Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно–інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних наук
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: Дослідження онлайн-процедур убезпечення персональних даних користувачів Інтернет

Виконав: студент VI курсу, групи СНмз–61
спеціальності 122 Комп'ютерні науки
(шифр і назва спеціальності)

_____ Катрич Р.В.
(підпис) (прізвище та ініціали)

Керівник _____ Дуда О.М.
(підпис) (прізвище та ініціали)

Нормоконтроль _____ Никитюк В.В.
(підпис) (прізвище та ініціали)

Завідувач кафедри _____ Боднарчук І.О.
(підпис) (прізвище та ініціали)

Рецензент _____ Стухляк Д.П.
(підпис) (прізвище та ініціали)

Тернопіль
2024

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра комп'ютерних наук
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Боднарчук І.О.
(підпис) (прізвище та ініціали)
« 26 » грудня 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 122 Комп'ютерні науки
(шифр і назва спеціальності)

Студенту Катричу Роману Володимировичу
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження онлайн-процедур убезпечення персональних даних користувачів Інтернет

Керівник роботи Дуда Олексій Михайлович, к.т.н., доцент кафедри КН
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 29 » листопада 2024 року № 4/7-1142

2. Термін подання студентом завершеної роботи 17 грудня 2024р.

3. Вихідні дані до роботи Наукові публікації про убезпечення персональних даних для користувачів Інтернету, аналіз дослідження онлайн-процедур, проведення анкетування та обґрунтування результатів.

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. 1 Теоретичні аспекти убезпечення персональних даних. 1.1 Персональні дані: визначення, види та правова база. 1.2 Методології та підходи до захисту персональних даних користувачів Інтернет. 1.3 Механізми шифрування для убезпечення персональних даних користувачів Інтернет. 1.4 Аутентифікація для убезпечення персональних даних користувачів Інтернет. 1.5 Політики управління правами доступу для убезпечення персональних даних користувачів. 2 Методологічні основи дослідження. 2.1 Проблеми та робочі гіпотези убезпечення даних. 2.2 Досліджувані змінні, показники та характеристики персональних даних користувачів Інтернет. 2.3 Методи, прийоми та засоби дослідження. 2.4 Область та організація процесу дослідження онлайн-процедур. 3 Аналіз захисту персональних даних та безпека користувачів інтернету на прикладі обраних онлайн-процедур. 3.1 Характеристики загроз безпеці користувачів мережі Інтернет. 3.1.1 Відчуття безпеки користувачів Інтернету 3.1.2 Відгуки про безпеку персональних даних та іншої приватної інформації користувачів Інтернет. 4 Охорона праці та безпека в надзвичайних ситуаціях. Висновки. Додатки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1 Титульна сторінка. 2 Тема, Мета, Об'єкт, Предмет дослідження. 3 Завдання дослідження. 4 Актуальність дослідження. 5 Типи вразливих даних при використанні незахищених мереж. 6 Основні аспекти витоків даних.7 Політики управління доступом. 8 Відчуття безпеки користувачів Інтернету. 9 Графічне відображення відповідей на питання анкети. 10 Пропозиції, щодо удосконалення систем онлайн-процедур убезпечення персональних даних користувачів Інтернет. 16 Висновки. 17 Завершальний слайд.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Сенчишин В.С., доцент		
Безпека в надзвичайних ситуаціях	Клепчик В.М., ст. викладач		

7. Дата видачі завдання 29 листопада 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	29.11.2024	*Виконано*
2.	Підбір наукових джерел про безпеку користувачів	29.11.2024-04.12.2024	*Виконано*
	Інтернету, аналіз досліджень онлайн-процедур,		
	розробка анкет та проведення анкетування, їх аналіз.		
3.	Опрацювання наукових публікацій та збір даних по	29.11.2024-04.12.2024	*Виконано*
	темі роботи		
4.	Виконання дослідження згідно мети кваліфікаційної	05.12.2024-09.12.2024	*Виконано*
	роботи		
5.	Оформлення розділу «Теоретичні аспекти	05.12.2024-09.12.2024	*Виконано*
	убезпечення персональних даних»		
6.	Оформлення розділу «Методологічні основи	05.12.2024-09.12.2024	*Виконано*
	дослідження»		
7.	Оформлення розділу «Аналіз захисту персональних	05.12.2024-09.12.2024	*Виконано*
	даних та безпека користувачів інтернету на прикладі		
	обраних онлайн-процедур»		
8.	Виконання завдання до підрозділу «Охорона праці»	02.12.2024-09.12.2024	*Виконано*
9.	Виконання завдання до підрозділу «Безпека в	02.12.2024-09.12.2024	*Виконано*
	надзвичайних ситуаціях»		
10.	Оформлення кваліфікаційної роботи	10.12.2024-11.12.2024	*Виконано*
11.	Нормоконтроль	12.12.2024-13.12.2024	*Виконано*
12.	Перевірка на плагіат	16.12.2024	*Виконано*
13.	Попередній захист кваліфікаційної роботи	17.12.2024	*Виконано*
14.	Захист кваліфікаційної роботи	27.12.2024	

Студент _____ Катрич Р.В.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Дуда О.М.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Дослідження онлайн-процедур убезпечення персональних даних користувачів Інтернет // Кваліфікаційна робота освітнього рівня «Магістр» // Катрич Роман Володимирович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, група СНмз-61 // Тернопіль, 2024 // С. 67, рис. – 16, табл. – 1, додат. – 2, бібліогр. – 80.

Ключові слова: персональні дані, онлайн-процедури, інформаційна безпека, користувачі Інтернету, незахищені мережі, витоки даних, шифрування, фішинг, аутентифікація.

Кваліфікаційна робота присвячена дослідженню онлайн-процедур убезпечення персональних даних користувачів Інтернет. В першому розділі кваліфікаційної роботи описані персональні дані їх види та правова база Розглянуто методології та підходи до захисту персональних даних. Проаналізовано механізми шифрування, суть аутентифікації, політики управління правами доступу. В другому розділі кваліфікаційної роботи висвітлено методологічні основи дослідження. Подано проблеми та робочі гіпотези убезпечення персональних даних користувачів Інтернет. Досліджено змінні, показники та характеристики параметрів убезпечення персональних даних користувачів Інтернет. Проаналізовано методи, прийоми, засоби дослідження онлайн-процедур убезпечення. Розглянуто область та організація процесу дослідження онлайн-процедур убезпечення персональних даних користувачів Інтернет. В третьому розділі кваліфікаційної роботи проведено аналіз захисту персональних даних та безпеки користувачів Інтернет на прикладі обраних онлайн-процедур. Проаналізовано характеристику загроз безпеці користувачів мережі Інтернет. Проведено опитування респондентів по підібраних питаннях безпеки. Проаналізовано відповіді зафіксовано в діаграмах та малюнках. Зроблено висновки результатів дослідження.

ANNOTATION

Study of online procedures for securing personal data of Internet users // The educational level "Master" qualification work // Katrych Roman // Ternopil Ivan Pulyuy National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Computer Science, SNnm-61 group // Ternopil, 2024 // P. 67, fig. – 16, tables – 1, annexes – 2, ref. – 80.

Key words: personal data, online procedures, information security, Internet users, insecure networks, data leaks, encryption, phishing, authentication.

The qualification work is devoted to the study of online procedures for securing personal data of Internet users. The first section of the qualification work describes personal data, its types and legal basis. The methodologies and approaches to protecting personal data are considered. Encryption mechanisms, the essence of authentication, access rights management policies are analyzed. The second section of the qualification work highlights the methodological foundations of the study. The problems and working hypotheses of securing personal data of Internet users are presented. The variables, indicators and characteristics of the parameters of securing personal data of Internet users are studied. The methods, techniques, and means of researching online security procedures are analyzed. The scope and organization of the research process of online procedures for securing personal data of Internet users are considered. In the third section of the qualification work, an analysis of the protection of personal data and the security of Internet users is carried out using the example of selected online procedures. The characteristics of threats to the security of Internet users are analyzed. A survey of respondents on selected security issues is conducted. The answers are analyzed and recorded in diagrams and figures. Conclusions were drawn from the research results.

ПЕРЕЛІК СКОРОЧЕНЬ І ТЕРМІНІВ

AES (англ. Advanced Encryption Standard) – алгоритм шифрування.

FPIR (англ. False Positive Identification Rate) – коефіцієнт помилково-позитивної ідентифікації.

GDPR (англ. General Data Protection Regulation of the European Union) – Загальний регламент Європейського Союзу про захист даних.

NIST (англ. National Institute of Standards and Technology) – Національний інститут стандартів і технологій (США).

RSA (англ. Rivest-Shamir-Adleman) –алгоритм асиметричної криптографії.

ІТ – інформаційні технології.

ШІ – штучний інтелект.

ЗМІСТ

ВСТУП

Актуальність теми. Актуальність теми кваліфікаційної роботи освітнього рівня «Магістр» полягає у необхідності розробки ефективних методів убезпечення персональних даних користувачів Інтернету в умовах зростання цифрових загроз і використання онлайн-процедур.

Мета і задачі дослідження. Мета даної кваліфікаційної роботи освітнього рівня «Магістр» полягає в аналізі та розробці ефективних онлайн-процедур захисту персональних даних користувачів Інтернету, а також у вивченні існуючих методів їх убезпечення.

Для досягнення поставленої мети необхідно вирішити такі завдання:

1. Дослідити основні теоретичні аспекти захисту персональних даних та визначити ключові загрози.
2. Вивчити сучасні методи та технології шифрування даних, аутентифікації користувачів та управління доступом.
3. Провести порівняльний аналіз найбільш популярних засобів захисту даних.
4. Розробити практичні рекомендації та модель захисту для веб-додатків.
5. Реалізувати запропоновані методи та провести їх оцінку ефективності.

Об’єкт дослідження є процеси забезпечення захисту персональних даних користувачів у мережі Інтернет.

Предмет дослідження. Це методи, алгоритми та процедури убезпечення даних при взаємодії користувачів з веб-ресурсами.

Наукова новизна одержаних результатів кваліфікаційної роботи полягає у розробці інтегрованої моделі захисту персональних даних, яка враховує сучасні загрози та підходи до захисту. Модель дозволяє оптимізувати процес захисту даних з мінімальним впливом на зручність користувачів.

Практичне значення одержаних результатів кваліфікаційної роботи полягає у розробці інтегрованої моделі захисту персональних даних, яка враховує сучасні загрози та підходи до захисту. Модель дозволяє оптимізувати процес захисту даних з мінімальним впливом на зручність користувачів.

Апробація результатів магістерської роботи. Основні результати проведених досліджень обговорювались на VII науково-технічної конференції «Інформаційні моделі, системи та технології» Тернопільського національного технічного університету імені Івана Пулюя (м. Тернопіль, 2024 р.).

Публікації. Основні результати кваліфікаційної роботи опубліковано у двох працях конференції (Див. додатки А).

Структура й обсяг кваліфікаційної роботи. Кваліфікаційна робота складається зі вступу, чотирьох розділів, висновків, списку літератури з 80 найменувань та 2 додатків. Загальний обсяг кваліфікаційної роботи складає 102 сторінки, з них 67 сторінки основного тексту, який містить 16 рисунків та 1 таблицю.

1 ТЕОРЕТИЧНІ АСПЕКТИ УБЕЗПЕЧЕННЯ ПЕРСОНАЛЬНИХ ДАНИХ

1.1 Персональні дані: визначення, види та правова база

Персональні дані – це будь-яка інформація, яка прямо чи опосередковано ідентифікує фізичну особу. Відповідно до законодавства України, наприклад, Закону України «Про захист персональних даних» [42], персональними даними є відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

У міжнародному контексті, наприклад, у Загальному регламенті захисту даних (GDPR) [11], персональні дані визначаються як будь-яка інформація, що стосується ідентифікованої або ідентифіковної фізичної особи (суб'єкта даних).

Види персональних даних.

Персональні дані поділяються на кілька видів залежно від їхнього характеру та рівня чутливості:

1. Звичайні персональні дані:
- Ім'я, прізвище, по батькові.
- Дата і місце народження.
- Місце проживання.
- Номер телефону, електронна пошта.
- Освіта, професійний досвід.
2. Спеціальні категорії персональних даних:
- Дані, що розкривають расову чи етнічну приналежність.
- Політичні, релігійні чи філософські переконання.
- Дані про стан здоров'я.
- Генетичні та біометричні дані для ідентифікації особи.
- Інформація про статеве життя чи сексуальну орієнтацію.
3. Конфіденційні дані:
- Фінансова інформація (банківські рахунки, кредити).
- Дані про кримінальні справи чи правопорушення.
- Інформація, пов'язана з безпекою (паролі, ключі доступу).

Правова база.

1. Міжнародне законодавство:

- Загальний регламент захисту даних (GDPR) [11] – регламент Європейського Союзу, що визначає принципи збору, обробки та захисту персональних даних. Діє з 25 травня 2018 року.
- Конвенція Ради Європи № 108 [51] – перший міжнародний документ щодо захисту персональних даних (1981 р.).

2. Українське законодавство:

- Закон України «Про захист персональних даних» [42] – базовий нормативний акт, що регулює збирання, обробку, зберігання та захист персональних даних в Україні.
- Конституція України [52] – стаття 32 гарантує право кожного на недоторканність особистого життя та захист персональних даних.
- Кримінальний кодекс України – ст. 182 передбачає відповідальність за порушення недоторканності приватного життя.
- Цивільний кодекс України – регулює питання захисту приватності у правовідносинах.

3. Інші нормативно-правові акти:

- Закон України «Про інформацію» [43].
- Закон України «Про доступ до публічної інформації».
- Постанови та роз’яснення уповноважених органів щодо захисту даних.

Основні принципи обробки персональних даних:

1. Законність, прозорість і чесність обробки.
2. Цільове обмеження (дані збираються з конкретною метою).
3. Мінімізація даних (обробка тільки необхідного обсягу даних).
4. Точність та актуальність даних.
5. Обмеження строку зберігання.
6. Забезпечення безпеки та конфіденційності.

Категорії персональних даних залежно від їх характеру та рівня чутливості.

1. Звичайні персональні дані – це базові дані, які дозволяють ідентифікувати особу, але не мають підвищеного рівня чутливості:

- Ім’я, прізвище, по батькові.
- Дата і місце народження.
- Місце проживання або реєстрації.
- Номер телефону, адреса електронної пошти.
- Інформація про освіту, професійний досвід, посаду.

2. Чутливі персональні дані. Ці дані вимагають підвищеного захисту, оскільки їх розголошення може завдати значної шкоди особі:

- Фінансова інформація (номери банківських рахунків, інформація про доходи).
- Паспортні дані, ідентифікаційний код.
- Інформація про місцезнаходження особи в реальному часі.
- Інтернет-ідентифікатори (IP-адреси, файли cookie, дані про поведінку в мережі).

3. Спеціальні категорії персональних даних. Визначені як особливо чутливі у багатьох правових системах, наприклад, у GDPR. Ці дані обробляються лише за наявності спеціальних підстав:

- Дані про расову або етнічну приналежність.
- Політичні, релігійні або філософські переконання.
- Дані про стан здоров’я (медичні записи, історія хвороби).
- Генетичні та біометричні дані, що використовуються для ідентифікації особи.
- Інформація про сексуальну орієнтацію або статеве життя.

4. Конфіденційні дані. Ця категорія включає інформацію, яка прямо або опосередковано стосується приватного життя особи та вимагає суворої конфіденційності:

- Листування, приватні фотографії, відео, записи.
- Дані про особисті фінансові операції.
- Інформація про судимості чи правопорушення.
- Паролі, PIN-коди, ключі доступу до електронних ресурсів.

5. Анонімізовані дані. Дані, які були оброблені так, що ідентифікувати особу більше неможливо без додаткової інформації. Анонімізовані дані не вважаються персональними в юридичному розумінні.

Особливості обробки даних кожної категорії.

- Звичайні персональні дані обробляються з мінімальними вимогами, за умови дотримання загальних принципів захисту.
- Чутливі та спеціальні категорії даних потребують згоди суб'єкта даних або іншої законної підстави для обробки, наприклад, виконання законодавчих зобов'язань.
- Конфіденційні дані вимагають додаткових заходів безпеки, таких як шифрування чи контроль доступу.
- Анонімізовані дані можуть використовуватися без обмежень, оскільки вони не дають змоги ідентифікувати особу.

Основні загрози для персональних даних у сучасних умовах включають несанкціонований доступ, фішинг, шкідливе програмне забезпечення, витік даних через людські помилки, несанкціоноване збирання даних, використання слабких або вразливих технологій, ідентифікаційне шахрайство, інсайдерські загрози, публічне розголошення даних і маніпуляції з використанням штучного інтелекту.

Несанкціонований доступ може включати злом баз даних організацій, використання вразливостей у програмному забезпеченні або фішингові атаки для викрадення даних облікових записів. Фішинг та соціальна інженерія полягають в обмані користувачів, щоб отримати їхні особисті дані, наприклад, паролі чи номери банківських карток, через підроблені електронні листи або повідомлення.

Шкідливе програмне забезпечення, як-от віруси, трояни чи програми-вимагачі, може викрадати дані, блокувати доступ до інформації або записувати натискання клавіш за допомогою кейлогерів. Людські помилки, наприклад, неправильна конфігурація систем або використання слабких паролів, також часто стають причиною витоку даних.

Несанкціоноване збирання даних відбувається через зловживання мобільними додатками, вебсайтами чи використання трекерів без згоди користувачів. Такі дані часто продаються або обмінюються між компаніями. Використання застарілих або вразливих технологій, зокрема незахищених мереж або відсутність оновлень програмного забезпечення, створює можливості для зловмисників.

Ідентифікаційне шахрайство включає крадіжку особистих даних для незаконних дій, наприклад, отримання кредитів, або створення фальшивих профілів. Інсайдерські загрози можуть походити від співробітників, які викрадають дані чи необережно з ними поводяться. Публічне розголошення інформації, наприклад, у соціальних мережах, також може становити ризик.

Маніпуляція даними за допомогою штучного інтелекту передбачає аналіз персональної інформації без згоди користувачів або створення фальшивих зображень, голосів чи відео. Це також може включати поєднання даних із різних джерел для створення детальних профілів.

Щоб зменшити ризики цих загроз, потрібно використовувати шифрування даних, сучасні протоколи безпеки, впроваджувати двофакторну аутентифікацію, регулярно оновлювати програмне забезпечення та навчати користувачів кібербезпеці. Також важливо обмежувати доступ до даних лише для тих, хто їх потребує, і дотримуватися законодавства щодо захисту персональних даних, як-от GDPR чи локальних нормативних актів. Сучасні загрози вимагають постійного вдосконалення технологій захисту та підвищення обізнаності користувачів.

Фішинг – це вид кіберзлочинності, метою якого є обман користувачів для отримання їхніх конфіденційних даних, таких як паролі, банківські реквізити, номери кредитних карток або інша особиста інформація. Зловмисники зазвичай видають себе за довірені організації або осіб, використовуючи підроблені електронні листи, вебсайти, SMS або дзвінки.

Розглянемо як працює фішинг. Зловмисники надсилають підроблені повідомлення, які виглядають правдоподібно, щоб змусити жертву:

- Натиснути на шкідливе посилання.

- Ввести конфіденційну інформацію на підробленому вебсайті.
- Завантажити шкідливий файл.

Після отримання даних кіберзлочинці можуть використовувати їх для викрадення грошей, доступу до облікових записів або інших шахрайських дій.

Розгдянемо приклади фішингу:

1. Підроблені електронні листи від банків або платіжних систем. Жертві надсилається лист із повідомленням, що її банківський рахунок заблокований або виявлено підозрілу активність. Лист містить посилання, яке веде на підроблений сайт, схожий на офіційний, де користувача просять ввести логін, пароль або дані картки.

Приклад: «Ваш акаунт у ПриватБанку заблоковано. Перейдіть за посиланням, щоб підтвердити вашу особу.»

2. Фішинг у соціальних мережах. Зловмисники створюють підроблені сторінки популярних соціальних мереж, таких як Facebook, Instagram чи LinkedIn. Користувач отримує повідомлення з проханням увійти до акаунту через підроблене посилання.

Приклад: «Ви виграли приз! Увійдіть у свій акаунт Instagram, щоб отримати подарунок.»

3. Підроблені повідомлення про оновлення безпеки. Надсилається електронний лист, у якому зазначено, що для вашого акаунту необхідно оновити пароль через «порушення безпеки». Посилання в листі веде на фальшивий сайт.

Приклад: «Google виявив підозрілий вхід у ваш акаунт. Оновіть пароль негайно!»

4. SMS-фішинг. Жертва отримує SMS із повідомленням про те, що її банківська картка заблокована, і просять зателефонувати за номером або перейти за посиланням.

Приклад: «Ваш рахунок у Monobank тимчасово заблоковано. Зателефонуйте за номером або перейдіть за посиланням, щоб розблокувати.»

5. Фішинг через телефонні дзвінки. Шахрай телефонує від імені банку або іншої організації та вимагає підтвердити дані картки або код із SMS.

Приклад: «Ми помітили підозрілу транзакцію на вашій картці. Надішліть, будь ласка, код із SMS, щоб її скасувати.»

6. Фішинг через підроблені вебсайти або онлайн-магазини Жертву заманюють на фальшивий вебсайт, який пропонує вигідні знижки чи акції, і просять ввести дані картки для покупки.

Приклад: «Суперакція! Айфон 14 за 5000 грн. Кількість обмежена – замовляйте зараз!»

7. Фішинг через файли та вкладення. Надсилається електронний лист із вкладенням, яке нібито містить важливу інформацію, наприклад, рахунок чи договір. Відкриття файлу призводить до встановлення шкідливого програмного забезпечення.

Приклад: «Будь ласка, ознайомтесь із доданим рахунком за послуги.»

Щоб захиститися від фішингу потрібно:

1. Не відкривати підозрілі посилання або вкладення.
2. Завжди перевіряти адресу відправника та домен сайту.
3. Використовувати двофакторну аутентифікацію.
4. Встановлювати антивірусне програмне забезпечення.
5. Не повідомляти нікому свої паролі, коди доступу чи дані банківських карток.
6. Пам’ятати, що банки та офіційні сервіси ніколи не просять надсилати конфіденційну інформацію через електронну пошту чи SMS.

Malware (скорочення від «malicious software») – це будь-яке програмне забезпечення, розроблене для нанесення шкоди комп’ютерам, серверам, мережам або користувачам. Воно використовується кіберзлочинцями для викрадення даних, шифрування, видалення інформації, шпигунства або отримання несанкціонованого доступу до систем.

Види Malware:

1. Віруси самовідтворюються, впроваджуючи свій код у файли або програми. Вони можуть поширюватися через флешки, електронні листи чи завантаження і зазвичай призводять до пошкодження системи або втрати даних.

2. Трояни (Trojan Horses) маскуються під легітимне програмне забезпечення, але виконують шкідливі дії. Наприклад, троян може виглядати як корисна програма, але насправді викрадає паролі або надає хакерам доступ до системи.

3. Черв'яки (Worms) – автономні програми, які самостійно розмножуються та поширюються через мережі, поштові сервіси або інші канали. Вони зазвичай уповільнюють роботу систем або викликають перевантаження мереж.

4. Програми-вимагачі (Ransomware) шифрують файли користувача або блокують доступ до системи, після чого вимагають викуп за розблокування. Це один із найнебезпечніших видів шкідливого програмного забезпечення.

