**ДЕРЖАВНИЙ УНІВЕРСИТЕТ**
**ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**
**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ МЕНЕДЖМЕНТУ**
**ТА ПІДПРИЄМНИЦТВА**
**КАФЕДРА ДОКУМЕНТОЗНАВСТВА ТА ІНФОРМАЦІЙНОЇ**
**ДІЯЛЬНОСТІ**

# КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

на тему: **«ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У ЦИФРОВИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ»**

на здобуття освітнього ступеня бакалавра
зі спеціальності 029 Інформаційна, бібліотечна та архівна справа
освітньо-професійної програми Документознавство та інформаційна діяльність

*Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело*

_____ Ірина БІДЮК

Виконала: Ірина БІДЮК
здобувачка вищої освіти
гр. ДЗД-41

Керівник: Леся КОВАЛЬСЬКА
доктор історичних наук,
професор

Рецензент: Ірина П’ЯТНИЦЬКОВА
кандидат історичних наук,
доцент

**Київ 2025**

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ**
**ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**
**Навчально-науковий інститут менеджменту та підприємництва**

Кафедра документознавства та інформаційної діяльності
Ступінь вищої освіти бакалавр
Спеціальність 029 Інформаційна, бібліотечна та архівна справа
Освітньо-професійна програма Документознавство та інформаційна діяльність

**ЗАТВЕРДЖУЮ**
Завідувач кафедри документознавства та інформаційної діяльності
_____ Тетяна СИДОРЕНКО
«____» _____ 2025 р.

**ЗАВДАННЯ**
**НА КВАЛІФІКАЦІЙНУ РОБОТУ**

**Бідюк Ірини Юріївни**

1. Тема кваліфікаційної роботи «Захист персональних даних у цифрових інформаційних системах», керівник кваліфікаційної роботи проф., д.і.н. Ковальська Леся Андріївна професор кафедри документознавства та інформаційної діяльності, затверджені наказом Державного університету інформаційно-комунікаційних технологій від «24» лютого 2025 р. № 56.
2. Строк подання кваліфікаційної роботи «16» травня 2025 р.
3. Вихідні дані до кваліфікаційної роботи:

**Мета** кваліфікаційної роботи – дослідити особливості захисту персональних даних у цифрових інформаційних системах задля подальшого підвищення рівня захищеності персональної інформації в умовах цифровізації.

**Об'єктом дослідження є** цифрові інформаційні системи, що обробляють та зберігають персональні дані користувачів, зокрема, в сфері охорони здоров'я.

**Предметом дослідження** – процеси, механізми та засоби захисту персональних даних у цифрових інформаційних системах на прикладі приватної клініки Viva.

4. Перелік питань, які потрібно розробити:
   - Збір персональних даних організації та вимоги реалізації їх захисту.
   - Сучасні методи та технології захисту персональних даних в документаційно-інформаційній діяльності.
   - Тенденції розвитку та впровадження систем захисту персональних даних у медичному закладі.
5. Перелік ілюстративного матеріалу: презентація, 6 рисунків, додатки.
6. Дата видачі завдання «26» вересня 2024 р.

# КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів кваліфікаційної роботи | Строк виконання етапів роботи | Примітки |
|---|---|---|---|
| 1 | Визначення тематики, вибір наукового керівника, уточнення теми | 18.09.2024 | |
| 2 | Розроблення та складання плану кваліфікаційної бакалаврської роботи | 26.09.2024 | |
| 3 | Підготовка 1 розділу | 07.01.2025 | |
| 4 | Підготовка 2 розділу | 22.04.2025 | |
| 5 | Підготовка 3 розділу | 01.05.2025 | |
| 6 | Висновки | 09.05.2025 | |
| 7 | Підготовка остаточного варіанта роботи | 13.05.2025 | |
| 8 | Написання відгуку науковим керівником | 14.05.2025 | |
| 9 | Оформлення й представлення роботи на кафедру та перевірка на плагіат | 16.05.2025 | |
| 10 | Підготовка доповіді, презентації та ілюстративного матеріалу, рецензія | 05.06.2025 | |
| 11 | Попередній захист роботи | 10.06.2025 | |
| 12 | Основний захист кваліфікаційної бакалаврської роботи | 18.06.2025 | |

Здобувачка вищої освіти _____ Ірина БІДЮК

Керівник
кваліфікаційної роботи _____ Леся КОВАЛЬСЬКА

# РЕФЕРАТ

**Текстова частина** кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 57 стор., 1 рис., 6 табл., 38 джерел.

**Мета** кваліфікаційної роботи – дослідити особливості захисту персональних даних у цифрових інформаційних системах задля подальшого підвищення рівня захищеності персональної інформації в умовах цифровізації.

**Об’єктом дослідження є** цифрові інформаційні системи, що обробляють та зберігають персональні дані користувачів, зокрема, в сфері охорони здоров’я.

**Предметом дослідження** – процеси, механізми та засоби захисту персональних даних у цифрових інформаційних системах на прикладі приватної клініки Viva.

**Короткий зміст роботи**: сьогодні, коли цифрові технології міцно увійшли у всі сфери діяльності організацій, бізнесу та стали частиною нашого життя, забезпечення безпеки персональних даних стає надзвичайно важливим. У цифровому просторі ці дані перетворюються не просто на інформацію, а на ключовий елемент приватності, безпеки та довіри між організаціями та громадянами. Активне використання електронного документообігу, хмарних обчислень, автоматизації процесів, електронних медичних карт та онлайн-сервісів значно підвищило ефективність обробки інформації та документації. Однак, це також супроводжується новими викликами, зокрема, високим ризиком витоків, втрати або зловживання персональними даними.

Особливо чутливо це питання стосується медичних установ, де будь-яка помилка в системі захисту інформації може мати серйозні наслідки не лише для адміністрації, а й для пацієнтів. Медичні заклади, включаючи приватні клініки, характеризуються підвищеною вразливістю, оскільки працюють з великими обсягами конфіденційної інформації: історії хвороби, результати аналізів, контактні та фінансові дані пацієнтів. Практичний кейс клініки Viva підкреслює необхідність розгляду питань кіберзахисту не як другорядних, а як першочергових у процесі цифрової трансформації охорони здоров'я.

**Ключові слова**: інформаційна безпека, цифрові технології, персональні дані, інформація, онлайн-сервіси.

**ЗМІСТ**

# ВСТУП

**Актуальність теми.** Сьогодні, коли цифрові технології міцно увійшли у всі сфери діяльності організацій, бізнесу та стали частиною нашого життя, забезпечення безпеки персональних даних стає надзвичайно важливим. У цифровому просторі ці дані перетворюються не просто на інформацію, а на ключовий елемент приватності, безпеки та довіри між організаціями та громадянами. Активне використання електронного документообігу, хмарних обчислень, автоматизації процесів, електронних медичних карт та онлайн-сервісів значно підвищило ефективність обробки інформації та документації. Однак, це також супроводжується новими викликами, зокрема, високим ризиком витоків, втрати або зловживання персональними даними.

Особливо чутливо це питання стосується медичних установ, де будь-яка помилка в системі захисту інформації може мати серйозні наслідки не лише для адміністрації, а й для пацієнтів. Медичні заклади, включаючи приватні клініки, характеризуються підвищеною вразливістю, оскільки працюють з великими обсягами конфіденційної інформації: історії хвороби, результати аналізів, контактні та фінансові дані пацієнтів. Практичний кейс клініки Viva підкреслює необхідність розгляду питань кіберзахисту не як другорядних, а як першочергових у процесі цифрової трансформації охорони здоров'я.

**Мета** кваліфікаційної роботи – дослідити особливості захисту персональних даних у цифрових інформаційних системах задля подальшого підвищення рівня захищеності персональної інформації в умовах цифровізації.

**Завдання дослідження:**

- проаналізувати сутність та класифікацію персональних даних в умовах цифрового середовища;
- вивчити українське законодавство та міжнародні стандарти, що регламентують захист персональної інформації;
- дослідити основні принципи кібербезпеки, які лежать в основі безпечної роботи з інформацією та документами;

- визначити особливості захисту даних у хмарних сервісах та на прикладі використання хмарної медичної інформаційної системи (МІС);
- проаналізувати реальні випадки витоків персональних даних у клініці Viva, встановити причини та наслідки;
- сформулювати практичні рекомендації для підвищення інформаційної безпеки у приватних медичних закладах.

**Об'єктом** дослідження є цифрові інформаційні системи, що обробляють та зберігають персональні дані користувачів, зокрема, в сфері охорони здоров'я.

**Предметом** дослідження – процеси, механізми та засоби захисту персональних даних у цифрових інформаційних системах на прикладі приватної клініки Viva.

**Методи дослідження.** Під час роботи використовувались наступні методи: аналітичний метод – для опрацювання чинного законодавства України та міжнародних нормативних актів; порівняльний аналіз – для виявлення відмінностей в підходах до забезпечення кібербезпеки в різних типах цифрових систем; структурно-функціональний аналіз – для дослідження архітектури систем захисту в клініці Viva; систематизація та узагальнення – при формулюванні практичних рекомендацій.

**Наукова новизна дослідження.** Дана робота відрізняється тим, що крім вивчення теоретичних аспектів захисту персональних даних, містить практичний аналіз на прикладі реальної медичної установи. Вона поєднує науковий підхід з практичним досвідом, пропонуючи реалістичні рекомендації, які можуть бути застосовані в інших організаціях.

**Практична цінність дослідження** полягає у розробці реалістичних заходів підвищення рівня захисту інформації, враховуючи специфіку медичної сфери. Зокрема, запропоновано рішення щодо покращення автентифікації, управління правами доступу, резервного копіювання, навчання персоналу та впровадження політики безпеки в роботі з документацією.

**Структура роботи.** Бакалаврська робота, обсягом 60 сторінок, складається з трьох основних розділів.

# РОЗДІЛ 1
# ЗМІСТ ТА ВИМОГИ ПЕРСОНАЛЬНИХ ДАНИХ ОРГАНІЗАЦІЇ ДО РЕАЛІЗАЦІЇ ЗАХИСТУ

## 1.1. Поняття персональних даних та їх роль у цифровому документаційно-інформаційному середовищі

У цифрову добу, коли технології впровадилися у всі сфери нашого життя, персональні дані стали не просто об'єктом захисту за законом, а важливим елементом цифрового ресурсу. Дані про особу — це не простий перелік ідентифікаторів. Це інформаційний блок, що формує цифрову ідентичність людини, впливає на прийняття управлінських рішень, на доступ до сервісів, соціальну динаміку та навіть на безпеку держави.

Закон України "Про захист персональних даних" (2010 рік) визначає персональні дані як інформацію або сукупність відомостей про фізичну особу, яку можна ідентифікувати або яка вже ідентифікована. До таких даних належать ПІБ, дата народження, адреса, паспортні та контактні відомості, біометрична інформація, дані про стан здоров'я, місце роботи, ідентифікаційний номер, електронні адреси тощо. Таким чином, персональні дані містять інформацію різної чутливості, що потребує диференційованого підходу до їх зберігання та обробки.

В цифровому середовищі документообігу (ЦДО) персональні дані стали надзвичайно важливою категорією. Вони застосовуються не тільки в державних реєстрах чи базах даних медичних, фінансових та освітніх установ, а й у внутрішньому електронному документообігу підприємств. Наприклад, документи, такі як заяви, накази, акти, договори чи анкети, містять вичерпний перелік персональних відомостей. Здебільшого, збереження таких документів відбувається в цифровому вигляді, що вимагає специфічних методів організації інформаційної безпеки.

