Міністерство освіти і науки України
Національний університет «Одеська політехніка»
Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій
Кафедра кібербезпеки та програмного забезпечення

Галицький Валерій Павлович,
студент групи ЗРЗ-171

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

Розробка інформаційної системи нормативного забезпечення кібербезпеки підприємства

Спеціальність:
125 Кібербезпека

Спеціалізація, освітня програма:
Кібербезпека

Керівник:
Стопакевич Олексій Аркадійович,
к.т.н., доцент

Одеса – 2022

Міністерство освіти і науки України
Національний університет «Одеська політехніка»
Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій
Кафедра кібербезпеки та програмного забезпечення
Рівень вищої освіти перший (бакалаврський)
Спеціальність 125 – Кібербезпека
Освітня програма – Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри КБПЗ

_____
д.т.н.,проф. А.А.Кобозєва
____ _____2022р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Галицькому Валерію Павловичу

1.Тема роботи: *Розробка інформаційної системи нормативного забезпечення кібербезпеки підприємства,*
керівник роботи *Стопакевич Олексій Аркадійович, к. т. н., доцент,*
затверджені наказом ректора від „18” березня 2022 р. № 67- *в* .
2.Зміст роботи: *розробка інформаційної системи нормативного забезпечення кібербезпеки підприємства, створення алгоритму роботи інформаційної системи та вибір мови програмування і середовище розробки, розробка програмного забезпечення, створення користувацького інтерфейсу, охорона паці*.
3. Перелік ілюстративного матеріалу: *презентація.*

4. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
Охорона праці	Ярова І.А., доцент	Завдання видав	Завдання прийняв

5. Дата видачі завдання "_____"_____2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання	Примітка
1	*Аналіз джерел з теми випускної кваліфікаційної роботи*	*18. 03. 2022*	*виконано*
2	*Обґрунтування вибору рішення. Збір даних*	*22. 03. 2022*	*виконано*
3	*Написання І розділу кваліфікаційної роботи. Формування списку інформаційних джерел*	*25. 03. 2022*	*виконано*
4	*Написання ІІ розділу кваліфікаційної роботи. Формування бази міжнародних стандартів. Розробка алгоритму використання інформаційної системи*	*01. 04. 2022*	*виконано*
5	*Розробка програмного забезпечення на мові програмування Python*	*08. 04. 2022*	*виконано*
6	*Тестування розробленого програмного забезпечення*	*15. 04. 2022*	*виконано*
7	*Підготовка тексту роботи*	*22. 04. 2022*	*виконано*
8	*Підготовка презентації та доповіді*	*26. 04. 2022*	*виконано*
9	*Попередній захист*	*03. 06. 2022*	*виконано*
10	*Нормоконтроль, рецензування*	*17. 06. 2022*	*виконано*

Здобувач вищої освіти _____ *Галицький В.П.*

Керівник роботи _____ *Стопакевич О.А.*

ЗАВДАННЯ

на розробку розділу «Охорона праці»

Галицькому Валерію Павловичу, група ЗРЗ-171

Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій

Кафедра кібербезпеки та програмного забезпечення

Тема роботи *Розробка інформаційної системи нормативного забезпечення кібербезпеки підприємства*

Зміст розділу:

1 Аналіз умов праці і вибір основних заходів виробничої безпеки.

2 Аналіз пожежної безпеки. Вибір заходів та засобів пожежної безпеки.

Керівник роботи	Консультант з охорони праці
_____ (Стопакевич О.А.)	_____ (Ярова І.А)
«____» _____ 2022 р.	«____» _____ 2022 р.

АНОТАЦІЯ

Кваліфікаційна робота на тему «Розробка інформаційної системи нормативного забезпечення кібербезпеки підприємства» на здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 125 – Кібербезпека, спеціалізація, освітня програма: Кібербезпека, містить 18 рисунків, 1 додаток, 63 літературних джерел за переліком посилань. Робота виконана на 84 сторінках загального тексту і 70 сторінках основного тексту.

Метою роботи є створення інформаційної системи нормативного забезпечення кібербезпеки підприємства.

У роботі проведено підбір міжнародних стандартів з менеджменту кібербезпеки та визначень.

У результаті виконання кваліфікаційної роботи розроблено проект інформаційної системи нормативного забезпечення кібербезпеки підприємства, що дозволяє скоротити час для пошуку цих документів.

Результат даної роботи може бути використаний на підприємствах та в навчальних закладах студентами та викладачами.

ІНФОРМАЦІЙНА БЕЗПЕКА, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, СТАНДАРТИЗАЦІЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ, КІБЕРБЕЗПЕКА, КІБЕРПРОСТІР.

ABSTRACT

Qualification work on "Development of information system for regulatory cybersecurity of the enterprise" for the first (bachelor's) level of higher education in specialty 125 – Cybersecurity, specialization, educational program: Cybersecurity, contains 18 figures, 1 appendix, 63 literature sources by reference. The work is performed on 84 pages of general text and 70 pages of main text.

The purpose of the work is to create an information system for regulatory support of cybersecurity of the enterprise.

The paper selects international standards on cybersecurity management and definitions.

As a result of the qualification work, a project of the information system of regulatory support of cybersecurity of the enterprise was developed, which allows to reduce the time for searching for these documents.

The result of this work can be used in enterprises and educational institutions, especially students and teachers.

INFORMATION SECURITY, INFORMATION SECURITY MANAGEMENT SYSTEM, STANDARDIZATION OF INFORMATION SYSTEM, CYBER SECURITY, CYBERSPHERE.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

AES – Advanced Encryption Standard

ARPANET – The Advanced Research Projects Agency Network

BS – British Standard

BSI – British Standards Institution

COBIT – Control Objectives for Information and Related Technologies

DoS – Відмови у наданні послуг

ISO – International Organization for Standardization

ITIL – Information Technology Infrastructure Library

QSA – Qualified Security Assessor

ВДТ – Відеодисплей термінал

ІБ – Інформаційна безпека

ПЗ – Програмне забезпечення

ПК – Персональний комп’ютер

СМІБ – Система менеджменту інформаційної безпеки

СУІБ – Система управління інформаційною безпекою

ВСТУП

Однією з визначних рис XXI століття є постійний розвиток інформаційних технологій. На сьогодні складно знайти соціальну сферу, яка б не була занурена в світ технології та інформації. Глобалізація всіх сфер життя окрім переваг, містить ряд загроз як для суспільства, організації в цілому так і для окремої людини. Захист інформаційних даних є одним з найбільш актуальних питання сьогодення, адже існує низка загроз інформаційної безпеки, що в свою чергу впливають на якість роботи підприємств тощо.

Вивченням даного питання займається низка як вітчизняних та і зарубіжних вчених А.В.Авраменко, А.Б.Агапов, О.І.Барановський, В.Богуш, А.В.Войцехівський, О.Д.Довгань та ін.

Актуальність створення інформаційної системи нормативного забезпечення зумовлено величезним зростанням розмірів інформаційних ресурсів та даних, якими володіють підприємства та організації.

Мета дослідження – аналіз стандартів інформаційної системи та розробка інформаційної системи нормативного забезпечення відповідно стандартів.

Для досягнення цієї мети були поставлені наступні завдання:

1) опрацювати аналітичний матеріал і дати визначення поняття «інформаційна безпека», розглянути його основні компоненти та типи, а також етапи становлення інформаційної безпеки в кіберпросторі;
2) проаналізувати основні види загроз в кіберпросторі з якими можуть зіштовхнутися підприємства під час діяльності;
3) розглянути сутність систем управління інформаційною безпекою та їх роль у забезпечення якісної роботи підприємства;
4) проаналізувати основні інформаційні стандарти та їхню суть;
5) розробити програмне забезпечення інформаційної системи по стандартизації в кібербезпеці.

Об’єктом дослідження є вивчення стандартів інформаційної безпеки для СУІБ.

Предметом дослідження є прикладні аспекти впровадження розробленого програмного забезпечення інформаційної системи по стандартизації в кібербезпеці.

Методологічне підґрунтя роботи. Під час дослідження використовувалися аналітичні та емпіричні методи. Аналітичні допомагали опрацювати та проаналізувати теоретичний матеріал, визначети сутності ключових понять дослідження та їх суть; узагальнети основні понять, а емпіричні включали власну розробку програмного забезпечення інформаційної системи по стандартизації в кібербезпеці.

Джерельну базу дослідження склали:

- праці таких вітчизняних і зарубіжних учених (А. В. Авраменко, А. Б. Агапов, О.І.Барановський, В.Богуш, А.В.Войцехівський, О.Д.Довгань, В.Ц.Жидецький, О.О.Золотар, С.В.Ковтун, В.Н.Лопатин та ін.);
- стадндарти інформаційної безпеки (ISO/IEC 27005 ISO/IEC 27005:2008; ISO/IEC 27006; ISO/IEC 27002 та ін..);
- ресурси мережі Інтернет.

Практична значимість полягає в можливості використання результатів при подальших дослідженнях у сфері кібербезпеки та застосовуватися у практичній діяльності підприємств з метою впровадження ефективного менеджменту, який буде якісно впливати на кінцевий результат підприємства.

1 АНАЛІЗ ТЕОРЕТИКО-МЕТОДОЛОГІЧНИХ ЗАСАД КІБЕРБЕЗПЕКИ

1.1 Аналіз розвитку поняття «інформаційна безпека» та його наукове тлумачення

В сучасному світі інформація стає стратегічним ресурсом, одним з основних багатств економічно розвиненої держави. У глобалізованому світі інформація є рушійною силою підприємств і економік. Розвиток сучасного суспільства багато в чому ґрунтується на використанні інформаційних ресурсів. Створення нових засобів зв’язку та алгоритмів обробки інформації (втілених у програмні продукти) сприяє зміцненню ролі інформації у суспільстві. Швидкі процеси інформатизації в Україні та їх проникнення у всі сфери життєво важливих інтересів особистості, суспільства та держави, окрім безперечних переваг викликали низку суттєвих проблем. Однією з проблем стала проблема захисту інформації [4].

В наш час у багатьох країнах світу на державному рівні створено концепції інформаційної безпеки. Це пов'язано з практичними потребами попередження негативних наслідків впливу на економічну та суспільну інфраструктуру шкідливого програмного забезпечення (ПЗ), а також інших факторів, що створюють загрози розвитку інформаційної сфери суспільства [7]. Щоб зрозуміти концепцію «інформаційної безпеки», потрібно зрозуміти походження даного поняття. Інформаційна безпека почалася задовго до виникнення перших комп’ютерів: перший відомий шифр було створено Юлієм Цезарем, який мав на меті захистити листування з його довіреними особами. Сьогодні криптографія використовується для захисту комп'ютерів [8]. В.М.Лопатін вважає, що інформаційна безпека, як самостійна категорія, виникла у зв'язку з появою в людей способів комунікації та усвідомленням того, що за допомогою цих комунікацій може бути завдано шкоди самим людям [36]. Можна виділити наступні етапи розвитку комунікаційних технологій:

– перший етап до 1816 року: способи комунікації були природними і під їх захистом передбачалося збереження справжньої інформації про факти історії або дані, які мали важливе значення для індивіда або цілої спільноти.

– другий етап починається з 1816: пов'язаний з ускладненням способу комунікації, а саме використанням технічних засобів. Принцип захисту інформації зберігався той самий, але став складнішим з технічної точки зору (застосування завадового кодування повідомлення (сигналу) з подальшим декодуванням прийнятого повідомлення (сигналу).

– третій етап бере свій початок у 1935 році та пов'язаний з появою радіолокаційних та гідроакустичних засобів. Основним вектором інформаційної безпеки у даний період була сукупність людської організації та технічних моментів, під час передачі інформації шляхом радіосигналу.

– четвертий етап починається у 1946 році: пов'язаний з винаходом та впровадженням у практичну діяльність електронно-обчислювальних машин (ЕОМ). Основним завданням інформаційної безпеки було обмеження допуску сторонніх осіб до ЕОМ, оскільки з їх допомогою здійснювалася передача, обробка і перехоплення інформації.

– п'ятий етап починається з 1965 року та бере свій початок у зв'язку з розвитком локальних інформаційно-комунікаційних мереж. Проблеми інформаційної безпеки, як і раніше, вирішувалися шляхом фізичного усунення сторонніх персон від адміністрування локальних мереж.

– шостий етап один із ключових, він бере свій початок у 1973 році та пов'язаний з появою мобільних комунікаційних пристроїв з широким спектром завдань. Забезпечення інформаційної безпеки ускладнилося у зв'язку з появою людей, які завдають шкоди інформаційним даним окремих користувачів або навіть цілих країн. Інформаційний ресурс стає одним з найважливіших, як і збереження його безпеки.

– сьомий етап починається у 1985 році у зв'язку зі створенням та розвитком мобільних комунікаційних мереж з використанням космічних засобів

забезпечення. Забезпечення інформаційної безпеки ще більше ускладнюється через прискорення засобів комунікації.

– восьмий етап з початку 1999 рік і до сьогодні: характеризується надінтенсивним прискоренням появи нових інформаційних технологій або, іншими словами, прискорення технологічних циклів. У зв'язку з цим забезпечення інформаційної безпеки з кожним роком стає все складнішим, як технологічно, так і організаційно, оскільки система постійно прибуває в стані очікування загрози. У зв'язку з цим доцільно вказати мету інформаційної безпеки [36].

На сьогодні не існує єдиного підходу до трактування поняття «інформаційна безпека» [47, с.67]. Одні науковці розглядають як стан, інші ж як процес, діяльність, здатність, властивість, функцію. Відповідно до законодавства України «інформаційна безпека» - це «стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації» [43]. Варто зазначити, що інтереси особи, суспільства та держави мають бути врівноважені та доповнювати один одного. Для досягнення балансу даних інтересів необхідно розкрити їхню сутність. Інтереси особистості в інформаційні сфері полягають у реалізації конституційних прав людини та громадянина на доступ до інформації, використання інформації, а також у захисті інформації, що забезпечує особисту безпеку. Інтереси суспільства в інформаційній сфері полягають у забезпеченні інтересів особистості у цій сфері, зміцненні демократії, створенні правової соціальної держави. Інтереси держави – це створення умов гармонійного розвитку інформаційної інфраструктури, для реалізації конституційних прав та свобод людини та громадянина в галузі отримання інформації та її використання з метою забезпечення непорушності конституційного ладу, суверенітету та територіальної цілісності країни, політичної, економічної та соціальної стабільності, у забезпеченні законності та

правопорядку, розвитку рівноправного та взаємовигідного міжнародного співробітництва [47, с.121].

Згідно з В.І.Ярочкіним, інформаційна безпека – це єдиний цілісний механізм, у якому поєднано різні засоби, методи та заходи, що спрямовані на захист інформації від розголошення, витоку та несанкціонованого доступу до неї. Поява даного феномену зумовлена тим, що суспільство починає подолання негативних наслідків інформатизації [50].

А.Б.Агапов розглядав інформаційну безпеку як один із елементів державної безпеки, що лише опрацьовує інформацію, яка представляє державну важливість. Інші питання у його підході виводяться за рамки поняття інформаційна безпека та належать до «забезпечення національної безпеки у сфері інформатизації та індивідуальних інформаційних прав» [2].

А.І.Поздняков розглядає проблему інформаційної безпеки, як наслідок феномена інформаційної війни. Він визначає інформаційну безпеку, як планування та нейтралізацію небезпечних інформаційних впливів [41].

В.Богуш визначає інформаційну безпеку як стан захищеності інформаційного середовища відповідно до інтересів держави при якому відбувається формування, використання і розвиток незалежно від внутрішніх та зовнішніх інформаційних загроз [8].

В.А.Ліпкан, В.А.Авраменко зазначають, що інформаційна безпека - це стан захищеності життєво важливих інтересів особи, суспільства та держави [34; 35].

Відповідно до Р.А.Калюжного, це стан захищеності інформаційного простору, що забезпечує розвиток та формування цього простору в інтересах особистості, суспільства та держави [27].

Н. Р.Нижник, Я.М.Жарков, В.Т.Білоус трактують «інформаційну безпеку» як стан правових норм та відповідних їм інститутів безпеки, що гарантують наявність даних для прийняття стратегічних рішень та захист інформаційних ресурсів країни [39].

О.І.Барановський вважає, що це стан захищеності національних інтересів України в інформаційному просторі, який не допускає або зводить до мінімуму

нанесення шкоди особі, суспільству або державі через неповноту, несвоєчасність, недостовірність інформації та її несанкціоноване поширення і використання, а також через негативний інформаційний вплив та негативні наслідки функціонування інформаційних технологій [6]. Типи інформаційної безпеки перелічені в табл.1.1.

Таблиця 1.1 – Типи інформаційної безпеки [10]

Безпека застосунків (Application security)	Охоплює вразливості програмного забезпечення у веб- та мобільних застосунках та інтерфейсах програмного забезпечення (API). Ці вразливості можна знайти в аутентифікації або авторизації користувачів, цілісності коду та конфігурацій. Уразливості програми можуть створити точки входу для значних порушень інформаційної безпеки. Безпека програм є важливою частиною захисту для інформаційної безпеки.
Безпека хмарного середовища (Cloud security)	Зосереджена на створенні та розміщенні безпечних застосунків у хмарних середовищах та безпечному використанні хмарних додатків сторонніх розробників. «Хмара» просто означає, що програма працює у спільному середовищі. Підприємства повинні переконатися, що існує достатня ізоляція між різними процесами в спільному середовищі.
Криптографія (Cryptography)	Шифрування даних, що передаються, і даних, що зберігаються, допомагає забезпечити конфіденційність і цілісність даних. Цифрові підписи зазвичай використовуються в криптографії для перевірки достовірності даних. Криптографія та шифрування стають все більш важливими. Хорошим прикладом використання криптографії є Advanced Encryption Standard (AES). AES – це алгоритм симетричного ключа, який використовується для захисту секретної урядової інформації.
Безпека інфраструктури (Infrastructure security)	Безпека інфраструктури займається захистом внутрішніх і зовнішніх мереж, лабораторій, центрів обробки даних, серверів, настільних комп’ютерів і мобільних пристроїв.
Реакція на інцидент (Incident response)	Реакція на інциденти – це функція, яка відстежує та досліджує потенційно шкідливу поведінку. Готуючись до порушень, IT-персонал повинен мати план реагування на інциденти для стримування загрози та відновлення мережі. Крім того, план має створити систему збереження доказів для судово-медичного аналізу та потенційного судового переслідування. Ці дані можуть допомогти запобігти подальшим порушенням і допомогти співробітникам виявити зловмисника.
Управління вразливістю (Vulnerability management)	Управління вразливими місцями – це процес сканування середовища на наявність слабких місць і визначення пріоритетів усунення на основі ризику. У багатьох мережах підприємства постійно додають програми, користувачів, інфраструктуру тощо. З цієї причини важливо постійно сканувати мережу на наявність потенційно вразливих місць. Завчасне виявлення вразливості може застерегти бізнес від великих втрат.

Основними компонентами інформаційної безпеки є [7]:

– Конфіденційність: дані вважаються конфіденційними, якщо доступ до них мають лише уповноважені особи. Для забезпечення конфіденційності мають використовуватися всі методи, що розролбені для безпеки, як-от надійний пароль, шифрування, аутентифікація та захист від атак проникнення.

– Цілісність: збереження даних і запобігання їх випадковим або зловмисним змінам. Методи, що використовуються для конфіденційності, можуть захистити цілісність даних, оскільки кіберзлочинець не може змінити дані, якщо не може отримати до них доступ.

– Доступність є ще одним основним елементом інформаційної безпеки. Доступність інформаційної безпеки означає узгодження мережевих і обчислювальних ресурсів для обчислення доступу до даних і впровадження кращої політики для цілей аварійного відновлення.

Отже, інформаційна безпека – це стан інформаційної системи, за якого вона має здатність протистояти впливу внутрішніх і зовнішніх ризиків, не ініціюючи їхнє виникнення для елементів системи й зовнішнього середовища та захистити конфіденційну інформацію від несанкціонованих дій, включаючи перевірку, модифікацію, запис та будь-які порушення чи знищення.

1.2 Аналіз становлення кібербезпеки як інформаційної безпеки у кіберпросторі

Інформація відіграє важливу роль у повсякденному житті кожної людини, незалежно від її соціального статусу. Інформація генерується в різних формах, що дає безліч можливостей для її викрадення, тому на сьогодні інформаційна безпека є необхідністю.

Інформаційна безпека призначена для захисту конфіденційності, цілісності та доступності даних від тих, хто має зловмисні наміри зловживати цими даними різними способами. Це набір методів, які використовуються для запобігання та

виявлення інформації, що зберігається в цифрових або нецифрових носіях. Інформаційна безпека є важливою частиною кібербезпеки [20].

Кіберзлочинність та кібербезпека беруть свій початок з 1940-х років, а саме з появи першого цифрового комп'ютера, який був створений у 1943. Розглядаючи історичні аспекти розвитку інформаційних відносин, можна виділити наступні періоди становлення інформаційного безпеки у кіберпросторі:

Перший період 1940-і роки умовно можна назвати «час перед злочином». Протягом майже двох десятиліть після створення першого в світі цифрового комп'ютера здійснювати кібератаки було досить складно, адже доступ до гігантських електронних машин був обмежений. У світі було лише кілька таких комп'ютерів, вони були великі, шумні та складні у використанні. Комп'ютери не були підключені до мережі, що унеможливлювало передачу файлів чи даних і створювало так званий «безпечний клімат», загроз майже не існувало [20].

Теорія, що лежить в основі комп'ютерних вірусів, була вперше оприлюднена в 1949 році, коли Джон фон Нейман припустив, що комп'ютерні програми можуть відтворюватися. А в 1966 році вийшла його стаття «Теорія самовідтворювання автоматів» [48].

Другий період – це початок 1950-х років, період «телефонних фриків», людей, які були зацікавлені в особливостях роботи. Вони намагалися захоплювати наявні протоколи, які дозволяли інженерам працювати в мережі на відстані. Як результат, це дало можливість людям здійснювати безкоштовні дзвінки та знизити плату за міжміські дзвінки. Телефонні компанії не могли вплинути на ці процеси та зупинити фриків, хоча ця практика зрештою зникла в 1980-х роках [20].

Вважається, що Стів Джобс та Стів Возняк, засновники Apple, цікавилися спільнотою телефонних фриків, тому що цифрові технології, що використовують подібні концепції, згодом були розроблені в комп'ютерах Apple [20].

Третій період (1960-ті роки) – даний період характеризується рядом інновацій в комп'ютерні індустрії, проте комп'ютери все ще залишалися досить великими та дорогими системами.

