

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

ЧОРНИЙ ВІКТОР ВІКТОРОВИЧ

Допускається до захисту:  
Завідувач кафедри  
інформаційних технологій,  
к.т.н., доцент  
\_\_\_\_\_ Т. В. Нескородева  
«\_\_» \_\_\_\_\_ 20\_\_ р.

ЗАХИСТ ІНФОРМАЦІЇ У СИСТЕМІ КОНТРОЛЮ ЗА САМОІЗОЛЯЦІЄЮ

Спеціальність 125 Кібербезпека

Кваліфікаційна (бакалаврська) робота

Керівник:  
Крижановський В. Г., професор кафедри  
інформаційних технологій  
д.т.н, професор

\_\_\_\_\_  
(підпис)

Оцінка : \_\_\_\_\_ / \_\_\_\_\_ / \_\_\_\_\_  
(бали за шкалою ЄКТС/за національною шкалою)

Голова ЕК: \_\_\_\_\_  
(підпис)

Вінниця 2021

## АНОТАЦІЯ

**Чорний В. В. Захист інформації у системі контролю за самоізоляцією.** Спеціальність 125 «Кібербезпека», спеціалізація .... Донецький національний університет імені Василя Стуса, Вінниця, 2021.

У кваліфікаційній (бакалаврській) роботі досліджено основні особливості додатку «Дій вдома», його переваги, недоліки, а також його основні напрямки удосконалення, з огляду на результати опитування людей, які користувалися додатком. Було проаналізовано зарубіжний досвід використання додатків для контролю за самоізоляцією. Були здійснені рекомендації щодо вдосконалення системи захисту інформації додатку «Дій вдома». Було визначено, що можна використовувати Cookies браузеру, не використовуючи персональних даних людини, а використовувати такі самі алгоритми, як використовує Google.

Ключові слова: захист інформації, додаток, самоізоляція, контроль, персональні дані.

47 с., 1 табл., 3 рис., 3 дод., 49 джерел.

## ABSTRACT

**Chorny V. V. Information protection in the system of self-isolation control.** Specialty 125 «Cybersecurity», specialization «...». Vasyl' Stus Donetsk National University, Vinnytsia, 2021.

The qualification (bachelor's) work explores the main features of the application "Action at home", its advantages, disadvantages, as well as its main areas of improvement, given the results of a survey of people who used the application. Foreign experience of using applications for self-isolation control was analyzed. Recommendations were made to improve the information protection system of the «Diya Vdoma» application. It has been determined that you can use browser cookies without using personal data, but use the same algorithms as used by Google.

Keywords: information protection, application, self-isolation, control, personal data.

## ЗМІСТ

ВСТУП .....	4
РОЗДІЛ 1. ТЕОРІЯ ТА ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ .....	6
1.1. Основні теоретичні положення системи захисту інформації .....	6
1.2. Напрями забезпечення інформаційної безпеки .....	15
РОЗДІЛ 2. АНАЛІЗ ПРОГРАМИ «ДІЙ ВДОМА», ЇЇ ПЕРЕВАГ, НЕДОЛІКІВ ТА БЕЗПЕКИ ОСОБИСТИХ ДАНИХ .....	23
2.1. Особливості роботи додатку «Дій вдома» .....	23
2.2. Переваги та недоліки додатку «Дій вдома», особливості системи захисту інформації додатку .....	30
РОЗДІЛ 3. ЗАРУБІЖНИЙ ДОСВІД ВИКОРИСТАННЯ ДОДАТКІВ ДЛЯ КОНТРОЛЮ ЗА САМОІЗОЛЯЦІЄЮ ТА НАПРЯМКИ ВДОСКОНАЛЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ ДОДАТКУ «ДІЙ ВДОМА» .....	37
3.1. Особливості використання додатків для контролю за самоізоляцією в іноземних країнах .....	37
3.2. Напрями вдосконалення додатку «Дій вдома» та підвищення захисту інформації додатку .....	44
ВИСНОВКИ .....	48
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ .....	51
ДОДАТКИ .....	57

## ВСТУП

**Актуальність теми дослідження.** Поява і бурхливий розвиток обчислювальної техніки призвели до створення різних автоматизованих інформаційних і керуючих систем. Зростання довіри до таких систем збільшувалося в міру підвищення надійності і продуктивності засобів обчислювальної техніки. Цим системам стали довіряти все більш відповідальну роботу, від якості виконання якої залежить життя і добробут окремих людей, організацій, держав і людства в цілому. Широке поширення обчислювальної техніки як засобу обробки інформації призвело до інформатизації суспільства і появи принципово нових, інформаційних технологій.