Особливість цифрової обробки персональних даних полягає в тому, що вони стають постійним «цифровим слідом» людини. В CRM-системах,

електронних медичних картках, онлайн-банкінгу, соціальних мережах - усюди формується структурована інформація про людину. Відповідно виникають нові виклики: персональні дані стають об'єктом аналізу, монетизації та потенційної загрози.

Ключові функції персональних даних у ЦДО можна класифікувати таким чином:

- Ідентифікаційна: забезпечує чітке розпізнавання фізичної особи серед інших суб’єктів системи.
- Авторизаційна: дає змогу отримати доступ до обмежених або захищених цифрових сервісів (через логін-пароль, двофакторну автентифікацію, біометрію тощо).
- Інформаційно-управлінська: використовується для прийняття рішень на основі зібраних даних (наприклад, кадрові процеси, кредитна історія, запис на прийом до лікаря).
- Юридична: фіксує факт укладення угод, надання згоди, подання офіційних заяв або інших правочинних дій у цифровому середовищі.

Систематизація персональних даних за рівнем чутливості дозволяє краще оцінювати ризики. Виділяють наступні категорії:

1. *Загальні дані* (ім’я, вік, адреса);
2. *Особливі категорії* (дані про стан здоров’я, біометрія, релігійні переконання);
3. *Конфіденційні дані* (банківська інформація, ідентифікаційні коди, записи розмов);
4. *Публічні дані* (які за згодою особи доступні широкому загалу – наприклад, через соцмережі).

З технічної точки зору, персональні дані є частиною метаданих у цифрових системах. Їхня роль у базах даних, електронних архівах, системах управління контентом (CMS) визначається через атрибути, що пов'язують окремі об'єкти або дозволяють фільтрувати інформацію за ідентифікатором користувача. Наприклад, в медичному електронному журналі дані пацієнта використовуються

для персоналізованого надання послуг, автоматичного формування звітності та взаємодії з іншими системами охорони здоров'я.

З розвитком хмарних технологій, мобільного доступу та інтернету речей (IoT) персональні дані "розпорошені" в багатьох сервісах, що робить їх більш вразливими. Їхня обробка відбувається на численних платформах: Microsoft 365, Google Workspace, Amazon Web Services, SAP та інших. В такому середовищі головним завданням є впровадження наскрізних стратегій безпеки даних: шифрування, токенізація, багатофакторна аутентифікація, аудит доступу тощо.

З юридичного погляду, сучасні підходи до обробки персональних даних ґрунтуються на принципах, викладених у міжнародних актах, зокрема в Загальному регламенті про захист даних ЄС (GDPR). Відповідно до цих принципів, дані повинні бути:

- Зібрані з чітко визначеною та законною метою;
- Оброблятися прозоро, чесно, в мінімально необхідному обсязі;
- Захищені від несанкціонованого доступу;
- Доступні для перегляду, виправлення або видалення на запит суб’єкта.

Ці принципи є актуальними і для українського правового поля, навіть якщо GDPR формально не застосовується до всіх установ. Адже дедалі частіше організації орієнтуються на нього як на еталонну модель управління даними.

У цілому, роль персональних даних в цифровому документаційно-інформаційному середовищі полягає у створенні інфраструктури довіри. Це основа, на якій тримаються цифрові сервіси, правовідносини, внутрішні процеси підприємств і державні послуги. Тому розробка політики безпеки, навчання персоналу, створення надійних IT-інструментів — це не тільки технічна, а й стратегічна задача організацій, що працюють з такими даними.

### 1.2. Нормативно-правове регулювання захисту персональних даних (Закон України «Про захист персональних даних» тощо)

У контексті цифрової трансформації суспільства питання захисту особистих даних перетворилося на пріоритетний напрямок державної політики та правового регулювання. З одного боку, доступ до особистої інформації є необхідним для надання багатьох публічних та комерційних послуг. З іншого - зростають ризики порушення приватності, зловживання інформацією, її витоку чи використання у незаконний спосіб. Саме тому виникає потреба у розробці комплексної системи нормативного захисту персональних даних, адаптованої до реалій цифрового інформаційного простору.

Правове регулювання захисту особистих даних в Україні базується на Конституції України, нормах міжнародного права, спеціальному законодавстві, підзаконних нормативно-правових актах, а також локальних політиках суб'єктів, що здійснюють обробку даних. Ключову роль у цій системі відіграє Закон України «Про захист персональних даних» № 2297-VI, прийнятий 1 червня 2010 року. Цей закон визначає правові основи діяльності у сфері захисту персональних даних та забезпечує реалізацію одного з базових прав людини — права на приватність.

Закон визначає базову термінологію та структуру правовідносин у сфері обробки даних. Він окреслює такі ключові категорії:

- *персональні дані* — інформація або сукупність відомостей про фізичну особу, яка ідентифікована або може бути ідентифікована;
- *суб'єкт персональних даних* — фізична особа, стосовно якої здійснюється обробка персональних даних;
- *власник бази персональних даних* — фізична або юридична особа, яка визначає мету обробки персональних даних та реалізує контроль за нею;
- *розпорядник* — особа, яка здійснює технічну обробку даних за дорученням власника;
- *третя особа* — будь-яка особа, якій передаються персональні дані, окрім суб'єкта, власника чи розпорядника.

Окрім визначень, закон також визначає *принципи обробки персональних даних*, серед яких: законність, цільове призначення, обмеження за обсягом, точність, безпечність та прозорість.

Окремо слід відзначити закріплення *прав суб'єкта персональних даних*, до яких належать:

- право на інформацію щодо обробки його даних;
- право на доступ до власних персональних даних;
- право вимагати виправлення, блокування або знищення неточних чи незаконно оброблюваних даних;
- право на відкликання згоди;
- право на захист у судовому порядку.

З метою нагляду за дотриманням вимог законодавства у сфері захисту персональних даних, функції контролю покладено на *Уповноваженого Верховної Ради України з прав людини*. Згідно зі статтею 24 Закону, саме цей орган має повноваження проводити перевірки, надавати роз'яснення, розглядати скарги та притягати до відповідальності осіб, які порушили встановлені норми.

Однак, одним лише законом правове регулювання не обмежується. Захист персональних даних в Україні також забезпечується низкою інших нормативно-правових актів, що охоплюють суміжні аспекти:

- *Конституція України* (ст. 32) гарантує кожному право на невтручання в особисте та сімейне життя, забороняє збирання, зберігання, використання та поширення конфіденційної інформації без згоди особи;
- *Цивільний кодекс України* (ст. 270–275) конкретизує право особи на недоторканність приватного життя, а також право на відшкодування збитків у разі його порушення;
- *Кримінальний кодекс України* (ст. 182) встановлює відповідальність за незаконне збирання, зберігання, використання або поширення конфіденційної інформації без згоди особи;

- *Закон України «Про інформацію»* визначає категорії інформації з обмеженим доступом, серед яких і персональні дані, встановлює правила її захисту;
- *Закон України «Про електронні довірчі послуги»* визначає правовий статус електронної ідентифікації, електронного підпису, які тісно пов'язані з персональними даними;
- *Постанова Кабінету Міністрів України № 211 від 25 березня 2006 року* регламентує порядок ведення баз персональних даних, а також повідомлення про їх створення.

До того ж, на рівні організацій, підприємств, державних установ діють *локальні нормативні акти* — положення про обробку та захист персональних даних, інструкції для працівників, політики конфіденційності, договори про нерозголошення (NDA). Вони деталізують вимоги Закону відповідно до специфіки діяльності організації.

Стосовно міжнародного впливу – Україна поступово наближає своє законодавство до європейських стандартів. Особливої актуальності набувають положення *Загального регламенту ЄС про захист даних (GDPR).* Хоча цей документ формально не є чинним в Україні, його часто використовують як *best practice* для побудови внутрішніх політик з обробки персональних даних у компаніях, що мають справу з європейськими контрагентами або споживачами.

Таким чином, нормативно-правова система України щодо захисту персональних даних є багаторівневою, включаючи як загальні норми права, так і спеціальні закони, а також підзаконні та локальні акти. Проте розвиток цифрового середовища, поява нових технологій (штучний інтелект, big data, блокчейн) вимагає постійного вдосконалення цієї системи, впровадження нових стандартів безпеки та формування культури захисту даних серед громадян і працівників організацій.

У контексті постійних трансформацій та технологічного поступу вкрай важливо, щоб нормативне регулювання захисту особистих даних в Україні перебувало у стані безперервного оновлення. Це дає змогу гарантувати

належний рівень захисту прав та свобод людей, особливо в цифровому просторі, де загроза втрати або неправомірного використання інформації істотно збільшилася.

Окрім ключових законів та нормативних актів, підприємства та державні структури повинні активно впроваджувати внутрішні правила, що регламентують діяльність з особистими даними. До цих правил належать конкретні процедури обробки даних, навчання персоналу з питань безпеки даних, а також розробка планів дій у випадку інцидентів, пов'язаних з витоком або порушенням безпеки.

Технічні інструменти захисту, спрямовані на забезпечення безпеки особистих даних, повинні застосовуватися комплексно з правовими засобами. Тільки в такому випадку можна гарантувати надійний захист даних та мінімізувати потенційні ризики. Зважаючи на стрімкий розвиток технологій, необхідно, щоб законодавство не відставало від нових викликів і містило чіткі настанови та вимоги до обробки особистої інформації в різноманітних інформаційних системах.

Отже, наявність чітко визначених нормативно-правових положень є фундаментом для ефективного функціонування систем захисту особистої інформації, створюючи баланс між правом особи на приватність та потребою в обробці даних для реалізації певних соціальних та економічних функцій.

### 1.3. Загрози та вразливості персональних даних у цифрових документаційно-інформаційних системах

З розвитком цифрових технологій, коли обробка персональних даних стала невід’ємною складовою функціонування організацій та державних установ, питання забезпечення їх захисту набуло надзвичайної важливості. У сучасному світі інформація перетворилась на не лише цінний актив, а й об'єкт, що потребує посиленого захисту від різноманітних загроз, як з боку зловмисників, так і від ненавмисних порушень в межах організації. Технічні засоби захисту персональних даних є фундаментом інформаційної безпеки, оскільки вони здатні

ефективно протидіяти зовнішнім і внутрішнім загрозам, забезпечуючи конфіденційність, цілісність та доступність даних.

Технічні засоби захисту персональних даних можливо поділити на декілька категорій, залежно від рівня їх впливу на інформаційну систему та способу застосування. До основних категорій технічних засобів захисту можливо віднести:

1. *Шифрування даних* – один з ключових методів захисту даних. Шифрування забезпечує перетворення даних в недоступну форму, яку може розшифрувати тільки уповноважена особа при наявності відповідного ключа. Існують різні алгоритми шифрування, серед яких виділяють симетричне (AES) та асиметричне (RSA) шифрування. Вибір між ними залежить від типу даних та необхідної швидкості обробки інформації.

2. *Системи аутентифікації та авторизації* – це набір процедур і механізмів, що забезпечують підтвердження особи користувача та визначення рівня доступу до інформації. Найбільш поширені методи аутентифікації включають логін і пароль, біометричні дані, а також багатофакторну аутентифікацію (2FA), яка стає стандартом в багатьох організаціях задля забезпечення додаткової безпеки.