Протягом наступного десятиліття відбувається розвиток терміну «хакерство». Передумовою став злом групою людей MIT Tech Model Railroad Club, високотехнологічних потягів, що мав на меті внести корективи в їх функціональність. Проте ранні хакерські атаки були спрямовані на отримання доступу до систем, не маючи жодної політичної чи комерційної вигоди [22].

З часом з'явилися нові, швидші та ефективніші способи злому. Одна з ключових подій відбулася в 1967 році. IBM запросила групу студентів, щоб випробувати нещодавно розроблений комп'ютер. Учні дізналися про мову комп'ютерної системи, отримали доступ до різних її частин системи, що в свою чергу дало IBM уявлення про вразливі місця системи. В результаті багато уваги стали приділяти розвитку оборонного мислення, розробці заходів безпеки. Це був важливий крок у розвитку стратегій кібербезпеки [22].

Четвертий період – 1970-ті роки: народжується комп'ютерна безпека, яка почалася з дослідницького проекту ARPANET (The Advanced Research Projects Agency Network), попередника Інтернету (див. рис.1.1) [31].

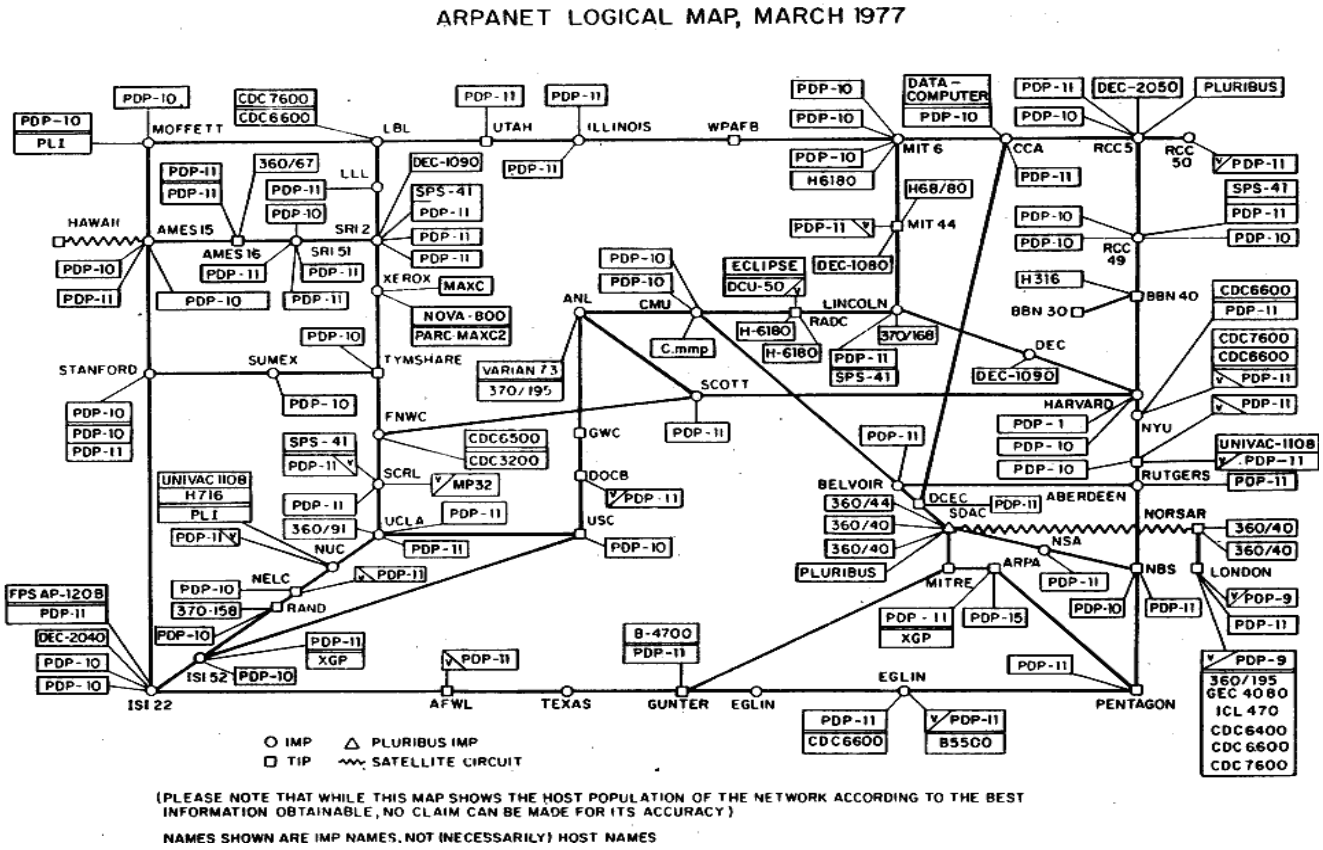

Рисунок 1.1 – Протоколи ARPANET для віддаленої комп'ютерної мережі

Інженер Боб Томас створив комп’ютерну програму під назвою Creeper, яка залишала слід у будь-якому місці, переміщаючись по мережі ARPANET. Creeper вважається першим комп’ютерним вірусом, хоч він і не мав на меті нанести шкоди. Дана програма залишала повідомлення: «I’M THE CREEPER: CATCH ME IF YOU CAN» (див. рис.1.2). Це викликало неабияку зацікавленість та певну стурбованість, тому винахідник електронної пошти Рей Томлінсон написав програму Reaper, яка переслідувала і видаляла Creeper. Reaper був не тільки першим прикладом антивірусного програмного забезпечення, це також була перша програма, що здатна до самовідтворення (перший комп’ютерний хробак) [31].

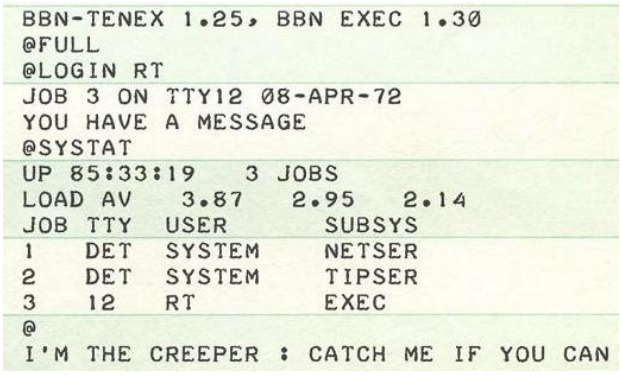

Рисунок 1.2 – Приклад послання Крипера

Це час активного розвитку комп’ютерних технологій, а оскільки більшість мереж залежали від телефонних систем, рівень попиту на способи захисту мереж постійно зростав. Кожне обладнання, що було підключено до мережі, створювало новий тип точки входу, а це в свою чергу робило мережу більш вразливою.

Уряди почали обговорювати шляхи зменшення цієї вразливості, адже несанкціонований доступ до цієї гігантської системи міг створити численні проблеми. Низка науковців працювало над дослідженням даної проблеми та над пошуком шляхів забезпечення цієї безпеки [31].

Відділ електронних систем (ESD) командування ВПС США почав працювати над проектами. Також було залучено підрозділ міністерства оборони США – гентство перспективних дослідницьких проектів (ARPA). Перед ними було поставлено завдання розробити систему безпеки для комп’ютерної системи

Honeywell Multics (HIS рівень 68). Інші організації такі як Стенфордський дослідницький інститут та UCLA почали працювати над мережевою безпекою [31]. Ключовим компонентом розвитку системи безпеки був проект аналізу захисту від ARPA, який включав широкий спектр тем: виявлення вразливості; робота над різними аспектами безпеки операційної системи; розробка автоматизованих методів виявлення вразливих місць у програмних системах [31].

До середини 1970-х років розвиток кібербезпеки зростав. У 1976 році в структурі операційної системи для підтримки безпеки та надійного програмного забезпечення було зазначено: «Безпека стала важливим та складним компонентом в розробці комп'ютерних систем».

У 1979 році було заарештовано першого кіберзлочинця, 16-річного Кевіна Мітніка. Йому вдалося зламати The Ark, комп'ютер у Digital Equipment Corporation, який використовувався для розробки операційних систем та зробити копії програмного забезпечення. Сьогодні він керує Mitnick Security Consulting [33].

П'ятий період – 1980-ті роки. Це десятиліття характеризується великою кількістю резонансних кібератак, зокрема атаки на AT&T, Лос-Аламосську національну лабораторію та National CSS. У 1983 році були розроблені нові терміни для опису цих атак, такі як «комп'ютерний вірус» і «троянський кінь» [20].

У цей час зростає страх загроз з боку інших урядів, оскільки це середина холодної війни. Кібершпигунство стає цілком реальним, тому уряд США створює нові рекомендації та ресурси для управління такими подіями та загрозами. В 1985 році Міністерством оборони США були розроблені критерії оцінки надійної комп'ютерної системи, що згодом отримали назву «Помаранчева книга». Це один з перших посібників із безпеки для комп'ютерів [33].

Незважаючи на це, у 1986 році німецькому хакеру Маркусу Гесс вдалося проникнути в урядові системи, використавши інтернет-шлюз у Берклі, Каліфорнія, щоб підключитися до мережі ARPANET. За лічені хвилини він зміг отримати доступ до 400 військових комп'ютерів, включаючи мейнфрейми в

Пентагоні, маючи намір продати інформацію КДБ [31]. З цього моменту ще більша увага почала приділятися безпеці, було розроблено стратегії для зменшення таких ризиків. Наприклад, було необхідно стежити за розміром файлів command.com, що надсилаються, адже збільшення їх розмірів було першою ознакою потенційного зараження. Ще однією ознакою було падіння доступної пам'яті, це може сигналізувати про зараження комп’ютерної системи.

В 1987 році, через рік після атаки Пентагону були розроблені та випущені перші комерційні антивірусні продукти: VirusScan розроблений Джоном Макафі; антивірусний продукт для Atari ST Kai Figge і Andreas Luning.; антивірусне рішення NOD випущено в Чехословаччині [20].

Також у 1987 році було одне з найперших задокументованих видалення вірусів, здійснено німцем Берндом Фіксом. Він нейтралізував сумнозвісний вірус Vienna – ранній приклад зловмисного програмного забезпечення, яке поширювало та пошкоджувало файли [20].

Орім цього, це рік появи зашифрованого вірусу Cascade, який заражав файли .COM. Через рік Cascade спричинив серйозний інцидент у бельгійському офісі IBM і став поштовхом для розробки антивірусного продукту IBM (див. рис. 1.3). До цього будь-які антивірусні рішення, розроблені в IBM, були призначені лише для внутрішнього використання [49].

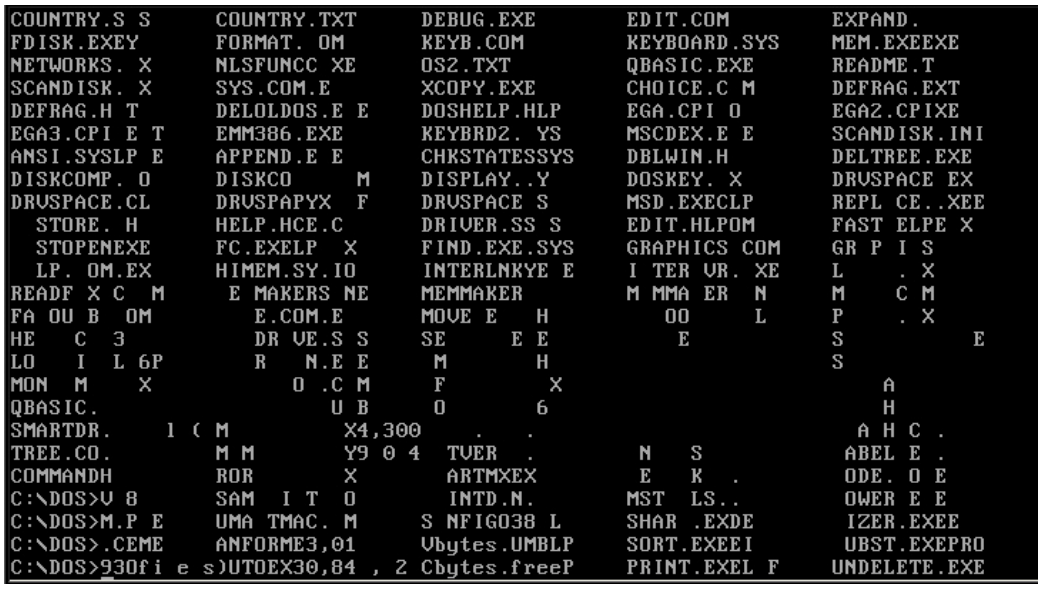

Рисунок 1.3 – Вірус Cascade

До 1988 року в усьому світі було створено багато антивірусних компаній, зокрема Avast, засновану Едуардом Кучерою та Павлом Баудішем у Празі, Чеська Республіка. Сьогодні Avast має команду з понад 1700 співробітників по всьому світу і зупиняє близько 1,5 мільярда атак щомісяця [49].

Десятиліття завершилося новими доповненнями до ринку кібербезпеки, зокрема F-Prot, ThunderBYTE та Norman Virus Control. У 1989 році IBM нарешті комерціалізувати свій внутрішній антивірусний проект, і IBM Virscan для MS-DOS надійшов у продаж за 35 доларів [20].

*Шостий період (*1990-ті роки) став періодом неймовірного зростання та розвитку Інтернету. Паралельно зростала індустрія кібербезпеки [31].

У 1990 році було:

- створено перші поліморфні віруси (код, який мутує, зберігаючи оригінальний алгоритм недоторканим, щоб уникнути виявлення);
- британський комп'ютерний журнал PC Today випустив видання з безкоштовним диском, який «випадково» містив вірус DiskKiller, який заразив десятки тисяч комп'ютерів;
- створено EICAR (Європейський інститут комп’ютерних антивірусних досліджень) [31].

Ранній антивірус був виключно на основі сигнатур, порівнюючи двійкові файли в системі з базою даних «сигнатур» вірусів, тому ранній антивірус давав багато помилкових спрацьовувань і використовував велику обчислювальну потужність, що розчаровувало користувачів, оскільки продуктивність уповільнювалася.

У 1990-х роках кількість нових вірусів і зловмисного програмного забезпечення виросла з десятків тисяч на початку десятиліття до 5 мільйонів щороку до 2007 року. До середини 90-х стало зрозуміло, що кібербезпеку потрібно масово створювати для захисту населення. Один дослідник NASA розробив першу програму брандмауера, моделюючи її на фізичних структурах, які запобігають поширенню реальних пожеж у будівлях [49].

Кінець 1990-х характеризується конфліктами і непорозумінням між розробниками антивірусів [49]:

– McAfee звинуватив Dr. Solomon в обмані, оскільки тестування незаражених дисків показало хороші результати швидкості, а тести сканування колекцій вірусів показали хороші результати виявлення. Dr. Solomon подав позов у відповідь.

– Тайванський розробник Trend Micro звинуватив McAfee і Symantec у порушенні патенту на технологію перевірки вірусів через Інтернет та електронну пошту. Потім Symantec звинуватила McAfee у використанні коду з Norton AntiVirus Symantec.

Наприкінці 1990-х років свого поширення набула електронна пошта, і хоча вона обіцяла революціонізувати комунікацію, вона також відкрила нову точку входу для вірусів [49].

У 1999 році з'явився вірус Melissa, який увійшов на комп'ютер користувача через документ Word, а потім надіслав свої копії електронною поштою на перші 50 адрес електронної пошти в Microsoft Outlook. Він залишається одним із найшвидше поширюваних вірусів, а його виправлення коштує близько 80 мільйонів доларів [31].

Сьомий період – 2000-ні роки, період неймовірного зростання Інтернету, комп'ютери почали з'являтися у більшості будинків та офісів, що незважаючи на всі переваги, створило більше можливостей для кіберзлочинців [20].

На початку десятиліття виник новий тип зараження, більше не було необхідності завантажувати файли, а досить було лише зайти на веб-сайт, заражений вірусом.

У цей час також утворилася перша група хакерів, яка розпочала кампанію кібератак для різних цілей. Одна із перших груп, яка стала відома, це група, що зламала Церкву Саєнтології та розповсюджувала атаки відмови в обслуговуванні (DDoS-атаки). Група, яка називається Anonymous, продовжує створювати атаки для різних високопоставлених цілей і сьогодні [20].

2000-ті роки – це період злому кредитних карток. Група Альберта Гонсалеса викрала конфіденційну інформацію з 45,7 мільйонів кредитних карток, отримавши доступ через базу даних роздрібного продавця. Це створило потребу зосередитися на інформаційній безпеці різних секторів, у тому числі роздрібних торговців [49].

Ще одним нововведенням цього десятиліття стала безпека ОС – кібербезпека, вбудована в операційну систему, що забезпечує додатковий рівень захисту.

Восьмий період – 2010-ті роки. Період, коли кібератаки почали впливати на національну безпеку країн та коштувати бізнесу мільйони [47]:

2012: Саудівський хакер 0XOMAR публікує в Інтернеті деталі більш ніж 400 000 кредитних карток.

2013: Колишній співробітник ЦРУ в уряді США Едвард Сноуден скопіював та злив секретну інформацію з Агентства національної безпеки (АНБ).

2013-2014: Зловмисники зламали Yahoo, зламавши облікові записи та особисту інформацію 3 мільярдів користувачів. Згодом Yahoo був оштрафований на 35 мільйонів доларів за нерозголошення новини.

2017: програма-викуп WannaCry заразила 230 000 комп’ютерів за один день.

2019: численні DDoS-атаки змусили фондовий ринок Нової Зеландії тимчасово закритися.

Кібербезпека нового покоління використовує різні підходи для підвищення рівня виявлення нових безпрецедентних загроз, це включає [47]:

- Багатофакторну аутентифікацію (MFA).
- Network Behavioral Analysis (NBA) – виявлення шкідливих файлів на основі поведінкових відхилень або аномалій.
- Розвідка загроз та автоматизація оновлення.
- Захист у режимі реального часу – також називається скануванням при доступі, захистом у фоновому режимі, постійним щитом та автозахистом.
- Sandboxing – створення ізольованого тестового середовища.
- Криміналістична експертиза.

- Резервне копіювання та дзеркальне відображення.
- Брандмауери веб-додатків (WAF) – захист від міжсайтового підроблення, міжсайтових сценаріїв (XSS), включення файлів та ін’єкції SQL.

Дев’ятий період – 2020-ті роки. Пандемія COVID-19 змусила величезну кількість людей залишити офіс і перейти онлайн, що зумовило збільшення кількості кібератак в різних галузях [31].

Мабуть, найбільш гучний злом 2020 року, завдяки клієнтам, включаючи Міністерство оборони США та корпорацію Microsoft, кіберзлочинці змогли пошкодити один із серверів, який надавав доступ до виправлень та оновлень для інструментів SolarWinds Orion [31].

Серед інших відомих зломів 2020 року – кілька акаунтів знаменитостей у Твіттері, облікові записи, на яких стався цей інцидент, включали Apple і Uber, а також таких осіб, як Ілон Маск, Білл Гейтс, Уоррен Баффет, Каньє Вест, Джефф Безос і Флойд Мейвезер [49].

Крім того, у 2020 році внаслідок злому Marriot близько 5,2 мільйонів гостей готелю було отримано доступ до даних, включаючи дати народження, номери телефонів, імена, адреси. Також, незважаючи на неймовірно швидке зростання та впізнаваність бренду за одну ніч, у Zoom було кілька помітних порушень безпеки, включаючи приблизно 500 000 облікових записів користувачів, які були опубліковані для продажу на темному веб-форумі [49]

1.3 Аналіз основних загроз кібербезпеці підприємств

На сьогодні існує низка загроз інформаційної безпеки у кіберпросторі. Під загрозою розуміється будь-яка можлива зловмисна атака, спрямована на незаконний доступ до даних, порушення цифрових операцій або пошкодження інформації. Щодня велика кількість підприємств та приватних систем зазнають кібератак, різноманітність яких швидко зростає. За словами колишнього генерального директора Cisco Джона Чемберса, «Є два типи компаній: ті, які були зламані, і ті, які ще не знають, що їх зламали» [34].

Розглянемо декілька основних типи інформаційних загроз у кіберпросторі [26]:

1. Шкідливе програмне забезпечення – це зловмисне програмне забезпечення, таке як шпигунські програми, програми-вимагачі, віруси та хробаки. Шкідливе програмне забезпечення активується, коли користувач натискає шкідливе посилання або вкладення, що призводить до встановлення небезпечного програмного забезпечення. Зловмисне програмне забезпечення після активації може: блокувати доступ до ключових мережевих компонентів; встановлювати додаткове шкідливе програмне забезпечення; приховано отримувати інформацію, передаючи дані з жорсткого диска (шпигунське програмне забезпечення); пошкоджувати окремі частини, що робить всю систему непрацездатною.

2. Рекламне програмне забезпечення – рекламне програмне забезпечення не зовсім шкідливе, але воно порушує конфіденційність користувачів. Вони показують рекламу на робочому столі комп’ютера або в окремих програмах. До них додається безкоштовне програмне забезпечення, що є основним джерелом доходу для таких розробників. Вони стежать за вашими інтересами та показують релевантну рекламу. Зловмисник може вбудувати шкідливий код усередину програмного забезпечення, а рекламне програмне забезпечення може стежити за діяльністю вашої системи і навіть може скомпрометувати вашу машину.

3. Шпигунське ПЗ – це програма або, можна сказати, програмне забезпечення, яке відстежує вашу діяльність на комп’ютері та розкриває зібрану інформацію зацікавленій стороні. Шпигунське програмне забезпечення зазвичай скидається троянськими програмами, вірусами або хробаками. Після падіння вони встановлюються самі і сидять мовчки, щоб уникнути виявлення. Одним із найпоширеніших прикладів шпигунського програмного забезпечення є KEYLOGGER. Основне завдання кейлоггера — записувати натискання клавіш користувача з міткою часу. Таким чином фіксує цікаву інформацію, як-от ім’я користувача, паролі, дані кредитної картки тощо.

4. Програми-вимагачі – це тип зловмисного програмного забезпечення, яке або зашифрує ваші файли, або заблокує ваш комп’ютер, зробивши його частково

або повністю недоступним. Потім з’явиться екран із запитом на гроші, тобто викуп в обмін.

5. Страшне програмне забезпечення – воно маскується як інструмент, який допомагає виправити вашу систему, але коли програмне забезпечення буде запущено, воно заразить вашу систему або повністю знищить її. Програмне забезпечення відобразить повідомлення, щоб налякати вас і змусити вжити певних дій, наприклад заплатити їм, щоб виправити вашу систему.