Уряди і корпорації все ширше використовують цифрові технології для боротьби з поширенням нового коронавірусу Covid-19. У той час як одні бачать в технологічних рішеннях важливий засіб відстеження контактів, забезпечення карантину і отримання картини поширення вірусу з виходом на адресне використання ресурсів охорони здоров'я, у інших ці практики викликають серйозні питання з точки зору прав людини. Багаторічний досвід реалізації надзвичайних заходів, таких як електронне стеження для боротьби з тероризмом, показує, що вони часто заходять занадто далеко, не забезпечують необхідних результатів і, будучи введеними, нерідко залишаються в силі і після зникнення вихідної причини введення. Це пояснює актуальність даної теми, оскільки захист даних, які збирають додатки для контролю за самоізоляцією, в деяких випадках є сумнівним, зважаючи на правове регулювання деяких країн.

**Метою дослідження** є визначення комплексу захисту інформації у системі контролю за самоізоляцією.

**Завдання дослідження:**

— визначити основні теоретичні положення системи захисту інформації;



- проаналізувати напрями забезпечення інформаційної безпеки;
- визначити особливості роботи додатку «Дій вдома»;
- проаналізувати переваги та недоліки додатку «Дій вдома», а також особливості системи захисту інформації додатку;
- визначити особливості використання додатків для контролю за самоізоляцією в іноземних країнах;
- порекомендувати напрями вдосконалення додатку «Дій вдома» та підвищення захисту інформації додатку.

**Об’єкт дослідження** – захист інформації в додатку «Дій вдома».

**Предмет дослідження** – система захисту інформації в мобільних додатках з контролю за самоізоляцією.

**Теоретичне та практичне значення одержаних результатів.**

Виконане дослідження дозволило визначити основні особливості додатку «Дій вдома», його переваги, недоліки, а також його основні напрямки удосконалення, з огляду на результати опитування людей, які користувалися додатком. Проаналізовано зарубіжний досвід використання додатків для контролю за самоізоляцією. Були здійснені рекомендації щодо вдосконалення системи захисту інформації додатку «Дій вдома».

**Апробація результатів дослідження.**

**Структура кваліфікаційної (бакалаврської) роботи.** Кваліфікаційна робота складається зі вступу, 3-х розділів, висновків, списку використаних джерел, який складається з 49 найменувань, та 3-х додатків. Основний текст роботи викладено на 47 сторінках.

## РОЗДІЛ 1. ТЕОРІЯ ТА ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ

### 1.1. Основні теоретичні положення системи захисту інформації

Базовими в теорії захисту інформації є терміни: «інформаційна безпека», «безпека інформації», «захист інформації». Їх сутність визначає в кінцевому підсумку політику і діяльність в області захисту інформації.

Інформаційна безпека – стан захищеності інформаційних ресурсів (інформаційного середовища) від внутрішніх і зовнішніх загроз, які могли б зашкодити інтересам особистості, суспільства, держави (національним інтересам) [41, с. 73].

Безпека інформації – захищеність інформації від небажаного (для відповідних суб'єктів інформаційних відносин) її розголошення (порушення конфіденційності), спотворення (порушення цілісності), втрати або зниження ступеня доступності інформації, а також незаконного її тиражування.

З визначень «інформаційна безпека» та «безпека інформації» випливає, що захист інформації спрямований на забезпечення безпеки інформації, безпека інформації забезпечується за допомогою її захисту [40, с. 165].

Аналіз стану справ у сфері захисту інформації показує, що вже склалася цілком сформована концепція і структура захисту, основу якої складають:

- дуже розвинений арсенал технічних засобів захисту інформації, зроблених на основі промислового виробництва;
- значне число фірм, що спеціалізуються на вирішенні питань захисту інформації;
- досить чітко окреслена система поглядів на цю проблему;
- наявність значного практичного досвіду та інше.

І тим не менше, як свідчать вітчизняні та зарубіжні праці, злочинні дії над інформацією не тільки не зменшуються, але і мають досить стійку тенденцію до зростання.

Досвід показує, що для боротьби з цією тенденцією необхідна злагоджена й цілеспрямована організація процесу захисту інформаційних ресурсів. Причому в цьому повинні брати активну участь професійні фахівці, адміністрація, співробітники і користувачі, що і визначає підвищену значимість організаційної сторони питання [37, с. 26].

