Excel у форматі .xlsx.

2. Відповідні запитанням, відповідям, оцінкам та рекомендаціям дані стовпчиків таблиці додають до певних змінних.

3. До обраного файлу формату .txt записують дані із заповнених змінних.

3.3 Опис інтерфейсу програмного застосунку оцінювання кібер-ситуаційної обізнаності

Розроблений програмний за стосунок є виконуваним файлом prog.py, який здійснює тестування CSA користувача (додаток А).

Після запуску програми на екрані з'являється вікно, вигляд якого зображено на рисунку 3.3.

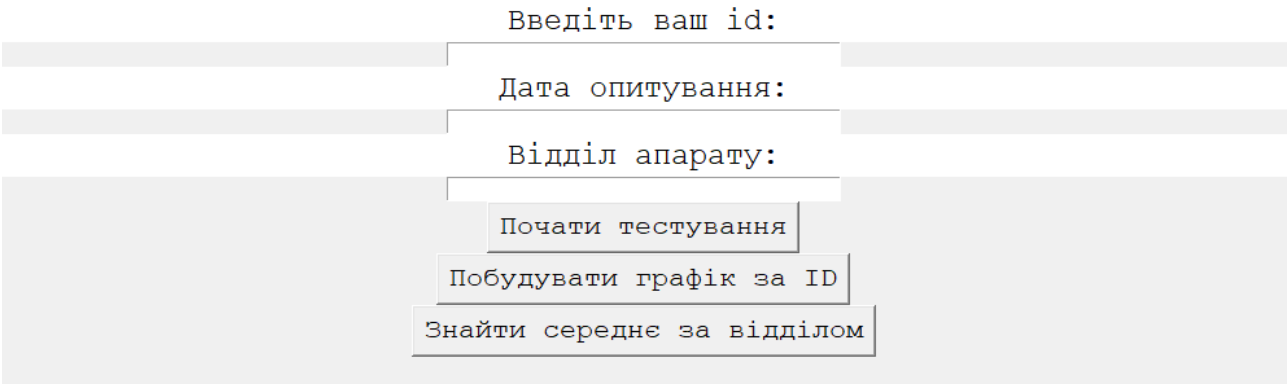

Рисунок 3.3 – Вікно авторизації

У вікні авторизації співробітник вводить ID, обирає дату проведення тестування та департамент, а потім натискає кнопку «Почати тестування». Після цього відкривається інша форма з тестовими запитаннями, приклад вигляду якої зображено на рисунку 3.4.

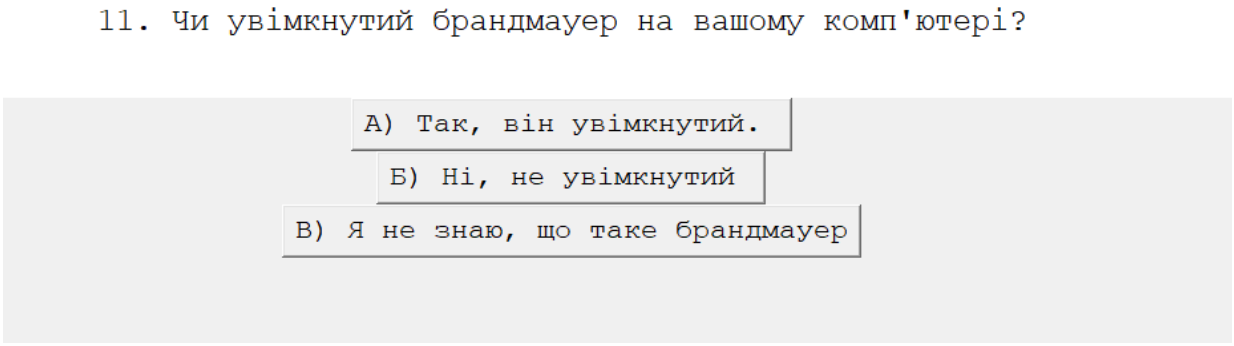

Рисунок 3.4 – Вигляд питання при тестуванні

Співробітник обирає один із трьох запропонованих варіантів відповіді, натискаючи відповідну кнопку. Після цього з’являється наступне питання, на яке відповідь дається аналогічним способом. Коли всі питання пройдено, програма виводить на екран повідомлення з оцінкою опитування та відповідними до цінки рекомендаціями.

У проведеному експерименті максимальна оцінка під час тестування становить 22 бали, що відповідає високому рівню CSA, а мінімальна – 2,4 бала, що свідчить про її низький рівень. Приклад вікна з оцінкою та рекомендаціями наведено на рисунку 3.5.

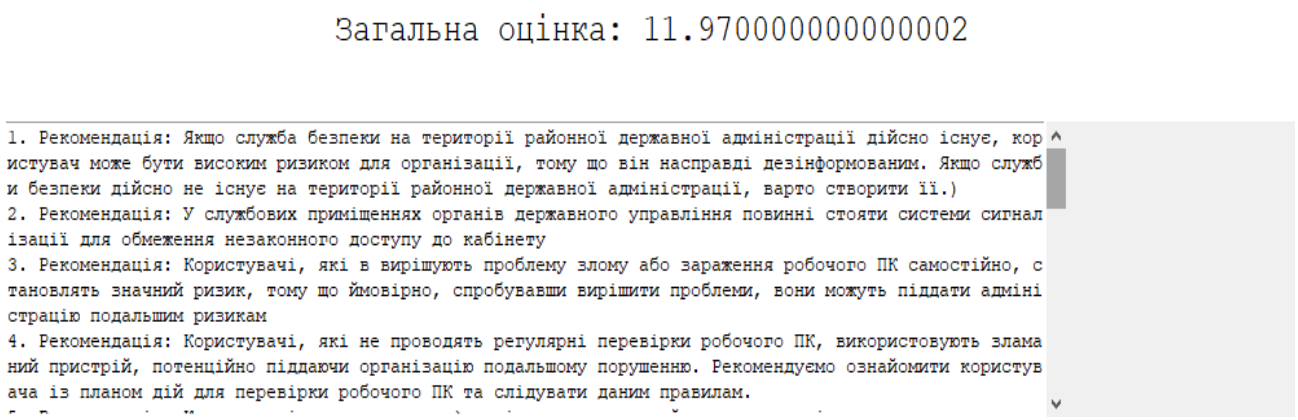

Рисунок 3.5 – Приклад оцінювання та рекомендацій

На стартовому вікні застосунку знаходяться такі дві кнопки:

– «Побудувати графік за ID», за її допомогою сам співрбітник після вводу свого ID може порівняти резульати попередніх та поточного опитування за отриманим графіком (рисунок 3.6);

– «Знайти середнє за відділом», за її допомогою сам працівник чи співробітник департаменту цифрового розвитку, інформаційної політики та кіберзахисту Одеської ОВА може отримати середнє значення рівня кібер-ситуаційної обізнаності при оцінюванні зазначеного департаменту/відділу на конкретну дату.