5. Програми-шпигуни (Spyware) таємно відслідковують дії користувача, записуючи інформацію про натискання клавіш (кейлогери), вебсерфінг або інші дії. Зловмисники використовують ці дані для викрадення паролів чи банківської інформації.

6. Adware показує надмірну кількість небажаної реклами, яка може бути шкідливою або дратівливою. У деяких випадках adware також збирає інформацію про користувача без його згоди.

7. Руткіти (Rootkits) забезпечують хакерам прихований доступ до системи. Руткіти часто використовуються для віддаленого управління комп'ютером і можуть бути складними для виявлення.

8. Ботнети – комп'ютери, інфіковані шкідливим програмним забезпеченням, утворюють мережу ботів, які використовуються для виконання різних завдань, таких як DDoS-атаки, розсилання спаму або майнінг криптовалют.

9. Keyloggers – програми, які записують натискання клавіш для викрадення паролів, логінів або іншої конфіденційної інформації.

Як поширюється Malware:

1. Завантаження з ненадійних джерел (піратські програми, підроблені оновлення).

2. Вкладення в електронних листах від невідомих відправників.

3. Клік на шкідливі посилання в електронній пошті, соціальних мережах або повідомленнях.

4. Використання заражених флешок або зовнішніх пристроїв.

5. Використання незахищених мереж або публічних Wi-Fi.

6. Відвідування заражених вебсайтів.

Щоб захиститися від Malware потрібно:

1. Використовуйте сучасне антивірусне програмне забезпечення та регулярно його оновлюйте.

2. Завантажуйте програми лише з офіційних джерел.

3. Уникайте відкриття підозрілих листів, посилань або вкладень.

4. Регулярно оновлюйте операційну систему та програмне забезпечення.

5. Використовуйте фаєрвол для захисту від несанкціонованого доступу.

6. Уникайте використання публічних Wi-Fi мереж без VPN.

7. Створюйте резервні копії важливих даних, щоб мінімізувати наслідки атак програм-вимагачів.

8. Використовуйте складні паролі та двофакторну аутентифікацію для важливих акаунтів.

Malware є серйозною загрозою для інформаційної безпеки, тому важливо бути пильним та дотримуватися заходів захисту.

Витоки даних – це ситуації, коли конфіденційна, особиста або корпоративна інформація стає доступною для сторонніх осіб без дозволу. Це може статися через зломи систем, технічні помилки, людську недбалість або навмисні дії.

Наприклад, витік може статися, якщо хакери отримують доступ до бази даних компанії, що містить паролі, номери кредитних карток або персональні дані клієнтів. Іншим прикладом є випадкове розголошення даних співробітником, який надіслав конфіденційну інформацію не тому адресату або опублікував її в загальному доступі.

Витоки даних можуть також відбуватися через втрату пристроїв, наприклад, ноутбуків чи флешок, на яких зберігається важлива інформація, або

через недбалість у налаштуванні хмарних сховищ. У багатьох випадках витоки призводять до фінансових втрат, репутаційного збитку, а іноді навіть до юридичних наслідків для організацій.

Основними причинами витоків є недостатній захист інформаційних систем, використання слабких паролів, відсутність оновлень програмного забезпечення, а також недотримання правил кібербезпеки. Для мінімізації ризиків необхідно запроваджувати сучасні технології захисту, навчати співробітників правилам безпеки та регулярно проводити перевірки систем.

В Україні витоки даних є поширеним явищем, зумовленим низьким рівнем захисту інформаційних систем, недоліками у впровадженні сучасних технологій безпеки та недостатньою обізнаністю користувачів у питаннях кібербезпеки. Часто витоки трапляються через недбалість у налаштуванні серверів або хмарних сховищ, використання слабких паролів, відсутність оновлень програмного забезпечення, а також через фішингові атаки.

Одним із прикладів є витоки даних із державних реєстрів чи баз даних приватних компаній, що містять персональну інформацію громадян. Ця інформація може потрапляти у відкритий доступ або використовуватися зловмисниками для шахрайства, крадіжки ідентичності чи інших незаконних дій.

Поширеність таких інцидентів також зумовлена тим, що не всі організації дотримуються вимог законодавства, наприклад, Закону України «Про захист персональних даних». Крім того, недостатнє фінансування та не увага до інформаційної безпеки на державному рівні також сприяють підвищенню ризиків.

Для боротьби з цією проблемою необхідно впроваджувати суворіші стандарти кіберзахисту, посилювати контроль за обробкою даних, навчати працівників та користувачів правил безпеки, а також проводити регулярні аудити інформаційних систем.

Основні аспекти викотів даних наведені та проаналізовані у таблиці 1.1.

Таблиця 1.1 – Основні аспекти витоків даних

Тип витоку	Причини	Наслідки	Приклади
1	2	3	4
Злом системи	Незахищені паролі, вразливості в ПЗ, слабкі системи аутентифікації	Втрата конфіденційних даних, репутаційні та фінансові збитки	Злом Equifax (2017), коли було викрадено дані 147 млн людей
Фішинг	Обман користувачів, які вводять свої дані на підроблених сайтах	Отримання доступу до облікових записів та персональної інформації	Фішингова атака на Facebook і Google (2017)
Витік через співробітників	Ненавмисна помилка, або навмисне викрадення даних з боку працівників	Втрата даних, штрафи, пошкодження репутації	Витік інформації у Tesla, що здійснювався співробітником
Недбале поводження з даними	Відсутність заходів безпеки при обробці, зберіганні або передачі даних	Ризик для приватності, фінансові втрати, витік особистої інформації	Marriott (2018): витік даних 500 млн клієнтів
Витік через незахищені мережі	Використання публічних Wi–Fi без шифрування даних	Перехоплення даних, несанкціонований доступ до облікових записів	Часті витоки при роботі користувачів у публічних Wi–Fi
Викрадення пристроїв	Втрата або крадіжка ноутбуків, телефонів, зовнішніх носіїв з чутливими даними	Можливість несанкціонованого доступу до важливої інформації	Втрата пристроїв із даними клієнтів у медичних установах
Неправильна конфігурація	Помилки у налаштуванні хмарних серверів, баз даних або інших систем	Публічний доступ до конфіденційної інформації, збитки для компанії	Відкриті бази даних компанії MongoDB
Використання сторонніх додатків	Ненадійні або небезпечні додатки, що мають доступ до конфіденційних даних	Витік особистої інформації, ризик компрометації облікових записів	Витік даних користувачів через сторонні розширення браузера

Соціальна інженерія – це метод маніпуляції людьми, спрямований на те, щоб змусити їх розкрити конфіденційну інформацію або виконати дії, вигідні зловмисникам. Цей метод базується на використанні довіри, страху або цікавості жертв, щоб отримати доступ до даних чи систем.

Прикладами соціальної інженерії є фішингові атаки, коли користувач отримує підроблений лист із проханням ввести паролі або дані картки на фальшивому сайті. Інший поширений випадок – телефонний дзвінок від шахрая, який видає себе за співробітника банку та просить надати код із SMS, нібито для захисту рахунку.

Соціальна інженерія також може використовуватися у фізичному середовищі. Наприклад, зловмисник може представитися працівником технічної підтримки, щоб отримати доступ до серверної кімнати або попросити співробітника компанії надати йому облікові дані.

Головна мета соціальної інженерії – обійти технічні заходи захисту, впливаючи на людський фактор. Щоб уникнути подібних атак, важливо бути пильним, перевіряти джерела запитів, ніколи не передавати особисту інформацію незнайомцям і регулярно навчатися правилам кібербезпеки.

Прикладами соціальної інженерії є такі ситуації:

1. Шахрай телефонує людині, видаючи себе за співробітника банку, і повідомляє про підозрілу активність на рахунку. Під приводом захисту рахунку він просить жертву надати код із SMS або дані банківської картки.

2. Користувач отримує електронний лист, який виглядає як офіційне повідомлення від популярного онлайн-магазину. У листі йдеться про необхідність «підтвердити акаунт» через посилання, яке веде на підроблений сайт для збору паролів.

3. Зловмисник видає себе за співробітника служби технічної підтримки, щоб переконати працівника компанії надати пароль до корпоративної системи або встановити шкідливе програмне забезпечення на комп’ютер.

4. У соціальних мережах шахрай створює фальшивий профіль, видаючи себе за знайомого жертви, і просить позичити гроші або надати доступ до спільних ресурсів.

5. У публічному місці, наприклад, кафе, зловмисник підходить до людини, яка залишила ноутбук без нагляду, і, представившись співробітником адміністрації, просить надати пароль для «перевірки налаштувань мережі».

6. Співробітники компанії отримують підроблений лист від імені керівника із проханням терміново надіслати копії конфіденційних документів чи зробити переказ грошей.

7. На вході до офісної будівлі зловмисник вдає, що забув свій пропуск, і переконує працівника пропустити його до внутрішніх приміщень.

Ці приклади демонструють, як зловмисники використовують людський фактор і психологічний тиск для досягнення своїх цілей.

Використання публічних Wi-Fi мереж без додаткового захисту становить серйозний ризик для безпеки даних. У таких мережах зловмисники можуть легко перехоплювати трафік, оскільки передача даних часто відбувається без шифрування. Це дозволяє отримувати доступ до конфіденційної інформації користувача, наприклад, логінів, паролів, номерів банківських карток або інших особистих даних.

Один із поширених методів атаки – це створення зловмисником фальшивої точки доступу з назвою, схожою на офіційну. Користувач, підключившись до такої мережі, не підозрює, що весь його трафік контролюється.

Щоб зменшити ризики, важливо використовувати віртуальну приватну мережу (VPN), яка шифрує передані дані, а також уникати передачі конфіденційної інформації через публічний Wi-Fi. Також слід відключати автоматичне підключення до відкритих мереж і використовувати лише ті сайти, які працюють через захищений протокол HTTPS.»

Для використання незахищених мереж можна створити кругову діаграму – рисунок 1.1, який ілюструє, які типи даних найчастіше опиняються під загрозою через використання таких мереж, або яка відображає основні ризики, пов’язані з публічним Wi-Fi.

Рисунок 1.1 – Типи вразливих даних при використанні незахищених мереж

Діаграма показує, що логіни та паролі становлять найбільшу частку вразливих даних під час використання незахищених мереж, складаючи 35%. На другому місці знаходиться фінансова інформація, що свідчить про значний ризик для користувачів, які проводять банківські операції через публічний Wi-Fi. Персональні дані складають 20%, тоді як конфіденційні документи та файли – 10%. Інші вразливі дані, такі як чати, історія вебпереглядів та подібна інформація, займають ще 10%.

1.2 Методології та підходи до захисту персональних даних користувачів Інтернет

Захист персональних даних є важливим аспектом сучасної інформаційної безпеки, особливо в умовах активного розвитку цифрових технологій. Основні

методології та підходи спрямовані на мінімізацію ризиків несанкціонованого доступу, втрати чи викрадення даних.

Організаційні методології включають розробку політик безпеки. Організації створюють внутрішні документи, які регламентують обробку, зберігання та доступ до персональних даних. Це також передбачає призначення відповідальної особи за захист даних. Навчання персоналу є ще одним важливим аспектом. Працівники регулярно проходять курси з кібербезпеки та правил роботи з персональними даними, що допомагає зменшити ризики помилок і витоків через соціальну інженерію. Контроль доступу забезпечується встановленням чітких правил, які дозволяють отримувати доступ до конфіденційної інформації лише тим, хто безпосередньо з нею працює.

Серед технічних методологій важливе місце займає шифрування даних. Криптографічні алгоритми забезпечують захист даних як під час їх передачі, так і зберігання, роблячи їх недоступними для зловмисників у разі викрадення. Брандмауери та антивірусні програми використовуються для моніторингу трафіку, блокування шкідливих програм і захисту від хакерських атак. Двофакторна аутентифікація додає додатковий рівень безпеки, вимагаючи підтвердження доступу через другий фактор, наприклад код із SMS. Системи виявлення та запобігання загрозам забезпечують моніторинг мережі та блокують підозрілу активність у реальному часі.

Процедурні підходи включають регулярний аудит систем, що дозволяє перевіряти відповідність стандартам безпеки, виявляти вразливості та усувати їх. Створення резервних копій даних допомагає відновити інформацію у разі втрати або пошкодження, наприклад, через атаки програм-вимагачів. Псевдонімізація та анонімізація даних знижують ризики, дозволяючи обробляти інформацію без прямої ідентифікації особи.

Правові підходи передбачають дотримання законодавства, зокрема міжнародних регламентів, таких як GDPR, та локальних законів, як-от Закон України «Про захист персональних даних». Укладання угод про конфіденційність забезпечує відповідальність працівників, підрядників та партнерів за збереження даних.

Інноваційні підходи включають використання штучного інтелекту, який допомагає виявляти загрози у реальному часі та аналізувати поведінку користувачів. Технології блокчейну забезпечують безпечне зберігання та передачу даних завдяки децентралізації та незмінності записів. Підхід Zero Trust Model передбачає постійну перевірку кожного доступу до системи, незалежно від джерела запиту.

Культурні та етичні аспекти зосереджені на підвищенні обізнаності користувачів щодо важливості захисту їхніх даних. Інформування громадян про ризики використання незахищених платформ і необхідність створення складних паролів допомагає зменшити ризики. Організації також повинні бути прозорими в обробці даних, інформуючи користувачів про те, які дані збираються, як вони використовуються та захищаються.

Захист персональних даних вимагає комплексного підходу, який об’єднує технічні, організаційні, процедурні та правові заходи. Ефективна реалізація цих методів допомагає зменшити ризики витоків даних і підвищити довіру користувачів до організації.

1.3 Механізми шифрування для убезпечення персональних даних користувачів Інтернет

Механізми шифрування в криптографії – це способи перетворення інформації у форму, яку неможливо зрозуміти без спеціального ключа. Вони захищають дані від несанкціонованого доступу під час їх передачі або зберігання.

Механізми шифрування є невід'ємною частиною сучасних систем захисту інформації, особливо в контексті зростаючих загроз кібербезпеки та необхідності захисту персональних даних користувачів Інтернету. Існує два основні типи шифрування: симетричне і асиметричне. У симетричному шифруванні використовується один і той самий ключ для шифрування і розшифрування даних. Цей метод швидший, але вимагає безпечної передачі ключа між сторонами. Прикладом є алгоритми AES і DES.

Асиметричне шифрування використовує два різні ключі: публічний і приватний. Публічний ключ застосовується для шифрування, а приватний – для розшифрування. Це дозволяє передавати дані без необхідності обміну секретним ключем. Прикладом є RSA і алгоритм Еліптичних кривих (ECC).

Також існує хешування – механізм, який створює унікальний цифровий «відбиток» даних. Цей відбиток незворотній і використовується для перевірки цілісності даних. Прикладами алгоритмів є SHA-256 і MD5.

Шифрування є основою для багатьох технологій безпеки, таких як VPN, HTTPS і електронний підпис. Воно гарантує конфіденційність, автентичність та цілісність даних у цифровому світі.

1.3.1 Симетричне шифрування

Симетричне шифрування – це метод криптографії, у якому для шифрування і розшифрування даних використовується один і той самий секретний ключ. Цей метод простий та ефективний, але потребує безпечної передачі ключа між сторонами.

Розглянемо як працює симетричне шифрування:

1. Відправник використовує секретний ключ, щоб зашифрувати повідомлення.
2. Отримувач застосовує той самий ключ для розшифрування отриманих даних.
3. Якщо ключ буде викрадений, зловмисник зможе отримати доступ до інформації.

Приклади алгоритмів симетричного шифрування:

– AES (Advanced Encryption Standard) – сучасний стандарт шифрування, який широко використовується через свою надійність і швидкість.

– DES (Data Encryption Standard) – раніше популярний алгоритм, але зараз вважається застарілим через низький рівень безпеки.

– 3DES (Triple DES) – покращена версія DES, яка застосовує шифрування три рази для підвищення безпеки.

– Blowfish – алгоритм, що забезпечує швидке та ефективне шифрування.

Переваги симетричного шифрування:

– Швидке виконання навіть на великих обсягах даних.

– Простота реалізації у програмному забезпеченні та апаратурі.

Недоліки симетричного шифрування:

– Проблема передачі секретного ключа. Його необхідно передати безпечним каналом, щоб уникнути викрадення.

– Ключ має залишатися таємним, а це складно забезпечити в масштабних системах.

Симетричне шифрування найчастіше використовується для забезпечення конфіденційності в таких системах, як VPN, зберігання файлів і передача даних у захищених мережах.

Розглянемо приклад шифрування за допомогою алгоритму симетричного шифрування AES (Advanced Encryption Standard). Цей алгоритм є одним із найпопулярніших методів захисту даних завдяки високій швидкості роботи та надійності.

Як працює AES:

1. Ключ: Вибирається секретний ключ певної довжини: 128, 192 або 256 біт. Від довжини ключа залежить рівень безпеки.

2. Вхідні дані: Повідомлення, яке потрібно зашифрувати, перетворюється у двійковий вигляд.

3. Шифрування: Повідомлення шифрується у кілька раундів, залежно від довжини ключа (10 раундів для 128-бітного ключа, 12 для 192-бітного і 14 для 256-бітного).

4. Результат: Зашифроване повідомлення, яке виглядає як набір випадкових символів.

Приклад шифрування.

Припустимо, що потрібно зашифрувати текст «Hello World» за допомогою AES-128.

1. Вибирається 128-бітний ключ, наприклад: Th1s1sA128b1tKey.

2. Текст «Hello World» конвертується у двійкову форму або використовується стандарт UTF-8.

3. Алгоритм AES виконує такі основні операції:

– SubBytes: Замінює кожен байт даних відповідно до фіксованої таблиці підстановок (S-box).

– ShiftRows: Зміщує рядки блоку даних для перемішування.

– MixColumns: Змішує стовпці для посилення зв'язків між байтами.

– AddRoundKey: Поєднує дані з ключем шифрування через операцію XOR.

4. Ці операції повторюються в декількох раундах, створюючи шифрований текст, наприклад: 4f3d2a1b0c5e7a8f.

5. Для розшифрування отриманих даних використовується той самий ключ, який застосовувався для шифрування.

6. Особливості.

– Довжина ключа: Чим довший ключ, тим безпечніший алгоритм, але повільніше виконання.

– Рівні безпеки: AES-128 є достатньо безпечним для більшості застосувань, але для критично важливих даних використовується AES-256.

– Застосування: AES використовується в шифруванні файлів, мережевому трафіку (наприклад, HTTPS), VPN, хмарних сховищах тощо.

Таким чином, AES забезпечує надійний і ефективний захист даних, що робить його стандартом у багатьох галузях.

1.3.2 Асиметричне шифрування

Асиметричне шифрування – це метод криптографії, який використовує пару ключів: публічний і приватний. Цей підхід забезпечує безпечну передачу даних без необхідності обміну секретним ключем.

Принцип роботи асиметричне шифрування:

1. Кожен користувач має пару ключів: публічний ключ (який можна вільно поширювати) і приватний ключ (який зберігається у таємниці).

2. Дані, зашифровані публічним ключем, можуть бути розшифровані лише відповідним приватним ключем. І навпаки: дані, зашифровані приватним ключем, розшифровуються публічним.

3. Таким чином, публічний ключ використовується для шифрування інформації, яку можуть безпечно передати навіть через незахищений канал.

Приклад:

1. Відправник отримує публічний ключ отримувача.

2. Використовуючи цей ключ, він шифрує повідомлення, наприклад: «Hello World».

3. Лише власник відповідного приватного ключа може розшифрувати це повідомлення та прочитати його.

Основні алгоритми асиметричного шифрування:

– RSA (Rivest-Shamir-Adleman) – один із найпоширеніших алгоритмів, що використовується для захисту даних і цифрових підписів.

– ECC (Elliptic Curve Cryptography) – алгоритм, що забезпечує високу безпеку з меншими розмірами ключів, тому часто використовується в мобільних і вбудованих пристроях.

– ElGamal – алгоритм, який використовується для шифрування та створення цифрових підписів.

– Diffie-Hellman – метод обміну ключами, який дозволяє безпечно створити спільний секрет між сторонами.

Переваги асиметричного шифрування:

– Не потрібно передавати секретний ключ, як у симетричному шифруванні.

– Забезпечує високий рівень безпеки завдяки складності математичних обчислень.

– Використовується для цифрових підписів, що гарантують автентичність і цілісність повідомлення.

Недоліки:

– Порівняно з симетричним шифруванням, алгоритми асиметричного шифрування працюють повільніше.

– Вимагає більших обчислювальних ресурсів, що може бути проблемою для обмежених пристроїв.

Застосування:

– Електронна пошта: шифрування повідомлень (наприклад, PGP).

– Цифрові сертифікати: забезпечення безпеки веб-сайтів через протоколи HTTPS.

– Електронний підпис: для перевірки автентичності та авторства документів.

– VPN: захист з'єднань між клієнтами та серверами.

Асиметричне шифрування є ключовою технологією для захисту інформації у відкритих мережах і забезпечення конфіденційності, автентичності та цілісності даних.

1.3.3 Гібридні методи убезпечення персональних даних користувачів Інтернет

Гібридні методи шифрування – це підхід, який об'єднує симетричне та асиметричне шифрування для досягнення високого рівня безпеки й ефективності. Такий метод дозволяє використати переваги обох підходів: швидкість симетричного шифрування і безпечну передачу ключів завдяки асиметричному шифруванню.

У гібридному шифруванні відправник спочатку генерує випадковий симетричний ключ, який називається сесійним ключем. Цей ключ використовується для шифрування основних даних симетричним алгоритмом, наприклад, AES. Потім сесійний ключ шифрується публічним ключем отримувача за допомогою асиметричного алгоритму, такого як RSA. Зашифровані дані разом із зашифрованим сесійним ключем передаються отримувачу. Отримувач розшифровує сесійний ключ своїм приватним ключем і використовує його для розшифрування основних даних.

Гібридні методи мають кілька важливих переваг. Вони забезпечують високу ефективність, оскільки основні дані шифруються швидким симетричним

алгоритмом, що значно економить час. Передача ключів є безпечною, оскільки сесійний ключ захищений асиметричним шифруванням. Крім того, гібридні методи легко масштабується, дозволяючи ефективно захищати великі обсяги даних.

Приклади застосування гібридних методів можна знайти в багатьох сучасних технологіях. Наприклад, у протоколі HTTPS асиметричне шифрування використовується для встановлення безпечного з'єднання через TLS/SSL, а симетричне – для передачі даних. В електронній пошті, зокрема у системах PGP (Pretty Good Privacy), гібридне шифрування забезпечує захист повідомлень. Також гібридний підхід застосовується для захисту великих файлів, спрощуючи передачу ключів.

Особливістю гібридних методів є те, що асиметричне шифрування використовується лише для передачі сесійного ключа, оскільки воно потребує більше ресурсів, ніж симетричне шифрування. Симетричне шифрування, своєю чергою, забезпечує швидке шифрування великих обсягів даних.

Завдяки поєднанню переваг обох підходів гібридні методи ідеально підходять для забезпечення конфіденційності, автентичності та цілісності даних у сучасних Інтернет-системах.

1.4 Аутентифікація для убезпечення персональних даних користувачів Інтернет

Аутентифікація – це процес перевірки особи або системи для підтвердження їхньої достовірності. Її основна мета – гарантувати, що доступ до даних або ресурсів отримує лише уповноважений користувач.