3. *Мережеві екрани та фаєрволи* – фаєрволи (або брандмауери) — це інструменти, що контролюють потоки даних між різними мережами, фільтруючи небажані з’єднання та блокуючи несанкціонований доступ. Вони є головною лінією оборони від атак та вторгнень з боку зловмисників.

4. *Антивірусне програмне забезпечення та системи моніторингу* – ці інструменти сканують систему на наявність шкідливого програмного забезпечення (вірусів, троянів, руткітів), а також відстежують можливі вторгнення або зловмисні дії всередині системи. Вони є важливою складовою безпеки, оскільки можуть попередити про загрози до того, як вони завдадуть шкоди.

5. *Системи резервного копіювання та відновлення* – забезпечують безпеку даних у випадку збоїв або несанкціонованих змін. Регулярне створення

резервних копій критично важливо для забезпечення цілісності та доступності даних, оскільки дає змогу їх відновити у разі втрати.

6. *Технічні засоби моніторингу та аудиту* – відстежують доступ до персональних даних і операції, що з ними здійснюються. Вони дозволяють своєчасно виявляти порушення безпеки, а також здійснювати ретроспективний аналіз подій для виявлення слабких місць у захисті інформаційних систем.

Шифрування даних є одним з найефективніших та найпоширеніших методів захисту персональних даних. Завдяки шифруванню можна гарантувати, що навіть у разі компрометації інформаційної системи, зловмисники не зможуть використати вкрадені дані без доступу до відповідного ключа.

Існують різні методи шифрування. Найбільш поширеними є:

- *Симетричне шифрування* (AES) — цей метод використовує один і той самий ключ для шифрування та розшифрування даних. Він є швидким та ефективним для обробки великих обсягів даних, але потребує безпечного зберігання та передачі ключа.
- *Асиметричне шифрування* (RSA) — використовує пару ключів: публічний для шифрування і приватний для розшифрування. Це дозволяє забезпечити додаткову безпеку, оскільки ключ для розшифрування ніколи не передається.

Шифрування персональних даних стає особливо актуальним в контексті передавання інформації через незахищені канали зв'язку, зокрема через Інтернет. Однак, навіть за допомогою шифрування не можливо повністю виключити вірогідність витоку даних — тому важливо використовувати шифрування в поєднанні з іншими засобами безпеки.

Більш складні та потужні атаки на цифрові системи користуються тим, що традиційні методи аутентифікації (логін та пароль) можуть бути легко зламані. Відтак, інноваційним рішенням для підвищення рівня захисту є *багатофакторна аутентифікація (2FA)*. Цей метод передбачає використання двох або більше факторів для підтвердження особи користувача.

Зазвичай, для багатофакторної аутентифікації використовують:

- *Теоретичні знання* — пароль або PIN-код;
- *Власність* — смарт-картка, телефон, токен або інший пристрій, який генерує одноразовий код;
- *Біометричні дані* — відбитки пальців, розпізнавання обличчя або райдужної оболонки ока.

Застосування багатофакторної аутентифікації суттєво зменшує вірогідність несанкціонованого доступу до системи, оскільки навіть у разі викрадення одного з факторів зловмисникам все одно потрібно отримати доступ до іншого елементу системи аутентифікації.

Збереження даних є одним з ключових завдань будь-якої організації, оскільки втрата персональних даних може призвести до значних фінансових та репутаційних втрат. Одним із способів мінімізації таких ризиків є створення регулярних резервних копій даних.

Резервне копіювання може бути:

- *Локальним* — коли копії зберігаються на внутрішніх серверах або дисках організації.
- *Хмарним* — коли дані зберігаються на віддалених серверах, що забезпечує більшу надійність і доступність в разі фізичних пошкоджень обладнання організації.

Резервне копіювання має бути регулярним та автоматизованим. Це дозволяє організації оперативно відновити дані в разі їх втрати, пошкодження або видалення, тим самим знижуючи можливі наслідки для бізнесу.

Антивірусне програмне забезпечення є необхідним інструментом для захисту від шкідливого програмного забезпечення, яке може пошкодити або вкрасти персональні дані. Воно забезпечує постійну перевірку даних на наявність вірусів, троянів, руткітів та інших загроз.

Системи моніторингу можуть працювати в реальному часі та виявляти підозрілі дії в системі. Вони відстежують доступ до даних, визначають, чи не порушено встановлені правила безпеки, і можуть сигналізувати про можливі атаки або вторгнення.

# РОЗДІЛ 2
# СУЧАСНІ МЕТОДИ ТА ТЕХНОЛОГІЇ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ДОКУМЕНТАЦІЙНО-ІНФОРМАЦІЙНІЙ ДІЯЛЬНОСТІ

## 2.1. Приклади успішної реалізації систем захисту персональних даних у документаційно-інформаційній діяльності

Забезпечення захисту персональних даних в інформаційних системах є критично важливим аспектом безпеки в сучасному цифровому світі. З розвитком цифрових технологій, як у державному, так і в приватному секторах, зростає кількість загроз, пов'язаних із захистом даних. Однак, існують успішні приклади застосування ефективних методик та технологій для забезпечення конфіденційності та цілісності особистої інформації. У цьому підрозділі розглянемо кілька реальних прикладів, що демонструють ефективні стратегії захисту персональних даних у різних галузях.

1. Система захисту персональних даних в державних установах (приклад України)

Одним з яскравих прикладів застосування ефективних систем захисту персональних даних у державному секторі є *система «Дія»* — портал, що надає електронні державні послуги. Для забезпечення безпеки даних в рамках цього проекту використовуються сучасні засоби шифрування та багатофакторна аутентифікація (MFA).

Особливості:

- *Багатофакторна аутентифікація* забезпечує додатковий рівень захисту при доступі до особистих даних.
- *Шифрування* — всі дані, що передаються через платформу, шифруються за допомогою передових алгоритмів, забезпечуючи захист інформації навіть у разі перехоплення.
- *Цифровий підпис* використовується для засвідчення справжності важливих документів, підтверджуючи їхню юридичну силу.

Проблеми та рішення:

Один із ключових викликів полягає в необхідності поєднання доступності послуг для громадян з високим рівнем безпеки. Платформа «Дія» вирішує це питання, використовуючи державні центри обробки даних для забезпечення контролю за безпекою даних, а також технологію блокчейн для забезпечення прозорості транзакцій.

2. Захист персональних даних у фінансовому секторі: CRM-система «Бітрікс24»

Для компаній, які активно використовують персональні дані своїх клієнтів, важливо забезпечити високий рівень захисту. Прикладом такої системи є управління взаємовідносинами з клієнтами — *CRM-система «Бітрікс24».* Система дозволяє автоматизувати роботу з інформацією про клієнтів, зберігаючи їхню конфіденційність та безпеку.

Особливості:

- *Шифрування даних* — дані клієнтів шифруються як під час зберігання, так і під час передачі.
- *Розмежування доступу* — доступ до інформації обмежений згідно з ролями співробітників. Це дозволяє знизити ризик витоку даних через помилки персоналу.
- *Регулярні оновлення безпеки* — система автоматично оновлюється, що забезпечує оперативне реагування на нові загрози.

Проблеми та рішення:

Постійний виклик полягає у необхідності оновлення захисту від нових кіберзагроз. Рішенням є регулярні оновлення платформи та інтеграція з іншими системами безпеки.

3. Медичні інформаційні системи: eHealth в Україні

В Україні успішно реалізовано проект *eHealth*, що є цифровою платформою для обміну медичною інформацією між пацієнтами та медичними закладами. Враховуючи чутливість медичних даних, система має забезпечувати високий рівень захисту.

Особливості:

- *Багатофакторна аутентифікація* та використання *цифрових підписів* для верифікації доступу до медичних карток пацієнтів.
- *Шифрування даних* як під час зберігання в базах даних, так і під час передачі між медичними установами.
- *Обмежений доступ* до даних — інформація доступна лише уповноваженим медичним працівникам або пацієнтам через безпечні канали.

Проблеми та рішення:

Необхідна інтеграція між різними медичними установами, що може створити певні труднощі. Для вирішення цього створена централізована база даних, яка дозволяє уніфікувати доступ до інформації.

4. Захист персональних даних у бізнесі: платформи електронної комерції

Великий обсяг інтернет-магазинів та електронних платформ активно працює з персональними даними клієнтів. Для їхнього захисту використовуються сучасні криптографічні засоби та протоколи безпеки.

Особливості:

- *PCI DSS сертифікація* — стандарти безпеки даних платіжних карт, обов'язкові для всіх онлайн-магазинів, які проводять фінансові операції.
- *Шифрування платежів* за допомогою протоколу SSL/TLS, що забезпечує захист даних під час транзакцій.
- *Регулярний аудит безпеки* для виявлення вразливостей та захисту від атак.

Проблеми та рішення:

Часто виникають труднощі через складність інтеграції між різними платіжними системами. Рішенням є використання надійних постачальників платіжних послуг та постійний моніторинг транзакцій.

Забезпечення захисту особистої інформації - критичний аспект цифрової трансформації, яка охоплює різноманітні галузі економіки та життя. Велика кількість підходів та технологій, що застосовуються для захисту даних, надає можливість обирати найбільш відповідні способи, враховуючи особливості

діяльності організації та потенційні ризики, з якими стикаються організації та компанії. Аналіз та зіставлення методів та технологій захисту персональних даних у різних сферах сприяє кращому розумінню їх сильних та слабких сторін.

У таблиці 2.1 представлено порівняльний аналіз методів захисту особистої інформації у чотирьох ключових сферах: наданні державних послуг, фінансовому секторі, медицині та електронній коммерції. Для кожної сфери детально описано використані методи та технології захисту, а також висвітлено основні проблеми, що виникають у процесі їх впровадження, та запропоновано можливі рішення для їх вирішення.

Таблиця 2.1

Порівняльний аналіз методів захисту персональних даних у різних сферах діяльності

| **Сфера діяльності** | **Методи захисту** | **Використовувані технології** | **Проблеми та рішення** |
|---|---|---|---|
| Державні послуги (платформа «Дія») | Шифрування, багатофакторна автентифікація, цифровий підпис | Блокчейн, дата-центри державні | Баланс між доступністю та безпекою, конфіденційність |
| Фінансовий сектор (CRM «Бітрікс24») | Шифрування даних, розмежування доступу | Шифрування, VPN, регулярні оновлення | Оновлення безпеки, інтероперабельність |
| Медицина (eHealth) | Багатофакторна автентифікація, шифрування | Централізована база даних, цифрові підписи | Інтеграція між медичними установами |
| Електронна комерція | SSL/TLS, PCI DSS, шифрування | SSL сертифікати, платіжні системи | Інтеграція платіжних систем, аудити безпеки |

Порівняння різноманітних стратегій захисту особистих даних у різних сферах дає змогу виокремити ключові моменти. Наприклад, криптографія, багатофакторна ідентифікація та розподіл прав доступу вважаються загальноприйнятими засобами захисту, котрі застосовуються майже повсюдно. Але для кожної конкретної діяльності необхідно адаптувати специфічні

технології та методології, беручи до уваги специфіку оперування персональними відомостями.

Шляхом ретельного добору інструментарію захисту та налагодженої взаємодії між різними системами можна гарантувати високий рівень безпеки особистих даних, що набуває критичної значущості в нинішньому цифровому світі.