Зокрема, середнє рівня обізнаності Департаменту екології та природних ресурсів на 19 вересня 2025 року дорівнювало 9,67 балам.

Рисунок 3.6 – Результати опитування співробітника

3.4 Експериментальне дослідження тестування обізнаності співробітників та аналіз результатів

Метою даного дослідження є вивчення CSA співробітників Одеської державної адміністрації. Працівники приходять із різних соціальних верств, мають різні звички, досвід і рівень інтелекту, що впливає на їхню обізнаність у сфері інформаційної безпеки на робочому місці. Водночас органи державного управління не завжди можуть гарантувати, що знання, ставлення та поведінка співробітників відповідають встановленим правилам. CSA може бути нижчою за очікувану або недостатньо доречною, що загрожує цілісності організації. Для ефективного впровадження програм інформаційної безпеки важливо враховувати рівень CSA персоналу [6].

Кількісне оцінювання дозволяє детально визначити, наскільки кожен співробітник обізнаний у питаннях інформаційної безпеки. Результати цього дослідження дають змогу прогнозувати можливі проблеми або загрози у сфері інформаційної безпеки та формувати цільові програми підвищення обізнаності. Вимірювання здійснюється за трьома основними етапами.

1. Побудова кібер-ситуаційних параметрів обізнаності.

Цей етап має на меті визначення сфери дослідження CSA. Він встановлює відповідні критерії для вимірювання обізнаності співробітника в конкретному контексті засобами моделі AIU(Awareness, Ignorance, Uncertainty) - обізнаність, необізнаність та невизначеність і ґрунтуються на дослідженнях Ханша та Бененсона [62].

2. Оцінювання CSA.

На цьому етапі застосовують 5-бальну шкалу Лайкерта [63](таблиця 3.1).

Таблиця 3.1 – Рівні ситуаційної обізнаності за Лайкертом

Рівень обізнаності	Кількісна оцінка рівня	Коментар
Високий рівень (I)	19,5-22	Для співробітників характерні глибокі знання про принципи кібербезпеки, загрози, вони гарно освічені, їх щоденна поведінка відповідає вимогам та рекомендаціям з кібербезпеки
Підвищений рівень (II)	15,5-19,49	Співробітники активно навчались на курсах з кібербезпеки, знають про загрози, але не завжди чи не в повній мірі дотримуються принципів кібергігієни та кіберкультури
Помірний (III)	11-15,49	Співробітники знають про небезпеку і обовязкове дотримання основних принципів кібербезпеки, але потребують подальшої освіти, Оскільки не визнають інцидентів і не орієнтуються як реагувати на них
Низький рівень (IV)	4,5-10,99	Співробітники не є обізнані як з небезпеками кіберпростору і принципами безпечности, ні з правилами забезпечення кібербезпеки в організації
Незадовільний рівень (V)	0,08-4,49	Такі співробітники не знають взагалі нічого про небезпеки і не дотримуються ніяких правил кібербезпеки

Шкала застосовується для оцінки ступеня згоди співробітників із твердженнями, що стосуються CSA. Результати використовуються для формування середнього балу за відсотковою шкалою. На основі агрегованих оцінок респонденти класифікуються за п’ятьма рівнями обізнаності, що наведено в таблиці вище.

3. Кібер-ситуаційний аналіз причинно-наслідкових зв'язків.

Цей етап має на меті досліджувати всі фактори, що впливають на результати оцінки CSA співробітників, що дозволяє виявити критичні питання та визначити цілі для підвищення обізнаності в майбутньому.

Для збору даних був розроблений онлайн-тест, про який згадувалося раніше, і розісланий співробітникам електронною поштою. У результаті було отримано 30 корисних зразків відповідей.

Важливою ініціативою для підвищення CSA є впровадження програми навчання з інформаційної безпеки. Такі програми зазвичай охоплюють політику безпеки організації/установи, стандарти обробки конфіденційних даних, передову практику роботи з електронною поштою, методи повідомлення про потенційні порушення та загальні принципи безпеки, які допомагають захистити як співробітника, так і орган державного управління.

Не менш важливою є оцінка ефективності заходів інформаційної безпеки обласних (військових) державних адміністрацій в умовах сьогодення. Для цього було створено тестування обізнаності співробітників щодо безпеки, яке дозволяє оцінити їхню реакцію на конкретні ситуації та питання, пов’язані з кібербезпекою. Отримані бали та рівень CSA доцільно використовувати з часом як індикатори ефективності навчальних програм та заходів, а також для порівняння результатів між відділами.

Для знаходження рівня CSA використаємо формулу, запропоновану Т. Бондом [64], американським вченим. Після зібрання результатів опитування їх можна використати для визначення рівня обізнаності організації/установи ($PO_{сп}$):

$$PO_{\text{сп}} = \frac{1 \cdot n_1 + 2 \cdot n_2 + 3 \cdot n_3}{K}, \quad (3.1)$$

де: n_1 – кількість балів «обізнаності»;

n_2 – кількість балів «необізнаності»;

n_3 – кількість балів «невизначеності»;

K – загальна кількість співробітників департаменту, організації тощо, для яких оцінювався рівень CSA.

Щоб одержати результат у відсотках ($PP_{відс}$), потрібно знайти відношення результату рівня ситуаційної обізнаності до максимально можливої кількості балів, що можна одержати в процесі тестування, й частку відповідно помножити на сто.

$$PP_{відс} = \frac{PP_{сп}}{22} \cdot 100. \quad (3.2)$$

Аналогічні результати можна формувати за кабінетами, відділами, департаментами для кожного співробітника окремо або по організації в цілому. Це дозволяє виявити конкретні недоліки, що потребують уваги, а також організувати відповідні заходи для профілактики можливих загроз у майбутньому.