Цей процес базується на використанні одного або кількох факторів перевірки. Найпоширеніший спосіб – введення імені користувача і пароля. Інші методи включають використання фізичних ключів, біометричних даних, таких як відбитки пальців або розпізнавання обличчя, або одноразових кодів, надісланих через SMS чи електронну пошту.

Аутентифікація є ключовим етапом у системах безпеки, адже вона захищає конфіденційну інформацію та обмежує доступ сторонніх осіб. У сучасних системах часто використовується багатофакторна аутентифікація, яка комбінує кілька способів перевірки для підвищення рівня безпеки.

Аутентифікація базується на трьох основних принципах перевірки особи або системи. Перший принцип – це те, що ви знаєте. Він передбачає використання інформації, яка відома лише користувачу. Найпоширенішими прикладами є паролі, PIN-коди або відповіді на секретні питання. Однак, якщо така інформація буде викрадена або розкрита, система може стати вразливою.

Другий принцип – це те, що ви маєте. Він базується на використанні фізичних об'єктів, які перебувають у розпорядженні користувача. Це можуть бути смарт-картки, токени, мобільні пристрої з додатками для генерування одноразових паролів або спеціальні ключі безпеки. Такий підхід додає ще один рівень захисту, оскільки зловмиснику необхідно отримати фізичний доступ до цих об'єктів.

Третій принцип – це те, хто ви є. Він використовує унікальні фізичні або поведінкові характеристики користувача. Прикладами є біометричні дані, такі як відбитки пальців, розпізнавання обличчя, сканування райдужної оболонки ока або навіть голос. Цей метод є одним із найскладніших для підробки, але його впровадження потребує складніших технологій.

Сучасні системи безпеки часто комбінують ці принципи у багатофакторній аутентифікації, щоб підвищити рівень захисту. Наприклад, користувач може вводити пароль, що відповідає принципу «те, що ви знаєте», і одночасно підтверджувати свою особу за допомогою одноразового коду, отриманого на мобільний пристрій, що належить до принципу «те, що ви маєте».

Багатофакторна аутентифікація – це метод перевірки особи, який використовує більше одного фактору для підтвердження доступу користувача до системи чи ресурсу. Цей підхід забезпечує додатковий рівень захисту, оскільки зловмиснику потрібно одночасно зламати кілька рівнів перевірки.

Багатофакторна аутентифікація зазвичай поєднує два або більше з трьох основних факторів: те, що ви знаєте (наприклад, пароль), те, що ви маєте

(наприклад, токен або смартфон), і те, хто ви є (наприклад, біометричні дані). Наприклад, під час входу в онлайн-акаунт користувач може спочатку ввести пароль, а потім підтвердити доступ за допомогою одноразового коду, надісланого на телефон.

Ця методика широко використовується для захисту банківських акаунтів, електронної пошти, корпоративних систем та інших критично важливих ресурсів. Вона значно ускладнює роботу зловмисникам, навіть якщо один із факторів (наприклад, пароль) буде скомпрометований. Таким чином, багатофакторна аутентифікація є одним із найефективніших способів забезпечення безпеки в цифровому середовищі.

1.5 Політики управління правами доступу для убезпечення персональних даних користувачів Інтернет

Політики управління правами доступу – це набір правил і процедур, які регулюють доступ користувачів до ресурсів, даних і систем організації. Їхня мета – забезпечити, щоб доступ отримували лише ті особи, які мають відповідні повноваження, та лише до тих ресурсів, які їм необхідні для виконання своїх обов'язків.

Одним із ключових принципів таких політик є принцип мінімальних привілеїв. Це означає, що кожен користувач отримує лише ті права доступу, які потрібні йому для виконання роботи, і нічого більше. Наприклад, співробітник відділу кадрів може мати доступ до особистих файлів співробітників, але не до фінансової звітності компанії.

Також важливим є розмежування обов'язків. Цей підхід передбачає, що певні дії, які можуть становити ризик для безпеки, повинні виконуватися різними особами. Наприклад, одна людина створює платіжні документи, а інша їх затверджує.

Політики управління правами доступу зазвичай включають механізми аутентифікації та авторизації. Аутентифікація перевіряє особу користувача, а

авторизація визначає, до яких ресурсів і з якими правами цей користувач має доступ.

Організації часто застосовують спеціальні системи управління доступом (IAM), які автоматизують контроль і моніторинг доступу. Такі системи можуть регулярно перевіряти актуальність прав користувачів і відключати доступ, якщо він більше не потрібен.

Дотримання політик управління правами доступу є важливим аспектом кібербезпеки, оскільки це допомагає запобігти несанкціонованому доступу до конфіденційної інформації та зменшити ризики внутрішніх і зовнішніх загроз.

Політики управління доступом об'єднують такі важливі аспекти, як:

– Аутентифікація. Це процес перевірки особи користувача перед наданням доступу до системи чи ресурсу. Він включає використання паролів, біометричних даних, токенів або багатофакторної аутентифікації для підтвердження особи.

– Авторизація. Після успішної аутентифікації визначається, які ресурси користувач має право використовувати і з якими привілеями, наприклад, тільки читання чи повний доступ.

– Принцип мінімальних привілеїв. Кожному користувачу надається лише той рівень доступу, який потрібен для виконання його обов'язків, що мінімізує ризик несанкціонованих дій.

– Розмежування обов'язків. Завдання, які можуть становити ризик безпеки, поділяються між кількома користувачами, щоб запобігти зловживанням.

– Моніторинг та аудит. Політики включають регулярне відстеження дій користувачів у системі та проведення перевірок доступу для виявлення підозрілої активності або невідповідностей.

– Контроль життєвого циклу доступу. Це управління доступом протягом усього часу роботи користувача в організації, включаючи надання доступу новим співробітникам, зміни привілеїв та своєчасне видалення доступу після звільнення.

– Захист даних. Політики передбачають шифрування, розмежування доступу до конфіденційної інформації та захист критично важливих систем.

– Ролі та групи. Політики дозволяють визначати доступ на основі ролей, що спрощує управління привілеями для великої кількості користувачів.

Ці аспекти допомагають створити комплексну систему управління доступом, яка забезпечує безпеку даних та ресурсів, захищає від внутрішніх і зовнішніх загроз і сприяє дотриманню вимог законодавства та стандартів.

1.6 Застосування коефіцієнта помилково-негативної ідентифікації (FNR) до убезпечення персональних даних користувачів Інтернет

Коефіцієнт помилково-негативної ідентифікації (False Negative Rate, FNR) – це показник, який використовується для оцінки ефективності систем аутентифікації або біометричних методів. Він показує частку випадків, коли справжній користувач не зміг пройти аутентифікацію через те, що система його помилково визначила як неавторизованого.

Формально, FNR можна виразити такою формулою 1.1.

$$\mathrm{FNR} = \frac{\mathrm{FN}}{\mathrm{FN} + \mathrm{TP}}, \tag{1.1}$$

де: FN (False Negatives) – кількість випадків, коли справжнього користувача система не ідентифікувала правильно.

TP (True Positives) – кількість випадків, коли система правильно ідентифікувала користувача.

Застосування FNR для убезпечення персональних даних.

FNR важливий у контексті убезпечення персональних даних в Інтернеті, оскільки занадто високий рівень помилково-негативних результатів може створити проблеми для користувачів. Наприклад, справжні власники акаунтів можуть втратити доступ до своїх даних або сервісів, що може знижувати зручність використання системи. З іншого боку, заниження FNR без врахування

інших показників, таких як False Positive Rate (FPR), може підвищувати ризик для безпеки даних.

Приклад.

Розглянемо систему розпізнавання обличчя, яка використовується для доступу до онлайн-банкінгу. Припустимо, за день 1000 користувачів спробували пройти аутентифікацію:

950 користувачів були справжніми (мали доступ).

З них 900 були правильно ідентифіковані (TP), а 50 – помилково відхилені (FN).

FNR для цієї системи буде розрахований так як наведено у формулі 1.2.

$$\mathrm{FNR} = \frac{\mathrm{FN}}{\mathrm{FN} + \mathrm{TP}} = \frac{50}{50 + 900} = \frac{50}{950} \approx 0.0526\,(5.26\%), \tag{1.2}$$

Це означає, що близько 5% справжніх користувачів не змогли пройти аутентифікацію через помилку системи.

Для зменшення FNR можна використовувати такі методи:

1. Оптимізація алгоритмів розпізнавання. Поліпшення точності алгоритмів аутентифікації шляхом використання машинного навчання чи більш точних біометричних моделей.

2. Комбіновані методи аутентифікації. Додавання багатофакторної аутентифікації, наприклад, використання розпізнавання обличчя разом із паролем або одноразовим кодом.

3. Регулювання порогів аутентифікації. Зниження порогових значень для прийняття рішень може зменшити FNR, але потрібно балансувати цей показник із FPR.

FNR є важливим інструментом для оцінки надійності систем аутентифікації в Інтернеті. Його оптимізація дозволяє забезпечити зручність і безпеку для користувачів, знижуючи ризики втрати доступу до персональних даних. Однак варто враховувати баланс між FNR та іншими показниками, щоб не знижувати загальний рівень безпеки системи.

1.7 Висновок до першого розділу

У першому розділі кваліфікаційної роботи освітнього рівня «магістр» розглянуто ключові теоретичні аспекти захисту персональних даних, які є актуальною темою в умовах цифрової трансформації суспільства.

У першому розділі магістерської роботи було проведено систематизацію понять і видів персональних даних, а також досліджено основні нормативно-правові акти, що регулюють їх захист. Встановлено, що забезпечення конфіденційності та безпеки персональних даних є фундаментальним елементом сучасного інформаційного середовища, яке регулюється міжнародними стандартами (GDPR, CCPA) та законодавством України (Закон України «Про захист персональних даних»).

Розглянуто методології та підходи до захисту персональних даних користувачів Інтернет. Виявлено, що поєднання організаційних, технічних та правових заходів дозволяє забезпечити комплексний підхід до убезпечення даних.

Досліджено механізми шифрування як основу технічного захисту персональних даних:

Симетричне шифрування характеризується високою швидкістю, але меншою гнучкістю через необхідність передачі ключів.

Асиметричне шифрування вирізняється більшою надійністю, але потребує більших обчислювальних ресурсів.

Гібридні методи поєднують переваги обох підходів, що дозволяє досягти оптимального балансу між ефективністю та безпекою.

Вивчено роль аутентифікації в забезпеченні безпеки персональних даних. Розглянуто різні методи аутентифікації, включаючи однофакторну, двофакторну та багатофакторну аутентифікацію, які суттєво підвищують рівень захисту даних.

Проаналізовано політики управління правами доступу, які є невід'ємною частиною сучасних систем убезпечення персональних даних. Використання

рольового розподілу доступу (RBAC) та інших підходів дозволяє ефективно обмежувати доступ до інформації залежно від потреб і прав користувачів.

Розглянуто застосування коефіцієнта помилково-негативної ідентифікації (FNR) для оцінки ефективності систем захисту персональних даних. Встановлено, що мінімізація FNR є критичною для забезпечення надійності системи ідентифікації користувачів.

Таким чином, дослідження теоретичних аспектів дозволило визначити ключові методи та механізми захисту персональних даних, які є основою для розробки практичних рекомендацій у подальших розділах роботи.

Загалом, для створення надійної системи захисту персональних даних необхідно поєднувати сучасні технології, законодавчі вимоги та усвідомлення важливості безпеки як з боку організацій, так і з боку користувачів. Такий підхід допоможе мінімізувати ризики і забезпечити конфіденційність даних в умовах цифрової епохи.

2 МЕТОДОЛОГІЧНІ ОСНОВИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

2.1 Проблеми та робочі гіпотези убезпечення персональних даних користувачів Інтернет

За останні роки Інтернет суттєво змінив життя людей, ставши невід'ємною частиною повсякденності. Попри очевидні переваги, такі як зручність доступу до інформації, можливість дистанційної роботи, навчання та онлайн-торгівлі, Інтернет також несе в собі численні ризики. Основна проблема полягає у забезпеченні безпеки користувачів та захисті їхніх даних. Значна частина матеріалів в Інтернеті має протизаконний характер, а використання недобросовісних методів у цьому середовищі може призводити до порушення прав людини, зокрема до втрати приватності, крадіжки даних та шахрайства.

Головною проблемою дослідження є аналіз стану безпеки користувачів Інтернету. Питання безпеки в мережі нерідко вважається ілюзорним, адже веб-сайти збирають дані користувачів так непомітно, що вони навіть не підозрюють про обсяг інформації, якою діляться. Цей процес посилюється відсутністю прозорості щодо обробки персональних даних власниками веб-сайтів. У результаті виникає загроза витоку персональних даних, а також зловживань інформацією з боку третіх осіб. Низький рівень обізнаності користувачів лише підсилює цю проблему.

Поява Інтернету змусила переглянути концепцію приватності. Дані, розміщені в мережі, стають доступними практично для необмеженого кола осіб, ставлячи під сумнів існування мережевої конфіденційності. Крім того, поширення кіберзлочинності, включаючи фішинг, несанкціонований доступ до даних та соціальну інженерію, створює додаткові ризики для користувачів. Ця проблема посилюється недостатньою прозорістю щодо обробки персональних даних власниками веб-сайтів та мобільних додатків, що ускладнює дотримання прав людини в Інтернеті.

Безпека користувачів Інтернету базується на кількох принципах, які є основою для забезпечення захисту даних та інформаційної конфіденційності:

1. Цілісність даних – гарантія, що інформація залишається незмінною під час зберігання чи передачі. Лише авторизовані користувачі мають право змінювати чи видаляти дані, що забезпечує захист від сторонніх втручань.

2. Доступність – інформація має бути доступною для легальних користувачів без затримок і перешкод. Системи безпеки мають забезпечувати швидкий доступ до даних навіть у разі аварій чи технічних несправностей.

3. Конфіденційність – обмеження доступу до даних лише для авторизованих осіб. Важливо забезпечити, щоб дані залишалися недоступними для сторонніх осіб без відповідних дозволів.

4. Достовірність інформації – гарантія того, що дані належать їхньому власнику чи джерелу. Цей принцип запобігає маніпуляції даними та їхньому неправомірному використанню.

Інформаційні загрози можна поділити на кілька основних груп залежно від їхнього характеру та впливу:

1. Загрози впливу недостовірної інформації – поширення фальшивих чи дезінформаційних даних, які можуть маніпулювати думкою громадськості або вводити в оману користувачів.

2. Загрози несанкціонованого доступу – спроби сторонніх осіб втручатися у роботу систем чи отримувати доступ до конфіденційних даних без дозволу. Такі дії можуть мати на меті викрадення фінансової інформації, маніпуляції чи шантаж.

3. Загрози інформаційним правам – порушення права на конфіденційність, інтелектуальну власність, зловживання особистими даними. Це включає випадки, коли дані використовуються без згоди їхнього власника або з порушенням законодавства.

Види загроз:

1. Загрози конфіденційності – несанкціонований доступ до даних через збої, віруси чи людські помилки. Відомо, що такі загрози можуть призводити до витоку чутливої інформації, включаючи фінансові дані, особисту інформацію чи корпоративну таємницю.

2. Загрози цілісності – модифікація даних внаслідок зловмисних дій або технічних проблем. Ці загрози особливо небезпечні для критичних систем, де навіть невеликі зміни можуть мати серйозні наслідки.

3. Загрози доступності – блокування доступу до ресурсів чи послуг. Це може бути наслідком атак типу DDoS, коли сервери перевантажуються фіктивними запитами, або технічних збоїв.

Для зменшення ризиків необхідно застосовувати комплексні заходи безпеки, які включають:

1. Створення складних паролів – унікальних і багатокомпонентних для кожного ресурсу. Це зменшує ймовірність злому облікових записів.

2. Використання двофакторної аутентифікації – подвійний рівень захисту, який ускладнює доступ до даних навіть у разі компрометації пароля.

3. Оновлення програмного забезпечення – своєчасне застосування оновлень, що закривають вразливості в системах безпеки.

4. Перевірка сайтів – введення даних лише на перевірених ресурсах із захищеними протоколами (HTTPS). Важливо перевіряти наявність захищеного з'єднання перед введенням особистих даних чи фінансової інформації.

5. Використання шифрування – застосування шифрування для захисту повідомлень та даних від несанкціонованого доступу.

На основі аналізу проблематики сформульовано основну та додаткові гіпотези:

1. Основна гіпотеза: Стан безпеки користувачів в Інтернеті, попри наявність ризиків, може вважатися задовільним за умови дотримання користувачами базових принципів безпеки та рекомендацій.

2. Додаткові гіпотези:

– Інтернет має вбудовані механізми захисту, такі як шифрування та антивірусні програми, які підвищують рівень безпеки.

– Загрози інформаційній безпеці виникають на кожному етапі використання Інтернету, і їх можна мінімізувати шляхом підвищення обізнаності користувачів.

– Більшість користувачів недооцінюють ризики, що виникають під час роботи в мережі, та ігнорують базові правила безпеки, що підвищує їхню вразливість.

– Успішність захисту залежить як від технологій, так і від свідомого ставлення користувачів до захисту своїх даних.

– Поширення освітніх програм із кібербезпеки може суттєво зменшити кількість випадків шахрайства та витоку даних.

Проблема інформаційної безпеки в Інтернеті є багатогранною та потребує комплексного підходу на державному, корпоративному та індивідуальному рівнях. Вивчення питань безпеки, підвищення обізнаності користувачів та впровадження рекомендацій є ключовими кроками для підвищення загального рівня захищеності в інформаційному просторі.

2.2 Досліджувані змінні, показники та характеристики параметрів убезпечення персональних даних користувачів Інтернет

Після формулювання гіпотез дослідження наступним кроком є визначення змінних, які необхідно досліджувати. Змінні поділяються на дві основні категорії: незалежні та залежні.

Незалежні змінні – це характеристики або фактори, які можуть впливати на залежні змінні та які дослідник може контролювати або вимірювати. У межах даного дослідження незалежними змінними є:

– Вік – визначається як кількісна змінна, яка впливає на обізнаність у питаннях безпеки та рівень технічної грамотності користувачів.

– Стать – розглядається як якісна змінна, що може впливати на ставлення до ризиків та методів захисту в Інтернеті.

– Місце роботи – ця змінна враховує специфіку професійної діяльності респондентів, яка може впливати на їхню поведінку в онлайн-середовищі.

– Сімейний стан – відображає соціальний контекст, що може впливати на активність користувача в мережі та його обізнаність щодо захисту персональних даних.

Залежні змінні – це змінні, які дослідник вивчає для визначення їхньої залежності від незалежних змінних. У цьому дослідженні залежними змінними є:

– Думки респондентів – суб'єктивні оцінки та судження користувачів щодо безпеки в Інтернеті, їхніх звичок, рівня знань про кіберзагрози та використання захисних інструментів.

Для коректного аналізу змінних необхідно визначити відповідні показники. Як стверджує Е. Баббі, показники – це об'єктивно спостережувані явища, поведінка чи процеси, на підставі яких дослідник може робити висновки про змінні [3].

Згідно з Й. Апановичем, показник є проявом змінної, що дозволяє з певністю чи ймовірністю зробити висновок про її наявність [2]. У цьому дослідженні показниками є:

1. Для змінної «вік»:

– Частота використання Інтернету (години на день).

– Типи активності в Інтернеті (навчання, робота, розваги тощо).

– Рівень обізнаності про основи кібербезпеки (оцінюється за допомогою опитування).

2. Для змінної «стать»:

– Відсоток чоловіків і жінок, які використовують антивірусні програми.

– Рівень схильності до ризикової поведінки в Інтернеті (наприклад, перехід за підозрілими посиланнями).

– Частота використання соціальних мереж.

3. Для змінної «місце роботи»:

– Наявність доступу до Інтернету на робочому місці.

– Використання захищених корпоративних мереж.

– Використання навчальних програм із кібербезпеки на підприємстві.

4. Для змінної «сімейний стан»:

– Рівень обізнаності про небезпеки для дітей в Інтернеті (зокрема, кібербулінг).

– Використання батьківського контролю.

– Частота спільного використання Інтернету членами сім’ї.

5. Для змінної «думки респондентів»:

– Рівень задоволеності безпекою в Інтернеті (оцінюється за шкалою від 1 до 10).

– Способи захисту персональних даних, які використовуються найчастіше (наприклад, складні паролі, двофакторна аутентифікація).

– Ставлення до ризиків у мережі (наприклад, думки щодо використання відкритих WiFi-мереж чи публікації приватної інформації).

Кожен показник є конкретною характеристикою, яка дозволяє спостерігати й оцінювати змінні. Наприклад:

– Вік респондентів може корелювати з рівнем їхньої технічної обізнаності та поведінковими звичками в Інтернеті.

– Стать впливає на уподобання щодо використання соціальних мереж чи інструментів захисту.

– Місце роботи може визначати рівень знань про кібербезпеку через доступ до навчальних програм чи корпоративних політик безпеки.

Показники дозволяють:

– Здійснювати кількісний аналіз результатів дослідження.

– Встановлювати зв’язок між незалежними та залежними змінними.

– Робити обґрунтовані висновки про характер явищ і процесів у досліджуваній сфері.

Підсумовуючи, змінні та їхні показники є ключовими елементами дослідження, які забезпечують його наукову обґрунтованість та достовірність. Визначення змінних і показників дозволяє структурувати дослідження, полегшуючи аналіз отриманих результатів та формулювання висновків.

2.3 Методи, прийоми та засоби дослідження

Дж. Штумський розглядає методи дослідження як «систему припущень і правил, що дозволяють упорядкувати практичну або теоретичну діяльність з

метою досягнення свідомо поставленої мети» [29]. На думку Дж. Апановича, метод дослідження є конкретним способом вирішення проблемної ситуації у рамках сформульованої дослідницької проблеми [2]. Метод дослідження поєднує у собі:

1. Визначення мети та завдань дослідження.
2. Планування та організацію дослідницького процесу.
3. Використання відповідних процедур, прийомів і засобів дослідження.

Суть методу дослідження полягає у забезпеченні відповідності між способом реалізації дослідження та поставленою метою. Методи повинні бути адекватними проблемі, доступними з огляду на ресурси та ефективними для досягнення цілей.

У цій роботі застосовуються такі основні методи дослідження:

1. Діагностичне опитування – цей метод дозволяє вивчити думки, оцінки та ставлення респондентів до проблеми безпеки в Інтернеті. Для реалізації опитування було розроблено анкету, яка включає питання щодо основних аспектів дослідження (Додаток Б).
2. Вивчення літератури – аналіз наукових джерел, нормативних документів та іншої літератури для визначення теоретичних засад досліджуваної проблеми. Цей метод дозволяє сформувати теоретичну базу для обґрунтування висновків і рекомендацій.

М. Цесларчик визначає прийоми дослідження як «збір інформації, необхідної для відповіді на проблемні питання» [6]. У даній роботі використано наступні прийоми:

1. Збір даних – проводився шляхом розповсюдження анкети серед респондентів із різними соціально-демографічними характеристиками.
2. Систематизація даних – отримані відповіді були впорядковані за тематичними категоріями для подальшого аналізу.
3. Аналіз даних – проведено обробку відповідей за допомогою кількісного та якісного аналізу для виявлення основних тенденцій і закономірностей.