6. Руткіти – призначені для отримання root-доступу, адміністративних привілеїв у системі користувача. Отримавши root-доступ, експлуататор може робити що завгодно: від крадіжки приватних файлів до приватних даних.

7. Емотет. Агентство з кібербезпеки та безпеки інфраструктури (CISA) описує Emotet як «розширений, модульний банківський троян, який в основному функціонує як завантажувач інших банківських троянів. Emotet продовжує залишатися однією з найдорожчих і найруйнівніших шкідливих програм».

8. Відмова в обслуговуванні (Denial of Service) – це тип кібератаки, яка переповнює комп’ютер або мережу, тому вони не можуть відповідати на запити. Розподілений DoS (DDoS) робить те ж саме, але атака відбувається з комп’ютерної мережі. Кібер-зловмисники часто використовують флуд-атаки, щоб порушити процес «рукостискання» та здійснити DoS. Можна використовувати кілька інших методів, і деякі кібер-зловмисники використовують час, коли мережа відключена, щоб запустити інші атаки. За словами Джеффа Мельника з Netwrix, компанії, що займається програмним забезпеченням безпеки інформаційних технологій, ботнет — це тип DDoS, при якому мільйони систем можуть бути заражені шкідливим програмним забезпеченням і контрольовані хакером. Ботнети, які іноді називають зомбі-системами, націлені й переповнюють можливості обробки цілі. Ботнети знаходяться в різних географічних місцях і їх важко відстежити.

9. Атака «людина посередині» (Man in the Middle) відбувається, коли хакери входять у двосторонню транзакцію. За словами Cisco, після переривання трафіку вони можуть фільтрувати та красти дані. Атаки MITM часто відбуваються, коли

відвідувач використовує незахищену загальнодоступну мережу Wi-Fi. Зловмисники вставляють себе між відвідувачем і мережею, а потім використовують зловмисне програмне забезпечення для встановлення програмного забезпечення та шкідливого використання даних.

10. Фішингові атаки використовують фальшиве спілкування, наприклад електронну пошту, щоб обманом змусити одержувача відкрити його та виконати інструкції всередині, наприклад вказати номер кредитної картки. «Мета — вкрасти конфіденційні дані, такі як дані кредитної картки та логіну, або встановити шкідливе програмне забезпечення на комп'ютер жертви», — повідомляє Cisco.

11. Ін'єкція мови структурованих запитів (SQL) — це тип кібератаки, яка виникає внаслідок вставки шкідливого коду на сервер, який використовує SQL. При зараженні сервер випускає інформацію. Надіслати шкідливий код можна так само просто, як ввести його у вікно пошуку уразливого веб-сайту.

12. Атаки паролем. За допомогою правильного пароля кібер-зловмисник має доступ до великої кількості інформації. Соціальна інженерія — це тип атаки паролем, яку Data Insider визначає як «стратегію, яку використовують кібер-зловмисники, яка в значній мірі залежить від взаємодії людей і часто передбачає обман людей, щоб вони порушили стандартні методи безпеки». Інші типи атак на паролі включають доступ до бази даних паролів або пряме здогадування.

Окрім цих, існує багато інших загроз, так званих «загроз нового покоління»:

Атаки в соціальних мережах – у цьому кіберзлочинці ідентифікують та заражають кластер веб-сайтів, які відвідують особи певної організації, щоб викрасти інформацію [28].

Шкідливе програмне забезпечення для мобільних пристроїв – існує приказка, коли є підключення до Інтернету, буде небезпека для безпеки. Те саме стосується мобільних телефонів, де ігрові програми призначені для того, щоб спонукати клієнтів завантажити гру, і вони ненавмисно встановлять на пристрій шкідливе програмне забезпечення або вірус [28].

Застаріле програмне забезпечення. Оскільки щодня з’являються нові загрози, оновлення програмного забезпечення є необхідною умовою, щоб мати повністю захищене середовище [28].

Корпоративні дані на персональних пристроях – сьогодні кожна організація дотримується правила BYOD (Bring your own device). BYOD означає принести на робоче місце свій власний пристрій, як-от ноутбуки, планшети. Очевидно, що BYOD становить серйозну загрозу для безпеки даних [28].

Соціальна інженерія – це мистецтво маніпулювання людьми, щоб вони передали свою конфіденційну інформацію, як-от реквізити банківського рахунку, пароль тощо. Ці злочинці можуть обманом отримати вашу особисту та конфіденційну інформацію, або завоювати вашу довіру, щоб отримати доступ до вашого комп’ютера та встановити шкідливе програмне забезпечення, яке дасть їм контроль над ним. Наприклад, електронна пошта або повідомлення від вашого друга, яке, ймовірно, не було надіслано вашим другом. Злочинець може отримати доступ до вашого пристрою друзів, а потім, отримавши доступ до списку контактів, він може надсилати заражену електронну пошту та повідомлення всім контактам. Оскільки повідомлення/електронний лист надійшло від відомої особи, одержувач обов’язково перевірить посилання або вкладений файл у повідомленні, таким чином ненавмисно заразивши комп’ютер [28].

2 РОЗРОБКА ІНФОРМАЦІЙНОЇ СИСТЕМИ ПО СТАНДАРТИЗАЦІЇ В КІБЕРБЕЗПЕЦІ

2.1 Вибір системи програмного забезпечення для розробки інформаційної системи по стандартизації в кібербезпеці

На сьогодні відбувається глобальна комп’ютеризація всіх сфер діяльності суспільства, тому для забезпечення інформаційної безпеки в кіберпросторі постала необхідність розробки системи управління інформаційною безпекою (СУІБ) та створення єдиної та загальної системи стандартів інформаційної безпеки.

Система управління інформаційною безпекою – це документована система управління, що складається з набору засобів контролю безпеки, які захищають конфіденційність, доступність і цілісність активів від загроз і вразливостей; це системний підхід до розробки, впровадження, функціонування, моніторингу, аналізу, забезпечення та покращення інформаційної безпеки організації для досягнення бізнес-цілей. Розробляючи, впроваджуючи, керуючи та підтримуючи СУІБ, організації можуть захистити свої особисті та конфіденційні дані від компрометації [23].

Дана система управління ґрунтується на оцінці ризиків та рівнях прийнятності ризиків організації, встановлених таким чином, щоб результативно обробляти ризики та керувати ними. Успішна реалізація СУІБ можлива за умови аналізу вимог щодо захисту інформаційних активів та застосування засобів управління для забезпечення захисту цих інформаційних активів відповідно до ситуації. Також чинниками, які сприяють успішній реалізації системи управління інформаційної безпеки є [41]:

- усвідомлення необхідності забезпечення інформаційної безпеки;
- призначення відповідальності за інформаційну безпеку;
- поєднання зобов'язань керівництва з інтересами заінтересованих сторін;
- підвищення значення соціальних цінностей;
- оцінка ризику, що визначає відповідні засоби управління для забезпечення
- прийнятних рівнів ризику;

- безпека як невід'ємний елемент інформаційних мереж та систем;
- активне попередження та виявлення інцидентів інформаційної безпеки;
- забезпечення комплексного підходу до управління інформаційною безпекою;
- постійна переоцінка рівня інформаційної безпеки та внесення змін.

за потреби.

Ефективне впровадження СУІБ є дуже складним процесом, при імплементації якого потрібно враховувати наступні кроки [46]:

1. Визначення обсягу послуг. Керівництво компанії має чітко визначити сфери застосування, цілі та межі СУІБ.

2. Визначення активів, які повинні бути захищені СУІБ. Це можуть бути інформація, програмне забезпечення, послуги та фізичні активи, такі як комп’ютери, кваліфікація, навички та досвід співробітників, а також інші нематеріальні активи, такі як репутація та репутація. Головна мета на даному етапі визначити критично важливі для бізнесу активи, від яких залежить виживання компанії.

3. Визначення та оцінка ризиків. Для кожного активу, який варто захищати, мають бути ідентифіковані та класифіковані потенційні ризики на основі юридичних вимог або вказівок щодо відповідності. Організації повинні визначити, який вплив мав би кожен ризик, якщо було б порушено конфіденційність, цілісність і доступність, або яка ймовірність виникнення ризиків, для того, щоб оцінити, які ризики є прийнятними, наприклад, з огляду на очікувану суму заподіяної шкоди, і які необхідно усунути за будь-яку ціну.

4. Визначення заходів. На основі попередньої оцінки ризику повинні бути обрані та впроваджені відповідні технічні та організаційні заходи для пом’якшення чи уникнення ризику. Це включає визначення чітких компетенцій та відповідальності.

5. Перевірка ефективності: застосовані та впроваджені заходи необхідно постійно контролювати та регулярно перевіряти на ефективність, наприклад, шляхом аудитів.

6. Внесення покращення. Якщо перевірка запроваджених заходів виявляє недоліки або були виявлені нові ризики, процес СУІБ необхідно запустити знову з самого початку. Таким чином, СУІБ можна постійно адаптувати до мінливих умов або вимог, постійно покращуючи інформаційну безпеку в компанії.

За допомогою СУІБ інформаційну безпеку можна систематично впроваджувати в усій компанії та забезпечувати дотримання всіх необхідних стандартів безпеки . Цей комплексний профілактичний підхід має ряд переваг [29]:

Захист конфіденційної інформації: СУІБ гарантує, що власні інформаційні активи (наприклад, інтелектуальна власність, дані персоналу або фінансові дані), а також дані, довірені клієнтами або третіми сторонами, будуть належним чином захищені від будь-яких загроз.

Підтримка безперервності бізнесу: використовуючи СУІБ для того, щоб зробити інформаційну безпеку невід’ємною частиною своїх бізнес-процесів, компанії можуть постійно підвищувати рівень безпеки та зменшувати ризики інформаційної безпеки; таким чином вони протидіють ризику інцидентів безпеки, які порушують безперервність бізнесу.

Відповідність вимогам: застосовуються суворі вимоги до відповідності, особливо в дуже регульованих секторах, таких як фінанси або критична інфраструктура; порушення законодавчих норм і договірних угод можуть призвести до великих штрафів; завдяки СУІБ компанії гарантують, що вони відповідають всім нормативним та договірним вимогам, що також надає їм більшу операційну та юридичну визначеність.

Перевірка інформаційної безпеки: сертифікуючи свої СУІБ, компанії можуть перевіряти третім сторонам, що конфіденційна інформація обробляється безпечно; це сприяє кращому зовнішньому іміджу та формуванню довіри, що, у свою чергу, означає конкурентну перевагу.

Підвищення економічної ефективності та зниження витрат: структурована координація та орієнтоване на ризики планування заходів у СУІБ допомагає розставляти пріоритети, ефективно використовувати ресурси та інвестувати в

потрібних місцях. Таким чином, після початкових додаткових витрат накладні витрати можна скоротити в довгостроковій перспективі.

Як правило, розробка систем управління інформаційною безпекою та впровадження необхідних заходів безпеки опирається на певні встановлені стандарти, які дають змогу визначити потенційні загрози на ранній стадії та пом'якшити їх за допомогою спеціально розроблених контрзаходів, що в свою чергу дозволяє компаніям гарантувати конфіденційність, доступність і цілісність будь-якої інформації [60].

Зародження перших принципів управління інформаційною безпекою відбулося в 1980-х роках у Великобританії, коли Міністерство торгівлі та промисловості ініціювало створення першої робочої групи, яка мала на меті розробити найкращі практики, щодо забезпечення інформаційної безпеки. Як результат роботи даної групи, у 1989 році було опубліковано перший стандарт PD 0003 «Практичні правила управління інформаційною безпекою», який містив перелік засобів управління безпекою. У 1995 році Британським інститутом стандартів (British Standards Institution) було прийнято національний стандарт BS 7799-1 «Практичні правила управління ІБ», який описував 10 областей та 127 механізмів контролю, що були необхідними для побудови системи управління інформаційною безпекою [53].

Саме цей стандарт вважається прабатьком всіх міжнародних стандартів системи управління інформаційною безпекою. Друга частина даного стандарту – BS 7799-2 «СУІБ. Вимоги та настанови щодо застосування» – з'явилася у 1998 році та містила вимоги до загальної моделі побудови СУІБ, а також набір інших обов'язкових вимог, на відповідність яким повинна була проводиться обов'язкова сертифікація. Це період початку активного розвитку системи сертифікації в галузі управління безпекою [53].

Кінець 1999 року експерти Міжнародної електротехнічної комісії (International Electrotechnical Commission), яка була створена в 1906 р., і мала на меті встановлення міжнародних стандартів у всіх галузях, пов'язаних з електрикою, електронікою та радіотехнікою та представники Міжнародної

організації зі стандартизації (International Organization for Standardization), котра була створена в 1947 р., для створення системи стандартів, які б сприяли міжнародній торгівлі, заявляють, що в рамках існуючих стандартів відсутній спеціалізований стандарт управління ІБ [53].

У результаті взявши за основу BS 7799-1 було прийнято відповідний міжнародний стандарт ISO / IEC. Згодом обидві частини стандарту BS 7799 були переглянуті та адаптовані до міжнародних стандартів систем управління якістю ISO / IEC 9001 та екологією ISO / IEC 14001, а через рік стандарт BS 7799-1 був прийнятий як міжнародний стандарт ISO / IEC 17799 2000 «Інформаційні технології. Практичні правила управління ІБ» [53].

У 2008 року Національний Банк України почав застосовувати вимоги міжнародного стандарту на практиці та зобов'язав всі місцеві банки виконувати його вимоги, створюючи систему управління інформаційною безпекою на основі стандартів безпеки ISO [58].

Оскільки за у складі ISO / IEC відповідальність за розробку сімейства міжнародних стандартів з управління ІБ несе підкомітет №27, нумерація даного сімейства стандартів починається схема з 27000 (27k).

Відповідно до міжнародного сімейства стандартів ISO 27000, цілі захисту інформаційної безпеки включають три основні аспекти [58]:

Конфіденційність: конфіденційну інформацію можуть переглядати та розголошувати лише уповноважені особи. Тому доступ до цієї інформації має бути належним чином захищений. Конфіденційність порушується, наприклад, якщо зловмисник може підслуховувати комунікації.

Цілісність: інформація повинна бути захищена від невиявлених маніпуляцій, щоб зберегти її точність і повноту. Цілісність порушується, якщо, наприклад, зловмисник може змінити дані дослідження без виявлення.

Доступність: інформація, послуги або ресурси мають бути доступними для використання для законних користувачів у будь-який час. Доступність може бути порушена, наприклад, через DDoS-атаку, яка навмисно перевантажує системи.

Інші аспекти – автентичність, підзвітність, відданість і надійність. Ступінь досягнення інформаційної безпеки можна визначити на основі того, наскільки цілі захисту виконуються.

2.2 Формування бази міжнародних стандартів по забезпеченню кібербезпеки

Міжнародна організація зі стандартизації (ISO) – це сімейство стандартів, що забезпечує організації загальною структурою щодо політики та стандартів інформаційної безпеки. Дані стандарти допомагають захистити інформаційні активи, такі як фінансові звіти, інформацію про співробітників, інтелектуальну власність або інформацію про клієнтів ISO [45]. Міжнародні стандарти ISO публікуються у такому форматі: ISO[/IEC][/ASTM] [IS] nnnnn [:yyyy] ЗАГОЛОВОК, nnnn – номер стандарту, yyyy – рік опублікування, в заголовку зазначається предмет. Якщо стандарт є результатом роботи Міжнародної електротехнічної комісії, то використовується наступне позначення ISO/IEC JTC1 (Об'єднаний технічний комітет ISO/IEC). Для стандартів, розроблених у співпраці з ASTM International, використовується ASTM. ISO налічує 157 національних членів із 195 країн світу. ISO має три категорії членства [40]:

– органи-члени – це національні органи, які вважаються найбільш представницькими органами зі стандартів у кожній країні. Це єдині члени ISO, які мають право голосу.

– члени-кореспонденти – це країни, які не мають власної організації стандартів. Ці члени інформовані про роботу ISO, але не беруть участі в оприлюдненні стандартів.

– члени-абоненти – країни з невеликою економікою. Вони сплачують зменшені членські внески, але можуть стежити за розвитком стандартів.

Серія ISO/IEC 27000 (також відома як «Сімейство стандартів ISMS» або скорочено «ISO27k») містить стандарти інформаційної безпеки, опубліковані спільно Міжнародною організацією зі стандартизації (ISO) та Міжнародною

електротехнічною комісією (IEC). Серія містить рекомендації щодо управління інформаційною безпекою, управління ризиками та впровадження засобів контролю в контексті загальної системи управління інформаційною безпекою (СУІБ). Системи менеджменту для забезпечення якості (серія ISO 9000) та захисту навколишнього середовища (серія ISO 14000) також за своїм дизайном схожі на стандарти серії ISO/IEC 27000. Серія застосовна до організацій будь-яких форм і розмірів, що охоплюють не тільки питання конфіденційності, а й технічної безпеки. Перший із стандартів серії 27000 (27001) був опублікований у 2005 році. Його попередник, ISO/IEC 17799, бере свій початок у 2000 році, коли розвиток Інтернету викликав швидке зростання усвідомлення важливості безпеки в IT-індустрії. Наразі в серії опубліковано чотири стандарти: 27001, 27002, 27005 і 27006. Ще десять знаходяться на різних стадіях проекту [40].

ISO/IEC27001 Стандарт 27001 визначає кроки, необхідні для отримання сертифікації системами управління інформаційною безпекою організації. Стандарт визначає сім ключових елементів у створенні сертифікованої СУІБ. Вони створюють, впроваджують, експлуатують, контролюють, переглядають, підтримують та покращують систему. Як стандарт управління, він не вимагає використання спеціальних засобів контролю, а лише визначає процеси управління, необхідні для визначення засобів контролю, які підходять для організації. Він призначений для використання разом із ISO/IEC 27002 (раніше ISO/IEC 17799), Кодексом практики управління інформаційною безпекою, в якому перераховані цілі контролю безпеки та рекомендований ряд конкретних засобів контролю безпеки. Організації, які впроваджують СУІБ відповідно до ISO/IEC 27002, імовірно, будуть одночасно відповідати вимогам ISO/IEC 27001, але сертифікація є абсолютно необов’язковою [45].

ISO/IEC 27002 ISO/IEC 27002 – це стандарт інформаційної безпеки, опублікований Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC) як ISO/IEC 17799:2005 і згодом перенумерований у ISO/IEC 27002:2005 у липні 2007 року. Він має назву Інформаційні технології – Методи безпеки – Кодекс практики управління

інформаційною безпекою. Нинішній стандарт є переглядом версії, вперше опублікованої ISO/IEC у 2000 році, яка була дослівною копією Британського стандарту (BS) 7799-1:1999 [16].

Мета стандарту 27002 полягає в тому, щоб встановити структурований набір буквально сотень засобів контролю інформаційної безпеки, використання яких допоможе досягти відповідності з 27001. Однак це не обов'язковий список: організації вільні впроваджувати засоби контролю, якщо вони ефективні та відповідають вимогам, викладеним у 27001. ISO/IEC 27002 надає рекомендації з найкращої практики з управління інформаційною безпекою для використання тими, хто відповідає за ініціювання, впровадження або підтримку систем управління інформаційною безпекою (СУІБ) [16].

Інформаційна безпека визначається в рамках стандарту в контексті тріади C-I-A: збереження конфіденційності (забезпечення доступу до інформації лише тим, хто має право на доступ), цілісності (забезпечення точності та повноти інформації та методів обробки) та доступності (забезпечення доступу авторизованих користувачів до інформації та пов’язаних активів, коли це необхідно).

ISO/IEC 27002 містить найкращі практики та засоби контролю безпеки в таких областях управління інформаційною безпекою як [16]:

- політика безпеки;
- організація інформаційної безпеки;
- управління активами;
- безпека людських ресурсів;
- фізична та екологічна безпека;
- управління зв'язком і операціями
- контроль доступу;
- придбання інформаційних систем;
- розробка та обслуговування;
- управління інцидентами інформаційної безпеки;
- управління безперервністю бізнесу;

– відповідність.

ISO/IEC 27005 ISO/IEC 27005:2008 містить рекомендації щодо управління ризиками інформаційної безпеки. Він підтримує загальні концепції, визначені в ISO/IEC 27001, і призначений для допомоги в реалізації інформаційної безпеки на основі підходу до управління ризиками. Знання концепцій і термінологій, описаних у ISO/IEC 27001 і ISO/IEC 27002, дуже важливо для повного розуміння ISO/IEC 27005:2008. ISO/IEC 27005:2008 застосовується до всіх типів організацій (наприклад, комерційних підприємств, державних установ, неприбуткових організацій), які мають намір керувати ризиками, які можуть поставити під загрозу інформаційну безпеку організації [53; 56].

ISO/IEC 27006 Стандарт 27006 описує процеси сертифікації та реєстрації, яких повинні дотримуватися органи сертифікації. Його головна мета – направляти акредитовані органи сертифікації щодо формальних процесів сертифікації або реєстрації систем управління інформаційною безпекою інших організацій. Сфера застосування ISO/IEC 27006 полягає в «визначенні загальних вимог, яким має відповідати сторонній орган, який здійснює сертифікацію/реєстрацію СУІБ, якщо він має бути визнаний компетентним і надійним у сертифікації/реєстрації СУІБ». ISO/IEC JTC1 розробляє такі стандарти [56]:

– ISO/IEC 27000 – введення та огляд сімейства стандартів СУІБ, а також глосарій загальних термінів.

– ISO/IEC 27003 – посібник із впровадження СУІБ.

– ISO/IEC 27004 - стандарт для вимірювань управління інформаційною безпекою.

– ISO/IEC 27007 - рекомендація з аудиту СУІБ (з акцентом на систему управління).

– ISO/IEC 27008 - рекомендація з аудиту управління інформаційною безпекою (з акцентом на контроль безпеки).

– ISO/IEC 27011 – рекомендація щодо впровадження ISMS для телекомунікаційної галузі (також відома як X.1051).

– ISO/IEC 27031 – специфікація готовності ІКТ для безперервності бізнесу.

– ISO/IEC 27032 – рекомендація щодо кібербезпеки (по суті, добре, сусіда в Інтернеті).

– ISO/IEC 27033 – IT-мережева безпека, багатокомпонентний стандарт, який зараз відомий як ISO/IEC 18028:2006.

– ISO/IEC 27034 – рекомендація для безпеки програми.