Для аналізу відповідності теоретичних викладок реальним результатам оцінювання у якості експерименту проведено початкове комп'ютерне тестування співробітників Одеської облдержадміністрації. Отримані та проаналізовані дані представлені у вигляді таблиці 3.2.

Для цього дослідження важлива якість набутих у процесі навчання та підготовки знань, умінь та навичок, це є вагомим показником рівня кібер-ситуаційної обізнаності співробітників адміністрації. Тому якість цих знань, умінь і навичок розглядається як відображення загальної ефективності CSA.

Для оцінки результативності методу тестування як інструменту контролю проведення експерименту виконано тестування співробітників департаментів повторно саме тих, що мали рекомендації за результатами попереднього тестування (таблиця 3.3).

Таблиця 3.2 – Результати оцінювання співробітників за департаментами

Назва департаменту	Кількість балів	Відсотковий рівень	Рівень обізнаності
Департамент охорони здоров'я	8,2	37	IV
Департамент міжнародного співробітництва та протоколу	8,5	38	IV
Департамент екології та природних ресурсів	9,67	43	III
Департамент освіти і науки	7,63	34	IV
Департамент фізичної культури, спорту і туризму	8,72	39	IV
Департамент соціальної та сімейної політики	7,5	34	IV
Департамент аграрної політики, продовольства та земельних ресурсів	7,85	37	IV

Таблиця 3.3 – Результати повторного оцінювання співробітників

Назва департаменту	Кількість балів	Відсотко-вий рівень	Рівень обізнаності	Різниця (%)
Департамент охорони здоров'я	15	65	II	20
Департамент міжнародного співробітництва та протоколу	15,83	73	II	33
Департамент екології та природних ресурсів	18,3	84	II	39
Департамент освіти і науки	17,99	83	II	47
Департамент фізичної культури, спорту і туризму	18,43	85	II	44
Департамент соціальної та сімейної політики	16,45	76	II	40
Департамент аграрної політики, продовольства та земельних ресурсів	16,8	77	II	40

Отже, результати дослідно-експериментальної перевірки показали, що метод тестування як інструмент оцінювання рівня CSA у поєднанні з методом аналізу ієрархій Томаса Сааті сприяє підвищенню рівня підготовленості співробітників [4] (рисунок 3.7). Ефективність використання MAI підтверджують і останні публікації Юдіної Д. та Сидоренка В. [59, 66].

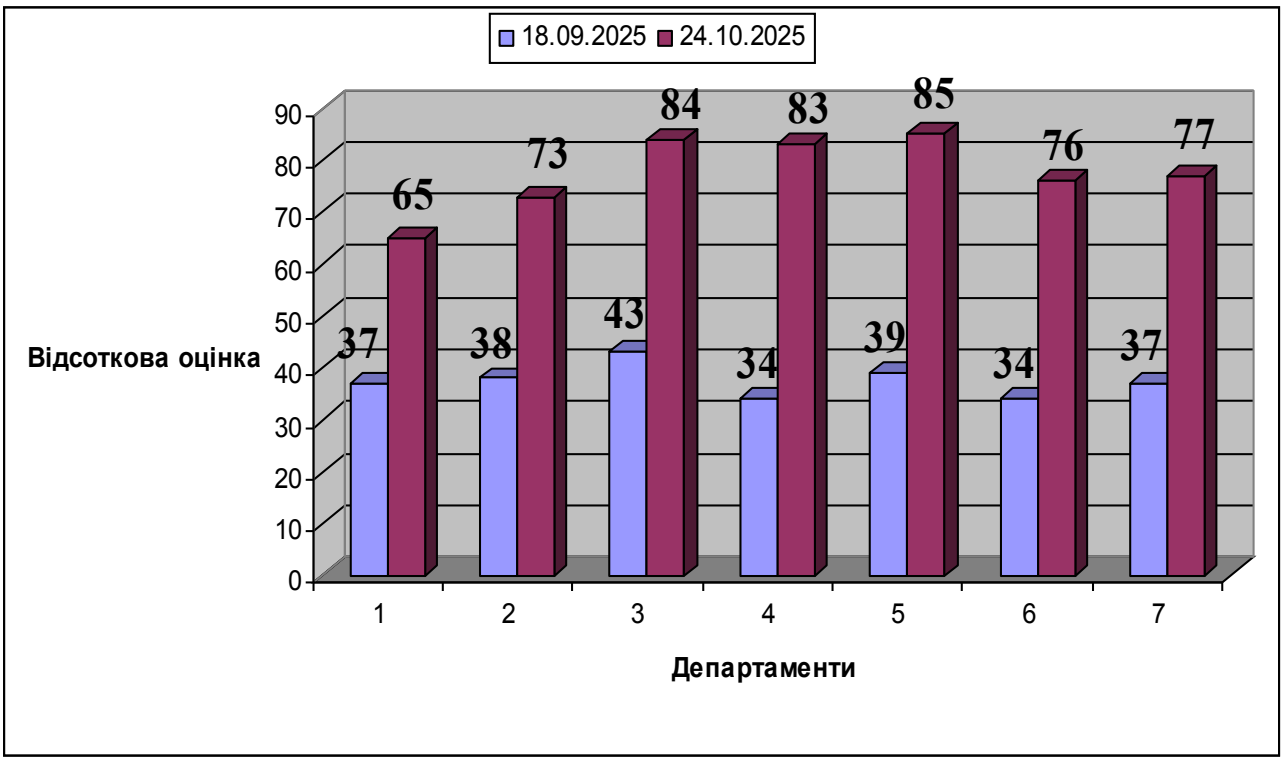

Рисунок 3.7 – Порівняльна гістограма оцінювання CSA співробітників

Отже, в результаті проведених експериментів в Одеській ОВА можна стверджувати – метод комп'ютерного тестування є ефективним засобом оцінювання CSA і сприяє підвищенню рівня обізнаності співробітників. Проте існують певні обмеження, які водночас відкривають шляхи майбутніх досліджень. Зокрема, процедура оціювання проводилась онлайн, а учасники самостійно обиралися серед співробітників. По-друге, дослідження охоплювало лише один орган державного управління. Таким чином, отримані результати відображають стан інформаційної безпеки лише в конкретних групах користувачів обласної державної адміністрації.