Засоби дослідження включають об’єкти, інструменти та технічні засоби, що використовуються для збору, обробки та фіксації даних. У сучасних умовах дослідницькі засоби охоплюють як традиційні методи, так і сучасні технології, включаючи електронні системи та програмне забезпечення.

У цій роботі використано такі засоби:

1. Анкета – основний інструмент для збору інформації. Анкета включає логічно сформовані питання, що спрямовані на отримання відповідей, які стосуються думок, ставлень і поведінки респондентів щодо безпеки в Інтернеті.
2. Програмні засоби – застосовувалися для обробки зібраних даних, включаючи програмне забезпечення для статистичного аналізу.
3. Документальні джерела – використані для формування теоретичної основи та доповнення результатів дослідження емпіричними даними.

Анкета є одним із найважливіших інструментів збору інформації. Вона має такі характеристики:

– Логічна побудова, що забезпечує послідовність питань.
– Змістовна спрямованість на ключові аспекти дослідження.
– Простота і зручність для респондентів, що сприяє високій якості відповідей.

Анкета дозволяє:

– Збирати якісну та кількісну інформацію.
– Виявляти індивідуальні та загальні тенденції серед респондентів.
– Отримувати структуровані дані для подальшого аналізу.

Методи, прийоми та засоби дослідження є ключовими елементами, які визначають наукову цінність роботи. Використання діагностичного опитування, аналізу літератури та сучасних засобів обробки даних забезпечує комплексний підхід до вивчення проблеми. Прийоми дослідження дозволяють зібрати релевантну інформацію, а засоби – реалізувати дослідницькі завдання максимально ефективно.

2.4 Область та організація процесу дослідження онлайн-процедур убезпечення персональних даних користувачів Інтернет

Основна мета дослідження – визначити рівень безпеки користувачів Інтернету під час здійснення обраних онлайн процедур. Дослідження зосереджене на вивченні поведінки, ставлення та обізнаності користувачів щодо питань безпеки в Інтернеті, зокрема під час:

- Використання онлайн-магазинів.
- Оплати товарів і послуг через Інтернет.
- Роботи з соціальними мережами.
- Надання особистих даних на веб-сайтах.

Область дослідження охоплює широке коло користувачів, які щодня взаємодіють із різними онлайн сервісами. Цільовою групою дослідження є звичайні користувачі Інтернету, незалежно від віку, статі чи професії, які активно користуються онлайн процедурами для роботи, навчання чи дозвілля.

Для досягнення поставленої мети дослідження автор підготував інструмент у вигляді анкети. Анкета була розроблена для збору інформації про звички, ставлення та рівень обізнаності користувачів щодо питань кібербезпеки. Опитування проводилось у період з 1 по 31 жовтня 2024 року.

Анкета складалася з 15 відкритих питань, які охоплювали такі аспекти:

1. Частота використання онлайн процедур.
2. Категорії онлайн процедур, які використовуються найчастіше.
3. Ставлення до використання соціальних мереж.
4. Рівень довіри до онлайн сервісів.
5. Ставлення до подання особистих даних на веб-сайтах.
6. Загальна обізнаність про ризики в Інтернеті.

Питання були спрямовані на аналіз не лише обізнаності користувачів, але й їхніх відчуттів щодо безпеки під час використання Інтернету.

Опитування було організовано у два основні етапи:

1. Розповсюдження анкет серед знайомих: 25 анкет було передано друзям, знайомим і сусідам для заповнення. Кожному учаснику надавалася можливість відповісти на питання у комфортних умовах без тиску чи обмежень у часі.

2. Онлайн опитування через соціальні мережі: анкету було опубліковано у соціальних мережах, де вона була доступна для ширшої аудиторії. У результаті онлайн етапу зібрано 30 відповідей.

Усього було зібрано 55 заповнених анкет, що забезпечило достатню вибірку для аналізу. Усі відповіді були систематизовані та проаналізовані для подальшого узагальнення результатів.

Організація дослідження дозволила охопити різноманітну аудиторію користувачів, які мають різний рівень досвіду та ставлення до питань кібербезпеки. Поєднання офлайн та онлайн методів збору даних забезпечило більшу достовірність і репрезентативність отриманих результатів. Розроблена анкета дозволила зібрати якісні дані, які сприятимуть глибшому розумінню проблематики безпеки в Інтернеті та формуванню рекомендацій для підвищення її рівня.

2.5 Висновки до другого розділу

У другому розділі магістерської роботи було розглянуто методологічні аспекти дослідження убезпечення персональних даних користувачів Інтернету, включаючи формулювання робочих гіпотез, визначення змінних, а також вибір методів і засобів дослідження.

Основною проблемою визначено недостатній рівень захищеності персональних даних користувачів через низьку обізнаність та відсутність комплексних захисних механізмів. Це стало основою для формулювання робочих гіпотез, зокрема: успішність захисту персональних даних залежить від поєднання технічних засобів і поведінкових факторів; підвищення рівня обізнаності користувачів про кіберзагрози суттєво зменшує ризики витоків

даних; ефективні політики конфіденційності й управління доступом впливають на сприйняття безпеки користувачами.

Визначено основні змінні дослідження, які включають незалежні змінні, такі як демографічні показники (вік, стать, рівень освіти, професійна зайнятість), і залежні змінні, до яких відносяться рівень обізнаності користувачів про захисні технології, частота використання методів безпеки, довіра до онлайн-сервісів. Для оцінки параметрів убезпечення персональних даних було сформовано кількісні та якісні показники, такі як рівень задоволення користувачів системами захисту, частота випадків витоків даних, застосування двофакторної аутентифікації.

У роботі застосовано комбінований підхід, що включає діагностичні методи (опитування та анкетування) для збору первинних даних, аналітичні методи для оцінки результатів опитувань і виявлення закономірностей у поведінці користувачів, а також програмне забезпечення для обробки даних, що забезпечило точність і надійність результатів.

Дослідження проводилося в контексті онлайн-процедур, таких як оплата послуг, використання соціальних мереж, надання особистих даних у реєстраційних формах. Організація процесу включала комбіновані методи збору даних через офлайн- та онлайн-опитування, що забезпечило репрезентативність вибірки та можливість аналізу поведінки користувачів різних категорій.

Таким чином, другий розділ магістерської роботи закладає методологічну основу для подальшого дослідження убезпечення персональних даних. Сформульовані робочі гіпотези, визначені змінні та застосовані методи дослідження дозволяють структурувати аналіз і забезпечити достовірність отриманих результатів. Це створює передумови для формулювання практичних рекомендацій у наступних розділах роботи.

Організація дослідження, яке включало офлайн та онлайн опитування, дозволила охопити різноманітну аудиторію користувачів Інтернету. Успішна реалізація збору даних забезпечила репрезентативність вибірки та точність отриманих результатів. Питання анкети охоплювали широкий спектр аспектів,

пов’язаних із безпекою в Інтернеті, від використання онлайн процедур до подання особистих даних. Це забезпечило глибокий аналіз поведінки користувачів і дозволило сформувати рекомендації щодо покращення безпеки в мережі.

Дослідження продемонструвало, що питання безпеки в Інтернеті є актуальним і багатогранним. Використання чітко визначених змінних, показників і методів дозволило досягти поставлених цілей. Організація дослідження та зібрані дані формують основу для подальшого аналізу та розробки рекомендацій щодо підвищення рівня обізнаності та безпеки користувачів у цифровому середовищі.

3 АНАЛІЗ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ТА БЕЗПЕКА КОРИСТУВАЧІВ ІНТЕРНЕТУ НА ПРИКЛАДІ ОБРАНИХ ОНЛАЙН-ПРОЦЕДУР

3.1 Характеристики загроз безпеці користувачів мережі Інтернет

Загрози безпеці в Інтернеті охоплюють різноманітні дії, спрямовані на порушення конфіденційності, цілісності або доступності інформації, а також створення небезпеки для користувачів. Ці загрози можуть бути технічними, соціальними, інформаційними або економічними за характером.

Технічні загрози включають комп'ютерні віруси, трояни, програми-шпигуни, хакерські атаки, зокрема DDoS і SQL-ін'єкції, а також експлуатацію вразливостей у програмному забезпеченні. Соціальні загрози стосуються обману користувачів через фішингові сайти або маніпуляцій соціальної інженерії. Інформаційні загрози виникають через поширення недостовірної інформації чи дезінформації, а економічні загрози стосуються онлайн-шахрайства та крадіжки фінансових даних.

Конфіденційність порушується через викрадення персональних даних, паролів або фінансової інформації за допомогою фішингових атак, програм-шпигунів або соціальної інженерії. Загрози цілісності пов'язані зі змінами в даних або системах без дозволу, наприклад, під час атак на бази даних чи веб-сайти. Загрози доступності виникають через дії, що блокують або обмежують доступ до ресурсів, як-от DDoS-атаки чи шифрування даних із метою вимагання викупу.

Загрози в Інтернеті реалізуються через віруси та шкідливе програмне забезпечення, яке використовує вразливості у системах. Фішинг обманом змушує користувачів передавати конфіденційні дані, часто за допомогою підроблених веб-сайтів або електронних листів. Хакерські атаки спрямовані на отримання доступу до даних або порушення роботи систем. Соціальна інженерія використовує маніпулятивні методи, щоб змусити користувачів виконувати небезпечні дії.

Загрози можуть мати зовнішнє або внутрішнє походження. Зовнішні джерела включають хакерів, конкурентів або злочинні угруповання. Внутрішні джерела можуть бути пов'язані з недбалістю або навмисними діями працівників чи користувачів.

Серед найбільш поширених загроз можна виділити фішингові сайти, які імітують вигляд відомих організацій для викрадення даних користувачів. Зараження вірусами через вразливості програмного забезпечення є ще однією популярною тактикою. Кібербулінг і психологічний тиск в Інтернеті можуть створювати небезпеку для емоційного стану користувачів. Шкідливі програми, такі як ransomware, шифрують дані користувачів, вимагаючи викуп за їх відновлення. Несанкціоноване стеження, яке здійснюється через трекери або шпигунські програми, також є серйозною загрозою.

Загрози безпеці в Інтернеті можуть призвести до фінансових втрат через крадіжку грошей чи шахрайські операції. Розголошення приватної інформації ставить під загрозу конфіденційність користувачів. Репутаційні збитки можуть торкнутися як фізичних осіб, так і організацій, які постраждали від атак. Збої в роботі систем або сервісів можуть викликати значні проблеми, особливо для критично важливих структур.

Характеристики загроз безпеці в Інтернеті показують, що вони є багатогранними та постійно змінюються. Для зниження ризиків необхідно поєднувати технічні методи захисту, такі як шифрування та багатофакторна аутентифікація, із підвищенням рівня обізнаності користувачів про основи кібергігієни. Ефективний захист інформації є ключовою умовою безпечного використання цифрових технологій у сучасному світі.

3.1.1 Відчуття безпеки користувачів Інтернету

Відчуття безпеки в Інтернеті є важливим аспектом, який впливає на довіру користувачів до цифрових технологій та їх готовність використовувати онлайн-сервіси. У сучасному світі, де особисті дані, фінансова інформація і навіть

приватне життя значною мірою перебувають у цифровому просторі, питання безпеки стає ключовим для комфортного користування Інтернетом.

Користувачі часто оцінюють свою безпеку в Інтернеті, ґрунтуючись на кількох факторах. До них належать рівень обізнаності про кіберзагрози, використання захисних механізмів, попередній досвід інцидентів, прозорість онлайн-сервісів і соціальне оточення. Люди, які знають про фішинг, віруси та хакерські атаки, зазвичай більше переймаються безпекою, але одночасно вживають більше заходів захисту. Ті, хто використовує антивіруси, багатофакторну аутентифікацію та VPN, відчувають себе захищенішими. Однак навіть вони можуть зберігати певний рівень тривоги, якщо раніше стикалися з кіберзагрозами.

Досвід інцидентів, таких як шахрайство або крадіжка даних, негативно впливає на відчуття безпеки. Прозорість роботи сервісів також відіграє важливу роль: сайти, які чітко пояснюють, як обробляються дані, викликають більше довіри. Навпаки, недовіра зростає, якщо користувачам не зрозуміло, як їхні дані зберігаються та використовуються. Медіа та соціальне оточення теж формують відчуття безпеки. Негативні новини про зломи даних часто підсилюють тривожність, тоді як позитивний досвід знайомих може сприяти впевненості.

Згідно з опитуваннями, лише 10% користувачів вважають себе повністю захищеними в Інтернеті завдяки впровадженню сучасних технологій безпеки, таких як двофакторна аутентифікація. Близько 67% відчувають лише часткову захищеність, а 25% вважають Інтернет небезпечним середовищем.

Психологічно відчуття небезпеки може викликати тривогу та страх, які знижують довіру до онлайн-сервісів і цифрових технологій загалом. Люди можуть уникати використання певних платформ, таких як онлайн-банкінг або електронна комерція, через побоювання втратити гроші або дані. Це може впливати на якість їхнього життя, викликаючи емоційний стрес у разі виникнення проблем із безпекою.

Покращення відчуття безпеки в Інтернеті можливе через кілька шляхів. Перш за все, необхідно підвищувати обізнаність про базові правила кібергігієни. Розробка більш зручних і прозорих інструментів безпеки також сприятиме

цьому. Наприклад, компанії можуть інтегрувати двофакторну аутентифікацію в сервіси так, щоб це не створювало незручностей для користувачів. Важливо, щоб онлайн-платформи відкрито повідомляли про свої політики конфіденційності та надавали інструменти для контролю особистих даних.

Державна підтримка у вигляді законодавчих норм, таких як регламенти захисту даних (наприклад, GDPR), також є важливою. Механізми подання скарг і можливість отримати компенсацію в разі інцидентів підвищують довіру користувачів до цифрових сервісів.

Отже, відчуття безпеки в Інтернеті є важливим чинником для впевненого користування цифровими технологіями. Поєднання технічних рішень, освітніх заходів і прозорості платформ може значно знизити рівень тривожності та покращити досвід користувачів у цифровому середовищі.

На рисунку 3.1 відображено види пристроїв яким найчастіше користуються для входу в мережу Інтернет.

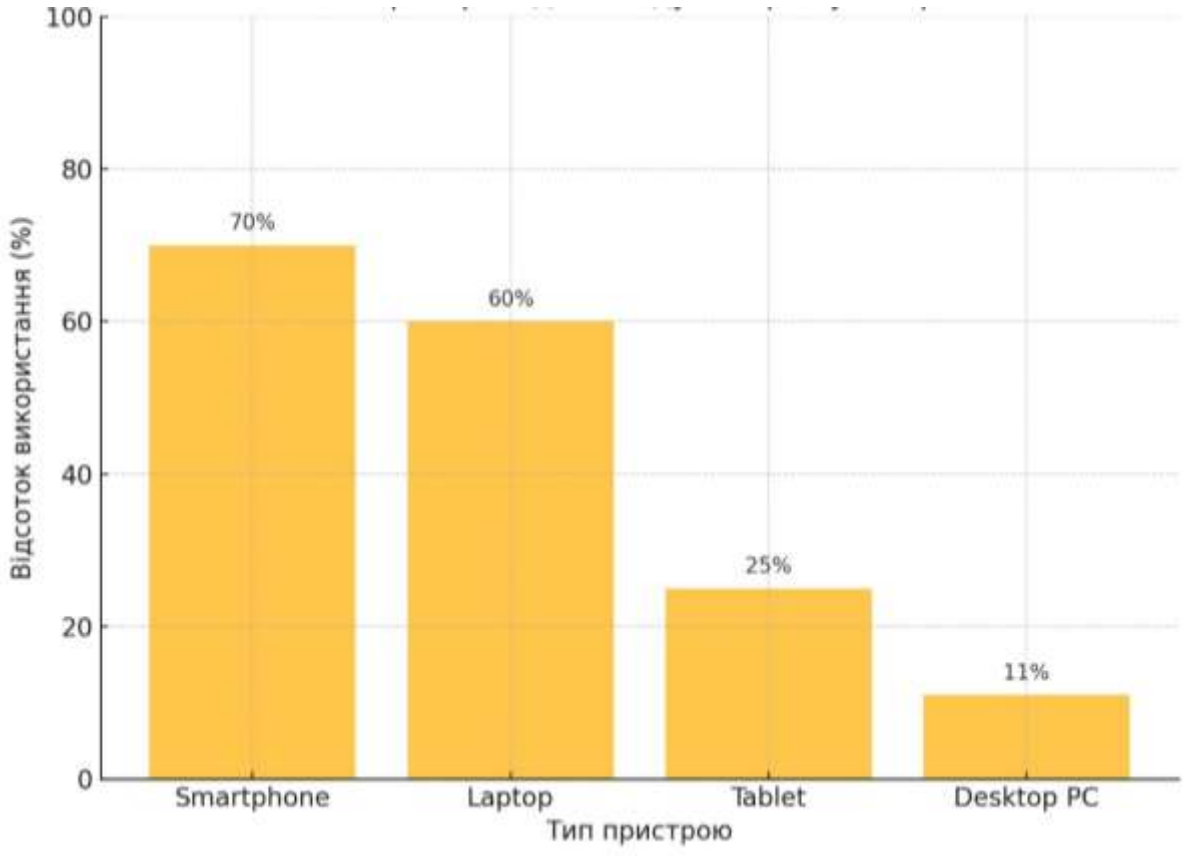

Рисунок 3.1 – Тип пристрою яким найчастіше користуються для входу в мережу

На основі представлених даних, найпоширенішим пристроєм для входу в Інтернет є смартфон (70%), за ним слідує ноутбук (60%). Значно менше користувачів використовують планшети (25%) та стаціонарні комп'ютери (11%). На діаграмі ці показники чітко відображаються, що дозволяє легко побачити переваги у використанні мобільних пристроїв.

Результати показують, що лише 25% опитаних надають перевагу покупкам в Інтернеті, причому більшість із них (85%) – молодь до 35 років. Натомість 75% користувачів все ще обирають традиційні магазини та торгові центри, що свідчить про переважання звичної форми шопінгу серед населення. Діаграма, яка зображена на рисунку 3.2 чітко ілюструє цей розподіл переваг.

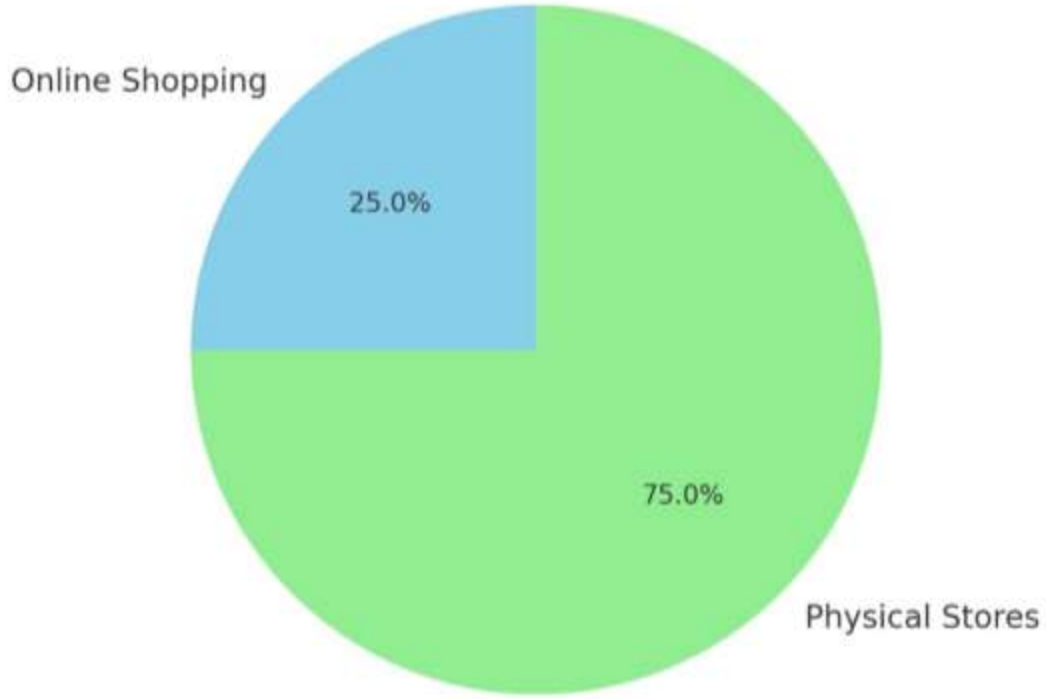

Рисунок 3.2 – Метод здійснення покупок

За результатами опитування, рисунок 3.3, 90% користувачів вважають використання онлайн процедур зручним, тоді як 10% вказали на труднощі або незручності. Діаграма наочно ілюструє цей розподіл, підкреслюючи високий рівень прийнятності цифрових сервісів.

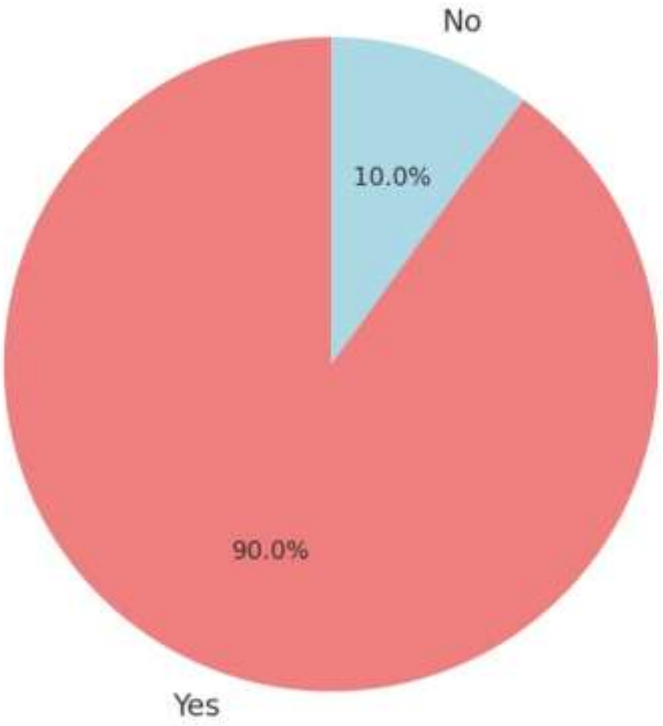

Рисунок 3.3 – Зручність використання процедур онлайн

На рисунку 3.4 зображено порівняння відсотка респондентів які віддають перевагу тій чи іншій онлайн процедурі

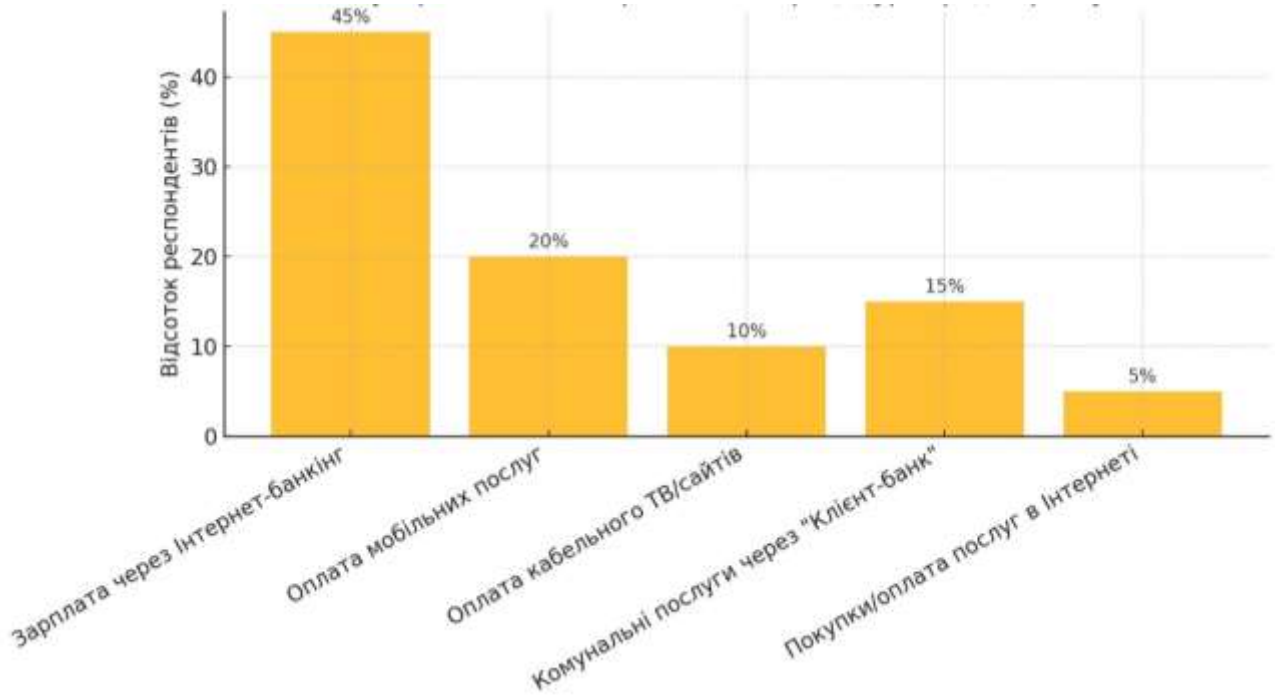

Рисунок 3.4 – Приклади онлайн процедур

На основі представлених даних рисунок 3.4, більшість користувачів (45%) отримують заробітну плату через інтернет-банкінг. Оплата мобільних послуг становить 20%, а оплата кабельного телебачення, послуг сайтів та поповнення карткових рахунків – 10%. Комунальні платежі через систему «Клієнт-банк» здійснюють 15% опитаних. Лише 5% користувачів здійснюють покупки в Інтернеті або отримують оплату за послуги через мережу. Діаграма наочно відображає ці тенденції, підкреслюючи популярність онлайн-банкінгу серед інших фінансових процедур.