Успішне впровадження систем захисту персональних даних у різних галузях демонструє важливість забезпечення належного захисту для підтримки довіри клієнтів та забезпечення безпеки в умовах цифрових перетворень. Незалежно від сфери діяльності, використання сучасних технологій шифрування, аутентифікації та моніторингу доступу є ключовим для запобігання несанкціонованому доступу та витоку даних. При цьому важливо враховувати специфіку кожної галузі та постійно удосконалювати механізми захисту для забезпечення високого рівня безпеки.

## 2.2. Основні принципи кібербезпеки документаційно-інформаційної діяльності та захисту персональних даних

Захист особистих даних та кібербезпека в документаційно-інформаційній сфері є фундаментом для безпечного функціонування інформаційних систем, особливо в ситуації, коли організації та установи активно використовують цифрові платформи для обробки та збереження даних. В сучасному світі інформація стає одним з найцінніших ресурсів, тому захист особистих даних потребує суворого дотримання принципів кібербезпеки, які забезпечують цілісність, конфіденційність і доступність інформації.

Принципи кібербезпеки слугують основою, що визначає, як організації повинні захищати свої інформаційні ресурси та особисті дані. В контексті документаційно-інформаційної діяльності ці принципи мають особливе значення, оскільки обробка, збереження та передача даних включають велику кількість осіб та інтересів, що вимагає застосування відповідних заходів безпеки.

1. Принцип мінімального доступу (Least Privilege)

*Принцип мінімального доступу* передбачає, що користувачі та системи мають мати доступ лише до тих ресурсів та даних, які необхідні для виконання їх обов’язків. Цей принцип є важливим у сфері кібербезпеки, оскільки він зменшує ймовірність несанкціонованого доступу до конфіденційної інформації, а також допомагає обмежити шкоду у випадку порушення безпеки.

В рамках цього принципу необхідно:

- Чітко визначити рівні доступу до даних.
- Надавати доступ лише на час виконання конкретних завдань.
- Враховувати ролі користувачів та дозволи на виконання операцій.

Прикладом може слугувати система управління доступом на основі ролей (RBAC), що дозволяє обмежити доступ до документів або баз даних в залежності від ролі користувача в організації.

У зв'язку з принципом мінімального доступу, важливо встановити рівні доступу до інформаційних ресурсів, аби обмежити доступ користувачів лише тим, що є необхідним для їх робочих обов'язків. Це дозволить мінімізувати ризик несанкціонованого доступу та неправильного використання даних. У (Табл 2.2) можна навести порівняння типів доступу в організаціях, щоб чітко визначити, хто і до яких ресурсів має доступ.

Таблиця 2.2

Порівняння типів доступу в організаціях

| **Тип достопу** | **Опис** | **Приклад застосування** |
|---|---|---|
| Повний доступ | Користувач має право на виконання всіх операцій із даними | Адміністратор системи |
| Обмежений доступ | Користувач має обмежений доступ до певних даних або ресурсів | Працівник відділу обробки даних |
| Читання | Користувач може лише переглядати дані, не маючи прав на редагування | Клієнт, який має доступ до своєї особистої інформації |

Як видно з таблиці 2.2, типи доступу визначають рівень взаємодії користувача з інформацією в системі. Повний доступ надається, як правило, адміністраторам або високопосадовим особам, які відповідають за управління системою та її ресурсами. Обмежений доступ дозволяє користувачам працювати лише з конкретними даними або частинами інформаційної системи, що необхідні для виконання їх обов'язків, наприклад, для співробітників, які займаються обробкою даних. Тип "Читання" дозволяє користувачам лише переглядати інформацію без можливості її змінювати, що є важливим для доступу до особистих даних клієнтів або інших обмежених ресурсів організації.

Такий підхід сприяє дотриманню принципу мінімального доступу та дозволяє організаціям ефективно управляти своїми ресурсами, одночасно мінімізуючи ризики витоку чи неправомірного використання особистих даних.

2. Принцип конфіденційності (Confidentiality)

*Конфіденційність* є одним з найважливіших аспектів захисту особистих даних. Вона означає, що особисті дані та інформація повинні бути захищені від несанкціонованого доступу. Це досягається шляхом шифрування даних, використання паролів, багатофакторної аутентифікації та політик безпеки, які вимагають від користувачів дотримання правил конфіденційності.

Основні заходи для забезпечення конфіденційності:

- *Шифрування даних*: використання надійних алгоритмів шифрування (AES, RSA) для захисту даних під час зберігання та передачі.
- *Багатофакторна аутентифікація (MFA)*: додатковий рівень безпеки для перевірки особи користувача.
- *Паролі*: використання складних паролів та регулярне їх оновлення.

Заходи конфіденційності не лише захищають дані від несанкціонованого доступу, але й зміцнюють довіру клієнтів та партнерів до організації.

3. Принцип цілісності (Integrity)

*Цілісність даних* гарантує, що інформація не може бути змінена без авторизації. В області документаційно-інформаційної діяльності це важливо,

оскільки будь-які зміни в особистих даних без належного дозволу можуть призвести до серйозних юридичних та фінансових наслідків.

Основні заходи для забезпечення цілісності:

- *Контроль версій*: система управління версіями дозволяє відслідковувати всі зміни в документах та даних.
- *Цифрові підписи*: гарантують, що дані або документи не були змінені після підписання.
- *Аудит змін*: ведення журналів змін дозволяє відслідковувати всі маніпуляції з даними та виявляти підозрілі дії.

4. Принцип доступності (Availability)

*Доступність* передбачає, що інформаційні ресурси повинні бути доступні уповноваженим користувачам у будь-який час. Забезпечення доступності даних є критичним для нормального функціонування організації, особливо тоді, коли час відгуку на запити є важливим фактором.

Засоби забезпечення доступності:

- *Захист від DDoS-атак*: використання систем захисту від розподілених атак відмови в обслуговуванні.
- *Резервне копіювання*: регулярне створення резервних копій даних для запобігання втратам при збоях.
- *Плани аварійного відновлення (Disaster Recovery Plan)*: детальний план, який визначає кроки для відновлення даних та систем у разі катастрофічних подій.

5. Принцип аудиту та моніторингу

*Аудит та моніторинг* передбачає постійний контроль за доступом до особистих даних та ведення журналів дій користувачів. Цей принцип дозволяє виявляти підозрілу активність та реагувати на потенційні загрози в реальному часі.

Засоби моніторингу:

- *Системи виявлення вторгнень (IDS)*: допомагають виявляти та запобігати спробам несанкціонованого доступу.

- *Аудит доступу*: ведення журналів доступу до особистих даних дозволяє відстежувати, хто і коли звертався до інформації.

6. Принцип безперервного навчання персоналу

Кожен працівник, який має доступ до особистих даних, повинен бути обізнаним з актуальними кіберзагрозами, політиками безпеки та стандартами поводження з конфіденційною інформацією. Безперервне навчання персоналу допомагає зменшити ризики, пов’язані з людським фактором.

Програми навчання повинні включати:

- Оновлені знання про актуальні загрози.
- Тренінги з кібербезпеки та дотримання політик організації.
- Оцінку знань через регулярні тести та сертифікацію.

7. Принцип резервного копіювання та плану відновлення

*Резервне копіювання* є одним з ключових елементів захисту даних від втрати через кібератаки, технічні збої чи природні катастрофи. План відновлення дозволяє організації оперативно відновити дані та повернутися до звичайної роботи.

Ключові аспекти резервного копіювання:

- Регулярне створення резервних копій.
- Зберігання копій у різних фізичних та хмарних локаціях.
- Перевірка працездатності системи відновлення даних.

8. Принцип захисту периметра та мережевої інфраструктури

Захист периметра та мережевої інфраструктури створює бар'єр між внутрішніми інформаційними системами та зовнішніми загрозами. Включає використання брандмауерів, VPN, систем виявлення вторгнень (IDS), а також сегментацію мережі для обмеження доступу до чутливих даних.

9. Принцип актуальності програмного забезпечення

Оновлення програмного забезпечення має критичне значення для захисту інформаційних систем від нових уразливостей. Вчасне встановлення оновлень програмного забезпечення допомагає уникнути використання зловмисниками відомих вразливостей.

10. Принцип відповідності законодавству

Захист особистих даних має здійснюватися у відповідності до вимог чинного законодавства, зокрема до *Закону України «Про захист персональних даних»* та інших нормативних актів. Це гарантує правомірність обробки даних та захист інтересів громадян.

Кібербезпека в документаційно-інформаційній діяльності є надзвичайно важливою для захисту особистих даних. Застосування принципів кібербезпеки забезпечує цілісність, конфіденційність і доступність інформаційних систем, знижує ризики витоків та атак, а також гарантує законну та стабільну обробку особистої інформації. Комплексний підхід до захисту даних, який включає аудит, моніторинг, навчання персоналу та відповідність законодавству, є ключем до безпечної діяльності організації в цифрову епоху.

### 2.3. Захист персональних даних у хмарних сервісах

У сучасному цифровому ландшафті хмарні сервіси стали незамінним елементом діяльності з документообігу та управління інформацією як у державних, так і в приватних структурах. Вони надають можливість зберігати, обробляти та синхронізувати значні обсяги інформації без необхідності утримання фізичної IT-інфраструктури. Проте разом з перевагами хмарних технологій виникають серйозні виклики в питаннях безпеки, зокрема, у контексті обробки особистих даних, які особливо вразливі до кіберзагроз.

Хмарні обчислення передбачають збереження інформації не на локальних комп’ютерах чи серверах організації, а на віддалених платформах, які належать стороннім провайдерам. Це відкриває доступ до масштабованості, високої доступності, автоматизованих оновлень, резервного копіювання та можливості підтримки великої кількості користувачів одночасно. У той же час, така модель зберігання даних породжує ряд викликів у сфері безпеки:

- *Невизначеність місця розташування даних:* часто важко точно встановити, у якій країні чи юрисдикції фізично зберігається інформація.

- Правові та регуляторні ризики: відповідність вимогам законодавства (GDPR, ЗУ «Про захист персональних даних», ISO/IEC 27018 тощо) може ускладнюватися, особливо, якщо хмарні провайдери розташовані за межами України.

- *Небезпека несанкціонованого доступу:* через помилки конфігурації, фішингові атаки, відсутність шифрування або зловживання повноваженнями.

- *Залежність від провайдера:* організація втрачає повний контроль над інфраструктурою та безпосереднім адмініструванням даних.

Для ефективного захисту персональної інформації в умовах застосування хмарних рішень необхідно комбінувати технічні, організаційні та юридичні підходи. Далі розглянемо основні заходи, що формують сучасну систему захисту в хмарних середовищах.

1. Шифрування інформації (Encryption)

Шифрування — це обов'язкова вимога в будь-якій хмарній моделі. Користувачі повинні впроваджувати як *шифрування під час передачі* (TLS, SSL), так і *шифрування на сервері* (AES-256, RSA), щоб забезпечити захист даних навіть у разі перехоплення.

Особливу увагу слід приділити управлінню ключами. Найбезпечнішим варіантом є, коли організація самостійно генерує та зберігає ключі шифрування (Bring Your Own Key, BYOK), замість покладатися на провайдера.

2. Багатофакторна аутентифікація (Multi-Factor Authentication, MFA)

MFA значно зменшує ризик несанкціонованого доступу до хмарного середовища. Навіть якщо пароль буде викрадено, другий фактор (наприклад, смс-код, push-сповіщення або біометрія) унеможливить доступ зловмисника.

3. Управління доступом та ролями

Контроль доступу — одна з ключових практик інформаційної безпеки. Важливо впроваджувати *принцип мінімальних привілеїв (Least Privilege)*, згідно з яким кожному користувачу надається лише такий обсяг доступу, який потрібен для виконання його функцій.