3.5 Висновки та рекомендації

Проведене оцінювання надає адміністрації органу державного управління як як критично важливій інфраструктурі у воєнний час інформацію для визначення пріоритетних напрямів удосконалення [67]. Для запобігання кібератакам на об’єкти критичної інфраструктури держави, шкідливим програмним забезпеченням та мінімізації ризиків несанкціонованого доступу до інформації рекомендується реалізувати низку першочергових заходів.

1. Забезпечувати недопущення відкриття вкладень з підозрілими повідомленнями, повідомлень з нестандартним спонукальним текстом до переходу на невідомі посилання.
2. Адміністраторам безпеки та системним адміністраторам звертати особливу увагу на фільтрацію вхідних та вихідних потоків.
3. Періодично оновлювати антивірусну базу до останньої версії.
4. Унеможливити користувачам працювати з правами адміністратора.
5. Обмежити можливості запустити на робочих комп’ютерах виконувані файли “.exe” .
6. Працювати з ліцензійнми чи відкритими операційними системами та програмними продуктами, оновлювати їх своєчасно і систематично .
7. Важливо використовувати програмний міжмережевий екран та інші засоби захисту від шкідливого програмного забезпечення.
8. Співробітникам варто здійснювати регулярно резервне копіювання даних, зберігати резервні копії на зовнішніх носіях інформації та налаштувати функцію «відновлення системи»;
9. Не підключати невідомі носії, не вставляти диски, якщо немає повної довіри до їх джерела. Знайдений в адміністрації чи на прилеглій території пристрій, отриманий поштою або з доставкою, або від незнайомця з проханням друку документа чи перевірки його змісту свідчить про високу небезпеку.
10. Не зберігати аутентифікаційні та конфіденційні дані в легкодоступних місцях, зокрема, на робочому столі. Використовувати для збереження паролів

спеціальні програмні засоби. Використовувати стійкі паролі.

11. Уникати за можливості використання електронних платіжних систем, Інтернет-банкінгу, вводу автентифікаційних даних в апроцесі доступу до інтернету через незахищені безпроводові мережі у публічних місцях.

12. Необхідно забезпечувати автоматичну перевірку різноманітних пристроїв при їх підключенні на присутність шкідливих програм.

13. Важливо ніколи не переходити за невідомими покликаннями,не завантажувати файли як з потенційно небезпечними розширеннями, наприклад: .exe, .bin, .ini, .dll, .com, .sys, і також безпечними - docx, .zip, .pdf, бо можуть використовуватись вразливості й інші загрози.

14. Бути уважними з іменами з електронної пошти: якщо вони навіть здалися легітимними, їх необхібно в будь-який спосіб перепровірити, чи справді особа відправила повідомлення з вкладенням.

15. Під час користування такими інтернет-ресурсами як інтернет-банкінг, соціальні мережі, меседжери, новии, не відкривати підозрілі покликання, особливо якщо вони вказують на зазвичай не відвідувані веб-сайти.

16. Звертати увагу на інтернет-шахрайсгво. Найпоширеніший засіб введення в оману в інтернеті – фішииг. Особлива увага має бути звернена до доменного імені, що запитує автентифікаційні дані до покликання,бо зловмисники і доменне ім'я маскують під якесь знайоме («facelook.com», «goooogle.com»).

17. Потрібно встановити на всіх пристроях обмеження на кількість вводу помилкових паролей та логінів.

На початковому етапі взаємодії зі співробітниками державних адміністрацій рекомендовано такі заходи.

1. Інформування персоналу про найважливіші події та проблемні питання щодо забезпечення кібербезпеки та інформаційної безпеки.

2. Регулярне доведення до співробітників органів державного управління відомих та нових фактів про викрадення персоналом конфіденційної інформації в інших органах державного управління.

3. Обов'язкова участь керівництва департаменту кіберзахисту в усіх заходах.

4. Участь керівництва державної установи в атестаціях співробітників для усіх посадових категорій, бо атестація виявляє ризики допущення помилок і порушень захищеності інформації співробітником.

5. Керівник повинен на основі аналізу даних про виявлених фактів заподіяння збитків організації/установи ініціювати тренінги та проведення навчань з підвищення рівня обізнаності у сфері забезпечення захисту кіберпростору та кіберкультури.

6. Обов'язкове проходження тестування з кібергігієни усіх співробітників та оприлюднення підсумків.

Отже, в третьому розділі розроблено програмне забезпечення для оцінювання CSA співробітників, виконано експерименти з оцінювання обізнаності співробітників,а також дано рекомендації для впровадження заходів інформаційної безпеки державних адміністрацій.

ВИСНОВКИ

1. Забезпечення ситуаційної обізнаності в кіберпросторі є вкрай важливим сьогодні для управління безпекою держави та відбиття постійних інформаційних атак ворога.

2. Аналіз нормативно-правового забезпечення та управління безпекою об’єктів критичної інфраструктури в Україні свідчить про посилену увагу держави до цих питань та стрімкий розвиток методів забезпечення кібербезпеки критично важливої інфраструктури в умовах воєнного сьогодення.

3. У результаті огляду і аналізу існуючого стану захищеності інформаційних ресурсів критично важливої інфраструктури, зокрема, Одеської обласної державної військової адміністрації, вивчили можливі загрози інформаційній безпеці.

4. Дослідження методів оцінювання ситуаційної обізнаності показали, що для оцінювання кібер-ситуаційної обізнаності співробітників державних адміністрацій доцільно використовувати комп’ютерне тестування та метод аналізу ієрархій.

5. Для програмної реалізації оцінювання кібер-ситуаційної обізнаності обгрунтувано використано поєднання середовища Python та табличного процесора Microsoft Excel.

6. Виконано експериментальне дослідження тестування для визначення рівня оцінювання кібер-ситуаційної обізнаності співрбітників в конкретному органі державного управління та проаналізавано одержані результати.

7. Розроблено заходи з підвищення рівня кібер-ситуаційної обізнаності та рекомендації по їх впровадженню для покращення захищеності інформаційних ресурсів органів державного управління.

8. Проведено повторне оцінювання кібер-ситуаційної обізнаності співробітників після запровадження заходів – навчання й тренінги з кібергігієни – та виконано аналіз одержаних змін. За рахунок впровадження заходів з

інформаційної безпеки рівень кібер-ситуаційної обізнаності персоналу підвищився в середньому на 38%.