На рисунку 3.5 діаграма відображає розподіл видів діяльності, якими молодь займається у вільний час, перебуваючи в Інтернеті. На основі результатів опитування, можна побачити, що найбільш популярними є розважальні та соціальні активності. Розглянемо кожну категорію детальніше:

1. Соціальні мережі та месенджери (94%).

Соціальні мережі та платформи для обміну повідомленнями є абсолютними лідерами серед активностей. Майже кожен респондент вказав, що використовує ці сервіси для спілкування з друзями, перегляду контенту, коментування чи обміну новинами. Такий високий показник пояснюється доступністю платформ, їх багатофункціональністю, а також звичкою молоді підтримувати зв’язок у цифровому форматі. Це також підкреслює тенденцію до заміщення живого спілкування віртуальним.

2. Слухання музики (80%).

На другому місці за популярністю знаходиться слухання музики. Молодь активно використовує онлайн-платформи для створення власних плейлистів і прослуховування треків «у фоновому режимі». Це пов’язано з тим, що сучасні сервіси, як-от Spotify або YouTube Music, забезпечують легкий доступ до улюбленої музики без перерв на рекламу чи обмеження радіостанцій. Музика часто супроводжує молодь під час інших занять, таких як навчання, спорт чи робота.

3. Пошук пропозицій і здійснення покупок онлайн (73%).

Значна частина молоді віддає перевагу покупкам в Інтернеті, шукаючи вигідні пропозиції на різних платформах. Це може включати одяг, техніку,

гаджети чи інші товари, які часто дешевші в онлайн-магазинах. Популярність цієї діяльності також зумовлена можливістю знайти унікальні товари, недоступні в місцевих магазинах, і зручністю доставки додому.

4. Перегляд фільмів і серіалів (67%).

Інтернет став основною альтернативою традиційному телебаченню, оскільки дозволяє молоді обирати контент відповідно до своїх уподобань і переглядати його у зручний час. Сервіси, такі як Netflix або YouTube, пропонують великий вибір фільмів, серіалів і відео, що робить цю активність однією з найулюбленіших серед молоді.

5. Читання новин і цікавих статей (53%).

Більше половини опитаних віддають перевагу отриманню інформації через Інтернет. Це може бути пов'язано з доступністю контенту різноманітних форматів, включно з новинами, науковими статтями, блогами чи інтерв'ю. Молодь шукає в Інтернеті як актуальні події, так і інформацію на теми, що її цікавлять.

6. Онлайн-ігри (27%).

Попри популярність ігрової індустрії, лише чверть опитаних відзначили ігри як основну діяльність в Інтернеті. Це може бути пов'язано з тим, що молодь більше часу приділяє соціальним мережам і мультимедійному контенту. Однак, для частини аудиторії онлайн-ігри залишаються способом відпочинку та соціалізації.

7. Пошук інформації для навчання (13%).

Ця активність виявилася найменш популярною серед опитаних. Хоча Інтернет пропонує безліч ресурсів для навчання, молодь використовує його переважно для розваг. Це свідчить про те, що освітні інструменти онлайн не є пріоритетом для більшості молодих людей.

Діаграма чітко ілюструє, що основна частина активностей молоді в Інтернеті пов'язана із соціалізацією та розвагами. Соціальні мережі, месенджери, музика, фільми й онлайн-шопінг займають провідні позиції. Водночас, активності, які спрямовані на розвиток чи навчання, такі як пошук інформації для освіти, мають значно меншу популярність.

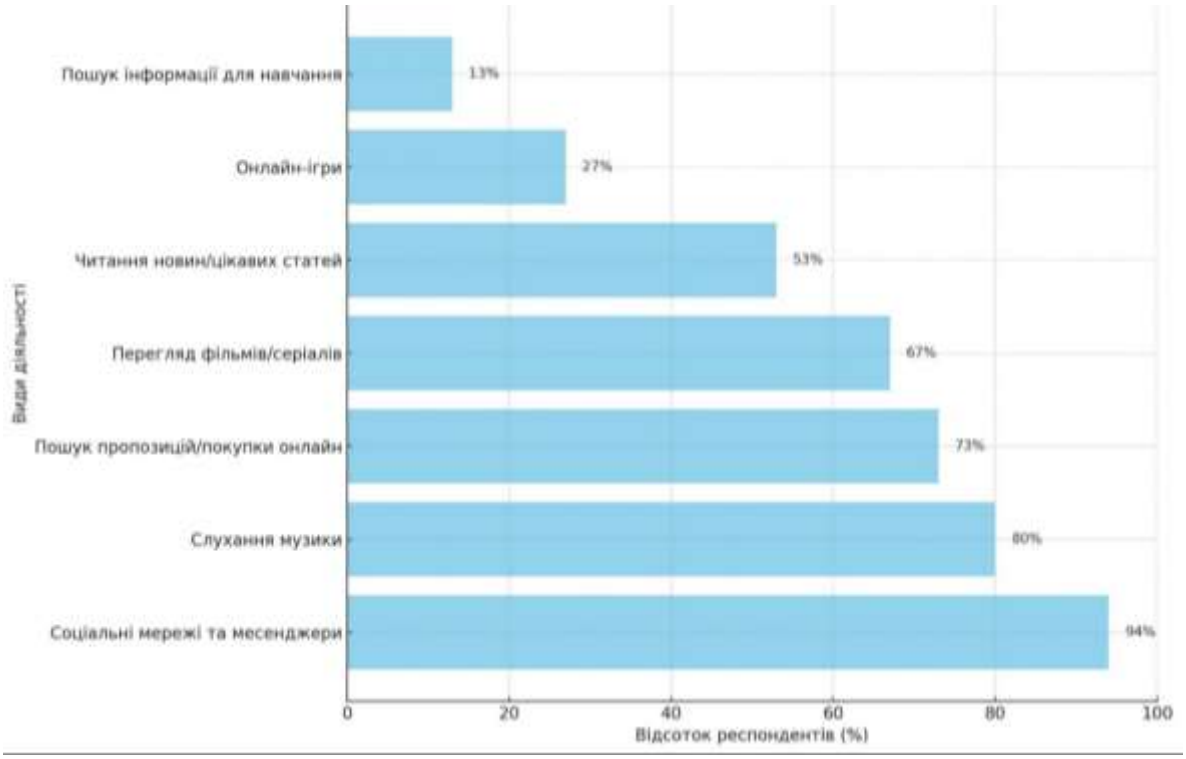

Рисунок 3.5 – На що тратять свій вільний час користувачі Інтернету?

На діаграмі (рисунок 3.6) відображені основні способи, за допомогою яких респонденти здобували знання про користування Інтернетом. Аналіз даних вказує на те, що значна частина опитаних навчалася самостійно, використовуючи метод спроб і помилок, а інші категорії підтримки були менш поширені.

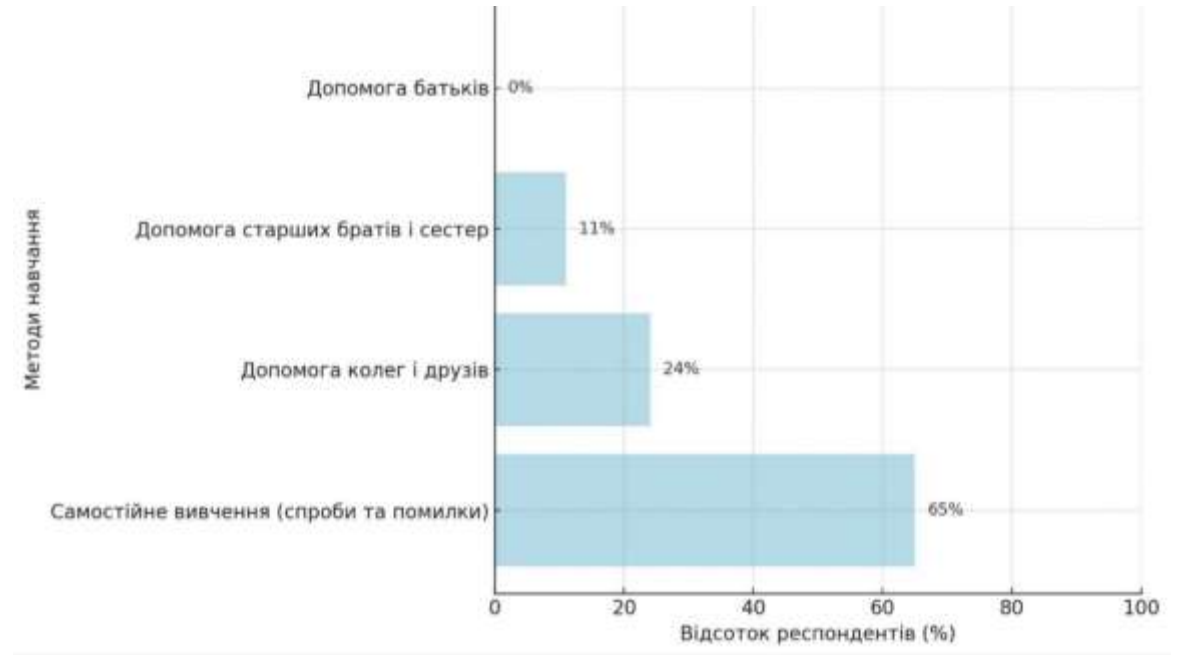

Рисунок 3.6 – Хто допоміг зробити перші кроки в мережі Інтернет?

Основні висновки:

1. Самостійне вивчення (65%) Найбільший відсоток респондентів вказав, що навчалися користуванню Інтернетом самостійно, експериментуючи та набуваючи досвіду через помилки. Це свідчить про відсутність організованої підтримки або навчання з цього питання в сім'ї чи соціумі. Самостійне освоєння може бути ефективним, але водночас може призводити до поганого розуміння питань безпеки в мережі.

2. Допомога колег і друзів (24%) Друге місце займають колеги та друзі, які допомагали освоювати Інтернет. Такий спосіб навчання відображає значення соціального оточення для здобуття нових навичок. Однак залежність від інших може обмежувати глибину знань.

3. Допомога старших братів і сестер (11%) Допомога від старших братів і сестер є менш поширеним методом. Це може бути пов'язано з тим, що не всі респонденти мають таких родичів або вони недостатньо компетентні в цьому питанні.

4. Допомога батьків (0%) Жоден із респондентів не вказав на допомогу батьків. Це підкреслює значний розрив між поколіннями у знаннях і навичках роботи в Інтернеті. Батьки не завжди володіють необхідними знаннями або вважають, що підростаюче покоління може самостійно опанувати ці навички.

Діаграма демонструє печальну тенденцію: більшість людей здобувають знання про Інтернет самостійно, часто без будь-якої підтримки. Це може впливати на якість знань, особливо в питаннях безпеки. Враховуючи стрімке зростання цифрових технологій і складність сучасного Інтернет-середовища, важливо забезпечити підростаюче покоління організованим навчанням і підтримкою для ефективного та безпечного використання мережі.

На рисунку 3.7 діаграма демонструє, де найчастіше респонденти використовують Інтернет.

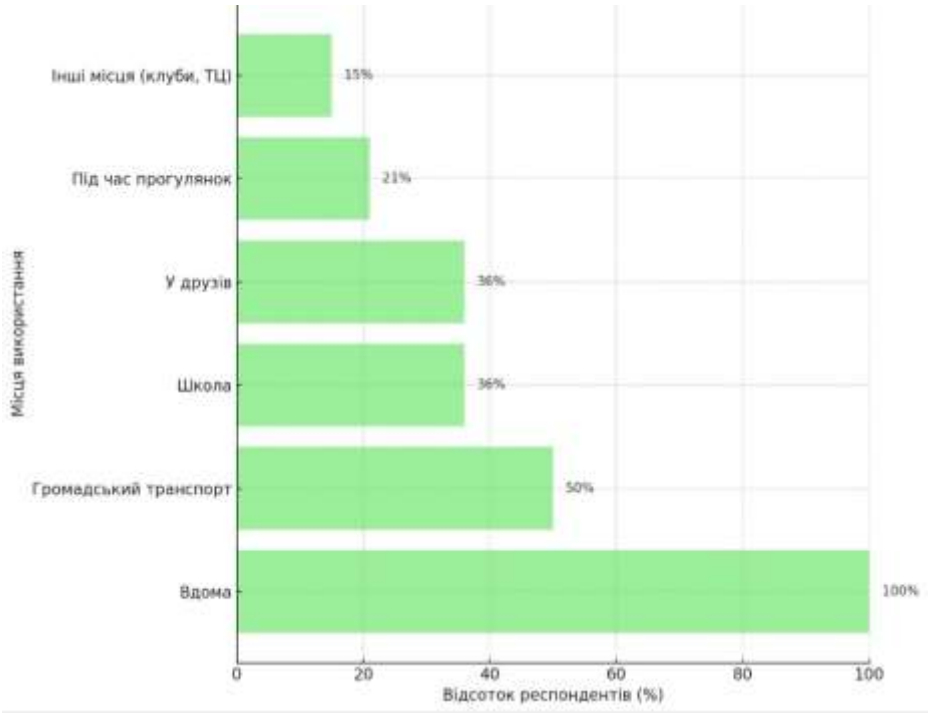

Рисунок 3.7 – Місце де користуєтесь Інтернетом?

Місця використання розподілилися наступним чином:

1. Вдома (100%) Абсолютна більшість респондентів зазначили, що користуються Інтернетом вдома. Це свідчить про комфортність домашніх умов для використання цифрових технологій. Удома люди мають доступ до стабільного підключення та можуть спокійно переглядати контент або виконувати онлайн-завдання.

2. Громадський транспорт (50%) Половина опитаних використовують Інтернет у громадському транспорті. Це може свідчити про те, що під час поїздок вони обирають віртуальний світ замість взаємодії з оточенням або спостереження за навколишнім середовищем. Ймовірно, користувачі витрачають цей час на соціальні мережі, перегляд відео або прослуховування музики.

3. Школа (36%) Рівно 36% респондентів користуються Інтернетом у школі. Це може бути пов’язано як з навчальними цілями, так і з відволіканням на соціальні мережі або розваги під час перерв.

4. У друзів (36%) Той самий відсоток респондентів (36%) використовує Інтернет під час перебування в гостях у друзів. Це демонструє тенденцію до заміщення живого спілкування віртуальним, навіть у соціальних обставинах.

5. Під час прогулянок (21%) Використання Інтернету під час прогулянок вказує на звичку залишатися підключеними до мережі навіть на свіжому повітрі. Це може включати активність у соціальних мережах, фотографування або пошук інформації.

6. Інші місця (15%) Серед інших місць, зазначених респондентами, були клуби та торгові центри. Використання Інтернету в таких місцях, ймовірно, пов’язане з пошуком інформації про покупки, соціалізацією або розвагами.

Дані показують, що Інтернет став невід’ємною частиною повсякденного життя користувачів. Навіть у місцях, де традиційно очікується взаємодія з реальним світом або людьми (громадський транспорт, друзі, прогулянки), значна частина респондентів віддає перевагу онлайн-активностям. Це підкреслює потребу у підвищенні культури використання Інтернету, включаючи баланс між віртуальним і реальним світом.

Одним із важливих і цікавих аспектів опитування стало питання про перспективи онлайн-процедур у майбутньому. Респонденти висловили свої думки щодо розвитку різних напрямків онлайн-активностей та їх значення для суспільства (рисунок 3.8).

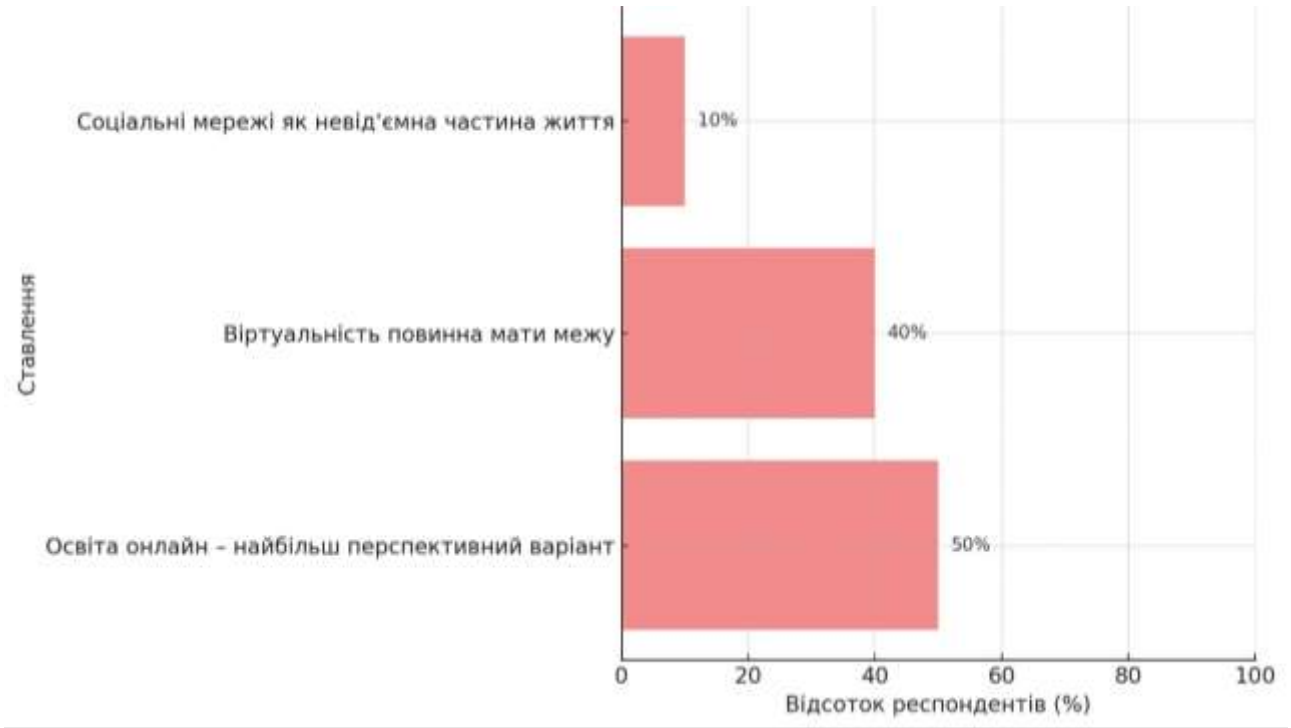

Рисунок 3.8 – Онлайн процедури майбутнього

На рисунку 3.8 діаграма ілюструє думки респондентів щодо впливу онлайн-технологій на їхнє життя та перспективи розвитку віртуального світу. Розподіл відповідей демонструє три основні погляди:

1. Освіта онлайн як найбільш перспективний варіант (50%) Половина опитаних вважає, що отримання освіти онлайн має найбільший потенціал у майбутньому. Ця відповідь підкреслює прагматичний підхід, враховуючи сучасні тенденції цифровізації та досвід дистанційного навчання під час пандемії COVID-19 [8] Технології, що стрімко розвиваються, сприяють популяризації онлайн-освіти, яка вже почала демонструвати свою ефективність.

2. Віртуальність повинна мати межу (40%) Близько 40% респондентів висловили думку, що надмірне занурення у віртуальність є небажаним. Ці люди вважають, що необхідно зберігати баланс між реальним і віртуальним світом, щоб уникнути залежності від ігор та інших цифрових розваг, які можуть відволікати від реальних проблем і соціальних взаємодій.

3. Соціальні мережі як невід'ємна частина життя (10%) Невелика частка респондентів (10%) не уявляє свого життя без соціальних мереж. Деякі з них використовують ці платформи для роботи або самореалізації, а інші – через залежність або звичку. Цей результат свідчить про значний вплив соціальних мереж на сучасний стиль життя.

Дані свідчать про те, що онлайн-технології мають значний вплив на сучасне суспільство, особливо в галузі освіти. Водночас, занепокоєння щодо надмірної віртуалізації життя підкреслює потребу у підтриманні здорового балансу. Соціальні мережі залишаються важливою частиною життя, але їхній вплив значно менший у порівнянні з іншими аспектами онлайн-реальності. Ці результати демонструють, як технології впливають на різні аспекти людського життя та які перспективи вони відкривають.

На рисунку 3.9 діаграма відображає заходи, яких дотримуються респонденти для забезпечення своєї безпеки під час користування Інтернетом. Розглянемо основні результати:

1. Звертаю увагу, де даю свої дані (67%) Найпоширеніший спосіб захисту – уважний підхід до передачі своїх даних. Респонденти зазначили, що

діляться особистою інформацією лише в разі крайньої необхідності, що свідчить про обізнаність щодо ризиків витоку персональних даних.

2. Використовую антивірусні програми (60%) Антивірусні програми є другим найпопулярнішим засобом захисту. Це вказує на те, що більшість користувачів усвідомлюють небезпеку вірусів і шкідливого програмного забезпечення.

3. Використовую безпечні WiFi-з'єднання (48%) Майже половина опитаних звертає увагу на безпеку з'єднань, що вказує на розуміння загроз, які можуть виникнути через використання незахищених мереж.