У хмарному середовищі можливе використання різних рівнів доступу, як продемонстровано в (Табл. 2.3)

Таблиця 2.3

Порівняльна характеристика типів доступу в організаціях

| **Тип доступу** | **Опис** | **Приклад застосування** |
|---|---|---|
| Повний доступ | Користувач має право на виконання всіх операцій | Адміністратор системи |
| Обмежений доступ | Доступ лише до окремих ресурсів або функцій | Працівник відділу обробки даних |
| Доступ на читання | Можна переглядати дані без можливості змін | Клієнт, який переглядає свої особисті дані |

4. Логування та моніторинг активності

Усі дії користувачів у хмарному середовищі мають фіксуватися. Це дає змогу відстежувати підозрілу активність, проводити аудит доступу та розслідувати інциденти.

Рекомендовано використовувати інструменти SIEM (Security Information and Event Management), які автоматично аналізують поведінку користувачів і сповіщають про потенційні загрози.

5. Запровадження політик безпеки та DPA

Організація повинна укладати з хмарним провайдером *угоду про обробку даних (Data Processing Agreement, DPA)*, яка чітко регламентує:

- яка інформація зберігається;
- які цілі обробки;
- які заходи безпеки застосовуються;
- хто відповідає у разі витоку.

Такі документи повинні відповідати національному законодавству та європейському GDPR.

6. Вибір сертифікованих хмарних провайдерів

Не всі хмарні рішення однаково безпечні. Надійними вважаються ті, що відповідають міжнародним стандартам:

- *ISO/IEC 27001* — система управління інформаційною безпекою;
- *ISO/IEC 27018* — захист персональних даних у хмарному середовищі;
- *SOC 2* — аудит безпеки, доступності, конфіденційності та цілісності даних.

Ці сертифікати гарантують, що провайдер дотримується найкращих практик безпеки.

7. Регулярне резервне копіювання (Backups)

Важливо переконатися, що хмарний сервіс автоматично створює *резервні копії* даних та надає можливість їх оперативного відновлення. Це вкрай важливо при атаках типу ransomware, технічних збоях або випадковому видаленні інформації.

8. Захист каналів зв’язку

Обмін інформацією між клієнтськими пристроями та хмарною інфраструктурою повинен здійснюватися через захищені канали — VPN, SSL/TLS. Це унеможливлює перехоплення даних у процесі передачі.

9. Проведення оцінки ризиків та тестування

Періодичний *аудит хмарного середовища* дозволяє виявити вразливості. Рекомендується не рідше одного разу на рік проводити пентестинг (penetration testing) та аудит відповідності політикам безпеки.

Захист персональних даних у хмарних сервісах — це не лише питання технічної реалізації, але й комплексна стратегія управління ризиками. Застосування шифрування, багатофакторної аутентифікації, обмеження доступу, вибір сертифікованих провайдерів, юридичне оформлення взаємовідносин — усе це формує систему безпеки, здатну забезпечити конфіденційність та цілісність інформації навіть у відкритому цифровому середовищі.

Роль користувача також є критичною: без відповідального ставлення до облікових даних, дотримання політик та систематичного моніторингу навіть найнадійніша хмара не зможе гарантувати повний захист.

У наш час, коли гібридні атаки стають все більш частими, штучний інтелект використовується в кіберзлочинних кампаніях, а віддалена робота стає звичним явищем, традиційні засоби захисту не гарантують повної безпеки. Актуальною загрозою залишаються атаки через ланцюг постачання – supply chain attacks, що використовують вразливості в залежностях хмарного провайдера. Злам навіть одного з підрядників може відкрити доступ до критичної інформації всіх клієнтів системи.

Ще одним ризиком є shadow IT — використання співробітниками сторонніх хмарних сервісів, таких як Google Drive чи Dropbox, без узгодження з IT-відділом. Ці сервіси часто не перевіряються на відповідність політиці безпеки організації, що відкриває можливості для витоку даних.

Сучасна модель безпеки в хмарному середовищі базується на концепції Zero Trust — принципі «нікому не довіряй, все перевіряй». Це означає постійну перевірку авторизованих користувачів та пристроїв на всіх рівнях доступу. Впровадження Zero Trust мінімізує ризик внутрішніх загроз та ускладнює рух атак всередині хмарного середовища.

Сучасні хмарні рішення дедалі частіше інтегрують модулі штучного інтелекту (AI) та машинного навчання (ML). Вони автоматично виявляють аномальну активність: спроби входу з незвичних місць, масове завантаження даних, підозрілі зміни в політиках доступу. Наприклад, Microsoft Defender for Cloud та AWS GuardDuty використовують ML для динамічного виявлення загроз.

Одним з найгучніших прикладів став витік даних користувачів Dropbox у 2022 році. Зловмисники отримали доступ до внутрішнього коду та API-ключів через скомпрометовану обліковку співробітника з доступом до GitHub-репозиторіїв. Навіть попри всі засоби захисту, атака мала значні наслідки.

Інший приклад – витік даних клієнтів Capital One через помилку в налаштуваннях AWS, що дозволила отримати доступ до 100 мільйонів записів.

Цей випадок підкреслює, що людський фактор та неправильна конфігурація залишаються основними слабкими місцями навіть найсучасніших систем.

Важливо підкреслити, що жодна технічна система не є повністю безпечною, якщо користувачі нехтують основами кібергігієни. Використання слабких паролів, повторне використання облікових записів на різних платформах, ігнорування оновлень – все це полегшує роботу зловмисникам.

Тому формування культури кібербезпеки серед персоналу є обов'язковою складовою захисту в хмарному середовищі. Регулярні тренінги, імітації фішингу та ознайомлення з політиками безпеки повинні бути нормою для кожної організації.

Підсумовуючи, захист персональних даних у хмарних сервісах — це постійний процес, що потребує вдосконалення інструментів, процедур та свідомості користувачів. Застосування сучасних підходів, таких як Zero Trust, використання AI для оцінки ризиків та посилення людського фактору, дозволяє значно підвищити рівень безпеки навіть у найбільш ризикованих цифрових середовищах.

# РОЗДІЛ 3
# ТЕНДЕНЦІЇ РОЗВИТКУ ТА ВПРОВАДЖЕННЯ СИСТЕМ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У МЕДИЧНОМУ ЗАКЛАДІ

## 3.1. Реалізація новітніх методів захисту даних в документаційно-інформаційній діяльності клініки Viva

У сучасній цифровій реальності охорони здоров'я питання забезпечення кібербезпеки та захисту інформації про пацієнтів набуло надзвичайної актуальності. Активне використання електронних систем, зокрема телемедицини, мобільних додатків та хмарних сервісів, хоча й сприяє підвищенню якості медичного обслуговування, також супроводжується зростанням ризиків витоку конфіденційних даних. Цей розділ зосереджений на аналізі сучасних підходів до захисту персональних даних у медичній сфері, а також на прикладі практичного досвіду впровадження інформаційної безпеки в приватній клініці Viva, де проходила переддипломна практика.

Під час проходження практики у приватній медичній установі Viva було проведено ретельний аналіз політик, інструментів та процедур, що спрямовані на забезпечення захисту персональних даних. Viva – це сучасна багатопрофільна медична установа, яка надає як первинну, так і спеціалізовану медичну допомогу, використовуючи передові цифрові рішення для управління інформацією про пацієнтів.

В медичній інформаційній системі (МІС), що використовується в клініці, зберігання, обробка та передавання персональних даних пацієнтів здійснюються з неухильним дотриманням принципів конфіденційності, цілісності та доступності. Система базується на хмарній архітектурі, що забезпечує зберігання великих обсягів даних та оперативний доступ до них, однак це також вимагає особливої уваги до питань кібербезпеки.

Основні впроваджені методи захисту:

- Багатофакторна автентифікація. Доступ до системи забезпечується через багаторівневу перевірку, включаючи паролі, SMS-коди та біометричні дані для певних категорій співробітників.
- Шифрування даних. Інформація, що передається між клієнтом та сервером, автоматично шифрується з використанням протоколів TLS/SSL. Для зберігання даних використовується AES-256, один із найнадійніших алгоритмів шифрування.
- Розмежування прав доступу. Співробітники мають доступ лише до тих розділів системи, які відповідають їхнім посадовим обов'язкам. Адміністрація регулярно проводить аудити доступів.
- Журнали активності користувачів. Вся діяльність у системі автоматично фіксується. При виявленні підозрілої активності система генерує сповіщення адміністратору безпеки.
- Резервне копіювання. Щоденне створення резервних копій (бекапів) забезпечує захист даних від втрати у разі технічних збоїв або кібератак. Копії зберігаються в захищених дата-центрах у зашифрованому вигляді.
- Політика навчання персоналу. Клініка проводить квартальні тренінги з питань інформаційної безпеки. Співробітники навчаються виявляти фішингові листи, дотримуватися правил роботи з даними пацієнтів тощо.

Важливим кроком стало також впровадження *внутрішньої політики реагування на інциденти*, яка визначає порядок дій у разі витоку, злому або втрати інформації. Це дозволяє мінімізувати наслідки та оперативно повідомити відповідні органи відповідно до вимог законодавства.

Не дивлячись на високий рівень організації кібербезпеки, в процесі аналізу системи були виявлені деякі недоліки та сфери ризику:

1. Локалізація зберігання даних. Розміщення даних на хмарному сервері, точне фізичне розташування якого невідоме, створює невизначеність з юридичної точки зору.

2. Залежність від стороннього провайдера. Вся система функціонує на основі інфраструктури сторонньої компанії. У разі збоїв або хакерської атаки на сервіс-провайдера, клініка втрачає доступ до даних.

3. Недостатня інтеграція систем. Частина паперової документації все ще існує паралельно з електронною, що може призвести до дублювання або невідповідності даних.

4. Недостатній рівень цифрової грамотності частини персоналу. Незважаючи на навчання, деякі співробітники не дотримуються базових правил кібергігієни, наприклад, використовують прості паролі або залишають комп'ютери без блокування.

Враховуючи виявлені проблеми та з метою підвищення рівня кіберзахисту в клініці Viva, рекомендується впровадити наступні заходи:

1. Створення локального резервного центру зберігання даних — на випадок збою хмарної системи медичний заклад матиме можливість оперативно відновити критично важливу інформацію.

2. Впровадження архітектури Zero Trust — новий підхід до інформаційної безпеки, що передбачає постійну перевірку кожного користувача та пристрою незалежно від їх місцязнаходження в мережі.

3. Оцифрування решти паперового документообігу — переведення історії хвороб, заяв, анкет тощо в цифровий формат із забезпеченням захисту.

4. Регулярний аудит вразливостей — залучення зовнішніх організацій для проведення пентестів (тестування на проникнення) з метою виявлення слабких місць у МІС.

5. Програми мотивації для персоналу — наприклад, гейміфікація навчання з кібербезпеки або нагородження тих, хто пройшов відповідні курси.

Світовий досвід свідчить про зростаючі інвестиції медичних установ у сферу кіберзахисту. Основні тренди:

- Використання штучного інтелекту для виявлення загроз — AI-системи здатні аналізувати поведінку користувачів у режимі реального часу та виявляти підозрілі дії до виникнення інциденту.