Результати даної роботи можуть бути використані в органах державного управління України та інших об’єктах критично важливої інфраструктури.

Як логічне продовження виконаної кваліфікаційної роботи магістра доцільно запропонувати вдосконалення системи оцінювання шляхом застосування додаткових кількісних методів при повторному тестуванні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Одеська політехніка» в проєкті USAID «Кібербезпека критично важливої інфраструктури України». URL: https://op.edu.ua/ international/projects/usaid.

2. Чепурной К., Тимошенко Л. Захист об’єкту критичної інфраструктури в умовах воєнного стану. *Інформаційна безпека та інформаційні технології* : зб. матеріалів доп. учасн. V Міжнар. наук.-практ. конф. : Львів, 2024. С. 102-105.

3. Чепурной К., Тимошенко Л. Заходи програмно-апаратного характеру для підвищення рівня захищеності об’єкту критичної інфраструктури. *Захист інформації* : зб. матеріалів доп. учасн. наук.-практ. симп. (м. Тернопіль, 05 груд. 2024 р.). Тернопіль, 2024. С. 93-95.

4. Тимошенко Л.М., Юр’єв Д.Л. Кіберситуаційна обізнаність співробітників об’єкту критичної інфраструктури. Матер. науково-практичної конференції молодих вчених, аспірантів та студентів “Кібернетична безпека та компютерно-інтегровані технології”. Т.: ЗУНУ, 2025. С. 35-36.

5. Бовнегра Л.В., Тимошенко Л.М, Накоряков О.Г. Дослідження систем оцінювання кібер-ситуаційної обізнаності. Матеріали науково-практичної конференції молодих вчених, аспірантів та студентів “Кібернетична безпека та компютерно-інтегровані технології”. 2022. (29-31 серпня 2022 року). Т. : ЗУНУ, 2022. С. 22-26.

6. Смольник А., Тимошенко Л., Бовнегра Л. Розробка ІТ-проєкту моніторингу кібер-ситуаційної обізнаності. Підприємництво та логістика в умовах сучасних викликів. Матеріали наук.-практ. конференції. Тези доповідей (25–27 травня 2023 р.) / Відп. ред. А. І. Крисоватий. Тернопіль, 2023. 109-113. URL:https://api.dspace.wunu.edu.ua/api/core/bitstreams/b6c77750-fc78-4aed-aa5f-4743d483ac3e/content

7. Тимошенко Л.М., Єрьоменко А.І. Використання моделі Ендслі для розробки систем кібер-ситуаційної обізнаності. Матеріали XIX Всеукраїнської науково-технічної конференції «Стан, досягнення і перспективи інформаційних

систем і технологій» Одеса: ОНАХТ, 2020. С. 74-76.

8. Сиропятов О.А., Тимошенко Л.М., Назарова І.В. Експрес-аудит як інструмент оцінки вразливостей в системах обробки даних: підходи, методики та рекомендації. *Інформатика та математичні методи в моделюванні.* 2024. №4. С. 279-289.

9. Яцків В.В., Івасьєв С.В., Давлетова А.Я., Тимошенко Л.М. Методологія впровадження системи управління інформаційною безпекою на основі багаторівневої моделі кіберзахисту згідно з вимогами законодавства України *Інформатика та математичні методи в моделюванні.* 2025. №1. С.137-148.

10. Марущак А.І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки. Державна безпека України. 2013. № 21. С. 92–95.

11. Литвинюк А.А. Основи інформаційної безпеки. Комплексна система захисту інформації: структура встановлення, підтримка функціонування. URL: http://wwwcvk.gov.ua/visnyk/pdf/ 20084/visnikst08.pdf.

12. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави : Постанова Кабінету Міністрів України від 23 серп. 2016 р. № 563. Режим доступу: http://zakon5.rada.gov.ua/laws/show/563-2016-%D0%BF

13. Про схвалення Концепції створення державної системи захисту критичної інфраструктури: розпорядження Кабінету Міністрів України від 6 груд. 2017 р. № 1009-р. Режим доступу: http://zakon3.rada.gov.ua/laws/show/1009-2017-%D1%80

14. Теленик С.С. Критична інфраструктура як об’єкт адміністративно - правового регулювання. Юридичний часопис Національної академії внутрішніх справ. 2018. № 1(15). С. 179–188.

15. Бірюков Д. Концепція захисту критичної інфраструктури як елемент загальноєвропейської безпекової політики. Наукові записки. К. : Інститут політичних і етнонаціональних досліджень імені І. Ф. Кураса НАН України, 2013. № 6 (68). С. 106-115.

16. Зелена книга з питань захисту критичної інфраструктури в Україні : зб. матеріалів міжнар. експерт. нарад / упоряд.: Д. С. Бірюков, С. І. Кондратов ; за заг. ред. О. М. Суходолі. Київ : НІСД, 2015. 176 с.

17. Ковалів М., Назар Ю., Єсімов С., Красницький І. Правове забезпечення кібербезпеки критичної інформаційної інфраструктури України. Traektoriâ Nauki = Path of Science. 2021. Vol. 7. - № 4. P. 2011-2018.

18. Порядок формування переліку об'єктів критичної інформаційної інфраструктури (Україна), 09.10.2020, № 943. Актуально на 28.03.2021. URL: https://zakon.rada.gov.ua/laws/show/943-2020-п#Text

19. Про основні засади забезпечення кібербезпеки: Закон України від 5.10.2017 № 2163-VIII: веб-сайт. URL: https://zakon.rada.gov.ua/laws/ show/2163-19.

20. Про невідкладні заходи щодо забезпечення національної безпеки, суверенітету і територіальної цілісності України: Рішення Ради національної безпеки і оборони України від 1.03.2014: веб-сайт. URL: https://zakon.rada.gov.ua/laws/show/n0001525-14

21. Указ президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України"» URL: https://zakon5.rada.gov.ua/laws/show/96/2016.

22. Суходоля О. М. Захист критичної інфраструктури: сучасні виклики та пріоритетні завдання сектору безпеки. Науковий часопис, 2017. Вип. 1-2 (13-14). С. 50-80.