4. Регулярно змінюю паролі (27%) Регулярна зміна паролів є менш популярним, але важливим заходом безпеки. Невеликий відсоток користувачів, які це практикують, може свідчити про недооцінку ризиків, пов'язаних із доступом до облікових записів.

5. Не зв'язуюсь з незнайомцями (24%) Одна чверть респондентів уникає спілкування з незнайомими людьми, що знижує ризик потрапити в пастки шахраїв чи кіберзловмисників.

6. Уважно вивчаю, кого додаю до друзів (24%) Такий самий відсоток респондентів приділяє увагу формуванню свого списку друзів у соціальних мережах, щоб уникнути небажаних контактів.

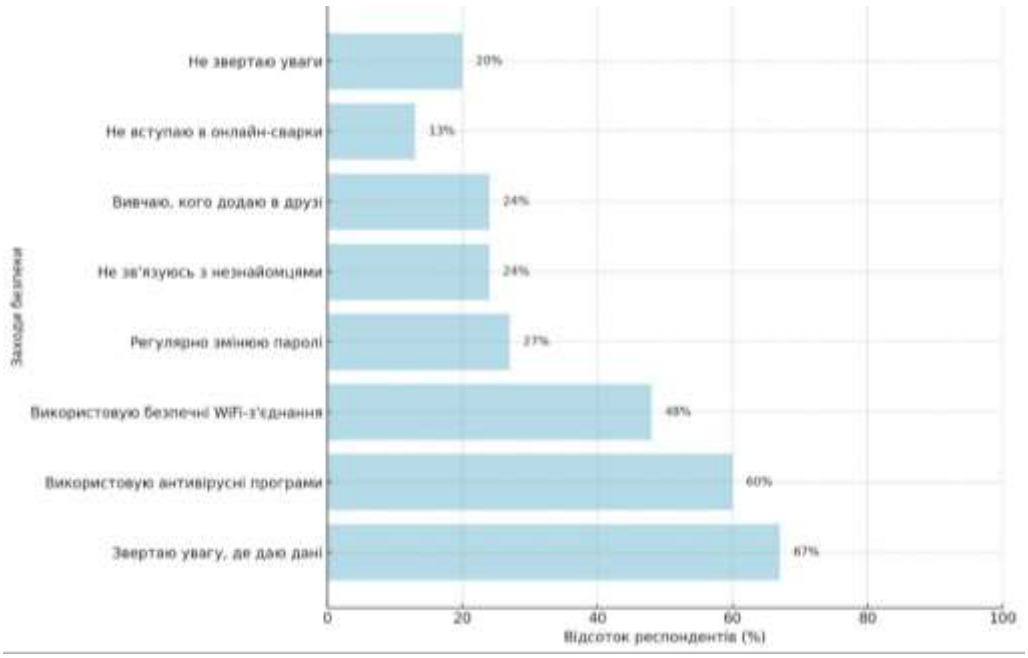

Рисунок 3.9 – Дії для забезпечення власної безпеки в онлайн просторі

7. Не вступаю в онлайн-сварки (13%) Лише невелика частина респондентів уникає конфліктів в Інтернеті, хоча це може бути важливим заходом для збереження приватності та безпеки.

8. Не звертаю уваги (20%) Кожен п’ятий респондент визнає, що не приділяє уваги питанням безпеки в Інтернеті, що є тривожним показником і свідчить про низький рівень кібергігієни у цієї групи.

Результати діаграми показують, що основна частина респондентів використовує базові заходи для забезпечення безпеки, такі як увага до надання даних і використання антивірусів. Водночас є значна кількість людей, які не змінюють паролі чи не звертають уваги на безпеку. Це свідчить про необхідність проведення освітніх кампаній із підвищення рівня кібергігієни. Важливими аспектами залишаються інформування про ризики в Інтернеті та популяризація більш ефективних методів захисту.

3.1.2 Відгуки про безпеку персональних даних та іншої приватної інформації користувачів Інтернет

Захист персональних даних і приватної інформації в Інтернеті є важливою темою, яка викликає занепокоєння у багатьох користувачів. Значна частина респондентів висловила побоювання щодо можливого використання їхніх особистих даних без дозволу для комерційних чи інших цілей. Також вони зазначили, що існує високий ризик витоку інформації через хакерські атаки або слабкий захист онлайн-сервісів.

Рівень довіри до платформ розподіляється нерівномірно. Великі міжнародні компанії, такі як Google чи Facebook, викликають більше довіри завдяки прозорим політикам конфіденційності, хоча й вони не завжди гарантують абсолютну безпеку. Натомість менші сервіси чи локальні платформи частіше викликають підозри, особливо якщо їхні політики обробки даних є незрозумілими.

Багато респондентів усвідомлюють важливість кібергігієни та активно застосовують заходи захисту, як-от створення складних паролів, використання

двофакторної аутентифікації та перевірка безпеки з’єднань. Водночас частина користувачів визнає, що не завжди має достатні знання для ефективного захисту своїх даних.

Деякі респонденти вказали на відсутність прозорості в обробці персональних даних. Сайти не завжди попереджають про використання cookies або збір даних, а політики конфіденційності часто складні для розуміння. Користувачі, обізнані про регуляції, такі як GDPR, зазначають, що ці ініціативи підвищують рівень довіри до сервісів. Проте вони наголошують на необхідності впровадження подібних заходів і в інших регіонах.

Ще одним питанням є використання персональних даних компаніями для персоналізації реклами чи передачі інформації третім сторонам. Це знижує довіру до платформ і змушує користувачів обмежувати обсяг наданої інформації. Водночас деякі респонденти зізналися, що не приділяють належної уваги безпеці своїх даних через брак обізнаності або відчуття, що вони не можуть вплинути на ситуацію.

Загалом, відгуки респондентів підтверджують важливість теми захисту персональних даних. Хоча багато користувачів дотримуються базових заходів безпеки, існує потреба у підвищенні цифрової грамотності, розширенні регуляцій і забезпеченні більш прозорих політик конфіденційності.

На рисунку 3.10 діаграма ілюструє, як користувачі ставляться до необхідності подання персональних даних для доступу до онлайн-послуг чи проходження реєстрацій. Розподіл відповідей показує, що більшість респондентів (67%) не погоджуються з необхідністю надавати особисту інформацію, тоді як лише 33% користувачів не мають заперечень щодо цього.

Основні висновки:

1. Негативне ставлення (67%) Значна частина респондентів висловлює незадоволення вимогою надати персональні дані. Це може свідчити про їхню стурбованість конфіденційністю, страх перед можливим витоком даних чи зловживанням ними з боку сервісів. Користувачі також можуть вважати, що деякі послуги вимагають більше інформації, ніж це насправді потрібно.

2. Позитивне ставлення (33%) Менша частка респондентів ставиться до надання особистих даних нейтрально або позитивно, вважаючи це необхідним кроком для отримання доступу до сучасних Інтернет-послуг. Вони можуть мати більше довіри до сервісів або не відчувати особливого ризику через обмеженість своїх даних.

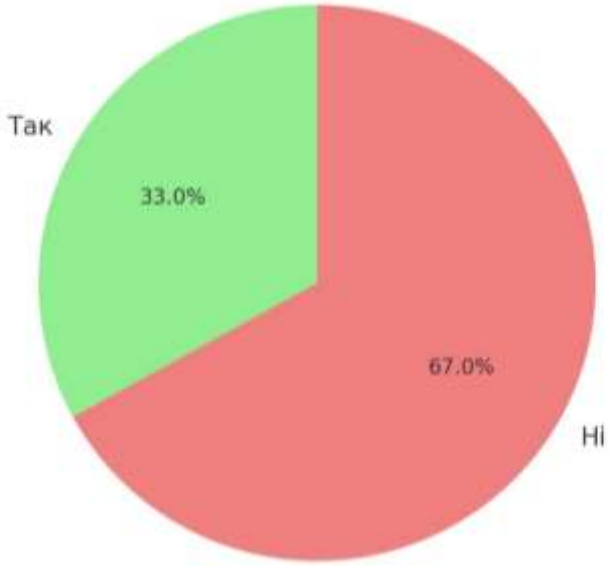

Рисунок 3.10 – Відношення до надання особистих даних

Результати діаграми показують, що користувачі здебільшого насторожено ставляться до подання персональних даних. Це підкреслює необхідність підвищення прозорості в обробці даних з боку сервісів, а також впровадження механізмів, які забезпечують безпеку й мінімізацію ризиків для користувачів. У свою чергу, користувачам потрібна більша поінформованість щодо того, як захистити свої дані та уникати потенційних загроз.

На рисунку 3.11 діаграма демонструє ставлення користувачів до читання правил та інструкцій перед реєстрацією або здійсненням покупок онлайн. Розподіл відповідей показує наступне:

1. Читають уважно правила (0%) Жоден із респондентів не зазначив, що завжди уважно читає правила та інструкції перед реєстрацією або покупками. Це свідчить про загальне нехтування деталями таких документів, які зазвичай містять важливу інформацію щодо умов використання послуг чи обробки персональних даних.

2. Читають часом (63%) Більшість користувачів зазначили, що читають правила лише час від часу. Це може свідчити про те, що увага до правил залежить від обставин або важливості послуги, якою вони збираються скористатися. Наприклад, у разі здійснення значних фінансових операцій вони можуть бути більш уважними, ніж при реєстрації на звичайному сайті.

3. Не читають зовсім (37%) Близько третини респондентів зізналися, що зовсім не читають правила та інструкції перед реєстрацією або покупками. Це вказує на ризиковану поведінку, адже такі користувачі можуть не знати про свої права та обов'язки або умови використання сервісу, що може призвести до неприємних наслідків.

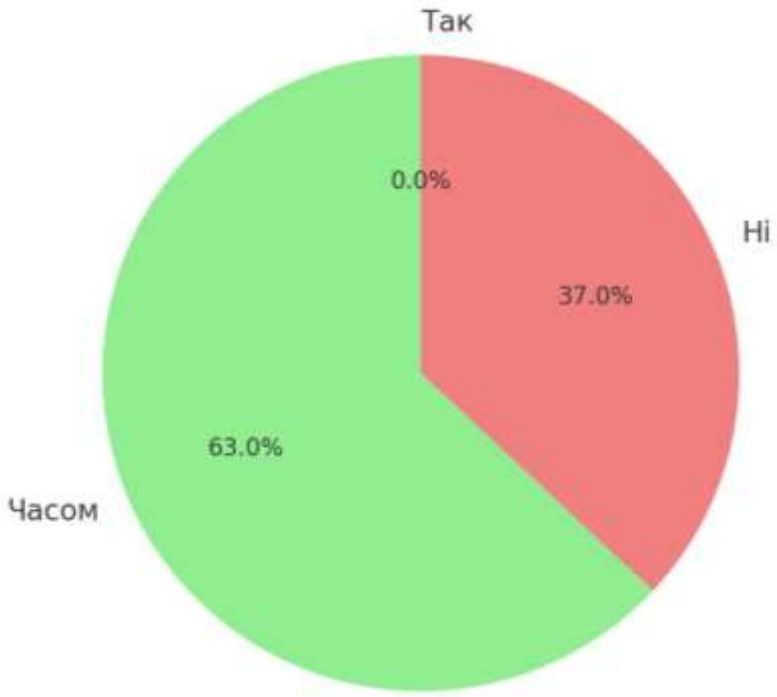

Рисунок 3.11 – Чи знайомитеся з інформацією перед початком проведення онлайн процедур?

Дані свідчать про загальну тенденцію ігнорування правил та інструкцій, які часто є важливими для захисту користувачів. Лише частина людей часом звертає увагу на ці документи, тоді як третина взагалі їх ігнорує. Це підкреслює необхідність створення коротших і зрозуміліших умов користування сервісами, а також проведення освітніх кампаній, спрямованих на підвищення обізнаності користувачів щодо важливості таких документів.

При дослідження було зроблено аналіз про вибір налаштувань для захисту персональних даних (рисунок 3.12).

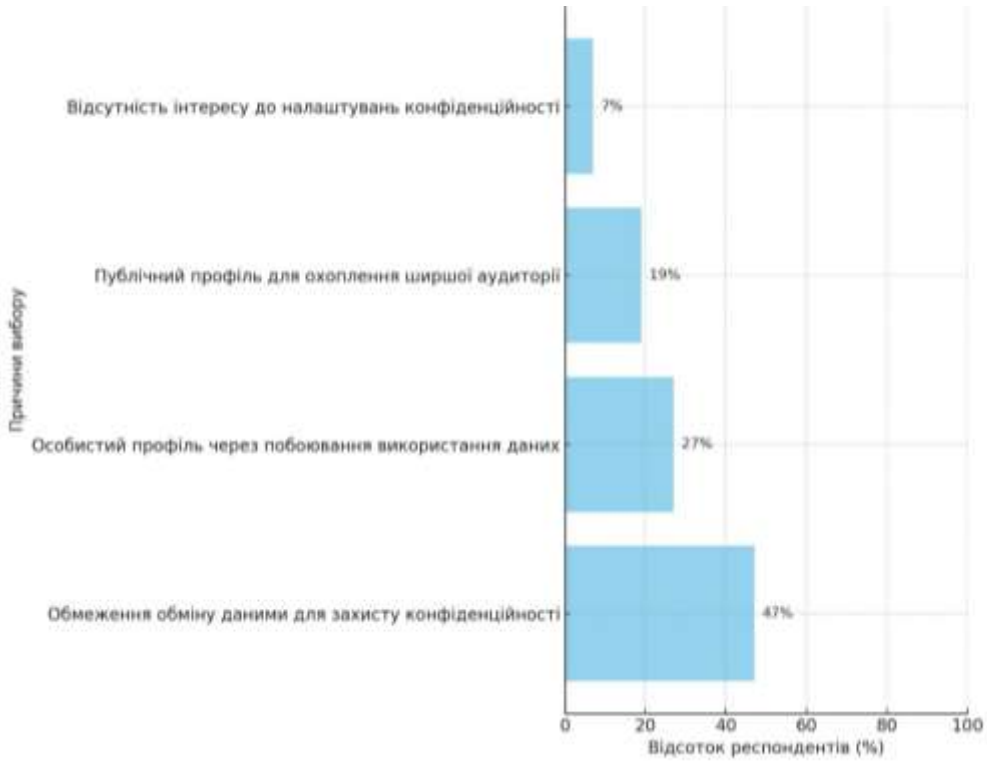

Рисунок 3.12 – Налаштування особистого профілю

На рисунку 3.12 діаграма демонструє розподіл відповідей респондентів щодо їхніх мотивів вибору налаштувань конфіденційності в соціальних мережах. Кожна відповідь відображає різний рівень обізнаності та пріоритетів у питаннях приватності.

Основні результати:

1. Обмеження обміну даними для захисту конфіденційності (47%) Майже половина респондентів обирають налаштування, які дозволяють контролювати доступ до їхньої інформації та профілю. Це свідчить про високий рівень усвідомлення важливості конфіденційності та прагнення захистити особисті дані від сторонніх осіб.

2. Особистий профіль через побоювання використання даних (27%) Близько чверті опитаних надають перевагу особистим профілям через страх використання їхніх персональних даних або фотографій іншими людьми. Ця

відповідь підкреслює зростання побоювань щодо можливих зловживань у цифровому середовищі.

3. Публічний профіль для охоплення ширшої аудиторії (19%) Менше п'ятої частини респондентів обирають публічний профіль, вважаючи, що доступність їхніх даних сприяє ширшій соціалізації або професійним можливостям. Це рішення характерне для тих, хто прагне бути відкритішим і готовий ризикувати конфіденційністю заради популярності чи контактів.

4. Відсутність інтересу до налаштувань конфіденційності (7%) Найменша частка опитаних (7%) визнає, що не приділяє уваги налаштуванням конфіденційності, залишаючи все за замовчуванням. Ця група користувачів або не усвідомлює важливості захисту даних, або не вважає це пріоритетом.

Результати діаграми підтверджують різноманітність підходів користувачів до налаштувань конфіденційності:

1. Більшість користувачів орієнтована на захист своїх даних, обираючи обмеження доступу до інформації.

2. Частина респондентів обирає відкритість, балансуючи між ризиками і перевагами публічного профілю.

3. Невелика група зовсім не приділяє уваги конфіденційності, що свідчить про потребу в освітніх кампаніях щодо цифрової грамотності.

4. Ці результати вказують на необхідність підтримки користувачів у розумінні ризиків та переваг, пов'язаних із налаштуванням приватності.

На рисунку 3.13 діаграма демонструє розподіл відповідей респондентів щодо того, яку персональну інформацію вони вважають доречною для ідентифікації в онлайн-просторі.

Основні результати:

1. Логін та пароль, абсолютна більшість респондентів (80%) вважає, що логін і пароль є достатніми для ідентифікації в Інтернеті. Це свідчить про популярність цього базового, але ефективного методу захисту даних. Такий вибір підкреслює орієнтацію користувачів на простоту та функціональність при забезпеченні конфіденційності.

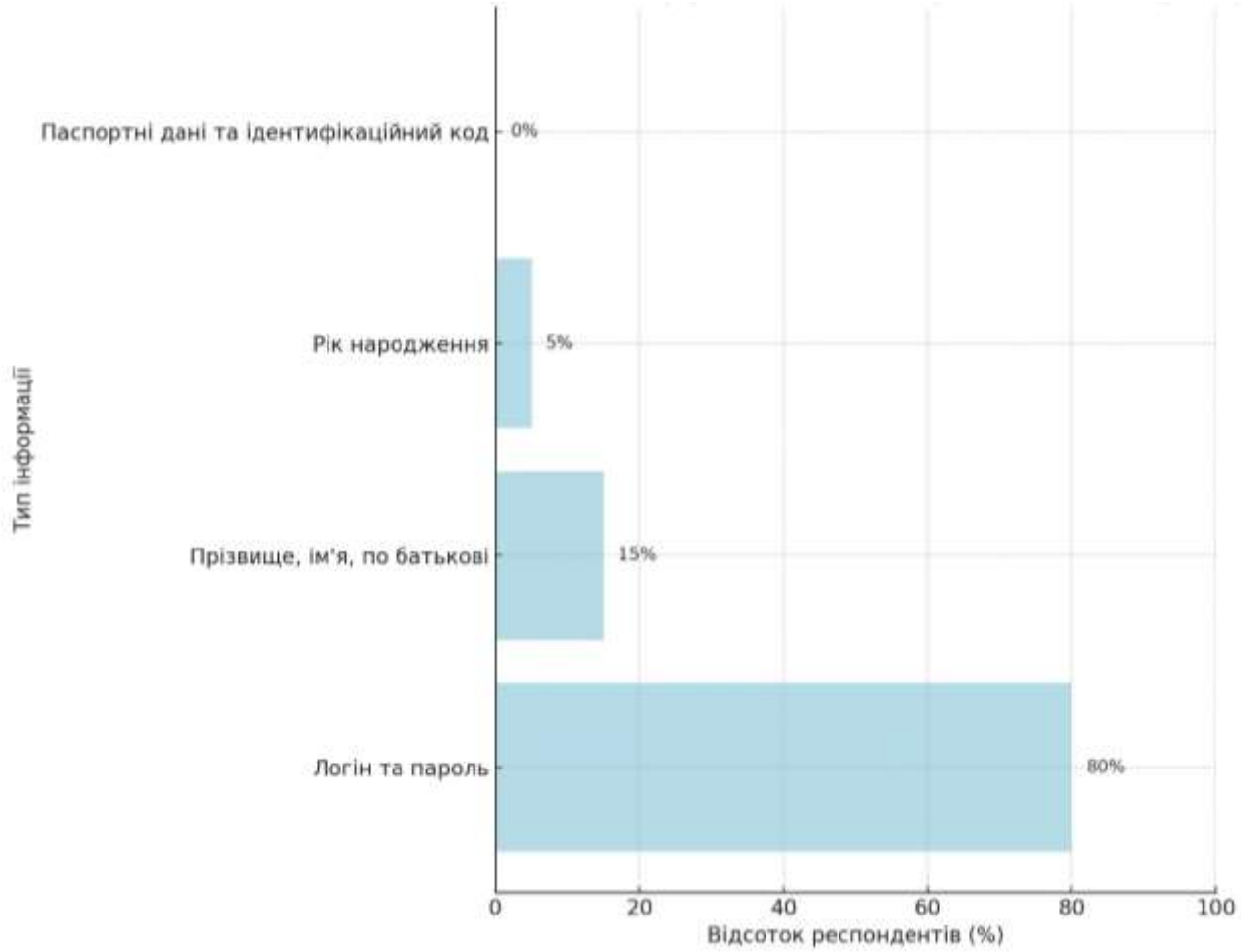

Рисунок 3.13 – Які дані на Ваш розсуд повинні бути ключовими для ідентифікації особистості в онлайн просторі?

2. Прізвище, ім’я, по батькові, невелика частина респондентів (15%) вважає, що для ідентифікації можуть використовуватися персональні дані, такі як ім’я та прізвище. Цей вибір може бути пов’язаний із традиційним підходом до особистої ідентифікації або відсутністю побоювань щодо використання цих даних.

3. Рік народження, лише 5% опитаних вказали рік народження як основний ідентифікатор. Ця відповідь, ймовірно, свідчить про бажання мінімізувати обсяг інформації, яка надається в Інтернеті, навіть якщо це не є надійним способом ідентифікації.

4. Паспортні дані та ідентифікаційний код (0%). Жоден респондент не вибрав паспортні дані чи ідентифікаційний код для ідентифікації. Це демонструє сильну недовіру до надання таких важливих даних під час використання онлайн-

процедур. Користувачі вважають ці дані занадто конфіденційними для подібних цілей.

Дані діаграми підкреслюють, що більшість користувачів прагнуть зберегти свою конфіденційність, обираючи прості та безпечні способи ідентифікації, такі як логін і пароль. Меншість респондентів готові використовувати персональні дані, як-от ім'я чи рік народження, але категорично проти надання паспортних даних або ідентифікаційного коду. Ці результати свідчать про обізнаність користувачів щодо ризиків, пов'язаних із наданням занадто особистої інформації.