PCIDSS Стандарт безпеки даних індустрії платіжних карток (PCIDSS) – це всесвітній стандарт інформаційної безпеки, визначений Радою зі стандартів безпеки індустрії платіжних карток. Стандарт був створений, щоб допомогти галузевим організаціям обробляти карткові платежі та запобігти шахрайству з кредитними картками за рахунок посилення контролю за даними та їх компромісом. Стандарт поширюється на всі організації, які зберігають, обробляють або обмінюються інформацією про власників карток з будь-якої картки з логотипом одного з брендів карток (див. рис.2.1). Перевірка відповідності може виконуватися як внутрішньо, так і зовні, залежно від обсягу карткових транзакцій, але незалежно від розміру організації відповідність має бути оцінюється щорічно. Організації, які обробляють великі обсяги транзакцій, повинні оцінювати відповідність вимогам незалежним експертом, який називається Qualified Security Assessor (QSA), тоді як компанії, які обробляють менші обсяги, мають можливість продемонструвати відповідність за допомогою анкети для самооцінки (SAQ) [51].

Рисунок 2.1 – Моделі безпеки транзакцій PCIDSS

Концепція бібліотеки інфраструктури інформаційних технологій (ITIL) виникла в 1980-х роках, коли британський уряд визначив, що рівень якості IT-послуг, що надаються їм, є недостатнім [51]. ITIL – це набір концепцій та практик для управління інформаційними технологіями (ITSM), розробки інформаційних технологій (IT) та операцій IT, частина якого зосереджена на безпеці.

ITIL виникла як збірка книг, кожна з яких охоплює конкретну практику в управлінні IT-послугами, була побудована на основі моделі процесу контролю та управління операціями, яку часто приписують В. Едвардсу Демінгу та його циклу «плануй-здійснюй-перевіряй-дій» (PDCA) [51], оскільки стандарти та найкращі методи управління IT-послугами містять 8 основних компонентів (див. рис.2.2): підтримка послуг, надання послуг, управління інфраструктурою ІКТ, керування безпекою, керування додатками, керування програмними активами, планування впровадження управління послугами, дрібномасштабне впровадження.

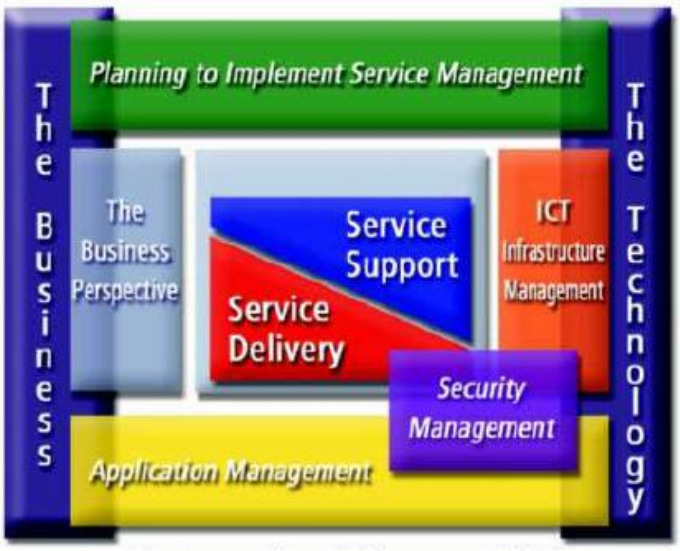

Рисунок 2.2 – Компоненти ITIL

Контрольні цілі для інформаційних та пов’язаних із ними технологій (COBIT) – це сертифікат, створений ISACA та Інститутом управління IT (ITGI) у 1996 році. Вони вважають, що це набір практик (фреймворків) для управління IT. COBIT — це структура управління IT та допоміжний набір інструментів, що

дозволяє менеджерам подолати розрив між вимогами контролю, технічними проблемами, бізнес-ризиками та проблемами безпеки. COBIT має п’ять напрямків управління IT [51]:

– Стратегічне узгодження зосереджується на забезпеченні зв’язку бізнес-планів та IT-планів; визначення, підтримка та підтвердження ціннісної пропозиції IT; і узгодження операцій IT з операціями підприємства.

– Надання цінності полягає у виконанні ціннісної пропозиції протягом усього циклу доставки, гарантуючи, що IT надає обіцяні переваги в порівнянні зі стратегією, концентруючи увагу на оптимізації витрат і доведенні внутрішньої цінності IT.

– Управління ресурсами – це оптимальні інвестиції та правильне управління критичними IT-ресурсами: додатками, інформацією, інфраструктурою та людьми.

– Управління ризиками – це чітке розуміння схильності підприємства до ризику, розуміння вимог щодо відповідності та прозорості в організації.

– Вимірювання ефективності відстежує та контролює реалізацію стратегії, завершення проекту, використання ресурсів, продуктивність процесів та надання послуг, наприклад, збалансовані системи показників, які переводять стратегію в дії для досягнення цілей, які можна виміряти за межами звичайного обліку.

Стандартна серія SP800 заснована в 1901 році, NIST є нерегулюючим федеральним агентством в рамках Міністерства торгівлі США. Місія NIST полягає в тому, щоб сприяти інноваційній та промисловій конкурентоспроможності США шляхом просування вимірювальної науки, стандартів і технологій способами, які підвищують економічну безпеку та покращують якість життя. Загальний бюджет NIST становить 931,5 мільйона доларів, у ньому працюють близько 2900 науковців, інженерів, техніків, а також допоміжний та адміністративний персонал. 2 лабораторії NIST надають вимірювання та стандарти для промисловості США [61]:

- Дослідження будівель та пожежі.
- Хімічна наука та технології.

- Електроніка та електротехніка.
- Інформаційні технології.
- Виробнича інженерія.
- Матеріалознавство та інженерія.
- Нанорозмірна наука та технології.
- Дослідження нейтронних технологій.
- Дослідження нейтронів.

Створена в 1990 році група документів NIST Special Publications 800 є найстарішою з усіх стандартів інформаційної безпеки. Він складається з понад сотні документів, що охоплюють майже всі аспекти інформаційної безпеки. Найбільш змістовним серед усіх цих документів є посібник із комп'ютерної безпеки SP800-12, який містить гарне уявлення про підхід NIST [61].

SP800-12 – основний документ серії. SP800-12 є посібником, який детально висвітлює центральні принципи інформаційної безпеки. Він узагальнює підхід NIST до цієї теми, визначаючи такі вісім основних керівних елементів [61]:

1. Комп'ютерна безпека повинна підтримувати місію організації.
2. Комп'ютерна безпека є центральним елементом надійного управління.
3. Комп'ютерна безпека має бути економічно ефективною.
4. Обов'язки та відповідальність за комп'ютерну безпеку повинні бути чітко визначені.
5. Власники систем мають відповідальність за безпеку за межами власних організацій.
6. Комп'ютерна безпека вимагає комплексної та інтегрованої підхід.
7. Комп'ютерну безпеку слід періодично переоцінювати.
8. Комп'ютерну безпеку обмежують соціальні фактори.

У документі, поряд з рештою серії, детально викладено конкретні стратегії, процедури та засоби контролю, за допомогою яких можна вирішувати питання безпеки відповідно до цих принципів. Вони охоплюють такі галузі, як Інструкції з безпеки електронної пошти (SP800-45), Побудова програми підвищення обізнаності та навчання з безпеки інформаційних технологій (SP800-50),

Інструкції з електронної автентифікації (SP800-63) та Рекомендації щодо безпечних веб-служб (SP800-95). Пояснюючи важливі концепції, міркування щодо вартості та взаємозв’язок засобів контролю безпеки, посібник надає допомогу у захисті комп’ютерних ресурсів (включаючи апаратне забезпечення, програмне забезпечення та інформацію). Хоча NIST сам по собі не надає програму сертифікації, він надає підтримку низці ініціатив у сфері інформування, навчання та освіти [61].

Alfantookh2009 визначив 11 суттєвих засобів контролю, названих 11EC, які повинні бути реалізовані організацією, як вимоги та відповідність критеріям інформаційної безпеки стандартним органом СУІБ [3]:

1. Політика інформаційної безпеки: як установа виражає свої наміри з акцентом на інформаційну безпеку, засоби за допомогою якого керівний орган установи виражає свій намір захистити інформацію, дає вказівки керівництву та персоналу та інформує інших зацікавлених сторін про пріоритетність зусиль.

2. Управління комунікаціями та операціями: визначена політика безпеки в організації, зниження рівня ризику безпеки і забезпечення правильних обчислень, включаючи операційні процедури, засоби контролю та чітко визначені обов'язки.

3. Контроль доступу: це система, яка дозволяє органу влади контролювати доступ до областей і ресурсів у певному фізичному об'єкті або комп'ютерній інформаційній системі.

4. Придбання, розробка та обслуговування інформаційної системи: інтегрований процес, який визначає межі та технічні інформаційні системи, починаючи з придбання та розробки, а останнє – це обслуговування інформаційних систем.

5. Організація інформаційної безпеки: це структура, що належить організації з реалізації інформаційної безпеки, складається з; прихильність керівництва до інформаційної безпеки, координація інформаційної безпеки, процес авторизації засобів обробки інформації. Два основних напрямки: внутрішня організація і зовнішні сторони.

6. Управління активами: ґрунтується на ідеї, що важливо ідентифікувати, відслідковувати, класифікувати та призначати право власності на найважливіші активи, щоб забезпечити їх належний захист.

7. Управління інцидентами інформаційної безпеки: це програма, яка готує до інцидентів. З точки зору управління, це передбачає визначення ресурсів, необхідних для обробки інцидентів. Хороше управління інцидентами також допоможе запобігти майбутнім інцидентам.

8. Управління безперервністю бізнесу: для забезпечення безперервності діяльності в ненормальних умовах. Плани сприяють готовності установ до швидкого відновлення після несприятливих подій або умов, мінімізують вплив таких обставин і забезпечують засоби для полегшення функціонування під час та після надзвичайних ситуацій.

9. Безпека людських ресурсів: гарантувати, що всі співробітники (включаючи підрядників і користувачів конфіденційних даних) мають кваліфікацію та розуміють свої ролі та відповідальність за виконання своїх посадових обов'язків, а також щоб доступ був закритий після припинення роботи.

10. Фізична та екологічна безпека: до заходів, що вживаються для захисту систем, будівель та відповідної допоміжної інфраструктури від загроз, пов'язаних з їх фізичним середовищем, будівлі та приміщення, в яких розміщені системи інформаційних та інформаційних технологій, мають бути забезпечені належним захистом, щоб уникнути пошкодження або несанкціонованого доступу до інформації та систем.

11. Відповідність: ці питання обов'язково поділяють на дві сфери; перша сфера включає дотримання безлічі законів, правил або навіть договірних вимог, які є частиною структури кожної установи. Друга сфера – дотримання політики, стандартів і процесів інформаційної безпеки.

Порівняємо п’ять великих стандартів СУІБ, які стосуються 11ЕС інформаційної безпеки (див. табл. 2.1)

Таблиця 2.1 – Особливості великої п’ятірки стандарту ISMS

	ISO 27001	**BS 7799**	**PCIDSS V2.0**	**ITIL V4.0**	**COBIT V4.01**
Політика інформаційної безпеки	✓	✓	✓	✓	✓
Управління комунікаціями та операціями	✓	✓	✓	✗	✓
Контроль доступу	✓	✓	✓	✓	✓
Придбання, розробка та обслуговування інформаційної системи	✓	✓	✓	✗	✓
Організація інформаційної безпеки	✓	✓	✓	✓	✓
Управління активами	✓	✓	✓	✓	✓
Управління інцидентами інформаційної безпеки	✓	✗	✓	✓	✓
Управління безперервністю бізнесу	✓	✓	✓	✓	✓
Безпека людських ресурсів	✓	✓	✓	✗	✓
Фізична та екологічна безпека	✓	✓	✓	✗	✓
Відповідність	✓	✓	✓	✓	✓

Стандарти інформаційної безпеки необхідні для того, щоб запровадити засоби контролю інформаційної безпеки, щоб відповідати вимогам організації, а також для контролю ділових відносин з іншими організаціями. Найефективніший спосіб зробити це – мати загальний стандарт найкращої практики управління інформаційною безпекою, наприклад стандарти, описані вище. Запроваджуючи один із цих стандартів, організації можуть отримати вигоду від загальноприйнятої передової практики на міжнародному рівні та можуть захистити бізнес-процеси та діяльність для задоволення бізнес-потреб.

2.3 Розробка алгоритму використання інформаційної системи по стандартизації в кібербезпеці, в діяльності підприємства.

В поняття підприємство я вкладаю більш широке визначення, в нього входять не тільки юридичні особи, а і фізичні (приватні підприємці, тощо), приватні особи. Великі підприємства можуть дозволити собі в штаті мати фахівця з кібербезпеки, а в деяких випадках і цілі відділи. А що робити приватному підприємцю, до кого йому звертатися, звідки чекати допомоги? Допомогу йому надасть «Інформаційна система нормативного забезпечення в кібербезпеці». В цій системі він знайде все саме головне, це – родина стандартів з менеджменту інформаційної безпеки в яких розписано як і що повинно бути, якими методами і засобами забезпечити безпеку. Це – Закони України, головні, «Про основні засади забезпечення кібербезпеки України» та Закон України «Про інформацію», а також є тлумачення визначень які використовуються в стандартах СМІБ. Так наприклад: слово атака в тлумачному словнику має два визначення які геть не схожі на визначення згідно стандарту ISO/IEC 27000 і це потрібно розуміти.

Для того, щоб дану систему використовувати її потрібно встановити на комп’ютер з операційною системою Windows (по бажанню замовника можна адаптувати під любу операційну систему) де встановлено інтерпретатор Python і це все що потрібно. Якщо в даній розробці виникне попит її можна запакувати та встановлювати за допомогою інсталятора.

Після встановлення інформаційної системи, визиваємо її та користуємося. У неї дуже зручний та простий графічний інтерфейс. В керуванні задіяні кнопки інтерфейсу, на них потрібно навести курсор і зробити «клік» лівою кнопкою «миші». Для вибору елементу з поля «Вибір потрібного терміну» чи з поля «Вибір потрібного Стандарту» наводимо курсор на потрібний елемент і лівою кнопкою «миші» робимо «клік». Для виходу з інформаційної системи потрібно навести курсор в провий верхній кут графічного інтерфейсу на значок «Закрыть» та натиснути на ліву кнопку «миші» (зробити одинарний «клік»). До програми буде надаватися інструкція користувачу, за потреби.

3 РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПО СТАНДАРТИЗАЦІЇ В КІБЕРБЕЗПЕЦІ

3.1 Пошук визначень за ключовими словами та за назвою стандарту в інформаційній системі.

Програмне забезпечення інформаційної системи буде написано на мові програмування Python. Може виникнути питання, чому саме Python? Ця мова програмування має простий синтаксис та гарний набір вбудованих інструментів. Програми на мові Python можуть виконуватися на самому широкому спектрі пристроїв [37]. Крім того, за допомогою Python ми можемо створювати графічні програми.

Для зручності роботи з інформаційною системою створимо графічний інтерфейс, який більш інтуїтивний і зручний для користувача чим консоль. Для цього використаємо модуль Tkinter. Цей модуль призначений для роботи з компонентами графічного інтерфейсу користувача GUI (graphical user interface). Щоб працювати з файлами потрібен модуль Failedialog. Модулі в мові Python – сама велика організаційна програмна одиниця, яка вміщує в себе програмний код і дані, які можна багаторазово використовувати [37]. Для нашої програми імпортуємо ці два модулі: from import tkinter*, from tkinter.filedialog import *.

Наступний крок – створення вікна, в якому будуть розміщені наші віджити. Вікну ми задамо потрібні розміри і воно, при запуску програми, буде з’являтися у визначеному нами місці екрану комп’ютера.

Нам потрібні наступні віджити.

Текстове поле (text) , в яке буде виводитись вся потрібна інформація.

Кнопки управління «Копіювати» (butt_2), «Зберегти» (butt_3), «Очистити» (butt).

Два Listbox – в яких будуть розміщуватися перелік ключових слів, це в Listbox (my_listbox) та в Listbox (my_listbox_2) буде знаходитися перелік Стандартів та Законів.

Надписи будемо розміщати в такому елементі, як Label, таких елементів буде три. В Label l1 розмістимо "Інформаційна система нормативного

забезпечення в кібербезпеці", l2 "Вибір потрібного терміну", l3 "Вибір потрібного Стандарту".

Графічний інтерфейс нашої інформаційної системи створений, запускаємо програму і отримуємо наступний інтерфейс (див. рис.3.1)

Потрібну нам інформацію, визначення ключових слів буде знаходитись в словнику, змінна яка має назву my_string, а Стандарти будуть знаходиться в файлах з розширенням .txt в змінні my_string2.

Для повноцінної роботи програми, щоб програма ожила, потрібно створити декілька функцій, які будуть виконувати наш задум.

Перша функція – функція def delete_text(), яка буде очищати наше поле виводу інформації при натисканні кнопки «Очистити».

Наступна функція – def to_copy() – копіює всю інформацію, що знаходиться в текстовому полі, в буфер обміну, а звідти вставити в потрібний та потрібне місце. Ця функція виконується при натисканні кнопки «Копіювати».

Функція def print_me(event) – при виборі слова в полі «Вибір потрібного терміну» виводить значення цього терміну в текстове поле. Це відбувається при наведенні курсору на потрібний термін і натисканні на ліву кнопку «миші».

Функція def print_my_ISO(event) – ідентична функції (def print_me(event)) тільки ми вибираємо потрібний Стандарт в полі «Вибір потрібного стандарту». Керування таке саме.

Функція def outText() – виконується при натисканні кнопки «Зберегти». Відкривається діалогове вікно за допомогою якого ми створюємо новий файл з розширенням .txt в потрібній нам дерикторії і, в нього записуємо всю інформацію з текстового поля.

Запускаємо наш програмний код (див. Додаток А) і в нас з’являється графічний інтерфейс нашої програми (див. рис.3.1).

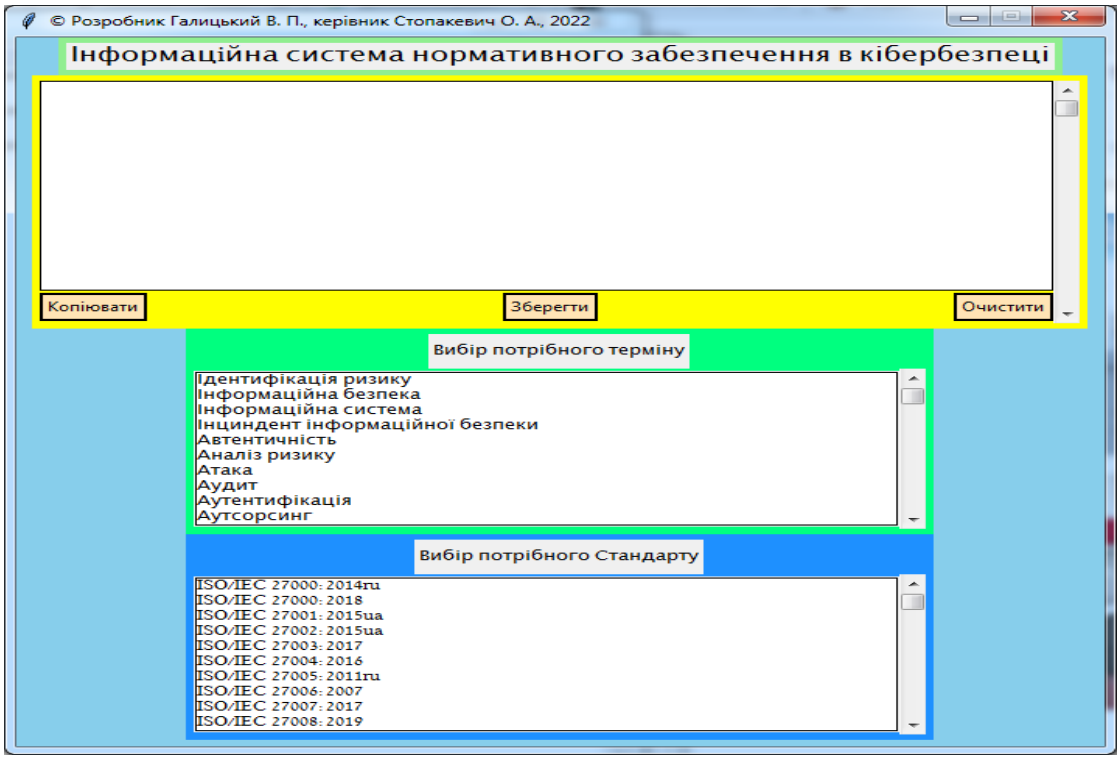

Рисунок 3.1 – Графічний інтерфейс інформаційної системи

Наводимо курсор на поле «Вибір потрібного терміну» і проводимо пошук потрібного терміну методом скролінгу. Терміни програма розміщує в алфавітному порядку. Вибравши потрібний термін натискаємо ліву кнопку миші і в текстовому полі з’являється визначення потрібного терміну (див. рис.3.2).

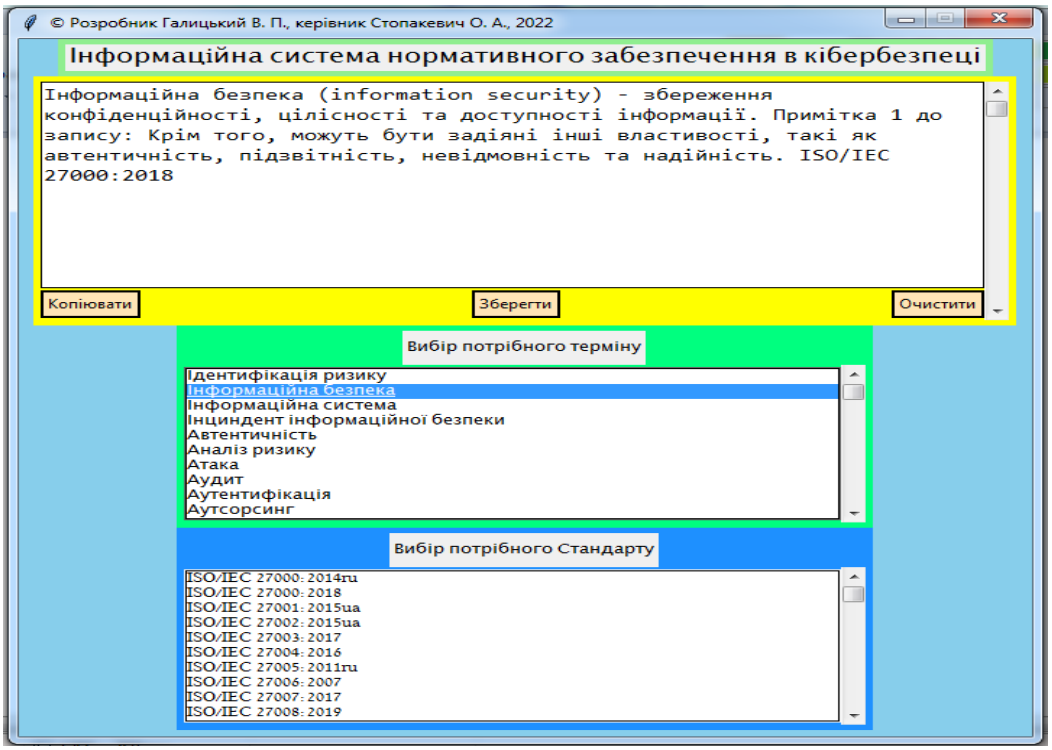

Рисунок 3.2 – Вибір потрібного терміну

З цим визначенням ми можемо зробити наступні дії: натиснувши на кнопку «Копіювати» ми копіюємо інформацію в буфер обміну для перенесення в потрібне нам місце. Створюємо файл з розширенням .docx з назвою «Документ», відкриваємо його, вибираємо місце куди будемо вставляти натискаємо на праву кнопку «миші», з'являється вікно, вибираємо «вставить» і в нашому документі з'являється те, що ми копіювали (див. рис.3.3).