23. Гончар С. Ф., Леоненко Г. П., Юдін О. Ю. Теоретико-методологічний аспект забезпечення інформаційної безпеки об'єктів критичної інфраструктури. Вісник Національного університету «Львівська політехніка». Комп'ютерні системи та мережі, 2014. № 806. С. 34-39: URL: http://nbuv.gov.ua/UJRN/VNULPKSM_2014_806_8.

24. Про критичну інфраструктуру та її захист : проєкт Закону України реєстр. № 10328 від 27 трав. 2019 р. Верховна Рада України : URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65996.

25. Концепція (основи державної політики) національної безпеки

України : постанова Верховної Ради України від 16 січ. 1997 р. № 3/97 ВР. Відомості Верховної Ради України. 1997. № 10. Ст. 85.

26. Ліпкан В. А. Концепція національної безпеки України: підходи до формування. Вісник прокуратури. 2003. № 10. С. 85–92.

27. Шипілова Л. М. Порівняльний аналіз ключових понять і категорій основ національної безпеки України : автореф. дис. … канд. політ. наук : 21.01.01. Київ, 2007. 20 с.

28. Іванченко, Є., Корченко, О., Заріцький, О., Зибін, С., Вишневська, Н. Аналіз поняття кіберстійкості критичної інфраструктури. Захист інформації. Том 25, №4, жовтень-грудень 2023, С. 221-233.

29. Суходоля О. (2022). Стійкість критичної енергетичної інфраструктури та життєдіяльності громад. Аналітична доповідь НІСД, 72 с. https://chtyvo.org.ua/.../ Stiikist_krytychnoi_enerhetychnoi_infrastruktury_ta_zhyttiediialnosti_hromad.

30. Корченко О., Іванченко Є., Бакалинський О., Зубков Д.. Метод оцінювання рівня підвищення стану кіберзахисту об’єктів критичної інфраструктури держави . Ukrainian Scientific Journal of Information Security. May 2024. 30(1): С.95-99. DOI:10.18372/2225-5036.30.18610.

31. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» : указ Президента України від 26 трав. 2015 р. № 287/2015. Верховна Рада України . URL: http://zakon3.rada.gov.ua/laws/show/287/2015.

32. Про основи національної безпеки України : Закон України 19 черв. 2003 р. № 964-IV. Відомості Верховної Ради України. 2003. № 39. С. 351. (Із змінами, внесеними згідно із Законом № 3200-IV від 15 груд. 2005 р. Відомості Верховної Ради України. 2006. № 14. С. 116).

33. Нормативно-правова база у сфері захисту об'єктів критичної інфраструктури України. Режим доступу: https://csirt.csi.cip.gov.ua/uk/pages/cio

34. Про критичну інфраструктуру: Закон України 1882-IX від 16.11.2021. Верховна Рада України . Відомості Верховної Ради (ВВР), 2023, № 5, ст.13.

35. Про затвердження Методики та Критеріїв і показників оцінки стану захищеності об’єктів критичної інфраструктури. Наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України, 14 січня 2025 року № 17. URL: https://zakon.rada.gov.ua/laws/show/z0375-25#Text.

36. Про місцеві державні адміністрації : Закон України № 2646-VIII від 06.12.2018 . Верховна Рада України . Відомості ВР України. 2019. № 4, 32 с.

37. Розпорядження «Про затвердження положень про апарат Одеської державної адміністрації та його структурні підрозділи». URL: https://drive.google.com/file/d/1JxegmhNS3Czdqg6i5aZRbpklCuTpOSiZ/view .

38. Структура Одеської обласної державної адміністрації. URL: http://odesa-oda.gov.ua/?page_id=10.

39. Інструкція про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, в Одеській обласній державній адміністрації. URL: http:// http://odesa-oda.gov.ua/?page_id=1999.

40. Програма розвитку інформаційного простору Одеської області на 2021-2025 роки. URL: http://ooda.gov.ua/departament-z-pitan-vnutrishno%25d1%2597-ta-informacijno%25d1%2597-politiki-oda-dopovidaye-deputatam-oblasno%25d1%2597-radi-pro-zaxodi-shhodo-informacijno%25d1%2597-bespeki-oblasti.

41. Система електронного документообігу в державному управлінні: навчально-метод. посібник/ О.В.Василенко, В.І.Шостка, О.М.Клейменов, І.В. Клименко, К.О. Линьов. К. : Видавництво НАДУ, 2016. 32 с.

42. Василенко О.В. Автоматизація документообігу в органах державного управління. Збірник тез науково-практичної конференції «Державне управління та місцеве самоврядування: історія і сучасність» - 2016. (26 вересня 2016 року). Х.: Вид-во ХарРІ НАДУ "Магістр", 2016. Режим доступу: http://www.kbuapa.kharkov.ua /e-book/conf/2016-2/doc/5/01.pdf.

43. Про утворення військових адміністрацій: Указ Президента України від 24.02.2022 № 68/2022. Сайт Президента України. Офіс Президента України. 24 лютого 2022.

44. Результати Глобального дослідження EY з інформаційної безпеки показують, що кібербезпека залишається важливим питанням порядку денного організацій. URL: https://www.ey.com/en_gl/news/2018/ 10/cybersecurity-in-organizations-must-enable-competitive-advantage-while-they-continue-to-protect-and-optimize-security-ey-report-reveals.

45. Українську систему ситуаційної обізнаності презентували на щорічному заході НАТО. URL: https://censor.net /ua/n3376484.

46. ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT)

47. NIST SP 800-50 Rev.1. Building a Cybersecurity and Privacy Learning Program. URL: https://doi.org/10.6028/NIST.SP.800-50r1.

48. Буров Є.В., Микіч Х.І. Формальна модель опрацювання знань у системах із ситуаційною обізнаністю. Вісник Національного університету «Львівська політехніка». Інформаційні системи та мережі. 2017. № 872. С. 25-35.

49. Fairfax T., T. Laing & P. Vickers. Network Situational Awareness: Sonification & Visualization in the Cyber Battlespace. Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance. 2015. 16-18. World Wide Web. URL: https://www.igi-global.com/chapter/network-situational-awareness/115766.

50. D'Arcy J.. A. Hovav, and D. Galletta. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach . 2009. P.128-135. URL: http://130.18.86.27/faculty/warkentin/_BIS9613papers/Darcy/D'ArcyHovavGalletta2009_ISR20_1_AwarenessDeterrence.pdf.