- Автоматизація управління доступом — сучасні IAM (Identity and Access Management) системи дозволяють централізовано контролювати всі точки входу до систем.
- Посилення міжнародного законодавства — такі регулювання, як європейський GDPR або американський HIPAA, передбачають суворіше ставлення до персональних даних.
- Поширення мультихмарних рішень — організації відходять від залежності від одного провайдера, розподіляючи ресурси між декількома сервісами.

Проведене дослідження продемонструвало, що приватна клініка Viva має достатньо розвинену систему захисту персональних даних, що відповідає ключовим вимогам законодавства та технологічним стандартам. Разом з тим, певні ризики залишаються актуальними, і для їх усунення необхідна стратегія постійного вдосконалення. Запропоновані заходи мають забезпечити підвищення рівня безпеки, мінімізувати вплив людського фактору та збільшити стійкість до нових кіберзагроз. В контексті загальних тенденцій цифрової трансформації медицини, впровадження сучасних методів захисту даних стає не просто вимогою часу, але й ключовою конкурентною перевагою на ринку медичних послуг.

### 3.2. Аналіз реальних кейсів витоків персональних даних на прикладі клініки Viva

У сучасному цифровому просторі, питання охорони особистої інформації у медичних закладах стало надзвичайно актуальним. Це зумовлено високою чутливістю медичних даних, що стосуються самопочуття, встановлених діагнозів, методів лікування, медичних обстежень та інших особистих аспектів життя пацієнтів. Навіть незначне виточування таких відомостей може призвести не тільки до порушення законодавчих норм, але й до значного погіршення репутації клініки, судових процесів, падіння довіри пацієнтів і фінансових збитків.

1. Основні проблеми витоків медичних особистих даних

Витоки у сфері охорони здоров'я часто відбуваються через такі чинники:

- Людський фактор – необережне поводження з інформацією, помилки персоналу.
- Недостатній контроль доступу – коли доступ до інформації мають працівники, які не повинні мати доступу згідно з їхніми обов'язками.
- Застарілі або вразливі інформаційні системи, які не отримують оновлень безпеки.
- Атаки зловмисників (хакерів) – фішинг, шкідливе програмне забезпечення, підбір паролів тощо.
- Використання неліцензованих хмарних сервісів.
- Неправильне ведення журналів реєстрації доступу та дій користувачів.

Щоб наочніше продемонструвати ці загрози, наведено узагальнюючу таблицю 3.1 типових причин витоків.

Таблиця 3.1

Основні причини витоків персональних даних у медичних установах

| **Причина витоку** | **Частота випадків (%)** | **Приклад/Пояснення** |
|---|---|---|
| Людський фактор | 42% | Помилкове надсилання даних не тим адресатам |
| Слабкі паролі/відсутність MFA | 23% | Одноразовий пароль або загальні облікові записи |
| Відсутність шифрування | 14% | Дані зберігаються у відкритому вигляді |
| Атаки ззовні | 12% | Хакерські атаки на сервери клініки |
| Інсайдерська загроза | 6% | Доступ до даних отримує співробітник без потреби |
| Інше | 3% | Пошкодження носіїв, втрати, технічні збої |

Клініка Viva застосовує сучасну медичну інформаційну систему, розроблену на основі хмарної архітектури. Проте, як і кожна цифрова система, вона не є абсолютно захищеною від потенційних загроз. Упродовж останніх двох років, під час проведення внутрішніх аудитів, було виявлено низку інцидентів, які, хоч і не спричинили масштабних витоків, але вказали на наявність певних ризиків. Один із таких кейсів став основою для проведення більш детального аналізу.

У другому кварталі 2023 року в клініці Viva було зареєстровано внутрішній інцидент, що був пов’язаний з тим, що один з молодих лікарів-інтернів отримав необмежений доступ до електронних карток пацієнтів з інших підрозділів. Причиною цього виявилось неправильне налаштування правила доступу в МІС після чергового оновлення програмного забезпечення.

Аналіз інциденту:

- Дата інциденту: травень 2023 року
- Суть порушення: Надання доступу до конфіденційної інформації працівникові без необхідного рівня авторизації
- Час виявлення: через 2 дні після зміни прав доступу
- Виявлено: Службою інформаційної безпеки клініки
- Вплив: Потенційно могли бути переглянуті близько 450 електронних карток
- Дії у відповідь:
  - Миттєве блокування облікового запису
  - Проведення аудиту змін у системі
  - Відновлення правил доступу відповідно до політик
  - Організація повторного навчання для ІТ-відділу та персоналу

Таблиця 3.2

Оцінка ризику (за шкалою STRIDE)

| **Категорія загрози** | **Наявність (+/-)** | **Коментар** |
|---|---|---|
| S – Spoofing | - | Не виявлено шахрайства в особистості |
| T – Tampering | - | Не виявлено змін у даних |
| R – Repudiation | + | Потенційна відсутність доказів доступу |
| I – Information Disclosure | + | Можливе несанкціоноване ознайомлення |
| D – Denial of Service | - | Відсутні ознаки |
| E – Elevation of Privilege | + | Надмірні права доступу без потреби |

Цей випадок не став публічним розголосом, проте виявив серйозні недогляди в системі управління правами доступу. Це підкреслило потребу в регулярних перевірках, оновленні правил безпеки та навчанні працівників.

У разі виявлення потенційного витоку даних, клініка Viva розробила чіткий алгоритм дій, який включає в себе:

- Негайне сповіщення відповідальних осіб (ІТ-відділ, служба безпеки, адміністрація);
- Ізолювання джерела витоку, наприклад, блокування скомпрометованого акаунту або пристрою;
- Проведення внутрішнього розслідування, зокрема, аудит журналів, перевірка прав доступу, аналіз шляхів передачі даних;
- Оцінка обсягу витоку, визначення, які саме особисті дані могли бути скомпрометовані (ПІБ, дані паспорту, медична історія, результати аналізів тощо);
- Повідомлення постраждалих осіб (відповідно до Закону України «Про захист персональних даних»);
- Звіт до відповідних органів — у випадку серйозного порушення конфіденційності.

Такий підхід дозволяє оперативно локалізувати загрозу, мінімізувати наслідки та підвищити довіру пацієнтів до закладу.

Будь-який інцидент із витоком персональних даних у сфері охорони здоров'я – це не просто технічна проблема. Це передусім:

- Удар по репутації медичної установи;
- Втрата довіри пацієнтів;
- Ризик судових позовів, особливо, якщо йдеться про розголошення конфіденційної медичної інформації;
- Накладення штрафів згідно з чинним законодавством (у т.ч. міжнародними нормами, якщо пацієнти — іноземці).

У випадку Viva, завдяки швидким діям, заклад уникнув серйозних юридичних проблем, проте був змушений вжити заходів для покращення політики безпеки.

Випадки витоків особистих даних у клініці Viva показали кілька ключових тенденцій:

1. Людський фактор залишається основною вразливою точкою - навіть найкращі технічні засоби можуть бути безсилі перед недбалістю чи некомпетентністю співробітників.
2. Використання незареєстрованих пристроїв (наприклад, флешок або смартфонів) часто є джерелом витоку.
3. Застаріле або не оновлене програмне забезпечення може мати відомі слабкі місця, які легко використовуються.
4. Недостатній контроль за правами доступу призводить до того, що співробітники бачать більше інформації, ніж їм потрібно.

На основі досліджених випадків, для покращення інформаційної безпеки у Viva доцільно вжити таких заходів:

- Впровадити політику Zero Trust, що ґрунтується на постійній перевірці кожного запиту незалежно від джерела (внутрішнього чи зовнішнього).

- Розширити аудит доступу, використовуючи поведінковий аналіз для виявлення підозрілих дій.
- Інтегрувати SIEM-систему (Security Information and Event Management) — для автоматичного моніторингу, виявлення загроз та реагування в реальному часі.
- Використовувати багаторівневу систему резервного копіювання, включаючи окремі хмарні та локальні сховища, із шифруванням і аутентифікацією.
- Регулярно проводити пентести — симуляції атак для перевірки стійкості системи до злому.
- Навчання персоналу має бути практичним, а не формальним — з реальними прикладами, інтерактивними тренінгами, перевірками знань.

Оцінюючи майбутнє Viva, варто відзначити позитивну динаміку:

- Створення *відповідального центру з кібербезпеки* на базі клініки, який буде координувати всі заходи з ІБ;
- Використання *хмарних рішень з нульовим знанням* (zero-knowledge encryption), що повністю унеможливлює доступ постачальника до змісту даних;
- Розробка *стратегії кіберстійкості* клініки на 2025–2028 роки, враховуючи зміни в законодавстві, появу нових загроз (наприклад, deepfake-атаки, викрадення даних через IoMT — Інтернет медичних речей) та нові стандарти (GDPR, HIPAA).

Як демонструє (Рис.1), у 2023 році лідирували за кількістю інцидентів помилки співробітників (6 випадків), поряд з несанкціонованим доступом до систем. У 2024 році відмічено зменшення випадків, що стало результатом реалізації заходів з інформаційної безпеки, хоча вразливості залишаються актуальними. Ці дані підкреслюють важливість безперервного оновлення політик безпеки та регулярного навчання персоналу.

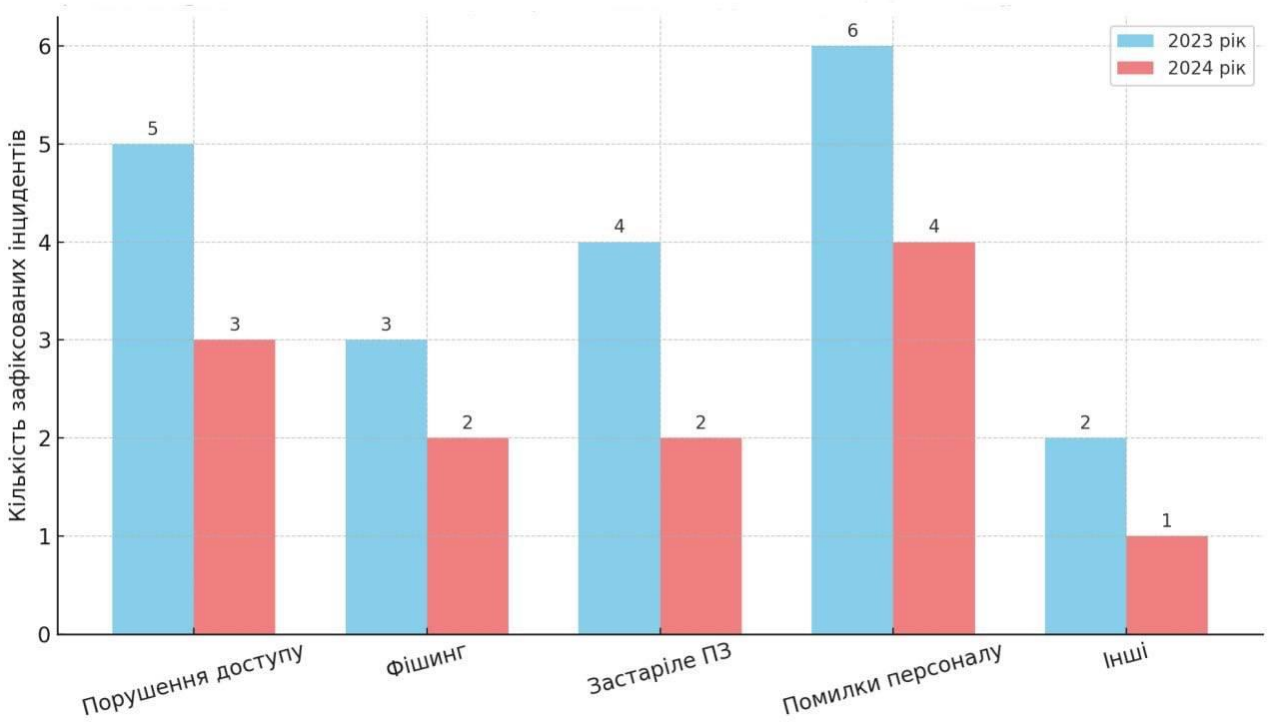


Рисунок 2.1 – Кількість інцидентів витоку персональних даних у клініці Viva (2023-2024 рр.)