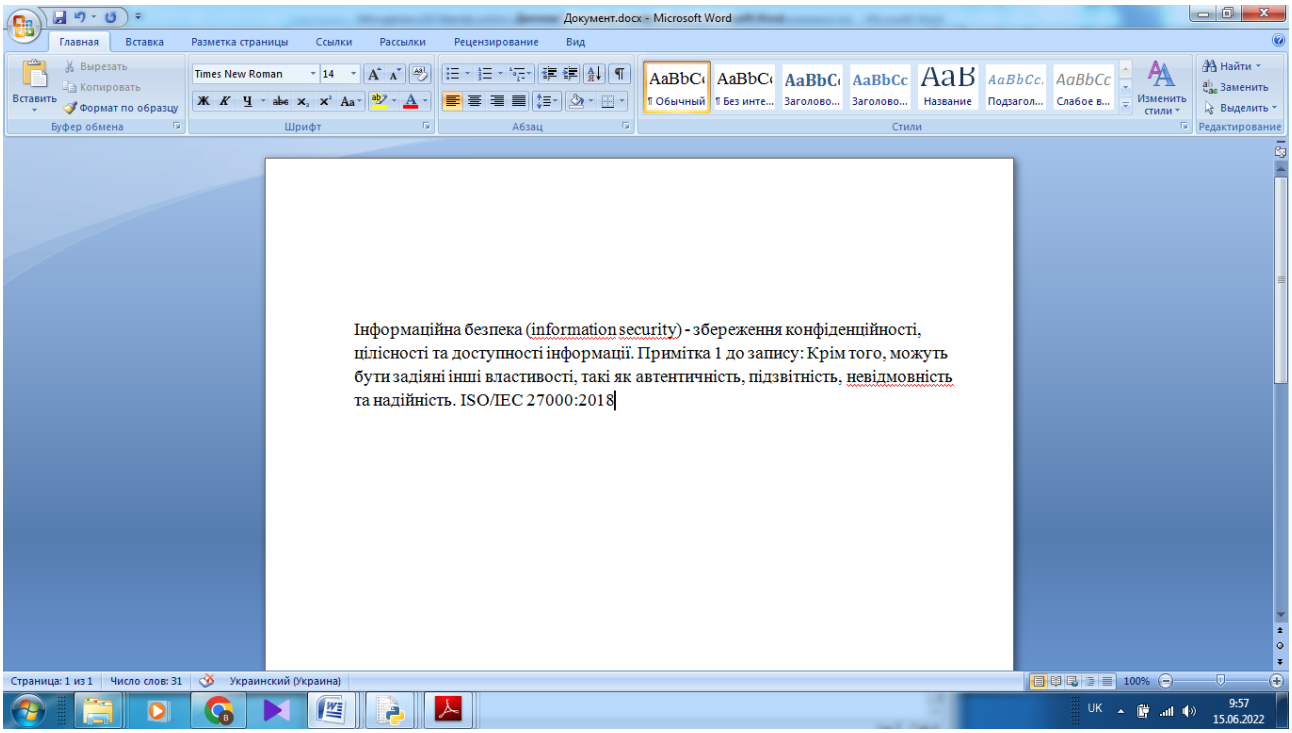

Рисунок 3.3 – Копіювання

При натисканні кнопки «Очистити» вся інформація яка знаходиться в текстовому полі зникає.

Для зберігання інформації в окремий файл з розширенням .txt потрібно натиснути кнопку «Зберегти». Натискаємо цю кнопку, випливає файл-діалогове вікно, де ми повинні вибрати в якій дерикторії буде зберігатися файл та присвоїти ім'я цьому файлу (див. рис.3.4). Дамо йому ім'я Test, натискаємо на кнопку «Сохранить» – діалогове вікно зникає. В вказаній нами дерикторії з'являється файл Test.txt, відкриваємо його і бачимо наше визначення (див.

рис.3.5). Так працює наша програма. Ми маємо можливість вивести в текстове поле 75-ть визначень.

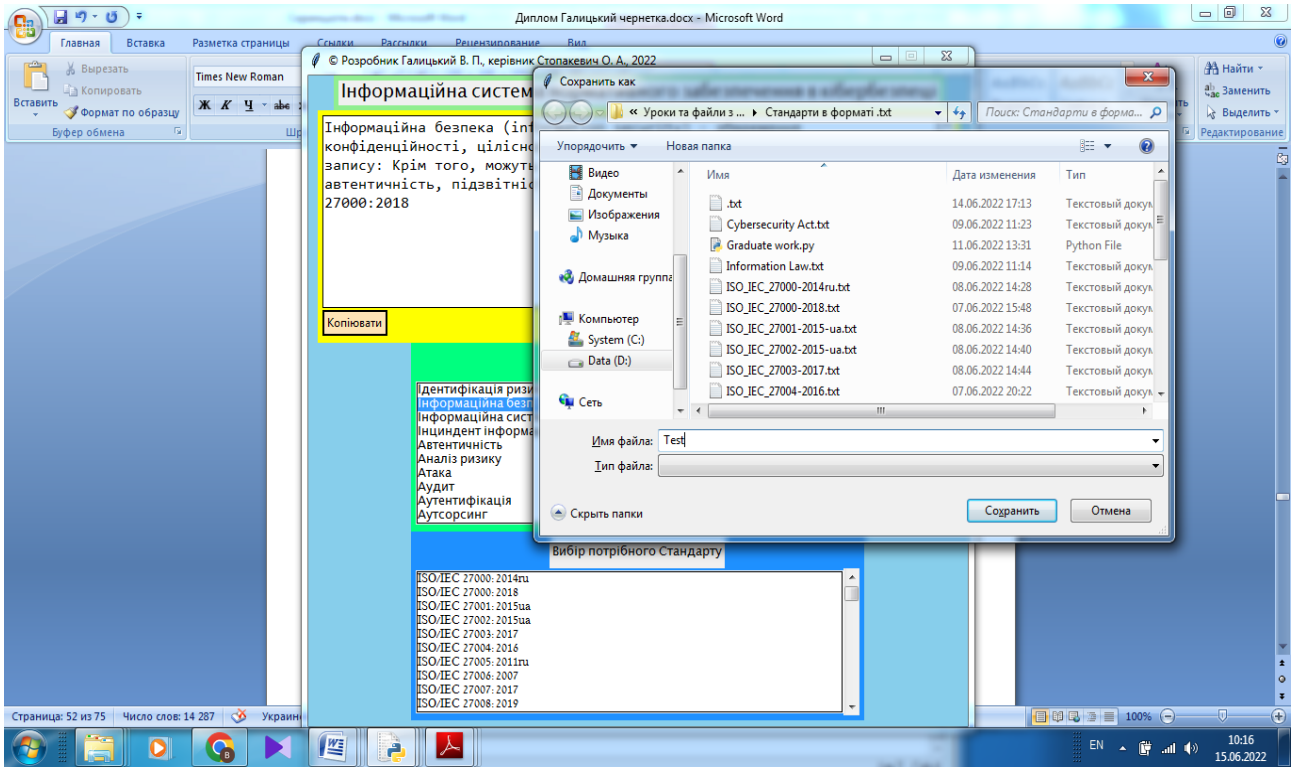

Рисунок 3.4 – Створення файлу

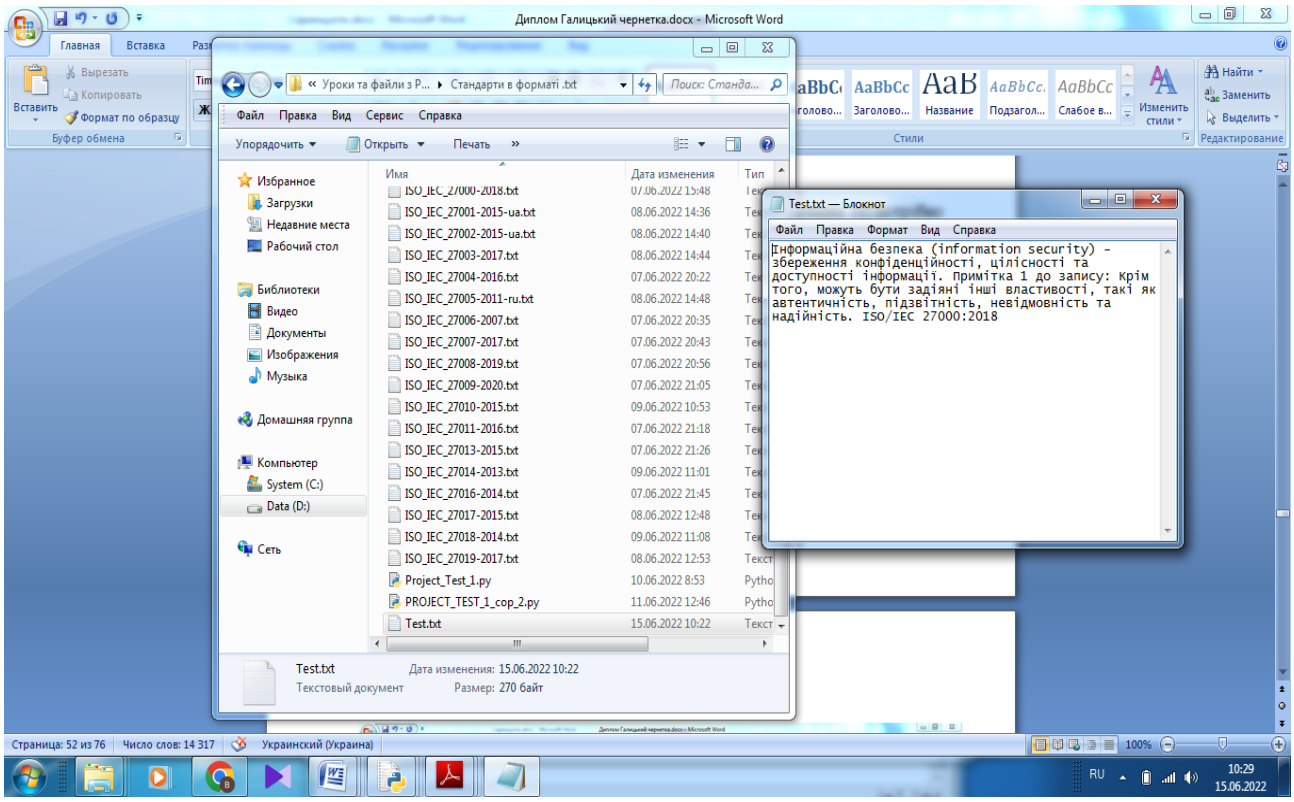

Рисунок 3.5 – Файл Test.txt

Розглянемо роботу з відтворенню в текстовому полі потрібного нам Стандарту чи Закону України. Ми маємо можливість вивести стандарти з менеджменту інформаційної безпеки та два Закони України. Закон України «Про основні засади забезпечення кібербезпеки України» та Закон України «Про інформацію». Алгоритм такий самий як і попередній, тільки ми вибираємо з поля «Вибір потрібного Стандарту».

Вибираємо «Закон України Про основні засади забезпечення кібербезпеки України» (поставивши стрілку курсору на потрібний рядок) та натиснувши ліву кнопку «миші». У текстовому вікні з'являється потрібний нам матеріал (див. рис.3.6)

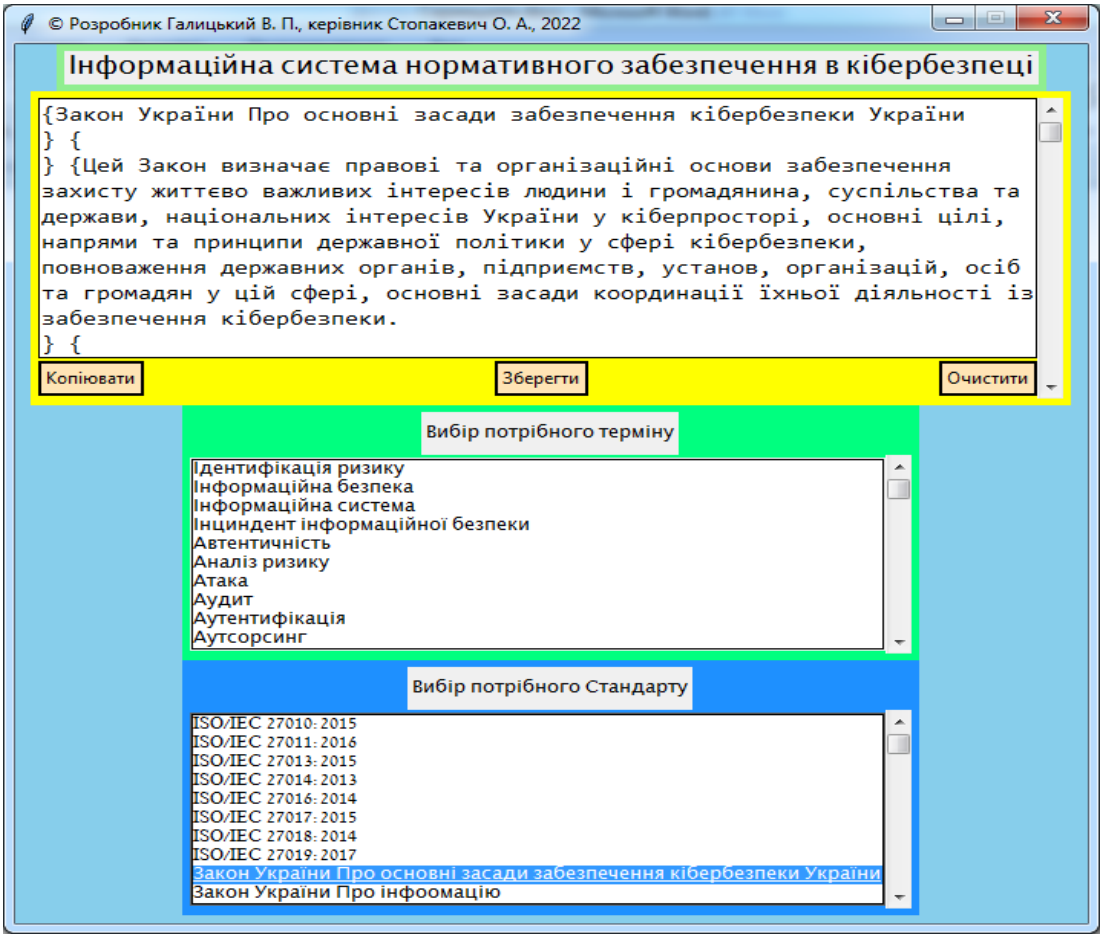

Рисунок 3.6 – Вибір потрібного стандарту

Так як тексту більше чим може вмістити текстове поле, то потрібно навести курсор «миші» на текстове поле і коліщам «миші» виконати скролінг. Ознайомившись з змістом ми збережемо нашу інформацію в текстовий файл,

якому дамо назву «Закон». Для цього натиснемо на кнопку «Зберегти», з’явиться діалогове вікно, в ведемо ім’я файлу та натиснемо кнопку «Сохранить» (див. рис.3.7).

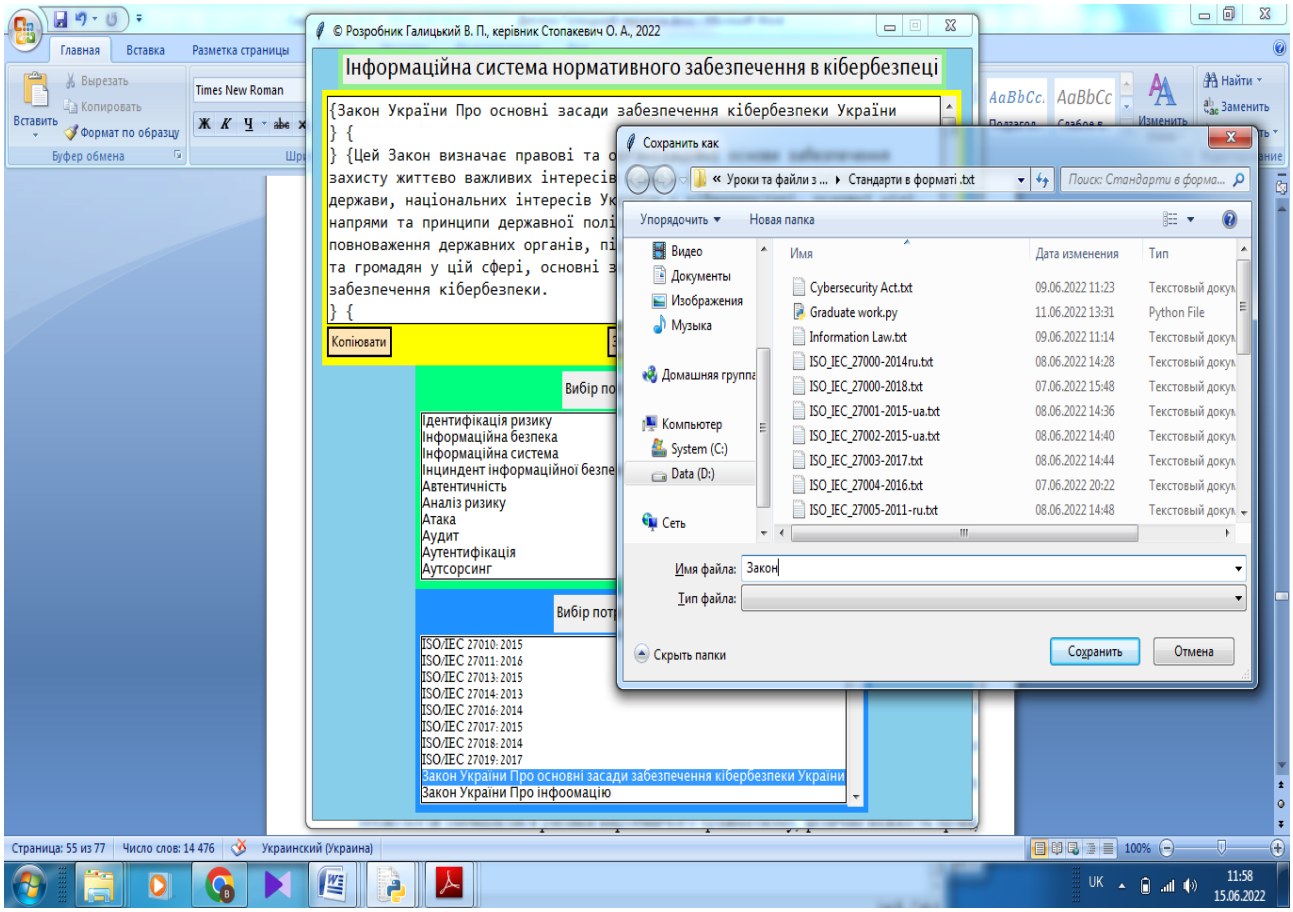

Рисунок 3.7 – Створення файлу «Закон»

Переходимо в потрібну дерикторію, знаходимо там файл «Закон.txt» і відкриваємо його. Та впевнюємося, що вся інформація з текстового поля записана в створений файл (див. рис.3.8).

Перевіримо, що відбудеться при натисканні кнопки «Копіювати». Тиснемо кнопку «Копіювати», відкриваємо файл «Документ.docx», там у нас зберігається запис попереднього копіювання. Ставимо курсор нижче запису, натискаємо праву кнопку «миші» вибираємо вставити і в даний файл добавляється копійована інформація (див. рис.3.9).