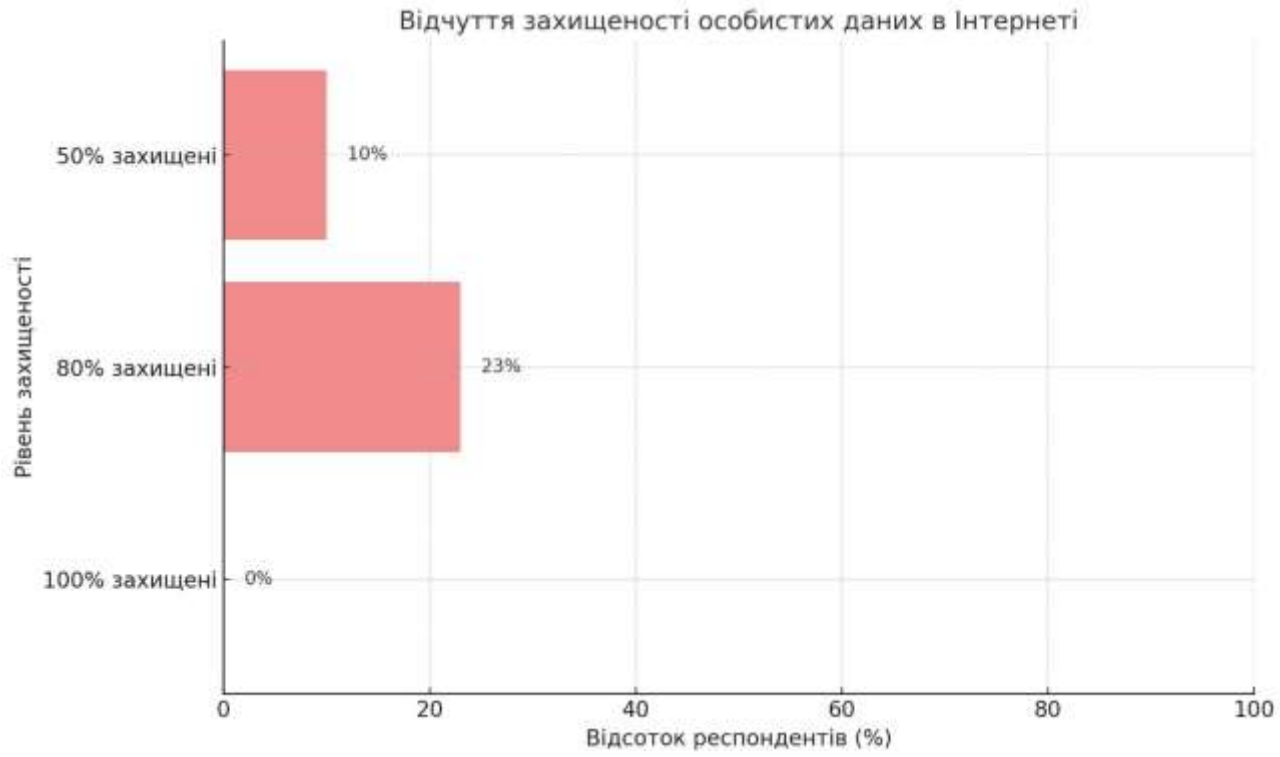

Рисунок 3.14 – На скільки вважаєте безпеку на захист особистих даних в Інтернеті?

На рисунку 3.14 діаграма ілюструє, як користувачі оцінюють рівень захисту своїх особистих даних під час онлайн-процедур. Результати показують, що більшість респондентів не вважають свої дані повністю захищеними в Інтернеті.

Основні результати:

1. 100% захищені (0%) жоден респондент не відчуває, що їхні дані в Інтернеті повністю захищені. Це свідчить про низький рівень довіри до онлайн-сервісів та систем безпеки, навіть у сучасних умовах, коли багато платформ активно впроваджують інновації для підвищення захищеності.

2. 80% захищені лише 23% опитаних відчувають себе значно захищеними, оцінюючи рівень безпеки своїх даних на 80%. Ця група респондентів, ймовірно, користується сучасними методами захисту, як-от двофакторна аутентифікація, шифрування даних або VPN.

3. 50% захищені невелика частка опитаних (10%) оцінює захист своїх даних на 50%. Це вказує на те, що ці користувачі усвідомлюють існування певного ризику при використанні Інтернету, але не мають достатньої впевненості в існуючих заходах безпеки.

Результати діаграми свідчать про недостатній рівень довіри користувачів до безпеки своїх даних в Інтернеті. Жоден із респондентів не вважає свої дані повністю захищеними, і лише меншість оцінює захист на високому рівні (80%). Ці результати підкреслюють важливість покращення систем безпеки на онлайн-платформах, а також необхідність підвищення обізнаності користувачів щодо сучасних методів захисту особистих даних.

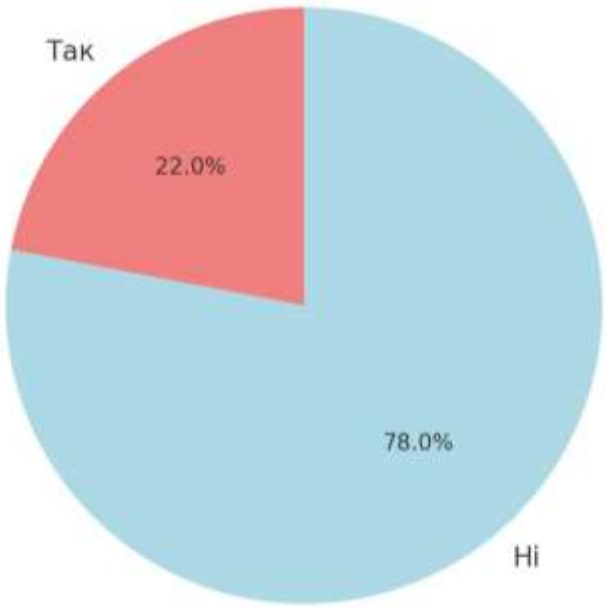

Рисунок 3.15 – Чи були Ви жертвою хакерських атак?

На рисунку 3.15 діаграма відображає розподіл відповідей респондентів на запитання про їхній досвід хакерських атак. Отримані результати показують, що більшість користувачів не стикалися з такими ситуаціями, однак значна частина все ж мала цей негативний досвід.

Основні результати:

1. Жертви хакерських атак (22%) Близько 22% респондентів зазначили, що ставали жертвами хакерських атак. Цей показник є суттєвим і демонструє існування реальної загрози в онлайн-просторі. Серед можливих типів атак, з якими могли стикатися користувачі, – крадіжка облікових записів, доступ до особистих даних чи фінансових ресурсів, а також вірусні атаки.

2. Не стикалися з хакерськими атаками (78%) Більшість опитаних (78%) не стикалися з хакерськими атаками. Це може свідчити про достатній рівень їхньої обережності, використання ефективних засобів захисту, таких як антивірусні програми, складні паролі або багатофакторна аутентифікація. Однак також це може бути результатом недостатньої обізнаності, коли користувачі не завжди помічають хакерські дії.

Дані діаграми свідчать про те, що хоча більшість респондентів не були жертвами хакерських атак, існує значна частка користувачів (22%), які мають негативний досвід у цій сфері. Це вказує на актуальність питань кібербезпеки, необхідність підвищення обізнаності про потенційні загрози та впровадження більш ефективних заходів захисту в цифровому просторі. Залишається важливим інформувати користувачів про сучасні ризики, способи їх виявлення та запобігання.

3.2 Висновок до третього розділу

В третьому розділі кваліфікаційної роботи освітнього рівня «Магістр» було проаналізовано сучасний стан безпеки персональних даних користувачів Інтернету під час використання різноманітних онлайн-процедур. Результати опитування демонструють високий рівень зацікавленості суспільства у забезпеченні безпеки приватної інформації, але водночас вказують на значну

кількість викликів та ризиків у цій сфері. Користувачі стикаються з різними загрозами, такими як хакерські атаки, витоки даних, несанкціонований доступ до особистої інформації, що підтверджує актуальність питання захисту даних.

Важливим аспектом виявилося те, що більшість респондентів обирають обмежений доступ до своїх профілів, обґрунтовуючи це прагненням до конфіденційності та уникненням ризику зловживання персональною інформацією. Однак значна частина користувачів все ще не приділяє належної уваги налаштуванням конфіденційності, що свідчить про потребу у проведенні інформаційно-освітніх кампаній для підвищення цифрової грамотності.

Аналіз отриманих даних також виявив значну недовіру до надання особистих даних під час онлайн-процедур. Лише третина опитаних готова ділитися своєю інформацією, що свідчить про обережність користувачів та їхнє прагнення захистити свої особисті дані від можливих загроз. Водночас понад 20% респондентів зізналися, що ставали жертвами хакерських атак, що підтверджує реальність і серйозність ризиків у цифровому просторі.

Користувачі вказали на різні рівні довіри до безпеки своїх даних. Жоден із респондентів не вважає свої дані повністю захищеними, а лише 23% оцінюють рівень безпеки як високий. Це вказує на існування прогалин у сучасних системах захисту, а також на недостатній рівень обізнаності користувачів щодо сучасних методів забезпечення конфіденційності та безпеки.

Значна частина респондентів використовує базові заходи безпеки, такі як складні паролі, антивірусні програми та захищені Wi-Fi-з’єднання, проте лише невеликий відсоток користувачів практикує регулярну зміну паролів або детальне ознайомлення з правилами та інструкціями перед реєстрацією. Це вказує на необхідність подальшого поширення знань про цифрову безпеку.

Проведене дослідження демонструє, що незважаючи на високий рівень обізнаності щодо важливості конфіденційності, багато користувачів стикаються з труднощами у забезпеченні власної безпеки в Інтернеті. Це зумовлює необхідність подальшого вдосконалення технологій захисту, розробки зручних

для розуміння політик конфіденційності, а також підвищення рівня освіти у сфері цифрової безпеки серед усіх вікових груп.

Результати роботи підтверджують необхідність комплексного підходу до забезпечення захисту персональних даних, який включає не лише впровадження технологічних рішень, але й активну просвітницьку діяльність та розвиток нормативно-правової бази у цій сфері.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Синдром професійного вигорання в ІТ

Синдром професійного вигорання (СПВ) – це стан фізичного, емоційного та розумового виснаження, що виникає внаслідок тривалого впливу стресових факторів на робочому місці. В галузі інформаційних технологій (ІТ) цей синдром є надзвичайно актуальним через високе навантаження, необхідність швидко адаптуватися до змін і тривалу роботу в умовах дедлайнів.

До основних чинників, що впливають на виникнення професійного вигорання серед ІТ-фахівців, належать:

– Перевантаження роботою – ІТ-спеціалісти часто працюють понаднормово, що призводить до фізичного та емоційного виснаження.

– Високі очікування від результатів роботи – постійна необхідність відповідати високим стандартам.

– Монотонність завдань – повторювані процеси без зміни діяльності можуть знижувати мотивацію.

– Відсутність балансу між роботою та особистим життям – через віддалений формат роботи чи постійні термінові задачі.

– Соціальна ізоляція – особливо поширена серед програмістів, які працюють у віддалених або індивідуальних проєктах [32].

Наслідки професійного вигорання:

a) Зниження продуктивності та креативності працівника.

b) Зростання рівня плинності кадрів у компаніях.

c) Погіршення фізичного та психічного стану (безсоння, депресія, проблеми із серцево-судинною системою) [33].

d) Втрата мотивації до професійного розвитку.

Методи профілактики вигорання в ІТ.

Оптимізація робочого часу: впровадження чітких графіків, відмова від понаднормової роботи.

Навчання стресостійкості: тренінги та коучинг з управління емоціями та стресом.

Розвиток корпоративної культури: створення умов для командної роботи, організація корпоративних заходів, менторська підтримка.

Заохочення здорового способу життя: забезпечення абонементів у спортзали, створення зон відпочинку в офісах.

Підтримка work-life balance: гнучкий графік, вихідні дні без робочих завдань.

Синдром професійного вигорання є серйозною проблемою в IT-сфері, яка впливає як на працівників, так і на компанії. Для зменшення ризиків необхідно впроваджувати ефективні стратегії управління стресом, створювати сприятливі умови роботи та надавати можливості для відпочинку.

4.2 Організаційні заходи та технічні засоби із забезпечення пожежної безпеки

Безпека в надзвичайних ситуаціях включає заходи, спрямовані на запобігання виникненню надзвичайних ситуацій, зменшення їх наслідків та забезпечення належної реакції на небезпеки. Основні аспекти включають:

– Пожежна безпека. Належне обладнання офісів автоматичними системами пожежогасіння, встановлення димових датчиків, розташування вогнегасників та розробка планів евакуації є ключовими елементами запобігання пожежам. Важливим є проведення регулярних навчань для співробітників щодо порядку дій під час пожежі.

– Захист від кібератак. У сфері інформаційних технологій критичним є питання захисту від кібератак та збереження інформаційних систем в умовах потенційних кібераварій. Необхідно передбачити резервне копіювання даних, використання захищених каналів передачі інформації та налаштування системи відновлення у випадку кібератак.

– Евакуація. Важливим аспектом є розробка та розміщення планів евакуації, а також проведення навчань серед співробітників щодо правильних дій

у випадку виникнення надзвичайних ситуацій (пожежа, землетрус, хімічна загроза тощо). Це допоможе мінімізувати ризик травмування та забезпечити злагодженість дій працівників.

– Захист у разі природних катастроф. Хоча ІТ-компанії рідко стикаються з прямими наслідками природних катастроф, важливо враховувати можливі ризики, пов'язані з землетрусами, паводками або штормами. Необхідно мати плани дій та відповідне обладнання для таких ситуацій.

4.3 Планування та порядок проведення евакуації населення з районів наслідків впливу НС техногенного та природного характеру

Організація евакуації населення у разі надзвичайних ситуацій техногенного та природного характеру регламентується Порядком, затвердженим постановою Кабінету Міністрів України від 30.10.2013 № 841. Цей документ визначає процедури вивезення (виведення) населення із зон ризику, забезпечення його безпечного розміщення, а також евакуацію матеріальних і культурних цінностей у разі виникнення безпосередньої загрози життю чи здоров'ю людей або ризику пошкодження цінностей.

Залежно від ситуації, може здійснюватися як загальна, так і часткова евакуація, яка може бути тимчасовою або безповоротною. Наприклад, загальна евакуація проводиться у випадках радіоактивного або хімічного забруднення, катастрофічного затоплення населених пунктів, а також у разі руйнування гідротехнічних споруд, коли хвиля прориву може досягнути території менш ніж за чотири години. Часткова евакуація організовується за рішенням місцевих органів влади.

До транспортних засобів, що залучаються для евакуації, належать як наявні ресурси адміністративної території, так і транспорт суб'єктів господарювання чи громадян у випадках загрози життю. Витрати, пов'язані із залученням транспорту, компенсуються з відповідного бюджету [58].

Рішення про евакуацію приймають органи державного рівня (Кабінет Міністрів України), регіонального рівня (обласні держадміністрації) та

місцевого рівня. У невідкладних випадках рішення може ухвалювати керівник аварійно-рятувальної служби, який першим прибув на місце події.

Евакуація матеріальних і культурних цінностей здійснюється за наявності часу, що визначається на підставі моніторингу, прогнозування та лабораторного контролю. Організація та планування евакуації матеріальних цінностей регламентується методикою, затвердженою Міністерством оборони України [66].

4.4 Організація оповіщення і зв'язку у надзвичайних ситуаціях техногенного та природного характеру

Пожежна безпека є важливою складовою діяльності посадових осіб, працівників підприємств та підприємців, яка повинна бути закріплена у трудових договорах і статутах підприємств.

Керівник підприємства зобов'язаний:

a) визначити обов'язки посадових осіб щодо пожежної безпеки;

b) призначити відповідальних за протипожежний стан будівель, споруд, приміщень, ділянок та обладнання;

c) забезпечити належне утримання та експлуатацію засобів протипожежного захисту.

На підприємстві має бути встановлений протипожежний режим, який регулює:

– місця для куріння та використання відкритого вогню;

– порядок проведення пожежонебезпечних робіт;

– правила зберігання сировини та готової продукції;

– заходи з очищення вентиляційних систем і збирання горючого пилу;

– дії персоналу у разі виявлення пожежі.

Працівники повинні бути ознайомлені з вимогами пожежної безпеки під час інструктажів, які проводяться при прийомі на роботу, періодично або в разі змін умов роботи.

Плани евакуації та інструкції. На об’єктах, де перебуває велика кількість людей або є підвищена пожежна небезпека, необхідно розробляти плани евакуації. Вони мають бути вивішені на видних місцях та оновлюватися при зміні планування або функціонального призначення приміщень. Для персоналу потрібно проводити практичні тренування з евакуації не рідше одного разу на півроку.

Навчання персоналу. Усі працівники повинні проходити інструктажі з пожежної безпеки:

– вступний – при прийомі на роботу;

– первинний – безпосередньо на робочому місці;

– повторний – регулярно, відповідно до нормативів.

Працівники, зайняті на пожежонебезпечних роботах, мають щорічно проходити навчання та перевірку знань правил пожежної безпеки.

Забезпечення пожежної охорони. На підприємствах із великою кількістю працівників створюються добровільні пожежні дружини (ДПД) або команди (ДПК), а також пожежно-технічні комісії (ПТК). Їх діяльність регулюється відповідними нормативно-правовими актами.

На території підприємств необхідно забезпечити:

– систему оповіщення про пожежу;

– розміщення знаків безпеки відповідно до стандартів;

– телефонні номери для виклику пожежної служби у доступних місцях.

Особливі вимоги до об’єктів із масовим перебуванням людей
У навчальних закладах, лікарнях, санаторіях, готелях тощо повинні бути розроблені спеціальні інструкції для евакуації персоналу та відвідувачів. Такі заклади зобов’язані проводити регулярні тренування та навчання.

Контроль та відповідальність. Керівник підприємства зобов’язаний забезпечити дотримання вимог пожежної безпеки, оперативно реагувати на порушення та притягувати винних до відповідальності.

Ці заходи спрямовані на зниження ризиків виникнення пожеж та забезпечення безпеки людей на підприємствах і об’єктах різного призначення.

4.5 Висновки до четвертого розділу

В четвертому розділі кваліфікаційної роботи описано фактори, що спричиняють вигорання в ІТ. Робота в галузі інформаційних технологій характеризується високим рівнем професійного навантаження, жорсткими дедлайнами, соціальною ізоляцією та відсутністю балансу між роботою та особистим життям. Ці фактори значною мірою сприяють розвитку професійного вигорання, яке знижує продуктивність і негативно впливає на психологічний стан працівників.

Наслідки професійного вигорання (СПВ) у ІТ-сфері призводить до серйозних наслідків, таких як зниження продуктивності працівників, високий рівень плинності кадрів, погіршення фізичного та психічного здоров'я. Це також сприяє формуванню негативної корпоративної атмосфери, яка може завдати шкоди репутації компанії та її конкурентоспроможності.

Ефективна профілактика професійного вигорання в ІТ включає раціональне планування робочого часу, тренінги з управління стресом, створення сприятливої корпоративної культури та підтримку здорового способу життя. Особливо важливим є заохочення work-life balance, що допомагає працівникам підтримувати мотивацію та відновлювати енергію.

Розуміння причин і наслідків синдрому професійного вигорання дозволяє не лише мінімізувати втрати компаній через низьку продуктивність працівників, але й сприяє покращенню якості життя ІТ-спеціалістів. Використання сучасних методів профілактики та управління стресом є необхідною умовою для збереження людського капіталу й довгострокового розвитку компаній.

В четвертому розділі кваліфікаційної роботи розглянуто питання планування та проведення евакуації населення. Евакуація є ключовим заходом захисту населення у випадку надзвичайних ситуацій техногенного та природного характеру. Вона забезпечується відповідно до затверджених нормативно-правових документів і може мати загальний або частковий характер. Ефективність евакуації залежить від своєчасного прийняття рішень на

державному, регіональному або місцевому рівні, а також від належного планування, моніторингу ситуації та використання доступних ресурсів.

В четвертому розділі роботи описано організацію сповіщення у надзвичайних ситуаціях. Своєчасне оповіщення населення є основою мінімізації ризиків у надзвичайних ситуаціях. Функціонування системи оповіщення забезпечується використанням сучасних засобів зв'язку, радіо- і телевізійних мереж та автоматизованих систем передачі інформації. Чітка організація оповіщення, включно з локальними системами на потенційно небезпечних об'єктах, дозволяє оперативно реагувати на загрози та знижувати рівень паніки серед населення.

Звернута увага на важливість забезпечення пожежної безпеки. Дотримання правил пожежної безпеки є важливим елементом запобігання надзвичайним ситуаціям. Це включає чітке розподілення відповідальності, розробку планів евакуації, регулярні інструктажі та навчання персоналу. На об'єктах із підвищеною небезпекою та масовим перебуванням людей необхідно особливо ретельно впроваджувати протипожежні заходи та проводити регулярні тренування.

Реалізація заходів із евакуації, оповіщення та забезпечення пожежної безпеки вимагає належного контролю та оперативного реагування на можливі порушення. Керівники підприємств та організацій несуть відповідальність за дотримання нормативних вимог і зобов'язані забезпечувати безпеку працівників і відвідувачів. Системний підхід до організації безпеки дозволяє мінімізувати ризики для життя та здоров'я людей.

ВИСНОВКИ

У кваліфікаційної роботи освітнього рівня «Магістр» досліджено теоретичні, методологічні та практичні аспекти забезпечення безпеки персональних даних і користувачів мережі Інтернет у сучасних умовах. Поставлені завдання виконано в межах чотирьох розділів роботи, що дозволило отримати наступні ключові результати.

В першому розділі кваліфікаційної роботи:

– Подано теоретичне обґрунтування проблеми убезпечення персональних даних.

– Проведено систематизацію понять і видів персональних даних, а також проаналізовано міжнародні (GDPR, CCPA) та національні (Закон України «Про захист персональних даних») нормативно-правові акти, які регулюють цю сферу.

– Визначено основні загрози безпеці даних, такі як фішинг, зловмисне програмне забезпечення, витоки даних, соціальна інженерія та використання незахищених мереж.

– Досліджено ключові теоретичні аспекти захисту персональних даних.

– Окрему увагу приділено технічним методам захисту, зокрема механізмам шифрування (симетричному, асиметричному, гібридному), методам аутентифікації (однофакторна, двофакторна, багатофакторна) та політикам управління правами доступу (RBAC).

– Сформовано методології та підходи до захисту персональних даних. Це створило основу для розробки методів протидії цим загрозам.

В другому розділі кваліфікаційної роботи:

– Описано основні проблеми та робочі гіпотези убезпечення персональних даних користувачів Інтерне.

– Досліджено методи, прийоми, засоби, змінні, показники та характеристики параметрів убезпечення персональних даних користувачів Інтернет

– Практичні рекомендації щодо області та організації процесу дослідження онлайн-процедур убезпечення персональних даних користувачів Інтернет.

У третьому розділі кваліфікаційної роботи:

– Проаналізовано характеристики загроз безпеці користувачів мережі Інтернет.

– Проведено збір та аналіз відгуків, що дало змогу ідентифікувати ключові недоліки у системах захисту даних та запропонувати ефективні рішення для їх усунення.

– На основі проведених досліджень проаналізовано рівень загроз для звичайних користувачів, окреслено особливості інформаційної безпеки та складність вирішення проблеми з урахуванням зростання цифрових загроз.

У четвертому розділі розглянуто питання ергономіки робочого місця, забезпечення електробезпеки та створення сприятливого мікроклімату для працівників. Окрема увага приділена заходам протидії пожежам, евакуаційним процедурам та плануванню дій у разі природних катастроф.

Загалом, магістерська робота поєднує теоретичний аналіз із практичними рекомендаціями, що мають значний потенціал для впровадження Це включає вдосконалення технологій шифрування, розвиток ефективних політик управління доступом, підвищення цифрової грамотності серед усіх вікових груп користувачів та активізацію просвітницької діяльності. Отримані результати створюють основу для розробки рекомендацій щодо підвищення рівня захисту персональних даних в Інтернеті, що має практичне й теоретичне значення для сучасного цифрового суспільства.

ПЕРЕЛІК ДЖЕРЕЛ

1 Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd Edition. New York: John Wiley & Sons, 2018. 1232 с.