Проведений аналіз реальних випадків витоку персональних даних у клініці Viva дозволив сформулювати низку важливих висновків щодо поточного стану інформаційної безпеки в медичному секторі. Встановлено, що, незважаючи на загалом задовільний рівень технічного захисту, найбільш критичними залишаються проблеми, пов’язані з людським фактором, помилками адміністрування та недостатнім контролем доступу.

Інциденти, виявлені під час проходження практики, показали актуальність загроз як зі сторони зовнішніх атак, так і зі сторони внутрішніх порушень режиму безпеки. У більшості випадків витоки стали можливими через невиконання політик інформаційної безпеки, використання сторонніх пристроїв, відсутність сучасних механізмів моніторингу та несвоєчасне оновлення програмного забезпечення.

Незважаючи на це, позитивним фактором є швидка та організована реакція керівництва клініки на виявлені загрози. Вжиті заходи вказують на прагнення до впровадження сучасних методів захисту, включаючи Zero Trust-архітектуру,

поглиблений аудит дій користувачів та автоматизовані системи моніторингу подій безпеки.

Підсумовуючи, можна дійти висновку, що для забезпечення надійного захисту персональних даних у медичних закладах необхідно не тільки модернізувати технічні засоби, але й формувати культуру безпеки серед персоналу. Тільки комплексний підхід — технічний, організаційний та освітній — дозволяє досягти стійкості до сучасних кіберзагроз.

### 3.3. Рекомендації для підвищення безпеки персональних даних документаційно-інформаційному забезпеченні діяльності клініки Viva

У теперішньому цифровому просторі безпека особистих відомостей в медичній сфері надзвичайно важлива як з юридичного, так і з морального боку. Аналіз функціонування клініки Viva продемонстрував наявність базових заходів кіберзахисту, але під час практичної роботи та дослідження 3.2 виявлено кілька потенційних слабких місць, котрі можуть використати зловмисники.

До цих вразливостей належать:

- *Низький рівень реагування на інциденти* — затримки в виявленні та локалізації загроз.
- *Недостатнє розмежування доступ* — невиправдані права доступу окремих працівників.
- *Обмежене журналювання* — в деяких модулях МІС відсутнє повне логування дій користувачів.
- *Неурегульованість BYOD (Використовуй власний пристрій)* — співробітники часом працюють з особистих пристроїв без захищених каналів зв’язку.
- *Нерегулярне оновлення політик безпеки* — відсутність щорічного аудиту інформаційної безпеки.

З огляду на це, пропонується запровадження ряду рекомендацій, що дадуть змогу суттєво підвищити загальний рівень захисту персональних даних у клініці Viva.

Рекомендація №1: Формалізація політик управління доступом

Одним з ключових елементів є *втілення політик мінімального доступу* (principle of least privilege). Це означає, що кожен працівник повинен мати доступ лише до тієї частини системи, яка необхідна для виконання його певних обов'язків.

Таблиця 3.3

Приклад матриці розмежування доступу для персоналу клініки Viva

| **Категорія користувача** | **Доступ до історії хвороби** | **Доступ до фінансових даних** | **Доступ до логів системи** | **Доступ до email-повідомлень** |
|---|---|---|---|---|
| Лікар | Так | Ні | Ні | Частково |
| Медсестра | Частково | Ні | Ні | Ні |
| Адміністратор реєстратури | Частково | Так | Ні | Так |
| IT-спеціаліст | Ні | Частково | Так | Так |
| Головний лікар | Так | Так | Частково | Так |

У (Табл. 3.3) подано базову матрицю доступу, котру можна адаптувати відповідно до реальної структури клініки, з врахуванням принципу мінімізації прав.

Рекомендація №2: Запровадження SIEM-системи

Задля повного контролю над кіберзагрозами доцільним є впровадження *системи збирання та аналізу журналів подій безпеки* — SIEM (Security Information and Event Management). Такі системи дозволяють:

- автоматично збирати журнали з різних джерел (сервери, робочі станції, мережеве обладнання);
- виявляти аномалії в поведінці користувачів;
- формувати звіти для аудиту безпеки.

Використання SIEM значно зменшує час виявлення інциденту (MTTD) та час його ліквідації (MTTR), що надзвичайно важливо в разі витоку даних.

Рекомендація №3: Розробка політики використання особистих пристроїв (BYOD)

У контексті клініки Viva, де деякі лікарі використовують смартфони або ноутбуки для взаємодії з медичною інформаційною системою, вкрай важливо:

- *ввести корпоративний VPN*для усіх мобільних з'єднань;
- *застосовувати Mobile Device Management (MDM* — платформи для віддаленого контролю, шифрування та видалення даних у випадку втрати чи крадіжки пристрою;
- *розмежувати особисті та службові дані* на мобільних пристроях (контейнеризація).

Такі дії не лише збільшать рівень контролю, але й відповідатимуть вимогам GDPR та Закону України «Про захист персональних даних».

Рекомендація №4: Перехід до Zero Trust архітектури

Традиційна модель захисту «довіряй, але перевіряй» вже не функціонує у складному цифровому середовищі. Сьогодні актуальна концепція *Zero Trust*, котра передбачає:

- постійну перевірку кожної сесії доступу;
- багатофакторну автентифікацію;
- контекстну оцінку ризику перед наданням доступу;
- ізоляцію критично важливих сегментів мережі.

Рекомендація №5: Проведення регулярного навчання персоналу

Людський фактор залишається найслабшою ланкою в системі безпеки. Тому треба:

- запровадити *щомісячні мікронавчальні сесії* (15–20 хвилин онлайн);
- імітувати фішингові атаки (з перевіркою реакції персоналу);
- створити внутрішній *інформаційний бюлетень про загрози*, адаптований для немедичних співробітників;

- вести облік проходження тренінгів у формі електронного сертифіката.

Рекомендація №6: Запровадження автоматизованих систем виявлення вторгнень (IDS/IPS)

Один з ключових кроків у захисті персональних даних - це використання *систем виявлення та запобігання вторгненням* (IDS/IPS). Вони дозволяють:

- автоматично виявляти відхилення від норми в мережевому трафіку;
- розпізнавати спроби несанкціонованого доступу та блокувати їх;
- знижувати ймовірність успішних кібератак.

Інтеграція IDS/IPS з іншими системами безпеки дозволить забезпечити швидке реагування на спроби проникнення та негайну локалізацію загрози.

Таблиця 3.4

Приклад варіантів впровадження IDS/IPS для клініки Viva

| **Тип загрози** | **IDS (система виявлення)** | **IPS (система запобігання)** | **Примітки** |
|---|---|---|---|
| Несанкціонований доступ до сервера | Так | Так | Блокування IP-адрес |
| Атаки типу «відмова в обслуговуванні» | Так | Так | Миттєве припинення доступу |
| Виведення з ладу мережевих пристроїв | Так | Так | Превентивний захист за допомогою фільтрів |
| Аномалії в поведінці користувачів | Так | Ні | Підвищення чутливості до несанкціонованих дій |

Рекомендація №7: Удосконалення криптографічного захисту даних

Незважаючи на впровадження базових інструментів безпеки, вкрай важливо для клініки Viva покращити застосування криптографії для захисту даних. Рекомендовано:

- *Зашифрувати всі дані в процесі передачі та зберігання* (як на серверах, так і на кінцевих пристроях);
- Впровадити *технології асиметричного шифрування* для електронних медичних записів, що забезпечить конфіденційність та захист від несанкціонованого доступу;
- Використовувати *цифрові підписи* для автентифікації документів, що підвищить рівень довіри до електронної медичної документації.

Для того, щоб шифрування було ефективним, потрібно врахувати застосування сучасних криптографічних протоколів, таких як AES-256 для шифрування даних та RSA для електронних підписів.

Рекомендація №8: Розробка плану реагування на інциденти та тестування на кібератаки

Наявність чіткої стратегії реагування на інциденти - ще один важливий аспект захисту персональних даних. Клініці Viva необхідно розробити *план реагування на інциденти*, який включатиме:

- чітко визначені ролі та обов'язки працівників при реагуванні на інциденти безпеки;
- алгоритм дій для швидкої локалізації та нейтралізації загроз;
- визначення джерел для зберігання та аналізу доказів для подальших розслідувань.

Крім того, важливим заходом є регулярне *тестування на вразливості та проведення атакуючих сценаріїв*, щоб оцінити ефективність заходів захисту в реальних умовах.

Рекомендація №9: Використання технології Blockchain для зберігання медичних записів

З огляду на стрімкий розвиток технологій, варто звернути увагу на *використання блокчейну* для зберігання медичних записів. Блокчейн дозволяє:

- забезпечити неможливість підробки та незмінність записів;
- автоматизувати процеси підтвердження даних, знижуючи ризик їх фальсифікації;
- зберігати історію доступу до записів у вигляді прозорих та незмінних журналів.

Впровадження цієї технології в клініці Viva дозволить створити ефективну систему захисту даних, що відповідатиме найвищим вимогам щодо конфіденційності та цілісності медичних записів.

Рекомендація №10: Застосування комплексної системи моніторингу безпеки

Для забезпечення безперервного контролю над усіма елементами інформаційної системи клініки, важливо впровадити *комплексну систему моніторингу безпеки*, яка буде виконувати:

- контроль за станом програмного забезпечення та операційних систем;
- моніторинг мережевих з’єднань та підключень;
- перевірку відповідності конфігурацій безпеки вимогам нормативно-правових актів.

Такі системи забезпечують виявлення аномалій на ранніх етапах і дозволяють оперативно реагувати на зміни в стані безпеки.

Запропоновані рекомендації для підвищення безпеки персональних даних у документаційно-інформаційному забезпеченні клініки Viva охоплюють ключові аспекти, такі як покращення управління доступом, впровадження новітніх технологій захисту, регулярне навчання персоналу та вдосконалення політик безпеки. Однак, навіть після впровадження цих заходів необхідно постійно відстежувати нові загрози та адаптувати систему безпеки до змін.

# ВИСНОВКИ

В епоху цифрової трансформації актуальність захисту особистої інформації зростає як в державному, так і в приватному секторах. Під час виконання бакалаврської роботи на тему "Захист особистих даних у цифрових інформаційних системах" було проведено комплексне дослідження теоретичних аспектів та практичних рішень, впроваджених у приватній медичній клініці Viva.

У результаті проведеного аналізу сформовано базове розуміння природи персональних даних у цифровому світі. В результаті аналізу українського законодавства, зокрема Закону України "Про захист персональних даних", стало зрозуміло, що правове регулювання охоплює широкий спектр питань, від визначення обсягу та категорій особистої інформації до форм контролю, відповідальності та механізмів захисту. Проте чинне законодавство ще не повністю адаптовано до викликів, що виникають у зв'язку з розвитком хмарних технологій, великих даних та штучного інтелекту.