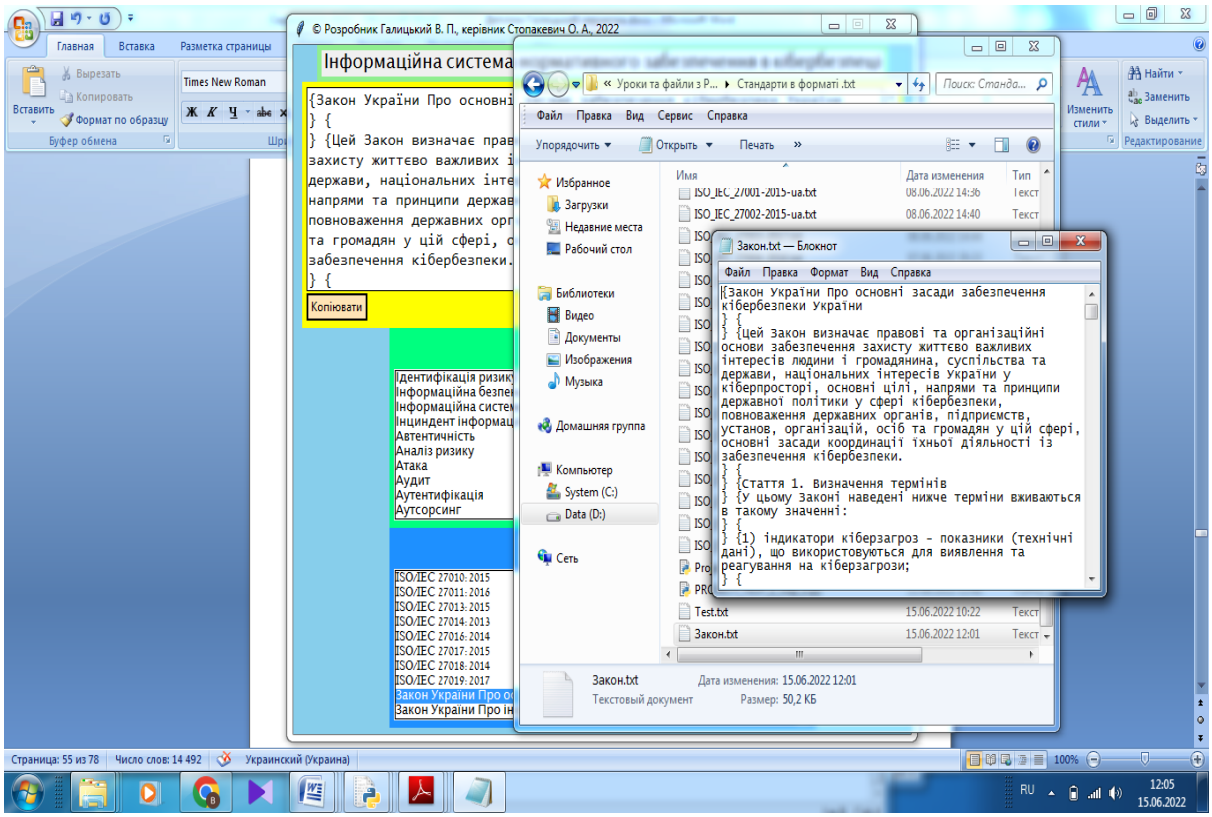

Рисунок 3.8 – Файл Закон.txt

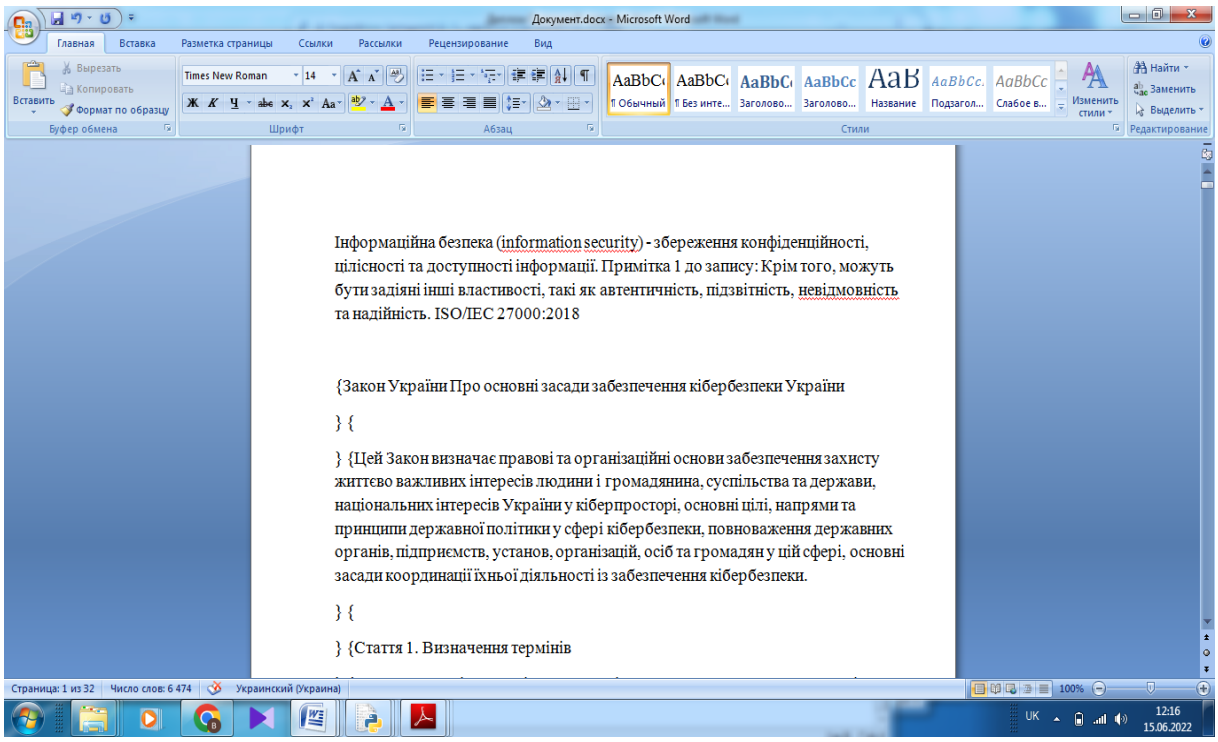

Рисунок 3.9 – Додавання інформації в файл «Документ.docx»

Як ми бачимо, програма працює згідно задуму.

3.2 Тестування розробленого програмного забезпечення інформаційної системи по стандартизації в кібербезпеці

Після написання програми її потрібно протестувати. Давайте з’ясуємо, що таке тестування? Тестування – це пошук багів [44]. Тепер з’ясуємо, що таке баг? Баг (bug) – це відхилення фактичного результату від очікуваного [44]. В більшості випадків баг – відхилення від специфікації [44]. Будемо з’ясовувати, що таке специфікація? Специфікація – це детальний опис того, як повинна працювати програма [44]. Писати специфікацію я не буду, моя специфікація буде складатися з таких пунктів: зручний графічний інтерфейс та правильна робота функціоналу.

При написанні програми ми фактично проводили модульне тестування [44]. Коли перевіряли відпрацювання кожної функції чи створена нами функція виконує наші задуми. Так вони виконують, а саме головне функції не конфліктують між собою. Підтвердження цьому (див. рис.3.10)

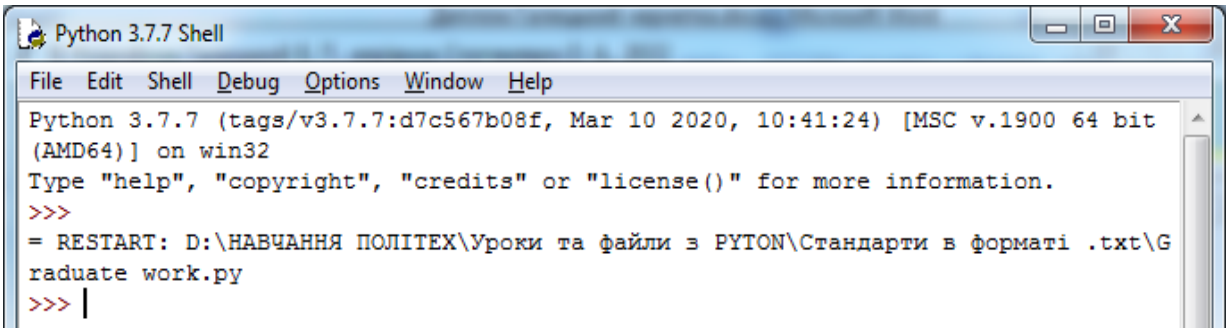

Рисунок 3.10 – Інтерактивне вікно

Ми не бачимо помилок, програма відпрацювала вірно.

Наступний крок – тестування інтерфейсу користувача [44]. В нашому випадку це графічний інтерфейс інформаційної системи (див. рис.3.1). Звертаємо увагу на розташування віджитів в головному вікні, їхні розміри, розміри головного вікна. Чи з’являється вікно у вказаному нами місці, за задумом воно не може змінювати свої розміри але може перетягуватись в інше місце. На надписи на кнопках та етикетках, відсутність граматичних помилок, зручність

розташування елементів. В правому верхньому куті знаходиться три кнопки «Згорнути», «Розгорнути», «Закрити» вони на місці. Згідно задуму кнопка «Розгорнути» відключена і так вона не працює, решта кнопок – виконують свої функції. Решта кнопок, такі як «Копіювати», «Зберегти», «Очистити» теж виконують свої функції за задумом. В текстовому полі ми можемо робити записи та натиснувши на відповідну кнопку виконати ту функцію, яка зазначена на кнопці або вивести потрібне значення, зробити ввод потрібної текстової інформації та натиснувши на кнопки «Копіювати», «Зберегти» виконати ці команди.

Наступне тестування – функціональне тестування це перевірка спроможності програмного забезпечення виконувати зазначені вимоги, іншими словами робота функціонала програмного забезпечення [44].

Запускаємо програму, з’являється графічний інтерфейс нашої інформаційної системи. Вибираємо значення із переліку поля «Вибір потрібного терміну», наводимо курсор на вибраний термін, натискаємо ліву кнопку «миші» в текстовому полі з’являється тлумачення вибраного терміну (див. рис.3.2) – функціонал працює. Наступний крок – перевірка роботи функцій «Копіювання», «Зберігання» ми натискаємо на відповідні кнопки та отримуємо те що нам потрібно (див. рис.3.3), (рис.3.4) та (рис.3.5). При натисканні на кнопку «Очистити» з текстового поля зникає раніше виведена інформація. В такій ж послідовності тестуємо відпрацювання з полем «Вибір потрібного Стандарту» (див. рис.3.6), (рис.3.7), (рис.3.8) та (рис.3.9).

В результаті тестування інформаційної системи помилок виявлено не було, тож ми робимо висновок, що розроблена програма працює правильно.

4 ОХОРОНА ПРАЦІ

Сучасне суспільство живе у період невпинного науково-технічного прогресу, відбувається комп’ютеризація майже всіх сфер діяльності людини, що призводить до значних змін у фаховій структурі праці. З появою комп’ютерних технологій зменшилися ризики виробничого травматизму, фізична важкість праці, проте з’явилися нові виклики, зокрема психофізіологічного характеру. На сьогодні гостро стоїть питання вдосконалення існуючих та розробки нових підходів до організації робочих місць, проведення профілактичних заходів для запобігання розвитку негативних наслідків впливу ПК на здоров'я користувачів; зростає роль та значення охорони праці, як системи правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів та засобів, що спрямованих на збереження здоров'я і працездатності людини в процесі праці [19].

Існує три основних аспекти на які спрямовані заходи з охорони праці користувачів ПК [19]:

1. Соціальний аспект – покращення умов праці, життя, відпочинку, харчування, побуду, розвиток культури.
2. Психологічний аспект – заходи, що мають на меті зменшити нервово-психічне напруження, оскільки психоемоційний стрес проявляється у більшості
3. Медичний аспект – заходи, що включають первинну профілактику здоров’я (професійний відбір) та вторинну, що спрямована на зниження ймовірності розвитку перевтоми та на відновлення функціонального стану здоров’я та опорно-рухового апарату.

За характером трудової діяльності осіб, які працюють з комп’ютерами, поділяють на групи, згідно з діючим класифікатором професій (ДК-003-95 і Зміна N1 до ДК-003-95):1) [19]:

– розробники програм (інженери-програмісти*)* мають справу переважно з відео терміналами, їх робота характеризується інтенсивною розумовою творчою

працею з підвищеним напруженням зору, вимушеною робочою позою, концентрацією уваги на фоні нервово-емоційного напруження, загальною гіподинамією, періодичним навантаженням на кисті рук;

– оператори електронно-обчислювальних машин виконують роботу, пов’язану з обліком інформації, одержаної з візуального дисплейного терміналу за попереднім запитом, або тієї, що самостійно надходить з нього, яка супроводжується перервами різної тривалості, пов’язана з виконанням іншої роботи і характеризується як робота з напруженням зору, невеликими фізичними зусиллями, нервовим напруженням середнього ступеня та виконується у довільному темпі;

– оператори комп’ютерного набору займаються одноманітною за характером роботою з документацією та клавіатурою, під час якої нечасто та ненадовго переключають погляд на екран дисплея, вводять дані з високою швидкістю. Робота характеризується як фізична праця з підвищеним навантаженням на кисті рук на фоні загальної гіподинамії з напруженням зору (фіксація зору переважно на документи), нервово-емоційним напруженням.

В залежності від характеру праці встановлюються наступні внутрішньо змінні режими праці та відпочинку при роботі з ЕОМ за умови 8-годинної денної робочої: для розробників програм із застосуванням ЕОМ має бути регламентована 15-хвилинна перерва для відпочинку через кожну годину роботи за ВДТ; для операторів із застосуванням ЕОМ рекомендовано регламентовані перерви для відпочинку тривалістю 15 хвилин кожні дві години; для операторів комп'ютерного набору маю бути призначено регламентовані перерви для відпочинку тривалістю 10 хвилин після кожної години роботи за ВДТ [13].

У випадках, коли регламентовані перерви не можуть бути застосовані, тривалість безперервної роботи з ВДТ повинна бути не більше 4 годин. Якщо ж робоча зміна триває 12 годин, перші 8 годин перерви слід призначати аналогічно перервам при 8-годинній робочій зміні, а протягом останніх 4-х годин 15 хвилин через кожну годину, незалежно від характеру трудової діяльності. Деякі перерви варто використовувати для виконання комплексу вправ, що спрямовані на

зниження нервово-емоційного напруження, поліпшення мозкового кровообігу, запобігання втомі тощо (вправи наведені у Державних санітарних правилах і нормах роботи з ПК електронно-обчислювальних машин ДСанПІН 3.3.2.007-98) [13].

Виокремлюють ряд різних профзахворювань серед користувачів ПК, а саме порушення зору; кістково-м'язові порушення; порушення, пов'язані зі стресовими ситуаціями та нервово-емоційним навантаженням; захворювання шкіри та отруєння організму [13].

Порушення зору чи не найчастіше зустрічається у осіб, які працюють за комп'ютерами, причиною виникнення даних порушень є нераціональне освітлення, світлотехнічна специфіка робочих місць з ПК, а також недотримання режиму праці. Як правило, робота за комп'ютером вимагає багаторазового переміщення лінії зору від одного об'єкта до іншого, через що відбувається постійна переадаптація з яскравих об'єктів на темні. При 8-годинному робочому дні користувач кидає близько 30000 поглядів на екран, око перебуває у постійному перевантажені і не встигає адаптуватися до ситуації. Це призводить до напруження м'язового та світло-сприймаючого апарату очей, що в свою чергу викликає біль в очах, різь, розпливчастість контурів, нечіткість зображення тощо. Також функціональні порушення очей можуть бути викликані засліплюючою дією світильників у приміщені. Окрім цього навантаження на зір збільшується через кольоровий шрифт, так як складові кольорів мають різні довжини хвиль і видимі на різній віддалі [13].

Інша проблема з якою зіштовхуються користувачі ПК тривале статичне напруження м'язів спини, шиї, рук і ніг, у наслідок чого виникають болі в області шиї, спини, голови, можливе ушкодження хребта за відсутності спеціального крісла. У працюючих за ПК у 7-12 разів частіше, ніж у інших спостерігається синдром зап'ястного каналу, перетискання нервів у вузьких місцях зап'ястя через неправильне положення рук при введені даних за допомогою клавіатури [19].

Робота за комп'ютером характеризується монотонністю, адже працівник здійснює більше ніж 600 однакових дій протягом 75 % робочого часу за 1 годину,

а це в свою чергу призводить до появи захворювань загально-невротичного характеру: підвищення загальної втоми, головного болю, відчуття важкості голови, поганого сну. Електормагнітними хвилями, які випромінює комп'ютер та монітор викликають роздратованість, зменшення швидкості реакцій, депресивний стан тощо [13].

У людей з чутливою шкірою спостерігаються висипи, подразнення та запалення шкіри, оскільки наелектризований екран монітора притягує частини завислого в повітрі пилу та заряджає їх. Також на користувача можуть впливати такі шкідливі гази як діоксини та фуран, що не мають запаху, але містяться в матеріалах корпусу і плат ПК та моніторах [13].

Враховуючи всі вище розглянуть шкідливі чинники мають бути створені такі умови праці, які б забезпечували зручність у роботі, зберігали здоров'я, сили та професійне довголіття. Для цього ж потрібно брати до уваги реальні можливості людини, її антропометричні, фізіологічні та психологічні особливості.

Антропометричні (фізичні розміри людини, вага тощо) дані маються використовуватися при проектуванні робочого простору, для того щоб людина могла виконувати роботу у зручні позі без надмірних зусиль (див. рис.4.1) [19].

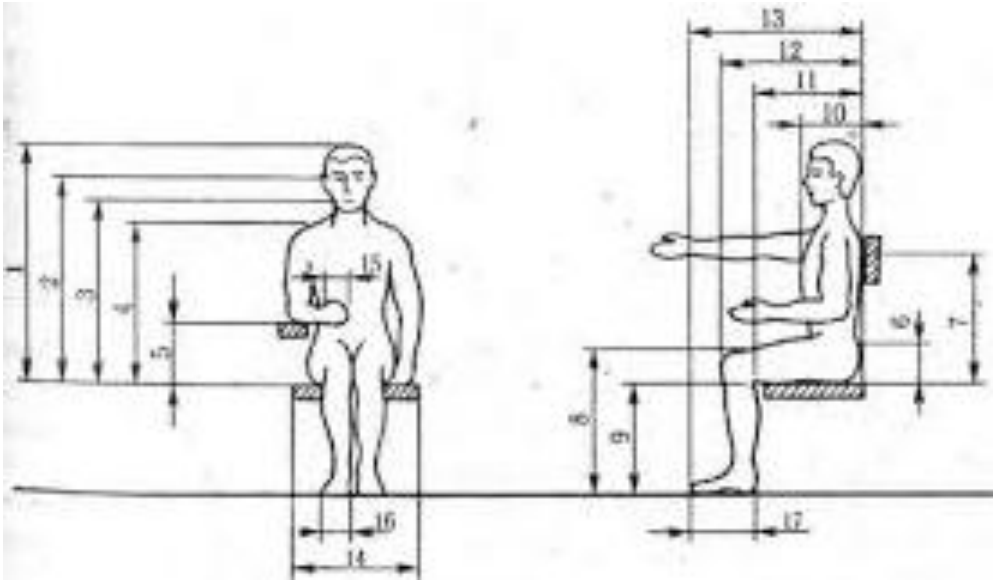

Рисунок 4.1 – Основні антропометричні дані для робочого положення «сидячи»

Так як при роботі за комп’ютером велике навантаження припадає на кисті рук, то при проектуванні клавіатури та раціональному вирішені її елементів потрібно враховувати її антропометричні дані (див. рис.4.2).

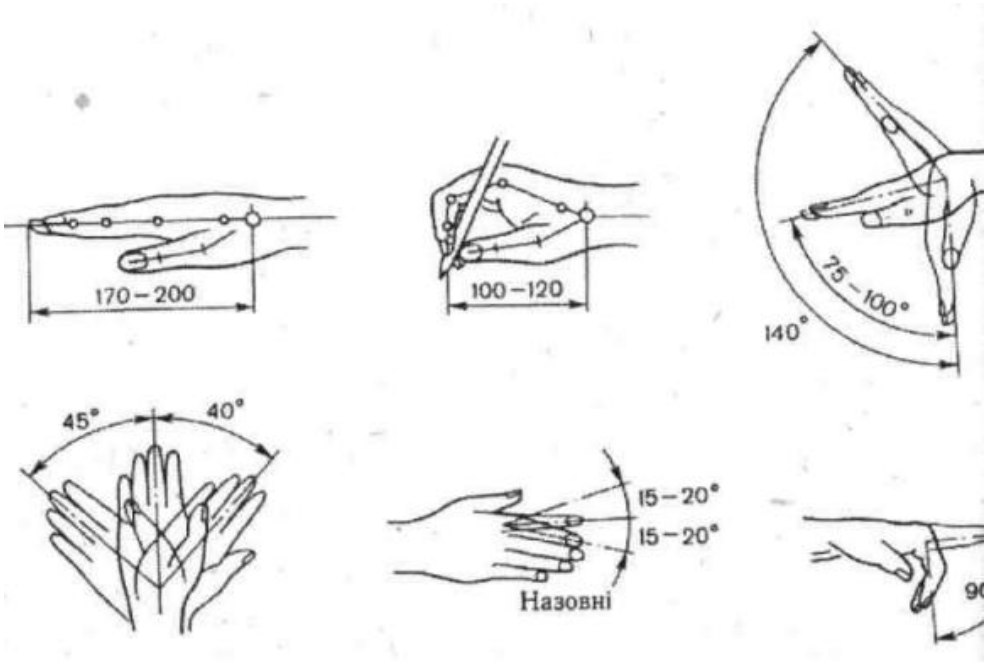

Рисунок 4.2 – Антропологічні дані кисті

Окрім створення умов для зручної робочої пози, робочі місця потрібно розташовувати так, щоб світло падало з лівого боку. При розміщенні робочих столів з ВДТ мають бути дотримані наступні дистанції: між бічними поверхнями ВДТ – 1,2 м; від тильної поверхні одного ВДТ до екрана іншого – 2,5 м. Оптимальна відстань від очей користувача на які має бути розташований екран становить 600...700 мм. Екран має бути розташований так, щоб забезпечити зручність зорового спостереження у вертикальній площині під кутом +30° до нормальної лінії погляду працюючого (див. рис.4.3) Клавіатура має бути розташована на поверхні столу на відстані 100...300 мм від краю, звернутого до працюючого. Поверхня клавіатури повинна бути з антистатичними властивостями [19].

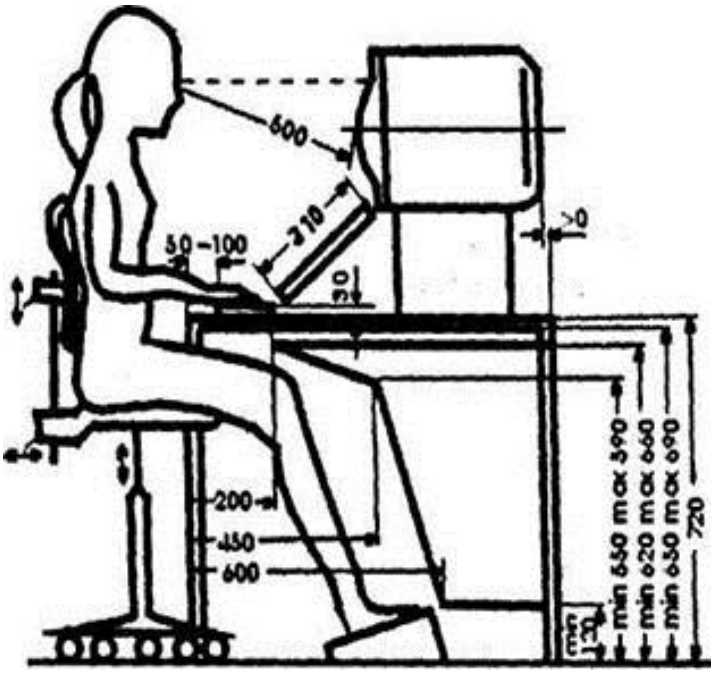

Рисунок 4.3 – Ергономічні характеристики робочого місця з ПК

Значний вплив на рівень працездатності та здоров’я користувачів комп’ютерів здійснює виробниче середовище, що включає мікроклімат, освітлення, наявність шкідливих речовин у повітрі, рівень шуму та випромінювання.