51. McGuinness B. , & L. Foy. A Subjective Measure of SA: The Crew Awareness Rating Scale (CARS). First Human Performance, Situation Awareness and Automation Conference. 2000. P.286-291. URL: https://www.tib.eu/en/search/id/BLCP%3ACN055350174/A-Subjective-Measure-of-SA-The-Crew-Awareness-Rating/

52. Onwubiko C. & T.J. Owens. Review of Situational Awareness for Computer

Network Defense. Situational Awareness in Computer Network Defense: Principles, Methods and Applications. 2011. P.125-140. URL: https://pdfs.semanticscholar.org/3b61/0853aacee755a2bfe8b2947f747b9463c00f.pdf

53. Посилення захисту критичної інфраструктури України: Стратегічні висновки й кращі міжнародні практики. «e-Governance Academy» / Академія електронного управляннія Ахтри 6, 10151, м. Таллінн, Естонія. https://ega.ee/wp-content/uploads/2025/06/ciip-ua-204x275mm-ua-webi.pdf.

54. Козубцова Л. М., Хлапонін Ю. І., Козубцов М.. Metodika ocinuvanna efektivnosti vikonanna zahodiv zabezpecenna kiberbezpeki ob'ektiv kriticnoi informacijnoi infrastrukturi organizacij. https://www.researchgate.net/ publication/354988857.

55. Голубєва Н.В.. В.О. Дурєєв, С.М. Бондаренко. Комп'ютерне тестування як одна з форм сучасного контролю знань. Інформаційно-телекомунікаційні технології в державному управлінні: досвід, проблеми, перспективи: збірник наукових праць Львів : ЛДУБЖД, 2016. Вип. 1. С. 309-313.

56. Dorosh M., Voitsekhovska M. Information Security Culture Wide-Scale Implementation Model. *Проблеми зняття з експлуатації об'єктів ядерної енергетики та відновлення навколишнього середовища (INUDECO 2020)* : зб. матеріалів IV Міжнар. конф. (м. Славутич, 27-29 квітня 2020 р.). Чернігів : ЧНТУ, 2020. С. 73-77.

57. Saaty R. W. The analytic hierarchy process: what it as and how it is used? Mathematical Modeling. 1987. Vol. 9. № 3–5. URL: https://www.researchgate.net/publication/247759937_The_Analytic_Hierarchy_Process_-_What_It_Is_and_How_It_Is_Used.

58. Vargas Luis L.; Saaty Thomas L. (2001). Models, Methods, Concepts & Applications of the Analytic Hierarchy Process.Boston: Kluwer Academic. ISBN 0-7923-7267-0

59. Сидоренко В. (2025). Метод оцінювання стійкості об'єктів критичної інформаційної інфраструктури держави. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, *1*(29), 837–853. https://doi.org/

10.28925/2663-4023.2025.29.944.

60. Shipman S.W. Tkinter . GUI for Python 2014. 8. P.168. World Wide Web. URL: https://www.hsg-kl.de/faecher/inf/python/tkinter/tkinter.pdf.

61. Downey A.B. Think Python. O'Reilly Media, 2012. URL: 300 p. https://www.twirpx.com/file /917165/

62. Hansch N., Z. Benenson. Specifying IT security awareness. In: 25th International Workshop on Database and Expert Systems Applications (DEXA), 2016. P. 326-330.

63. Gleen F. Gamification for Measuring Cyber Security Situational Awareness / F. Glenn, D. Best , D. Manz, V. Popovsky and B. Endicott-Popovsky. Lecture Notes in Computer Science, 2013. P. 656-665.

64. Bond T. Employee Security Awareness Survey . 2012. Vol. 9. 7 p. URL: http://fliphtml5.com/ugpo/xtmr/basic.

65. Gleen F. Gamification for Measuring Cyber Security Situational Awareness / F. Glenn, D. Best , D. Manz, V. Popovsky and B. Endicott-Popovsky. Lecture Notes in Computer Science, 2013. P. 656-665.

66. Юдіна Д. (2025). Метод розрахунку рівня кіберзахисту об’єктів критичної інформаційної інфраструктури . *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(*30), 473–487. https://doi.org/10.28925/2663-4023.2025.30.986

67. Корченко О.Г. Методи та моделі оцінювання стану кіберзахисту об’єктів критичної інфраструктури держави (стенограма доповіді на засіданні Президії НАН України 18 червня 2025 р.). *Вісник НАН України*. 2025. № 8. С. 59-62. https://doi.org/10.15407/visn2025.08.059.