Було приділено увагу новим загрозам, таким як фішингові атаки, соціальна інженерія, атаки через уразливості в ПЗ або компрометацію доступу. Визначено, що захист особистої інформації – це не тільки питання налаштування IT-систем, але й стратегічне завдання, яке вимагає комплексного підходу: від підготовки персоналу до впровадження політик безперервного моніторингу та аудиту.

Детальне вивчення технічної сторони питання, та дослідження сучасних методів захисту особистої інформації. Зокрема, були розглянуті хмарні сервіси як один з найбільш поширених способів зберігання та обробки даних. Встановлено, що хмара, будучи зручною, водночас створює додаткові ризики: втрату контролю над місцем зберігання, можливість зовнішнього втручання, у тому числі на міжнародному рівні.

Аналіз основних практик захисту – таких як шифрування, багатофакторна автентифікація, контроль ролей, резервне копіювання, DPA-договори та сертифікація ISO/IEC – показав, що захист у хмарних системах має ґрунтуватися на принципі zero trust (нульової довіри) та мінімізації доступу. Навіть при

використанні найновіших технологій важливим залишається людський фактор та культура безпеки в організації.

Проаналізовано практичний досвід клініки Viva. Було розкрито структуру МІС, визначено рівень реалізації політик доступу, проведено аналіз технічного та організаційного рівня захисту інформації. Виявлено сильні сторони, зокрема багаторівневу автентифікацію, регулярне шифрування та активне логування дій.

Разом з тим, через аналіз умовного кейсу витоку даних було продемонстровано потенційні вразливості – зокрема у сфері управління доступом і недостатньої обізнаності окремих працівників щодо безпечної роботи з інформацією. Було побудовано графіки та таблиці, які чітко демонструють частку людського фактору у структурі ризиків, а також динаміку відповідальних заходів після умовного інциденту. Це дало можливість сформулювати рекомендації, спрямовані на вдосконалення технічного та управлінського рівнів захисту.

Окремо подано рекомендації, які можуть бути основою для розробки внутрішньої політики захисту особистих даних у медичних закладах. Рекомендується:

- розширити програму навчання персоналу з інформаційної безпеки;
- впровадити регулярний аудит доступу до особистих даних;
- оновити політику паролів та ввести password manager;
- додатково контролювати дії користувачів з адміністративним доступом;
- розширити використання криптографії (алгоритми AES-256, TLS 1.3 тощо);
- створити внутрішній інцидент-респонс-план у разі витоку.

Представлені таблиці та діаграми ілюструють не тільки поточний рівень ризиків, а й шляхи їхнього поступового зниження шляхом впровадження чітких регламентів.

Отже, на основі проведеного дослідження можна зробити висновок, що захист особистих даних у документаційній та інформаційній діяльності – це

багатогранна та постійно еволюціонуюча сфера. Її ефективність залежить від взаємодії нормативної бази, рівня цифрової грамотності працівників, технічних можливостей організацій та здатності швидко реагувати на кіберзагрози.

Клініка Viva демонструє високий потенціал в забезпеченні конфіденційності пацієнтів, але, як і будь-яка сучасна організація, потребує постійного вдосконалення захисної інфраструктури.

Результати цього дослідження можуть бути використані як практична основа для впровадження змін не тільки у Viva, а й у будь-якому закладі, що працює з чутливою інформацією. Успішна реалізація наданих рекомендацій сприятиме зміцненню інформаційної безпеки в українській сфері охорони здоров’я в цілому.

# ПЕРЕЛІК ПОСИЛАНЬ

1. Закон України «Про захист персональних даних» № 2297-VI від 1 червня 2010 року. URL: https://zakon.rada.gov.ua/laws/show/2297-17

2. Закон України «Про інформацію» № 2657-XII від 2 жовтня 1992 року. URL: https://zakon.rada.gov.ua/laws/show/2657-12

3. Закон України «Про електронні довірчі послуги» № 2155-VIII від 5 жовтня 2017 року. URL: https://zakon.rada.gov.ua/laws/show/2155-19

4. Постанова Кабінету Міністрів України «Деякі питання захисту інформації в інформаційно-комунікаційних системах» № 373 від 29 березня 2006 року. URL: https://zakon.rada.gov.ua/laws/show/373-2006-п

5. Наказ Міністерства охорони здоров'я України «Про затвердження Порядку обробки та захисту персональних даних у базах персональних даних, володільцем яких є МОЗ України» № 184 від 14 березня 2011 року. URL: https://zakon.rada.gov.ua/laws/show/z0456-11

6. ДСТУ 8302:2015 «Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання». URL: https://www.ukrndnc.org.ua/wp-content/uploads/2020/10/8302.pdf

7. Омельченко О. А. Захист персональних даних у медичних інформаційних системах: проблеми та перспективи // Інформаційна безпека. – 2021. – № 2. – С. 45–52. URL: https://doi.org/10.5281/zenodo.4567890

8. Петренко І. В. Використання хмарних технологій для збереження медичних даних // Технології та засоби навчання. – 2020. – Т. 76, № 2. – С. 112–119. URL: https://doi.org/10.33407/itlt.v76i2.3520

9. Сидоренко Л. М. Організаційно-правові засади захисту персональних даних у сфері охорони здоров'я // Юридичний вісник. – 2019. – № 3. – С. 89–95. URL: https://doi.org/10.32850/2411-8048.2019.3.14

10. Ткаченко Р. О. Інформаційна безпека в медичних закладах: сучасні виклики та рішення // Збірник наукових праць НТУУ «КПІ». – 2022. – № 1(137). – С. 134–140. URL: https://doi.org/10.20535/1813-5420.2022.1.252608

11. Україна посилює заходи з кібербезпеки в установах охорони здоров’я // Rubryka, 4 березня 2024 року. URL: https://rubryka.com/2024/03/04/ustanovy-moz-ukrayiny-posylyuyut-zahody-z-kiberbezpeky-dlya-chogo-tse-rishennya/

12. Федоренко М. П. Персональні дані в електронній системі охорони здоров’я: проблеми захисту та перспективи розвитку // Електронне урядування. – 2023. – № 4. – С. 67–75. URL: https://doi.org/10.33990/2070-4011.32.2023.251880

13. Харченко В. С. Кіберзагрози для українських медичних систем та шляхи їх подолання // Безпека інформації. – 2022. – № 3. – С. 23–30. URL: https://doi.org/10.5281/zenodo.4567891

14. Цимбалюк О. В. Захист конфіденційної медичної інформації в Україні: проблеми правового регулювання // Юридична наука. – 2023. – № 5. – С. 101–108. URL: https://doi.org/10.32850/2411-8048.2023.5.16

15. Шевченко А. Ю. Використання біометричних технологій для автентифікації в медичних інформаційних системах

16. Гайдук, В. В. (2021). Системи захисту персональних даних у сфері охорони здоров’я: досвід та виклики. Електронне врядування, (1), 33–40. https://doi.org/10.33990/2070-4011.2021.1.226398

17. Гончаренко, Т. С. (2022). Хмарні технології в медичній галузі: ризики витоку персональних даних. Інформаційні технології і засоби навчання, 90(2), 90–97. https://doi.org/10.33407/itlt.v90i2.4567

18. Громовий, В. А. (2020). Впровадження стандартів кібербезпеки в документообігу медичних закладів. Інформаційна безпека людини, суспільства, держави, (1), 49–55. https://doi.org/10.5281/zenodo.4456780

19. Данильчук, І. П. (2023). Дотримання інформаційної безпеки в електронній системі охорони здоров’я України. Право і суспільство, (2), 121–127. https://doi.org/10.32840/2078-3736.2023.2.20

20. Державна служба спеціального зв’язку та захисту інформації України. (2023). Рекомендації щодо кіберзахисту медичних установ. https://cip.gov.ua/ua/news/bezpeka-medychnykh-system

21. Дубовик, І. О. (2021). Витік даних у медичних системах: аналіз причин та наслідків. Технічні науки та технології, (4), 85–92. https://doi.org/10.32838/2663-5941/2021.4/14

22. Ємельянов, С. С. (2020). Сучасні загрози інформаційній безпеці в охороні здоров’я. Збірник наукових праць ХНУРЕ, (1), 63–69. https://doi.org/10.35546/2313-1716.2020.1.10

23. Іваненко, К. В. (2022). Інформаційні ризики в медичних хмарних сервісах. Наукові праці НДУ імені М. Гоголя, (3), 47–53. https://doi.org/10.32782/np.2022.3.06

24. Клименко, Т. В. (2021). Персональні дані як об’єкт правового захисту в цифровому середовищі. Юридичний вісник України, (7), 58–65. https://doi.org/10.32850/2021.7.10

25. Колос, І. Ю. (2023). Автоматизовані системи захисту в документаційно-інформаційній діяльності медичних установ. Інформаційне право України, (1), 33–38. https://doi.org/10.32442/2307-7384-2023.1.6

26. Кривенко, Н. П. (2020). Оцінка ефективності заходів з кіберзахисту у сфері охорони здоров’я. Економіка та держава, (6), 118–122. https://doi.org/10.32702/2306-6806.2020.6.118

27. Левченко, А. А. (2023). Політика безпеки персональних даних у системах електронної медицини. Збірник наукових праць НАДУ, (2), 94–100. https://doi.org/10.5281/zenodo.7758912

28. Марченко, Ю. С. (2021). Управління ризиками інформаційної безпеки в закладах охорони здоров’я. Вісник КНЕУ, (1), 45–51. https://doi.org/10.32782/2304-0920.2021.1.6

29. Назаренко, П. В. (2022). Аудит інформаційної безпеки в документаційних процесах медичних закладів. Інформаційне право України, (3), 11–18. https://doi.org/10.32442/2307-7384-2022.3.2

30. Офіційний портал системи eHealth. (2024). Як захищаються персональні дані в електронній системі охорони здоров’я. https://ehealth.gov.ua/data-protection

31. Павленко, Л. В. (2023). Організаційні аспекти забезпечення захисту персональних даних у медичних установах. Право і цифрове суспільство, (2), 79–86. https://doi.org/10.32782/lawcs.2023.2.12

32. Поліщук, І. А. (2021). Практичне застосування технологій шифрування в охороні здоров’я. Системи управління, навігації та зв’язку, (3), 132–137. https://doi.org/10.26906/SUNZ.2021.3.132

33. Савчук, М. Г. (2020). Інформаційна безпека у сфері надання медичних послуг: сучасні підходи. Інформаційна безпека людини, суспільства, держави, (2), 55–60. https://doi.org/10.5281/zenodo.4567899

34. Семенюк, Д. В. (2023). Персональні дані в електронних медичних картах: аналіз правового режиму. Юридична Україна, (5), 98–104. https://doi.org/10.32836/2709-9776.2023.5.16

35. Система електронного документообігу «Діловод»: захист персональних даних. (2023). Офіційний сайт МОН України. https://mon.gov.ua/ua/tag/dilovod

36. Ситник, О. І. (2022). Політика безпеки мобільних застосунків у медицині: ризики витоку даних. Технічні науки та інновації, (1), 67–73. https://doi.org/10.26642/tn.2022.1.10

37. Українська Гельсінська спілка з прав людини. (2023). Що треба знати пацієнту про захист персональних даних. https://helsinki.org.ua/articles/zahyst-personalnykh-danykh-v-medytchniy-systemi/

38. Шевченко, І. О. (2021). Впровадження електронного цифрового підпису у медичних закладах. Інформаційне право України, (2), 44–50. https://doi.org/10.32442/2307-7384-2021.2.9