У теплий період року температура повітря повинна бути у межах 22-25 °С, швидкість руху повітря – до 0,1 м/с, відносна вологість повітря – 40-60%. У холодний період року температура повітря може коливатися у межах 21-24 °С, швидкість руху повітря – до 0,1 м с, вологість повітря – 40-60% [13].

Температура та вологість повітря впливають на загальне самопочуття, стан слизових оболонок очей, верхніх дихальних шляхів та шкіри працівників. Згідно з рекомендаціями вологе прибирання має проводитися не менше одного разу на день. Поверхня столу має бути протерта серветкою з антистатиком, оскільки позитивні іони з’єднуються з частинками пилу. Низка проведених досліджень підтвердили негативний вплив великої кількості позитивних іонів на фізичну та розумову діяльність, розвиток втоми, діяльність серцево-судинної ситеми, вегетативної нервової системи тощо. Серед офісних працівників поширені

захворювання ЛОР-органів, а саме хронічні катаральні фарингіти, алергічні риніти тощо [13].

Основним джерелом шуму на робочих місцях з великою кількістю комп'ютерів є вентилятори системного блоку, накопичувачі, принтери ударної дії. Нормативним значенням еквівалентного рівня звуку для програмістів є 50 дБА, для операторів у залах оброблення інформації – 65 дБА, для операторів у приміщеннях, де розташовані гучні агрегати – 75 дБА. Для зменшення шуму мають бути застосовані наступні заходи: зниження рівня шуму в джерелі утворення, використання звукоізолюючих та звукопоглинаючих засобів, раціональне планування виробничих приміщень та робочих місць [13].

Робота працівників з ПК пов'язана зі шкідливим впливом електромагнітних полів, оскільки монітори сучасних комп'ютерів рідкокристалічні, вплив електромагнітного поля від них майже відсутній, проте він залишається на поверхні монітора та клавіатури. Напруженість електростатичного поля на поверхні монітора та клавіатури не повинна перевищувати 150 В/см. Рівень напруженості в свою чергу залежить від пологості повітря, та регулярного вологого прибирання робочого місця з метою усунення запиленості.

«Правила охорони праці під час експлуатації електронно-обчислювальних машин» – є основним нормативним документом щодо забезпечення охорони праці користувачів ВДТ. В ньому встановлені вимоги безпеки та санітарно-гігієнічні вимоги до обладнання робочих місць користувачів електронно-обчислювальних машин і персональних комп'ютерів та працівників тощо [19].

Для уникнення пожежі на робочому місці перед початком роботи за комп'ютером користувач повинен пересвідчитися у цілісності корпусів і блоків ПК, перевірити справність і цілість кабелів живлення, місця їх підключення. При виявленні несправності вмикати ПК забороняється [42].

Якщо ПК ввімкнений забороняється проводити перемонтаж, замінювати або знімати певні елементи, з'єднувати та роз'єднувати вилки і розетки, змінювати запобіжники під напругою, залишати комп'ютер ввімкненим без нагляду тощо. В

кінці робочого дня потрібно відключити електроживлення комп’ютера, вийняти вилку кабелю живлення з розетки [42].

У разі виникнення пожежі необхідно негайно повідомити пожежну охорону за номером 101, назвати адресу, кількість поверхів у будівлі, місце виникнення пожежі, наявність людей, своє прізвище. По можливості вжити заходи спрямовані на евакуацію людей, локалізацію пожежі з використанням первинних засобів пожеже гасіння та збереження матеріальних цінностей. Окрім цього про виникнення пожежі мають бути повідомлені керівник (заступники керівника) чи відповідальна компетентна посадова особа та черговий охорони. Також у разі необхідності потрібно викликати інші аварійно-рятувальні служби (медичну, газорятувальну тощо) [42].

ВИСНОВОК

Використання розробленої «Інформаційної системи нормативного забезпечення кібербезпеки підприємства» дасть змогу підвищити правову грамотність в сфері кібербезпеки та інформаційної безпеки керівництва підприємства та працівників, яких це стосується. А також впровадження ефективного менеджменту, який буде якісно впливати на кінцевий результат підприємства.

Окрім того, така система необхідна для викладачів та студентів учбових закладів, які пов’язані з даною тематикою. Особливо для студентів. Вона здатна зберегти час та нерви. Дати можливість якісної підготовки до занять, курсових робіт тощо.

ПЕРЕЛІК ПОСИЛАНЬ

1. Авраменко А.В., Гасеський В.К. Інформаційна безпека в Україні як складова національної безпеки. *Зб. наук. праць. УАДУ*. К.:УАДУ, 2012. №18. С. 9-18.
2. Агапов А.Б. Основы государственного управления в сфере информатизации в Российской Федерации. М.: Юристъ, 1997. 344 с.
3. Аніловська Г.Я. Інформаційна безпека підприємства в умовах використання сучасних інформаційних технологій. *Науковий вісник НЛТУ України*. 2008, вип. 18.9. С. 270.
4. Архипова Є. О. Інформаційна безпека: соціально-філософський вимір: дис. кандидата філософ. наук: 09.00.03 / НТУ України «Київський політехнічний інститут». К., 2012. 199 с.
5. Барановський О.І. Фінансова безпека. К.: Фенікс, 1999. 338 с.
6. Барановський О.І. Фінансові кризи: передумови, наслідки і шляхи запобігання:монографія. К.: Київ. нац. торг.-екон. ун-т, 2009. 754 с.
7. Бєлай С.В., Корнієнко Д.М. Інформаційна безпека сьогодення – невід'ємна складова воєнної безпеки. Актуальні проблеми управління інформаційною безпекою держави. Київ: Національна академія Служби безпеки України, 2018. 408 с.
8. Богуш В. Інформаційна безпека держави. Київ: МК-Прес, 2005. 431 с.
9. Вашему бизнесу угрожают хакеры? Стандарт ISO/IEC 27031:2011 предлагает решения. URL: http://www.klubok.net/article3.html.
10. Веруш, А.И. Национальная безопасность Республики Беларусь: курс лекций. Минск: Амалфея, 2012. 204 с.
11. Войціховський А.В. Кібербезпека як важлива складова системи захисту національної безпеки європейських країн. Журнал східноєвропейського права. 2018. № 53. С. 26–37.
12. Гавловський В. Інформаційна безпека: захист інформації в автоматизованих системах (організаційно-правовий аспект) // Правове,

нормативне та метрологічне забезпечення системи захисту інформації в Україні. К., 2000. С. 50 – 52.

13. Гігієнічна класифікація умов праці за показниками шкідливості та небезпечності факторів виробничого середовища, важкості та напруженості трудового процесу. К.: МОЗ України, 1998. 34 с.
14. Даценко І.І., Габович Р.Д., Йонда М.Є. Умови праці з комп'ютером і їх оптимізація. Львів: ЛДМУ, 1998. 46 с.
15. Довгань О.Д. Забезпечення інформаційної безпеки в контексті глобалізації: теоретико-правові та організаційні аспекти. К.: Нац. б-ка України ім. В І. Вернадского, 2015. 388 с.
16. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT). URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66911.
17. ДСТУ ISO/IEC 27001-2015.
URL: https://www.assistem.kiev.ua/doc/dstu_ISOIEC_27001_2015.pdf.
18. Жарков Я.М., Дзюба М.Т., Замаруєва І.В. Інформаційна безпека особистості, суспільства, держави :підручник. Київ: Київський університет, 2008. 274 с.
19. Жидецький В.Ц. Охорона праці користувачів ПК. Львів:Афіша, 2000. 350 с.
20. Заплотинський Б.А. Основи інформаційної безпеки. Конспект лекцій. Одеса: ОЮА, 2017. 128 с.
21. Застосування міжнародного стандарту ISO/IEC 27003: 2010 у практиці корпоративних систем України.
URL: https://www.slideshare.net/VladislavChernish/isoiec-270032010.
22. Золотар О.О. Інформаційна безпека людини: теорія і практика : монографія. Київ : АртЕк, 2018. 446 с
23. Зубок М.І. Інформаційна безпека в підприємницькій діяльності: підручник. К.: ГНОЗІС, 2015. 216 с.
24. Информационная безопасность. М.: «Оружие и технологии», 2009 [рос.]

25. Информационная безопасность. М.: Оружие и технологии, 2009.
26. Кавун С. В., Носов В. В., Мажай О. В. Інформаційна безпека : навч. посіб. Харків: ХНЕУ, 2008. Ч.1., 352 с.
27. Калюжний Р. А., Цимбалюк В.С. Координація діяльності органів влади у боротьбі організованою кіберзлочинністю. *Боротьба з організованою злочинністю і корупцією*. 2002. № 6. С. 105-111.
28. Калядин А.Н. Агапов А.В., Угрозы информационной безопасности в кризисах и конфликтах XXI век . М.: ИМЭМО РАН, 2015.
29. Золотар О.О. Інформаційна безпека людини: теорія і практика : монографія. Київ : АртЕк, 2018. 446 с.
30. Керування механізмами захисту. Міжнародні стандарти інформаційної безпеки. URL: https://naurok.com.ua/keruvannyamehanizmami-zahistu-mizhnarodnistandarti-informaciyno-bezpeki-1047html.
31. Ковтун С. В. Інформаційна безпека: підручник. Харків. ХНЕУ, 2009. 368 с.
32. Конституція України. Прийнята Верховною Радою України 28 червня 1996 року. *Відомості Верховної Ради України*. 1996. №30. Ст. 14.
33. Кормич Б.А. Інформаційна безпека: організаційно-правові основи : Навч. посібн. К.: Кондор, 2008. 382 с.
34. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник. К.: КНТ, 2006. 280 с.
35. Ліпкан В.А., Максименко Ю. Є., Желіховський В.М Інформаційна безпека України в умовах євроінтеграції. К.: КНТ, 2006. 280 с.
36. Лопатин В.Н. Информационная безопасность России: Человек. Общество. Государство. СПб.: Фонд «Университет», 2000. 428 с.
37. Лутц М. Изучаем Python. СПб.: Символ-Плюс, 2011. 1280 с.
38. Макаренко В. Правове регулювання захисту конфіденційної інформації, що є власністю держави: становлення, розвиток, проблемні питання. П*раво України*. 2006. № 1. С. 132-135.
39. Нижник Н.Р., Ситник Г.П., Білоус В. Т. Національна безпека України (методологічні аспекти, стан і тенденції розвитку). Ірпінь, 2000. 304 с.

40. Общие сведения о стандартах серии ISO 27000. URL: http://www.iso27000.ru/standarty/iso-27000-mezhdunarodnyestandarty-upravleniya-informacionnoibezopasnostyu-1/iso-27000-mezhdunarodnye-standarty-upravleniyainformacionnoi-bezopasnostyu.
41. Поздняков А.И. Основы теории национальной безопасности. *Альманах Пространство и Время*. 2013. Т. 2. Вып. 1. С. 17.
42. Правила пожежної безпеки в Україні НАПБ А.01.001-14. На заміну НАПБ А.01.001-04 ; чинний від 2014-12-30. К.:МВС України, 2014. 47 с.
43. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр. Закон України від 09 січня 2007 р. № 537-V. URL: http://zakon.rada.gov.ua/laws/show/537-16?find=1&text=%E1%E5%E7%E.
44. Савин Р. С. Тестирование Дот Ком, или Пособие по жестокому обращению с багами в интернет-стартапах. М.: Дело, 2007. 312 с.
45. Стандарти ISO/IEC захистять від кіберзагроз. URL: http://csm.kiev.ua/index.php?option=com_content&view=article&id=3631%3A-isoiec---&catid=122%3A2015-09-15-07-01-23&lang=uk.
46. Танцюра М.Ю. Забезпечення ефективності системи інформаційного забезпечення підприємства (на прикладі туристичних підприємств АР Крим): автореф. дис.на здобуття канд. екон. наук: 08.00.04. Сімферополь, 2012.
47. Теоретические и прикладные проблемы информационной безопасности. *Междунар. науч.-практ. конф*. (Минск, 21 июня 2012 г.). *Тез. Докл*. Минск: Акад. МВД, 2012. 331 с.
48. Нейман Дж. Фон. Теорія самовідтворювання автоматів. М.: Світ, 1971.
49. Юдін О.К., Богуш В.М. Інформаційна безпека держави: Навчальний посібник. Харків: Консум. 576 с.
50. Ярочкін В. І. Система безпеки фірми. URL: http : // www. nbuv.gov. ua.
51. Guldentops E., Betts T., Hodgkiss G. Aligning COBIT, ITIL and ISO 17799 for Business Benefit. URL: https://www.isaca.org/

52. Federal Office for Information Security (BSI), BSI Standard 100-1 Information Security Management System.
URL: https://www.bsi.bund.de/english/publications/bsi_standards/index.htm%20 2008
53. ISO/IEC 17799 Information technology. Security techniques. Code of practice for information security management, 2005.
54. ISO 27000 – группа стандартов по информационной безопасности. URL: http://www.klubok.net/article2543.html.
55. ISO/IEC 27004:2009(E). URL: http://www.klubok.net/Downloads-index-reqviewdownloaddetails-lid-425.html.
56. ISO/IEC 27005:2011(E). URL: http://www.klubok.net/Downloads-index-reqviewdownloaddetails-lid-421.html.
57. ISO/IEC 27035:2011. URL: http://www.klubok.net/article2523.html
58. ISO/IEC 27000.
URL: http://pqmonline.com/assets/files/pubs/translations/std/isomek-27000-2014.pdf.
59. Kaliuzhnyi R., Hovlovskyi V., Tsymbaliuk V., Huzaliuk M., The question of reform concepts of information legislation Ukraine// Pravove, normatyvne ta metrolohichne zabezpechennia systemy zakhystu informatsii v Ukraini, K.: NTUU «KPI», 2000. P. 17-21.
60. Kissel. Computer Security Division, Information Technology Laboratory. Revision 2. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2013. P.222. URL: https://csrc.nist.gov/
61. An introduction to Computer Security. The NIST Handbook. SP 800-12, NIST 1995. URL: https://csrc.nist.gov/
62. Richard L. NIST Interagency or Internal Report 7298: Glossary of Key Information Security Terms. URL: https://csrc.nist.gov/
63. Zharkov Ya.M., Biesiedina L.M. Directions of external information and psychological influence on Ukraine. URL: http//www.nbuv.gov.ua / portal / natural/ znpviknu / 2009-19 / vip19-21.pdf.

Додаток А. Лістинг програми

```
from tkinter import *
from tkinter.filedialog import *


root=Tk()
root['bg'] = 'SkyBlue'
root.title("© Розробник Галицький В. П., керівник Стопакевич О. А., 2022")
root.geometry("700x655+300+20")
root.resizable(False, False)
#################################
frame1 = Frame(root,bg = 'LightGreen',bd=5)
frame1.pack()
frame = Frame(root,bg = 'yellow',bd=5)
frame.pack()
frame2 = Frame(root, bg = 'SpringGreen',bd=5)
frame2.pack()
frame3 = Frame(root, bg = 'DodgerBlue',bd=5)
frame3.pack()
#################################
def delete_text():
    text.delete(1.0, END)
#############################
def to_copy():
    tex_copy = text.get(1.0, END)
    root.clipboard_clear() # Очищуємо буфер обміну
    root.clipboard_append(tex_copy) # Добавляємо в буфер обміну
#################################
def print_me(event):
    text.delete(1.0,END)
```

```
    select = my_listbox.curselection()

    #text.delete(1.0,END)

    my_list = my_listbox.get(select)

    #print(my_list)

    my_string = {'Управління доступом' : 'Управління доступом
(access control) – механізми, покликані гарантувати, що доступ до
активів дозволено та обмежено відповідно довимог бізнесу та безпеки.
ISO/IEC 27000:2018',

'Атака' : 'Атака (attack) –  спроба знищити, розкрити, змінити,
зробити недоступним, вкрасти чи отримати несанкціонований доступ чи
зробити несанкціоноване використання активу. ISO/IEC 27000:2018',

'Аудит' : 'Аудит (audit) – систематичний,незалежний і документований
процес для отримання аудиторських доказів та оцінки, які об’єктивно
визначать ступінь виконання критеріїв аудиту. Примітка 1 до
визначення: Аудит може бути внутрішнім (перша сторона) або зовнішнім
аудитом (друга сторона або третя сторона), і ще може бути
комбінований аудит (об’єднанням двох і більше напрямків).Примітка 2
до визначення: Внутрішній аудит проводиться самою організацією або
зовнішньою стороною від її імені.Примітка 3 до визначення:
«Аудиторське свідчення» та «критерії аудиту» визначенні в ISO 19011.
ISO/IEC 27000:2018',

'Обсяг аудиту' : 'Обсяг аудиту (audit scope) – обсяг та межі аудиту.
ISO/IEC 27000:2018',

'Аутентифікація' : 'Аутентифікація (authentication) – забезпечення
гарантій того, що заявлені характеристики об’єкта є справжніми.
ISO/IEC 27000:2018',

'Автентичність' : 'Автентичність (authenticity) – властивість, що
вказує, що об’єкт є те, що він заявляє про себе. ISO/IEC
27000:2018',

'Доступність' : 'Доступність (availability) – властивість бути
доступною та використаною на вимогу уповноваженої особи. ISO/IEC
27000:2018',

'Базова міра' : 'Базова міра (base measure) – міра, визначена в
термінах атрибута та методу його кількісного визначення. Примітка 1
до запису: Базовий показникфункціонально не залежить від інших
показників. ISO/IEC 27000:2018',

"Компетентність" : "Компетентність (competence) – вміння
застосовувати знання та навички для досягнення намічених
результатів. ISO/IEC 27000:2018",

"Конфіденційність" : "Конфіденційність (confidentiality) –
властивість, що вказує на те, що інформація залишається недоступною
або нерозкритою для неавторизованих приватних та юридичних осіб або
процесів. ISO/IEC 27000:2018",
```

"Відповідність" : "Відповідність (conformity) - виконання вимог. ISO/IEC 27000:2018",

"Наслідок" : "Наслідок (consequence) - результат події, що впливає на цілі. Примітка 1 до визначення: Подія може викликати низку наслідків. Примітка 2 до визначення: Наслідок може бути відомим або невідомим і в контексті інформаційної безпеки, як правило, є негативним. Примітка 3 до визначення: Наслідки можуть оцінюватися кількісно та якісно. Примітка 4 до визначення: Початкові наслідки можуть погіршуватися ефектом ланцюгової реакції. ISO/IEC 27000:2018",

"Постійне вдосконалення" : "Постійне вдосконалення (continual improvement) - повторювана діяльність для підвищення продуктивності. ISO/IEC 27000:2018",

"Контроль" : "Контроль (control) - міра, яка змінює ризик.Примітка 1 до запису: Контроль включає будь-який процес, політику, пристрій, практику або інші дії, які змінюють ризик. Примітка 2 до запису: Можливо, що засоби керування не завжди мають передбачуваний або передбачуваний ефект модифікації. ISO/IEC 27000:2018",

"Ціль управління" : "Ціль управління (control objective) - опис того, що має бути досягнуто в результаті впровадження контролю. ISO/IEC 27000:2018",

"Корекція" : "Корекція (correction) - дія щодо усунення виявленної невідповідності. ISO/IEC 27000:2018",

"Коригувальні дії" : "Коригувальні дії (corrective action) - дії для усунення причини невідповідності та запобігання повторенню. ISO/IEC 27000:2018",

"Похідна міра" : "Похідна міра (derived measure) - міра, яка визначається як функція двох або більше значень базових мір. ISO/IEC 27000:2018",

'Документована інформація' : 'Документована інформація (documented information) - інформація, яка повинна контролюватися та підтримуватися організацією та носій на якому вона міститься. ISO/IEC 27000:2018',

'Ефективність' : 'Ефективність (effectiveness) - ступінь реалізації запланованих заходів і досягнення запланованих результатів. ISO/IEC 27000:2018',

'Подія' : 'Подія (event) - настання або зміна певної сукупності обставин. Примітка 1 до запису: Подія може бути одним або кількома подіями і може мати кілька причин. Примітка 2 до запису: Подія може полягати в тому, що щось не відбувається. Примітка 3 до запису: Подію іноді можна назвати "інцидентом" або "аварією". ISO/IEC 27000:2018',

'Зовнішній контекст' : 'Зовнішній контекст (external context) - зовнішнє середовище, в якому організація прагне досчгти своїх цілей. ISO/IEC 27000:2018',

'Управління інформаційною безпекою' : 'Управління інформаційною безпекою (governance of information security) - система, за допомогою якої спрямовується та контролюється діяльність організації з інформаційної безпеки. ISO/IEC 27000:2018',

'Орган управління' : 'Орган управління (indicator) - особа або група людей, які відповідають за результати діяльності і відповідність організації. Примітка 1 до запису: У деяких юрисдикціях органом управління може бути рада директорів. ISO/IEC 27000:2018',

'Потреба в інформації' : 'Потреба в інформації (information need) - розміння, необхідне для управління даними, цілями, ризиками та проблемами. ISO/IEC 27000:2018',

'Засоби обробки інформації' : 'Засоби обробки інформації (information processing facilities) - будь-яка система обробки інформації, служба чи інфраструктура або фізичне місце, де вони розміщені. ISO/IEC 27000:2018',

'Інформаційна безпека' : 'Інформаційна безпека (information security) - збереження конфіденційності, цілісності та доступності інформації. Примітка 1 до запису: Крім того, можуть бути задіяні інші властивості, такі як автентичність, підзвітність, невідмовність та надійність. ISO/IEC 27000:2018',

'Безперервність інформаційної безпеки' : 'Безперервність інформаційної безпеки (information security continuity) - процес та процедури забезпечення безперервної роботи інформаційної безпеки. ISO/IEC 27000:2018',

'Подія інформаційної безпеки' : 'Подія інформаційної безпеки (information security event) = індифікований стан системи, служби або мережі, що вказує на можливе порушення політики інформаційної безпеки або збій засобів керування, або раніше невідому ситуацію, яка може мати значення для безпеки. ISO/IEC 27000:2018',

'Інциндент інформаційної безпеки' : 'Інцидент інформаційної безпеки (information security incident) - одна або кілька небажаних, неочікуваних подій інформаційної безпеки, які мають значну ймовірність компроментації бізнес-операцій та загрози інформаційній безпеці. ISO/IEC 27000:2018',