2 Apanowicz, J. Metodologiczne uwarunkowania pracy naukowej. Warszawa, 2005. S. 54.

3 Babie, E. Podstawy badań społecznych. Warszawa, 2008. S. 166.

4 Chen, L., Wang, H., & Zhou, S. Role–Based Access Control: Benefits and Challenges in Large–Scale Systems. Information Security Journal. 2020. T. 24, № 8. P. 65 – 80.

5 Cheng, L., Wang, H., & Zhou, S. Role–based access control: benefits and challenges. Information Security Journal. 2020. Vol. 29, No. 1. P. 76 – 85.

6 Cieślarczyk, M. Metody, techniki i narzędzia badawcze oraz elementy statystyki stosowane w pracach magisterskich i doktorskich. Akademia Obrony Narodowej, 2006. P. 20 – 21.

7 Dmytriv, Dmytro, et al. «Industry 4.0 technologies for smart households.» (2024).

8 Duda, Oleksii, et al. «Information technology platform for the selection and analytical processing of information on COVID-19.» 2021 IEEE 16th International Conference on Computer Sciences and Information Technologies (CSIT). Vol. 2. IEEE, 2021.

9 Duda, Oleksii, et al. «Information technology sets formation and» TNTU Smart Campus» services network support.» ITTAP. 2023.

10 ENISA. European Union Agency for Cybersecurity. URL: https://enisa.europa.eu (дата звернення: 10.10.2024).

11 GDPR, General Data Protection Regulation. URL: https://gdpr.eu (дата звернення: 10.10.2024).

12 Hong, S. Innovation and Growth: The Role of International Trade. New York: Springer, 2012. 324 p.

13 Infosecurity. Cybersecurity Trends Report 2021. London: Infosecurity Group, 2021. 112 p.

14 Jakobsson, M., & Myers, S. Statistical Methods in Genetics. Cambridge: Cambridge University Press, 2006. 312 p.

15 Johnson, M., & Zhang, H. Multi-Factor Authentication in Online Systems: A Comprehensive Analysis. International Journal of Cybersecurity. 2021. T. 34, № 5. P. 87 – 102.

16 McAfee. Threats Report: Navigating a Digital Age. Santa Clara: McAfee LLC, 2019. 98 p.

17 NIST SP 800-63B. URL: https://nvlpubs.nist.gov (дата звернення: 12.11.2024).

18 Pasichnyk, Volodymyr. «Information and technological tools for analysis and visualization of open data in smart cities.» (2024).

19 Ponemon Institute. 2021 Cost of Data Breach Report. URL: https://ponemon.org (дата звернення: 12.11.2024).

20 Rescorla, E. SSL and TLS: Designing and Building Secure Systems. Addison–Wesley, 2018. 300 p.

21 Rivest, R. L., Shamir, A., & Adleman, L. A method for obtaining digital signatures and public–key cryptosystems. Communications of the ACM, 21 (2), 1978, 120 – 126 pp.

22 Rodriguez, C. Privacy Policy Transparency as the Foundation of User Trust in Online Services. Data Privacy Research Journal. 2020. T. 15, № 3. C. 45 – 61.

23 Schneier, B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. New York: John Wiley & Sons, 1996. 758 p.

24 Skarga.ua. URL: www.skarga.ua.

25 Smith, D., & Taylor, G. Automated Privacy Policy Enforcement Using Machine Learning Techniques. Journal of Data Protection. 2021. T. 12, № 4. C. 122 – 135.

26 Stanko, Andrii, et al. «Artificial Intelligence of Things (AIoT): Integration Challenges and Security Issues» (2024).

27 Stinson, D. R., & Paterson, M. B. Cryptography: Theory and Practice. CRC Press, 2018. 350 p.

28 Symantec. Internet Security Threat Report. Mountain View: Symantec Corporation, 2020. 120 p.

29 Sztumski, J. Wstęp do metod i technik badań społecznych. Katowice, 2005. P. 68.

30 Zillya! Антивірусні рішення. URL: https://zillya.ua (дата звернення: 22.11.2024).

31 Zimmermann, P. PGP User's Guide. MIT Press, 2017. 250 p.

32 Бакшаєва О. В., Ковальчук І. М. Психоемоційний стан працівників ІТ-сфери в умовах сучасного робочого середовища. Науковий журнал «Психологія праці». – 2020. – № 4 (15). – С. 45 – 48.

33 Воронова Н. Професійне вигорання: причини, наслідки, шляхи подолання Журнал «Охорона праці». – 2019. – № 2 (8). – С. 32 – 37.

34 Гончаренко, С. М. Системи і методи захисту інформації. Дніпро: ДДУ, 2017. 272 с.

35 Гринчишин, Я. М. Конспект лекцій з навчальної дисципліни «Методологія наукових досліджень у фінансах». Львів, 2018. С. 4.

36 Держспецзв'язку. Стратегія кібербезпеки України. URL: https://dsszzi.gov.ua (дата звернення: 25.11.2024).

37 Джонсон, Р. Ефективність багатофакторної аутентифікації в інформаційних системах. Journal of Security and Privacy. 2021. Vol. 10, No. 2. P. 32 – 45.

38 ДССЗЗІ України. Аналітичний звіт про стан кібербезпеки України за 2022 рік. Київ: Державна служба спеціального зв'язку та захисту інформації України, 2022. 85 с.

39 ДСТУ ISO/IEC 27001:2015. Інститут стандартизації України. Київ: ДП «УкрНДНЦ», 2015.

40 Жеребкін, В. Є. Логіка. Харків-Київ: «Основа», «Знання», 1999. С. 12.

41 Журнал «Кібербезпека та захист інформації». Видається НТУУ «КПІ ім. І. Сікорського».

42 Закон України «Про захист персональних даних». Відомості Верховної Ради України, 2010, № 34, ст. 481.

43 Закон України «Про інформацію». Відомості Верховної Ради України, 1992, № 48, ст. 650.

44 Закон України «Про телекомунікації». Відомості Верховної Ради України, 2004, № 12, ст. 155.

45 Зварич, І. В. Інформаційна безпека в мережі Інтернет: правові та технічні аспекти. Львів: Науковий вісник НУ «Львівська політехніка», 2021. 284 с.

46 Іваненко, Т. О. Сучасні підходи до управління інформаційною безпекою. Харків: Видавництво ХНУ, 2021. 150 с.

47 Іванов, В. П. Захист інформації в Інтернет-мережах. Київ: Техніка, 2022. 198 с.

48 Карачка, А. Ф. Технології захисту інформації. Тернопіль: ТНЕУ, 2017. С. 7.

49 Климаш, О. М. Використання інноваційних підходів у сучасній освіті. Київ: Наукова думка, 2022. 256 с.

50 Ковальчук, О. П. Технології захисту персональних даних в умовах кіберзагроз. Київ: Видавництво КНУ ім. Т. Шевченка, 2019. 198 с.

51 Конвенція Ради Європи «Про захист фізичних осіб при автоматизованій обробці персональних даних» від 28 січня 1981 року.

52 Конституція України. Відомості Верховної Ради України, 1996, № 30, ст. 141.

53 Кудряшов, М. І. Інформаційна безпека та захист даних. Київ: Наукова думка, 2020. 312 с.

54 Лі, М., & Чжан, Х. Багатофакторна аутентифікація: сучасні підходи та перспективи. International Journal of Cybersecurity. 2020. Vol. 12, No. 3. P. 145 – 158.

55 Маклюен, Г. М. Понимание Медиа: Внешние расширения человека / Пер. з англ. В. Николаева; Закл. Вавилова, М. Жуковский: «КАНОН-пресс-Ц», «Кучково поле», 2003. 464 с. (Приложение к серии «Публикации Центра Фундаментальной Социологии»). С. 288 – 295.

56 Мельник, І. В., Петренко, Л. С., & Бойко, А. Ю. Методи і засоби захисту інформаційних систем. Львів: ЛНУ, 2019. 318 с.

57 Мельничук, В. С. Методи криптографічного захисту даних у цифрових мережах. Науковий вісник КПІ, 2022. № 12. С. 67 – 74.

58 Методика планування заходів з евакуації: затверджена наказом Міністерства внутрішніх справ України від 10 липня 2017 року № 579. – Київ: Міністерство внутрішніх справ України, 2017. – 50 с.

59 Міністерство освіти і науки України. Офіційний сайт. URL: https://mon.gov.ua, 2021.

60 Національна поліція України. Аналітичний звіт щодо інформаційної безпеки, 2022.

61 Олійник, В. Г. Актуальні питання інформаційної безпеки. Львів: Видавництво «Світ», 2023.

62 Павленко, О. М. Біометрична аутентифікація в сучасних інформаційних системах. Одеса: ОНПУ, 2021. 224 с.

63 Петренко, О. М., та ін. Захист інформації: практичні аспекти. Одеса: ОНУ, 2022.

64 Петров, І. В. Інформаційна безпека: підходи та методи. Київ: Політехніка, 2021.

65 Поняття загроз інформаційній безпеці. URL: https://pidru4niki.com/12800528/politologiya/ponyattya_zagroz_informatsiyniy_bezpetsi.

66 Постанова Кабінету Міністрів України від 30.10.2013 № 841.

67 Романенко, О. С. Основи криптографії та захисту інформації. Харків: ХНУРЕ, 2018. 256 с.

68 Савчук, Л. М. Розвиток креативного мислення у школярів. Львів: Видавництво Львівського університету, 2021. 198 с.

69 Самсонов, В. В. Методи та засоби Інтернет-технологій. Київ: Видавництво «Техніка», 2015. С. 225.

70 Семенюк, Р. П. Правові аспекти захисту персональних даних в Україні. Харків: Юридичний вісник, 2020. 215 с.

71 Сергієнко, І. П. Інформаційна безпека в сучасних умовах. Київ: Видавництво «Наукова думка», 2022. 200 с.

72 Сидоренко, В. Ю. Методи аналізу даних. Київ: Наука, 2020.

73 Сидоренко, В. Ю. Нові тенденції в інформаційній безпеці. Київ: Наука, 2024.

74 Татаров, І. В. Інформаційні технології у забезпеченні конфіденційності персональних даних. Запоріжжя: Видавництво ЗНУ, 2019. 174 с.

75 Українська мережа інформаційної безпеки. Київ: Видавництво «Безпека», 2021. 150 с.

76 Українська мережа інформаційної безпеки. Річний звіт, 2021.

77 Харківський національний університет радіоелектроніки (ХНУРЕ). Офіційний сайт. URL: https://nure.ua (дата звернення: 01.12.2024).

78 Цивільний кодекс України. Відомості Верховної Ради України, 2003, № 40 – 44, ст. 356.

79 Ченга, І. В., та ін. Захист інформації в комп'ютерних мережах. Харків: ХНУ, 2020. 220 с.

80 Янковський, А. Шифрування та його роль у забезпеченні конфіденційності даних. Журнал інформаційної безпеки. 2019. № 4. С. 112 – 119.

ДОДАТКИ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
імені ІВАНА ПУЛЮЯ
НАУКОВЕ ТОВАРИСТВО ім. ШЕВЧЕНКА

М А Т Е Р І А Л И

XII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

18–19 грудня 2024 року

ТЕРНОПІЛЬ
2024

УДК 001
М34

ПРОГРАМНИЙ КОМІТЕТ

Голова: Приймак Микола – професор кафедри комп'ютерних систем та мереж, д.т.н., професор.
Співголови: Марущак Павло – проректор з наукової роботи, докт. техн. наук, професор.
Баран Ігор – канд. техн. наук, доцент, декан факультету ФІС.
Науковий секретар: Надія Крива– старший викладач.

Члени: Василь Кривень – завідувач кафедри математичних методів в інженерії д.ф.-м.н., професор; Галина Осухівська – завідувач кафедри комп'ютерних систем та мереж, к.т.н., доцент; Микола Карпінський - професор кафедри кібербезпеки, д.т.н., професор; Жанна Баб'як - завідувач кафедри української та іноземних мов, к.пед. н., доцент; Ярослав Литвиненко – професор кафедри комп'ютерних наук, д.т.н., професор; Михайло Петрик - завідувач кафедри програмної іженерії, д.ф.-м.н., професор; Наталія Загородна – завідувач кафедри кібербезпеки, к.т.н., доцент.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова: Скоренький Юрій Любомирович – канд. техн. наук, доцент кафедри фізики.
Члени: доцент кафедри комп'ютерних наук, к.т.н. В. Никитюк; доцент кафедри програмної інженерії, к.т.н. Д. Михалик; доцент кафедри кібербезпеки, к.т.н. М. Стадник; доцент кафедри комп'ютерних систем та мереж, к.т.н. Є. Тиш; ст. викладач Л. Джиджора.

М34 Матеріали XII науково-технічної конфції «Інформаційні моделі, системи та технології» Тернопільського національного технічного університету імені Івана Пулюя, (Тернопіль, 18–19 грудня 2024 р.). – Тернопіль : Тернопільський національний технічний університет імені Івана Пулюя, 2024. – 238 с.

Адреса оргкомітету: ТНТУ ім. І. Пулюя, м. Тернопіль, вул. Руська, 56, 46001,
тел. (0352) 52-41-33, факс (0352) 25-49-83.
E-mail: conffis2024@gmail.com
Редагування, оформлення та верстка: Надія Крива

СЕКЦІЇ КОНФЕРЕНЦІЇ, ЯКІ ПРЕДСТВЛЕНІ В ЗБІРНИКУ

- Математичне моделювання
- Інформаційні системи та технології, кібербезпека
- Комп'ютерні системи та мережі
- Програмна інженерія та моделювання складних розподілених систем
- Новітні фізико-технічні та освітні технології

В збірнику надруковано тези доповідей XII науково-технічної конференції «Інформаційні моделі, системи та технології» (Тернопіль, 18–19 грудня 2024 р.) за такими науковими напрямками: математичне моделювання; інформаційні системи та технології, кібербезпека; комп'ютерні системи та мережі; програмна інженерія та моделювання складних розподілених систем; новітні фізико-технічні та освітні технології.

Розрахований на науковців, викладачів та студентів вузів.

За зміст тез та дотримання норм академічної доброчесності відповідальність несе автор.

УДК 004.032
О. Ловчук; Р. Катрич; В. Дуда
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

АКТУАЛЬНІСТЬ ХМАРНОГО МАСШТАБУВАННЯ ТА KUBERNETES

UDC 004.032
O. Lovchuk; R. Katrych; V. Duda

THE RELEVANCE OF CLOUD SCALATION AND KUBERNETES

На даний час в процесі розширення хмарних платформ та послуг зростає потреба в підвищенні продуктивності інфраструктур центрів обробки даних. Високопродуктивні обчислення, передові мережеві рішення та стратегії динамічної оптимізації обчислювальних ресурсів зможуть допомогти персоналу центрів хмарного опрацювання даних забезпечувати високу швидкість та ефективність, що необхідні для надання високоякісних послуг [1]. При цьому однією з ефективних стратегій оптимізації хмарних обчислювальних процесів є запуск контейнерних програм. Він забезпечує покращення портативності програмно-алгоритмічних засобів, підвищення безпеки, прискорення перебігу процесів використання ресурсів, пришвидшення процедур розгортання та масштабування, а також покращення процесів інтеграції та взаємодії. Зазначені переваги зможуть допомогти установам та організаціям покращити протікання процесів розгортання застосунків, їх супроводу, обслуговування та керування, даючи змогу оперативніше та ефективніше реагувати на динамічні потреби бізнес-процесів.

Kubernetes – це система оркестровки контейнерів. Вона призначена для автоматизації процесів розгортання, масштабування та управління контейнерними програмно-алгоритмічними засобами. Однією з ключових її особливостей є функціональні можливості планувати процедур розгортання та виконання контейнерів у кластерах обчислювальних вузлів за допомогою алгоритмів планування [2]. Ці алгоритми визначають найкраще розміщення контейнерів на доступних обчислювальних вузлах у кластері. Система оркестрації контейнерів Kubernetes, пропонує можливість автоматизованого керування та масштабування цих розумних служб, забезпечуючи високі показники надійності та стійкості роботи за допомогою динамічного планування обчислювального навантаження. Тому алгоритми планування в Kubernetes для розумних міст є ключовими компонентами ефективного управління та розподілу ресурсів в міській обчислювальній інфраструктурі.

Тому актуальним напрямком сучасних досліжень є вичерпний аналітичний огляд різнотипових алгоритмів планування Kubernetes [1]. При дослідженні характеристик алгоритмів планування Kubernetes їх можна згрупувати у чотири підкатегорії:

- загальне планування;
- планування з підтримкою автоматичного масштабування;
- планування на основі багатоцільової оптимізації;
- орієнтоване на штучний інтелект планування.

Алгоритми планування Kubernetes функціонують на основі різнотипових параметрів, як от обчислювальні ресурси, мережеві вимоги, характеристики зв'язку та інші критерії.

Література

1. Senjab, Khaldoun, et al. «A survey of Kubernetes scheduling algorithms». Journal of Cloud Computing 12.1 (2023): 87.
3. Wen, Shilin, et al. «K8sSim: A Simulation Tool for Kubernetes Schedulers and Its Applications in Scheduling Algorithm Optimization». Micromachines 14.3 (2023): 651.

УДК 004.9
Р. Ставицький; Р. Катрич; А. Лисий
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ШТУЧНИЙ ІНТЕЛЕКТ В РОЗУМНИХ МІСТАХ

UDC 004.9
R. Stavytskyi; R. Katrych; A. Lysyi

ARTIFICIAL INTELLIGENCE IN SMART CITIES

Штучний інтелект має значний потенціал для аналітичного опрацювання зібраних та інтегрованих в середовищі «розумних міст» великих за обсягом наборів та колекцій даних, що дає змогу ефективно використовувати отримані інсайти для оперативної оптимізації витрат ресурсів та забезпечення високоефективної взаємодії з громадянами. Як зазначено в [1], програмно-алгоритмічні засоби на основі штучного інтелекту можуть сприяти підвищенню безпеки та захисту громадськості завдяки використанню вдосконалених технологій спостереження, моніторингу аварійних та надзвичаних ситуацій, поєднанню баз даних. Розподілене та високоефективне управління процесами постачання ресурсів, зокрема енергії та води, є ще однією актуальною сферою використання штучного інтелекту [2]. Аналітичне опрацювання соціальних джерел для розуміння потреб громадян у режимі реального часу та використання інтерактивних чат-ботів на основі штучного інтелекту для повсякденної комунікації з «розумними» міськими системами та послугами також показали високу ефективність [3].

На даний час у середовищах «розумних міст» продукуються обширні множини різнотипових даних. З часом зростатиме їх різноманіття: від зображень і відео до сенсорних даних, показників споживання ресурсів, а саме електроенергії та води, даних із соціальних джерел, текстів тощо. Важливим фактором є те, що в «розумних» середовищах можуть виникати нескінченна множина потенційних ситуацій [4]. Хоча використання технології хмарних обчислень, штучного інтелекту, машинного навчання та аналітичного опрацювання принесло значну користь «розумним містам», існують ключові обмеження, які стримують реалізацію переваг від таких інформаційно-технологічних досягнень. Зокрема обмеження полягає в тому, що використання штучного інтелекту наразі відбувається ізольовано, у вигляді окремих застосунків, через відсутність ефективних механізмів інтеграції та обміну інформацією.

Література

1. Guelzim, T., & Obaidat, M. S. (2016). Cloud computing systems for smart cities and homes. In M. S. Obaidat & P. Nicopolitidis (Eds.), Smart Cities and Homes (pp. 241–260). Morgan Kaufmann. https://doi.org/10.1016/B978-0-12-803454-5.00012-2.
2. De Silva, D., Sierla, S., Alahakoon, D., Osipov, E., Yu, X., & Vyatkin, V. (2020). Toward intelligent industrial informatics: A review of current developments and future directions of artificial intelligence in industrial applications. IEEE Industrial Electronics Magazine, 14(2), 57–72. https://doi.org/10.1109/MIE.2019.2952165.
4. Adikari, A., De Silva, D., Alahakoon, D., & Yu, X. (2019). A cognitive model for emotion awareness in industrial Chatbots. 2019 IEEE 17th international conference on industrial informatics (INDIN), 1, 183–186.
5. Mohammad, N., Muhammad, S., Bashar, A., & Khan, M. A. (2019). Formal analysis of human-assisted smart city emergency services. IEEE Access, 7, 60376–60388.

Анкета дослідження **Додаток Б**

щодо почуття безпеки користувачів інтернету

1. Вкажіть тип пристрою, який Ви найчастіше використовуєте для входу в мережу

а) телефон

б) планшет

в) ноутбук

г) комп'ютер

2. Чи Ви здебільшого здійснюєте покупки в інтернет-магазинах?

а) так

б) ні

3. Як Ви вважаєте, чи зручно використовувати онлайн процедури?

а) так

б) ні

4. Якими онлайн процедурами Ви користуєтесь?

а) комунальні платежі

б) покупка товарів та одягу

в) поповнення банківських рахунків

г) послуги поповнення зв'язку

д) збір коштів для надання власних послуг

е) виплата заробітної плати

5. В який спосіб використовуєте вільний час у інтернеті?

а) граю в ігри

б) використовую соцмережі

в) купую товари в інтернеті, шукаю цікаві знижки

г) слухаю музику

д) дивлюсь фільми/серіали

е) читаю новини/статті

є) розмовляю з друзями через месенджери

ж) інше

6. Хто допоміг Вам зробити перші кроки в інтернеті?

а) сам(а)

б) старший брат/сестра

в) друзі

г) родина

7. Місце де найчастіше використовуєте інтернет?

а) дім

б) школа/університет

в) громадський транспорт

г) у друзів

д) на прогулянці

е) інше

8. Які онлайн-процедури мають бути перспективними в майбутньому?

а) можливість отримати освіту

б) соціальні медіа повинні становити 90% нашого життя

в) віртуальність має мати межі

9. Яким способом дбаєте про свою безпеки у інтернеті?

а) приділяю особливу увагу тому, де я надаю свої особисті дані, і роблю це лише за необхідності

б) використовую антивірус

в) використовую лише захищені Wi-Fi з'єднання

г) регулярно змінюю паролі

д) не контактую з незнайомими у інтернеті

е) добре перевіряю кого додаю до друзів у соцмережах

є) не беру участі у конфліктах онлайн

ж) не звертаю на це уваги

10. Чи прийнятно для Вас ділитися особистою інформацією під час використання онлайн-сервісів?

а) так

б) ні

11. Чи уважно Ви читаєте правила та інструкції, які з'являються перед реєстрацією або здійсненням покупок онлайн?

а) так

б) деколи

в) ні

12. Які у Вас налаштування особистого профілю?

а) обмежую спільний доступ до друзів лише тому, що я ціную свою конфіденційність і хочу мати контроль над своїм профілем і тим, хто може його переглядати

в) створив(ла) особистий профіль, тому що боюся, що хтось може використати мої дані чи фотографії

б) вибираю загальнодоступний профіль, тому що хочу, щоб усі могли бачити мої дані та публікації

г) У мене загальнодоступний профіль, оскільки його було встановлено після того, як я створив(ла) обліковий запис

13. Які дані, на Вашу думку, мають бути вирішальними для ідентифікації Вашої особи в інтернеті?

а) прізвище, ім'я, по батькові

б) дата народження

в) серія та номер паспорта/ідентифікаційний номер

г) логін та пароль

14. Наскільки важливі безпека та захист Ваших особистих даних в інтернеті?

а) на 100%

б) на 80%

в) на 50%

г) на 25%

15. Ви були жертвою хакерських атак?

а) так

б) ні