ДОДАТОК А

Лістинг програмного коду

```
from tkinter import *
import pickle
from datetime import datetime, date, time
import os.path
from pandas import DataFrame
import matplotlib.pyplot as plt
from matplotlib.backends.backend_tkagg import FigureCanvasTkAgg

f=open('q_list.txt', 'r');
v=[]
q_list=[]
a=[]
r=[]
b=[]
point=0;

k=0;
for line in f:

    line=line.replace('\n','')

    if line[0:4]=='q:::':
        q=line[4:]
    if line[0:5]=='a1:::':
        a.append(line[5:]);
    if line[0:5]=='a2:::':
        a.append(line[5:]);
    if line[0:5]=='a3:::':
        a.append(line[5:]);
    if line[0:5]=='a4:::':
        a.append(line[5:]);
    if line[0:5]=='r1:::':
        r.append(line[5:]);
    if line[0:5]=='r2:::':
        r.append(line[5:]);
    if line[0:5]=='r3:::':
        r.append(line[5:]);
    if line[0:5]=='r4:::':
        r.append(line[5:]);
    if line[0:5]=='b1:::':
        b.append(line[5:]);
    if line[0:5]=='b2:::':
        b.append(line[5:]);
    if line[0:5]=='b3:::':
        b.append(line[5:]);
    if line[0:5]=='b4:::':
        b.append(line[5:]);
```

```
    if line[0:5]=='b5:::':
        b.append(line[5:]);
    if line[0:3]=='///' and line!='///1':
        v.append(q)
        v.append(a)
        v.append(r)
        v.append(b)
        q_list.append(v)

        a=[]
        v=[]
        r=[]
        b=[]
        k=k+1;

print('Зчитано питань: ', k)

ans=[]
rec=[]
n=-1;

root = Tk()
root.geometry("1000x300")
e1=''
e2=''
e3=''
data=[]

def av():
   if e3.get():
    data=e2.get();
    dep=e3.get();
    if os.path.exists("database.pickle") and
os.path.getsize("database.pickle") > 0:
        with open('database.pickle', 'rb') as handle:
            results = pickle.load(handle)
    y=0
    k=0
    for i in results:
        if i[2]==dep and i[1]==data:
                y+=i[3]
                k+=1
    window = Toplevel(root)
    l1= Label(window, bg='white', fg='black', width=30,
height=1, wraplength=900)
    l1['text']="Середнє: " + str(y/k)
    l1.config(font=("Courier", 18))
    l1.pack()

def plot1():
    if e1.get():
        id=int(e1.get())
```

```
        if os.path.exists("database.pickle") and
os.path.getsize("database.pickle") > 0:
                with open('database.pickle', 'rb') as handle:
                    results = pickle.load(handle)

        y=[]
        x=[]
        k=1
        for i in results:
            if int(i[0])==id:
                y.append(i[3])
                x.append(k)
                k+=1

        Data2 = {'Stage': x,
                'Awareness Rate': y}

        df2 = DataFrame(Data2,columns=['Stage','Awareness
Rate'])
        df2 = df2[['Stage', 'Awareness
Rate']].groupby('Stage').sum()

        window = Toplevel(root)

        figure2 = plt.Figure(figsize=(5,4), dpi=100)
        ax2 = figure2.add_subplot(111)
        line2 = FigureCanvasTkAgg(figure2, window)
        line2.get_tk_widget().pack()
        df2.plot(kind='line', legend=True, ax=ax2,
color='r',marker='o', fontsize=10)
        ax2.set_title('Awareness Level / Time')

def start():
    global n
    global data
    n=0
    data.append(e1.get())
    data.append(e2.get())
    data.append(e3.get())
    for widget in root.winfo_children():
        widget.destroy()
    loop(n)

def begin():
    global e1
    global e2
    global e3
    l1= Label(root, bg='white', fg='black', width=100,
height=1, wraplength=900)
    l1['text']="Введіть ваш id:"
    l1.config(font=("Courier", 18))
    l1.pack()
```

```
    e1=Entry(root, width=50)
    e1.pack()

    l2= Label(root, bg='white', fg='black', width=100,
height=1, wraplength=900)
    l2['text']="Дата опитування:"
    l2.config(font=("Courier", 18))
    l2.pack()

    e2=Entry(root, width=50)
    e2.insert(0,datetime.today().strftime('%Y-%m-%d'))
    e2.pack()

    l3= Label(root, bg='white', fg='black', width=100,
height=1, wraplength=900)
    l3['text']="Відділ апарату:"
    l3.config(font=("Courier", 18))
    l3.pack()

    e3=Entry(root, width=50)
    e3.pack()

    b1= Button(root, text="Почати тестування", command=start,
font=("Courier", 16), wraplength=900)
    b1.pack()

    b2= Button(root, text="Побудувати графік за ID",
command=plot1, font=("Courier", 16), wraplength=900)
    b2.pack()

    b3= Button(root, text="Знайти середнє за відділом",
command=av, font=("Courier", 16), wraplength=900)
    b3.pack()

def displ():
    global rec
    for widget in root.winfo_children():
        widget.destroy()

    l= Label(root, bg='white', fg='black', width=100, height=4,
wraplength=900)
    l['text']="Загальна оцінка: " + str(point)
    l.config(font=("Courier", 18))
    l.pack()

    text=Text(width=100, height=20)
    text.pack(side=LEFT)

    scroll=Scrollbar(command=text.yview)
    scroll.pack(side=LEFT, fill=Y)
    text.config(yscrollcommand=scroll.set)

    rec=[x for x in rec if x]
```

```
    for i in range(0, len(rec)):

a=str(rec[i]).replace("'","").replace("[","").replace("]","")
        text.insert((i+1)+0.0,str(i+1)+". "+a+"\n")

    rrr=[];
    rrr.append(data[0])
    rrr.append(data[1])
    rrr.append(data[2])
    rrr.append(point)
    rrr.append(rec)

    if os.path.exists("database.pickle") and
os.path.getsize("database.pickle") > 0:
        with open('database.pickle', 'rb') as handle:
            results = pickle.load(handle)
    else:
        results=[]

    results.append(rrr)

    with open('database.pickle', 'wb') as handle:
        pickle.dump(results, handle,
protocol=pickle.HIGHEST_PROTOCOL)

def but0():
    global ans
    global n
    global rec
    global point

    ans.append(0)
    rec.append(q_list[n][2][0])
    point+=float(q_list[n][3][0])
    for widget in root.winfo_children():
        widget.destroy()
    n+=1;
    if n<k:
        loop(n)
    else:
        displ()

def but1():
    global ans
    global n
    global rec
    global point

    ans.append(1)
    rec.append(q_list[n][2][1])
    point+=float(q_list[n][3][1])
    for widget in root.winfo_children():
```

```
        widget.destroy()
    n+=1;
    if n<k:
        loop(n)
    else:
        displ()

def but2():
    global ans
    global n
    global rec
    global point

    ans.append(2)
    rec.append(q_list[n][2][2])
    point+=float(q_list[n][3][2])
    for widget in root.winfo_children():
        widget.destroy()
    n+=1;
    if n<k:
        loop(n)
    else:
        displ()

def but3():
    global ans
    global n
    global rec
    global point

    ans.append(3)
    rec.append(q_list[n][2][3])
    point+=float(q_list[n][3][3])
    for widget in root.winfo_children():
        widget.destroy()
    n+=1;
    if n<k:
        loop(n)
    else:
        displ()

def loop(n):

    l= Label(root, bg='white', fg='black', width=100, height=4,
wraplength=900)
    l['text']=q_list[n][0]
    l.config(font=("Courier", 18))
    l.pack()


    b1= Button(root, text=q_list[n][1][0], command=but0,
font=("Courier", 16), wraplength=900)
    b1.pack()
```

```
    if q_list[n][1][1]!="":
        b2= Button(root, text=q_list[n][1][1], command=but1,
font=("Courier", 16), wraplength=900)
        b2.pack()

    if q_list[n][1][2]!="":
        b3= Button(root, text=q_list[n][1][2], command=but2,
font=("Courier", 16), wraplength=900)
        b3.pack()

if n==-1:
    begin()
elif n<k:
    loop(n)

root.mainloop()
```