'Управління інцидентами інформаційної безпеки' : 'Управління інцидентами інформаційної безпеки (information security incident management) - набір процесів для виявлення, звітування, оцінки, реагування на інциденти інформаційної безпеки та навчання на них. ISO/IEC 27000:2018',

'Спеціаліст по системі управління інформаційною безпекою (СУІБ)' : 'Спеціаліст по системі управління інформаційною безпекою (СУІБ) () - особа, яка встановлює, впроваджує, підтримує та постійно покращує

один або кілька процесів системи управління інформаційною безпекою. ISO/IEC 27000:2018',

'Спільнота обміну інформацією' : 'Спільнота обміну інформацією (information sharing community) - група організацій, яка погоджується обмінюватися інформацією. Примітка 1 до запису: Організацією може бути фізична особа. ISO/IEC 27000:2018',

'Інформаційна система' : 'Інформаційна система (information system) - набір програм, послуг, активів інформаційних технологій або інших компонентів обробки інформації. ISO/IEC 27000:2018',

'Цілісність' : 'Цілісність (integrity) - властивість точності і повноти. ISO/IEC 27000:2018',

'Зацікавлена сторона' : 'Зацікавлена сторона (interested party (бажаний термін) stakeholder (допустимий термін)) - особа або організація, які можуть вплинути, піддавтися впливу рішення чи діяльність або відчувати на себе вплив рішень чи дій. ISO/IEC 27000:2018',

'Внутрішнй контекст' : 'Внутрішній контекст (internal context) - внутрішнє середовище, в якому організація прагне досягнути свох цілей. Примітка 1 до запису: Внутрішній контекст може включати: а) управління, організаційна структура, ролі та підзвітність; б) політика, цілі та стратегії, які існують для їх досягнення; в) можливості, що розуміються як ресурси та знання; г) інформаційні системи, інформаційні потоки та процеси прийняття рішень; д) відносини з внутрішніми зацікавленими сторонами, сприйняття та ціннсті; є) культура організації; ж) стандарти, настанови та моделі, прийняті організацією; з) форма та обсяги договірних відносин. ISO/IEC 27000:2018',

'Рівень ризику' : 'Рівень ризику (level of risk) - величина ризику виражена через комбінацію наслідків та їх ймовірність. ISO/IEC 27000:2018',

'Ймовірність' : 'Ймовірність (likelihood) - можливість того, що щось станеться. ISO/IEC 27000:2018',

'Система менеджменту' : 'Система менеджменту (management system) - сукупнісить взаємоповязаних або взаємодіючих елементів організації для розробки політики та цілей, а також процесів для досягнення цих цілей. Примітка 1 до визначення: Система управління може бути спрямована на один або кілька обєктів управління. Примітка 2 до визначення: До елементів системи управління відносяться структура організації, ролі та відповідальність, функціонування і т. д. Примітка 3 до визначення: Область дії системи менеджменту може включати всю організацію, певні та ідентифіковані частини організації, або одну чи більше наскрізних. ISO/IEC 27000:2018',

'Міра' : 'Міра (measure) - змінна, якій присвоюється значення як результат вимірювання. ISO/IEC 27000:2018',

'Вимір' : 'Вимір (measurement) - процес визначення значення. ISO/IEC 27000:2018',

'Функція вимірювання' : 'Функція вимірювання (measurement function) - алгоритм або обчислення, виконані для поєднання двох або більше базових мір. ISO/IEC 27000:2018',

'Метод вимірювання' : 'Метод вимірювання () - логічна послідовність операцій, описана в загальних рисах, що використовується для кількісної оцінки атрибута щодо заданого масштабу. Примітка 1 до запису: Тип методу вимірювання залежить від характеру операцій, що використовуються для кількісної оцінки атрибута. Можна виділити два види: а) суб'єктивна: кількісна оцінка, що включає людське судження; і б) кількісне визначення на основі числових правил. ISO/IEC 27000:2018',

'Моніторинг' : 'Моніторинг (monitoring) - визначення статусу сиситеми, процесу або діяльності. Примітка 1 до запису: Щоб визначити статус, може виникнути потреба перевірити, наглядати або критично спостерігати. ISO/IEC 27000:2018',

'Невідповідність' : 'Невідповідність (nonconformity) - невиконання вимог. ISO/IEC 27000:2018',

'Не відмова' : 'Не відмова (non-repudiation) - здатність довести настання заявленої події або дії та її джерела. ISO/IEC 27000:2018',

'Ціль' : 'Ціль (objective) - результат, якого необхідно досягти. Примітка 1 до запису: Ціль може бути стратегічною, тактичною або оперативною. Примітка 2 до запису: Цілі можуть стосуватися різних дисциплін (таких як фінансові, охоронні та екологічні цілі) і можуть застосовуватися на різних рівнях (наприклад, стратегічний, загальноорганізаційний, проект, продукт і процес). Примітка 3 до запису: Ціль може бути виражена іншими способами, як предбачуваний результат, мета, оперативний критерій, як ціль інформаційної безпеки або за допомогою інших слів зі схожим значенням. Примітка 4 до запису: У контексті системи управління інформаційною безпекою цілі інформаційної безпеки встановлюються організацією, узгоджені. ISO/IEC 27000:2018',

'Організація' : 'Організація (organization) - особа або група людей, які мають власні функції з обовязками, повноваженнями та відносинами для досягнення своїх цілей. Примітка 1 до запису: Поняття організація включає, але не обмежується ними, приватного підприємця, компанію, фірму, підприємство, орган влади, партнерство, благодійну організацію чи установу або їх частину чи комбінацію, незалежно від того, чи є зареєстровані чи ні, державні чи приватні. ISO/IEC 27000:2018',

'Аутсорсинг' : 'Аутсорсинг (outsource) - укласти угоду, коли зовнішня організація виконує частину функції або процесу організації. Примітка 1 до запису: Зовнішня організація не входить до сфери дії системи управління, хоча функція або процес, переданий на аутсорсинг, входить до сфери дії. ISO/IEC 27000:2018',

'Продуктивність' : 'Продуктивність (performance) - вимірювальний результат. Примітка 1 до запису: Продуктивність може стосуватися як кількісних, так і якісних результатів. Примітка 2 до запису: Продуктивність може стосуватися управління діяльність, процесами, продуктами (включаючи послуги), системами або організаціями. ISO/IEC 27000:2018',

'Політика' : 'Політика (policy) - наміри та напрямок діяльності організації офіційно виражений її вищим керівництвом. ISO/IEC 27000:2018',

'Процес' : 'Процес (process) - набір взаємоповязаних або взаємодіючих видів діяльності, що перетворює входи у вихідні дані. ISO/IEC 27000:2018',

'Надійність' : 'Надійність (reliability) - властивість послідовної наміченої поведінки та результатів. ISO/IEC 27000:2018',

'Вимога' : 'Вимога (requirement) - заявлена потреба або очікування, загалом маються на увазі чи обовязковим. Примітка 1 до запису: "Загалом мається на увазі" означає, що це звичай або звичайна практика для організації та зацікавлених сторін, що потреба чи очікування, що розглядаються, маються на увазі. Примітка 2 до запису: Вказана вимога - це вимога, яка вказана, наприклад, у документованій інформації. ISO/IEC 27000:2018',

'Огляд' : 'Огляд (review) - діяльність, здійснена для визначення придатності, адекватності та ефективності предмета для досягнення встановлених цілей. ISO/IEC 27000:2018',

'Обєкт огляду' : 'Обєкт огляду (review object) - конкретний предмет, що розглядається. ISO/IEC 27000:2018',

'Мета огляду' : 'Мета огляду (review objective) - констатування того, що має бути досягнуто в результаті огляду. ISO/IEC 27000:2018',

'Ризик' : 'Ризик (risk) - вплив невизначеності на цілі. Примітка 1 до запису: Вплив - це відхилення від очікуваного - позитивне чи негативне. Примітка 2 до запису: Невизначеність -це стан, навіть частковий, дефіциту інформації, повязаної з подією, її наслідками чи ймовірнісю, розуміння чи знання про неї. Примітка 3 до запису: Ризики часто характеризуються посиланням на потенційні "події" і "наслідки", або поєднання цих. Примітка 4 до запису: Ризик часто виражається у теріінах комбінацій наслідків подій (включаючи зміни обставин) та повязаної "ймовірності" настання. Примітка 5 до запису: У контексті системи управління інформаційною безпекою ризики інформаційної безпеки можуть бути виражені як впливи невизначеності на цілі інформаційної безпеки. Примітка 6 до запису: Ризик інформаційної безпеки повязаний з можливістю того, що загрози будуть використовувати вразливі місця інформаційного активу або групи інформаційних активів і тим самим завдавати шкоди організації. ISO/IEC 27000:2018',

'Прийняття ризику' : 'Прийняття ризику (risk acceptance) - обгрунтоване рішення піти на певний ризик. Примітка 1 до запису: Прийняття ризику може відбуватися без обробки ризику або під час процесу обробки ризику. Примітка 2 до запису: Прийняті ризики підлягають моніторингу та перегляду. ISO/IEC 27000:2018',

'Аналіз ризику' : 'Аналіз ризику (risk analysis) - процес, щоб зрозуміти природу ризику і визначити рівень ризику. Примітка 1 до запису: Аналіз ризику забезпечує основу для оцінки ризику та прийняття рішень щодо обробки ризику. Примітка 2 до запису: Аналіз ризику включає оцінку ризику. ISO/IEC 27000:2018',

'Оцінка ризику' : 'Оцінка ризику (risk assessment) - загальний процес ідентифікації ризику, аналізу ризику та ступені ризику. ISO/IEC 27000:2018',

'Обмін інформацією з ризиків та консультації' : 'Обмін інформацією з ризиків та консультації (risk communication and consultation) - набір безперервних і повторювальних процесів, які організація проводить для надання, обміну або отримання інформації та для ведення діалогу із зацікавленими сторонами щодо управління ризиками. Примітка 1 до запису: Інформація може стосуватися існування, природи, форми, ймовірності, значущості, оцінки, прийнятності та обробки ризику. Примітка 2 до запису: Консультація - це двосторонній процес інформованого спілкування між організаціями та її зацікавленими сторонами щодо питання перед прийняттям рішення або визначенням напрямку щодо цього питання. Консультація є а) процес, який впливає на рішення через вплив, а не через силу; і б) внесок у прийняття рішень, а не спільне прийняття рішень. ISO/IEC 27000:2018',

'Критерії ризику' : 'Критерії ризику (risk criteria) - технічне завдання, за яким оцінюється значущість ризику. Примітка 1 до запису: Критерії ризику засновані на організаційних цілях, зовнішньому контексті і внутрішньому контексті. Примітка 2 до запису: Критерії ризику можуть бути отримані зі стандартів, законів, політики та інших вимог. ISO/IEC 27000:2018',

'Ступень ризику' : 'Ступень ризику (risk evaluation) - процес порівняння результатів аналізу ризику з критеріями ризику, щоб визначити чи ризик та/або його величина є прийнятними чи допустимими. Примітка 1 до запису: Ступінь ризику допомагає прийняти рішення про ставлення до ризику. ISO/IEC 27000:2018',

'Ідентифікація ризику' : 'Ідентифікація ризику (risk identification) - процес пошуку, розпізнавання та опису ризиків. Примітка 1 до запису: Ідентифікація ризику включає визначення джерел ризику, подій, їх причини та їх потенційних наслідків. примітка 2 до запису: При ідентифікація ризику можуть використовуватися дані за минулий період, теоретичний аналіз, обізнані та експертні думки, а також потреби зацікавлених сторін. ISO/IEC 27000:2018',

'Управління ризиками' : 'Управління ризиками (risk management) - скоординована діяльність щодо керівництва та контролю організацією щодо ризиків. ISO/IEC 27000:2018',

'Процес управління ризиками' : 'Процес управління ризиками (risk management process) - систематичне застосування управлінської політики, процедур і практик до діяльності з комунікації, консультацій, встановлення контексту та виявлення, аналізу, оцінки, визначення ступеня, моніторингу та огляду ризику. Примітка 1 до визначення: ISO/IEC 27005 використовує термін "процес" для опису управління ризиками в цілому. Елементи процесу управління ризиками називаються "діяльністю". ISO/IEC 27000:2018',

'Власник ризику' : 'Власник ризику (risk owner) - фізична або юридична особа, яка має відповідальність та повноваження щодо управління ризиком. ISO/IEC 27000:2018',

'Обробка ризику' : 'Обробка ризику (risk treatment) - процес для зміни ризику. Примітка 1 до запису: Обробка ризику може включати: а) уникнення ризику шляхом прийняття рішення не починати або продовжувати діяльність, яка спричиняє ризик; б) прийняття або збільшення ризику, щоб скористатися можливістю; в) усунення джерела ризику; г) зміна ймовірності; д) зміна наслідків; є) розподіл ризику з іншою стороною або сторонами (включаючи контракти та фінансові ризики); ж) збереження ризику шляхом усвідомленого вибору. Примітка 2 до запису: Обробка ризику, яка стосується негативних наслідків, іноді називають "зменшення ризику", "усунення ризику", "попередження ризику" та "зменшення ризику". Примітка 3 до запису: Обробка ризиків може створити нові ризики або змінити існуючі ризики. ISO/IEC 27000:2018',

'Стандарт забезпечення безпеки' : 'Стандарт забезпечення безпеки (security implementation standard) - документ, що визначає дозволені способи реалізаціїї безпеки. ISO/IEC 27000:2018',

'Загроза' : 'Загроза (threat) - потенційна причина небажаного інциденту, який може призвести до шкоди системі або організації. ISO/IEC 27000:2018',

'Топ-менеджмент' : 'Топ-менеджмент (top management) - особа або група людей, які керують і контролюють на найвищому рівні. Примітка 1 до запису: Вищий менеджмент має право делегувати повноваження та надавати ресурси в межах організації. Примітка 2 до запису: Якщо сфера управління охоплює лише частину організації то вище керівництво відноситься до тих, хто керує та контролює цю частину організації. Примітка 3 до запису: Вищий менеджмент іноді називають виконавчим керівництвом і може включати керівників, фінансових директорів, інформаційних дирокторів та подібні ролі. ISO/IEC 27000:2018',

'Довірений субєкт інформаційного звязку' : 'Довірений субєкт інформаційного звязку (trusted information communication entity) - автономна організація, що підтримує обмін інформацією в спільноті, що обмінюється інформацією. ISO/IEC 27000:2018',

```
'Вразливість' : 'Вразливість (vulnerability) - слабкість активу або
контролю, яка може бути використана однією або кількома загрозами.
ISO/IEC 27000:2018'}

    #print(my_string[my_list])

    text.insert(1.0, my_string[my_list])

#####################################

def print_my_ISO(event):

    select_ISO = my_listbox_2.curselection()

    text.delete(1.0,END)

    my_list_ISO = my_listbox_2.get(select_ISO)

    #print(my_list_ISO)

    my_string2 = {'ISO/IEC 27000:2014ru' : 'ISO_IEC_27000-
2014ru.txt',
                  'ISO/IEC 27000:2018' : 'ISO_IEC_27000-2018.txt',
                  'ISO/IEC 27001:2015ua' : 'ISO_IEC_27001-2015-
ua.txt',
                  'ISO/IEC 27002:2015ua' : 'ISO_IEC_27002-2015-
ua.txt',
                  'ISO/IEC 27003:2017' : 'ISO_IEC_27003-2017.txt',
                  'ISO/IEC 27004:2016' : 'ISO_IEC_27004-2016.txt',
                  'ISO/IEC 27005:2011ru' : 'ISO_IEC_27005-2011-
ru.txt',
                  'ISO/IEC 27006:2007' : 'ISO_IEC_27006-2007.txt',
                  'ISO/IEC 27007:2017' : 'ISO_IEC_27007-2017.txt',
                  'ISO/IEC 27008:2019' : 'ISO_IEC_27008-2019.txt',
                  'ISO/IEC 27009:2020' : 'ISO_IEC_27009-2020.txt',
                  'ISO/IEC 27010:2015' : 'ISO_IEC_27010-2015.txt',
                  'ISO/IEC 27011:2016' : 'ISO_IEC_27011-2016.txt',
                  'ISO/IEC 27013:2015' : 'ISO_IEC_27013-2015.txt',
                  'ISO/IEC 27014:2013' : 'ISO_IEC_27014-2013.txt',
                  'ISO/IEC 27016:2014' : 'ISO_IEC_27016-2014.txt',
                  'ISO/IEC 27017:2015' : 'ISO_IEC_27017-2015.txt',
                  'ISO/IEC 27018:2014' : 'ISO_IEC_27018-2014.txt',
```

```
                    'ISO/IEC 27019:2017' : 'ISO_IEC_27019-2017.txt',
                    'Закон України Про інфоомацію' : 'Information
Law.txt',
                    'Закон України Про основні засади забезпечення
кібербезпеки України' : 'Cybersecurity Act.txt'
                    }
    my_txt_ISO = my_string2[my_list_ISO]
    #print(my_txt_ISO)

    file_ISO = open(my_txt_ISO,'r')
    my_tex_ISO = file_ISO.readlines()

    file_ISO.close()
    text.insert(1.0, my_tex_ISO)
#####################################################
def outText():
    sf = asksaveasfilename()
    final_text = text.get(1.0, END)
    file_text = open(sf + '.txt', 'w')
    file_text.write(final_text)
    file_text.close()

#####################################################################
#####
l1=Label(frame1,text="Інформаційна система нормативного забезпечення
в кібербезпеці",
         font="David 14",height = 1)
l1.pack()
#################################
text = Text(frame, height=10, width=72, font = 'Consolas',
            relief = 'solid', wrap = WORD)
my_scrollbar_1 = Scrollbar(frame, orient = VERTICAL)
```

```
my_scrollbar_1.config(command = text.yview)
my_scrollbar_1.pack(side = RIGHT, fill = Y)
text.pack()
butt = Button(frame, text="Очистити", relief = 'solid',
              command = delete_text, bg = 'Moccasin')
butt.pack(side = RIGHT, pady = 2)
butt_2 = Button(frame, text="Копіювати", relief = 'solid',
              command = to_copy, bg = 'Moccasin')
butt_2.pack(side = LEFT, pady = 2)
butt_3 = Button(frame, text="Зберегти", relief = 'solid',
               bg = 'Moccasin', command = outText)
butt_3.pack(pady = 2)
############################
l2=Label(frame2,text="Вибір потрібного терміну",
         font="David 10",height = 2)
l2.pack()
########################################
mylist = ['Атака', 'Управління доступом', 'Аудит', 'Аутентифікація',
'Автентичність',
          'Доступність', 'Компетентність', 'Конфіденційність',
'Відповідність', 'Обсяг аудиту',
          'Базова міра', 'Наслідок', 'Постійне вдосконалення',
'Контроль', 'Ціль управління',
          'Корекція', 'Коригувальні дії', 'Похідна міра',
'Ефективність', 'Документована інформація',
          'Подія', 'Зовнішній контекст', 'Управління інформаційною
безпекою', 'Орган управління',
          'Потреба в інформації', 'Засоби обробки інформації',
'Інформаційна безпека',
          'Безперервність інформаційної безпеки', 'Подія
інформаційної безпеки',
          'Інциндент інформаційної безпеки', 'Управління інцидентами
інформаційної безпеки',
```

```
          'Спеціаліст по системі управління інформаційною безпекою
(СУІБ)', 'Спільнота обміну інформацією',

          'Інформаційна система', 'Цілісність', 'Зацікавлена
сторона', 'Внутрішнй контекст', 'Рівень ризику',

          'Ймовірність', 'Система менеджменту', 'Міра', 'Вимір',
'Функція вимірювання', 'Метод вимірювання',

          'Моніторинг', 'Невідповідність', 'Не відмова', 'Ціль',
'Організація', 'Аутсорсинг', 'Продуктивність',

          'Політика', 'Процес', 'Надійність', 'Вимога', 'Огляд',
'Обєкт огляду', 'Мета огляду', 'Ризик',

          'Прийняття ризику', 'Аналіз ризику', 'Оцінка ризику',
'Обмін інформацією з ризиків та консультації',

          'Критерії ризику', 'Ступень ризику', 'Ідентифікація
ризику', 'Управління ризиками',

          'Процес управління ризиками', 'Власник ризику', 'Обробка
ризику', 'Стандарт забезпечення безпеки',

          'Загроза', 'Топ-менеджмент', 'Довірений субєкт
інформаційного звязку', 'Вразливість']

mylist.sort()

#############################################################

my_scrollbar = Scrollbar(frame2, orient = VERTICAL)

my_listbox = Listbox(frame2, width = 75, height = 10, font="David
10",

                     yscrollcommand = my_scrollbar, relief =
'solid',

                     exportselection=False)

my_scrollbar.config(command = my_listbox.yview)

my_scrollbar.pack(side = RIGHT, fill = Y)

my_listbox.pack(pady = 2)


for i in mylist:

    my_listbox.insert(END, i)

l3=Label(frame3,text="Вибір потрібного Стандарту",

         font="David 10",height = 2)

l3.pack()
```

```
mylist_2 = ['ISO/IEC 27000:2014ru', 'ISO/IEC 27000:2018', 'ISO/IEC
27001:2015ua',

            'ISO/IEC 27002:2015ua', 'ISO/IEC 27003:2017', 'ISO/IEC
27004:2016',

            'ISO/IEC 27005:2011ru', 'ISO/IEC 27006:2007', 'ISO/IEC
27007:2017',

            'ISO/IEC 27008:2019', 'ISO/IEC 27009:2020', 'ISO/IEC
27010:2015',

            'ISO/IEC 27011:2016', 'ISO/IEC 27013:2015', 'ISO/IEC
27014:2013',

            'ISO/IEC 27016:2014', 'ISO/IEC 27017:2015', 'ISO/IEC
27018:2014',

            'ISO/IEC 27019:2017', 'Закон України Про інфоомацію',

            'Закон України Про основні засади забезпечення
кібербезпеки України']

mylist_2.sort()

#######################################################

my_scrollbar_2 = Scrollbar(frame3, orient = VERTICAL)

my_listbox_2 = Listbox(frame3, width = 75, height = 10, font="David
10",

                       yscrollcommand = my_scrollbar_2, relief =
'solid',

                         exportselection=False)

my_scrollbar_2.config(command = my_listbox_2.yview)

my_scrollbar_2.pack(side = RIGHT, fill = Y)

my_listbox_2.pack(pady = 2)

for i in mylist_2:

    my_listbox_2.insert(END, i)

my_listbox.bind("<<ListboxSelect>>", print_me)

my_listbox_2.bind("<<ListboxSelect>>", print_my_ISO)

root.mainloop
```