Досвід також показує, що:

- забезпечення безпеки інформації не може бути одноразовим актом. Це безперервний процес, що полягає в обґрунтуванні і реалізації найбільш раціональних методів, способів і шляхів вдосконалення та розвитку системи захисту, безперервному контролю її стану, виявленні її вузьких і слабких місць і протиправних дій;

- безпеку інформації може бути забезпечена лише при комплексному використанні всього арсеналу наявних засобів захисту у всіх структурних елементах виробничої системи і на всіх етапах технологічного циклу обробки інформації. Найбільший ефект досягається тоді, коли всі використовувані засоби, методи і заходи об'єднуються в єдиний цілісний механізм – систему захисту інформації (СЗІ). При цьому функціонування системи має контролюватися, оновлюватися і доповнюватися в залежності від зміни зовнішніх і внутрішніх умов;

- ніяка СЗІ не може забезпечити необхідного рівня безпеки інформації без належної підготовки користувачів і дотримання ними всіх встановлених правил, спрямованих на її захист (рис 1.1).

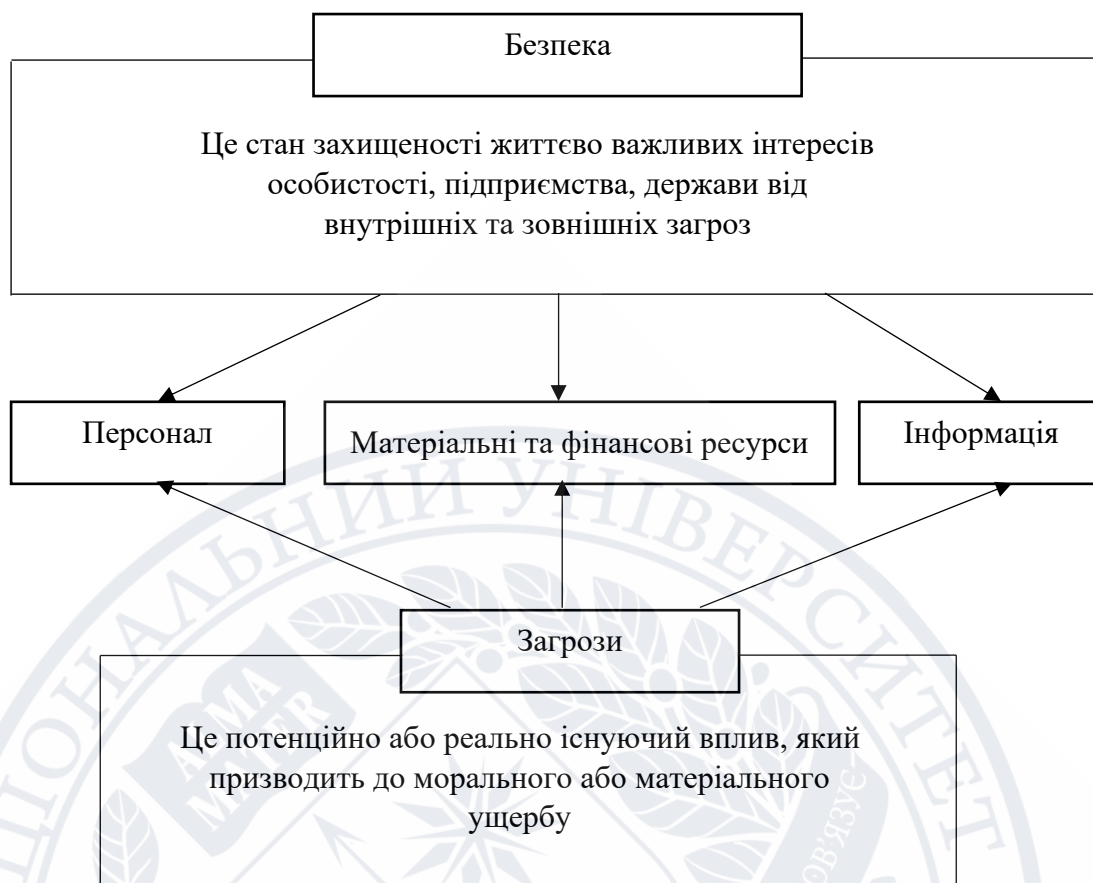


Рисунок – 1.1. Система безпеки інформації [29, с. 227]

З урахуванням накопиченого досвіду можна визначити систему захисту інформації як організовану сукупність спеціальних органів, засобів, методів і заходів, що забезпечують захист інформації від внутрішніх і зовнішніх загроз.

З позицій системного підходу до захисту інформації пред'являються певні вимоги. Захист інформації повинен бути:

- безперервним. Ця вимога випливає з того, що зловмисники тільки і шукають можливість, як би обійти захист інформації, яка їх цікавить;
- плановим. Планування здійснюється шляхом розробки кожною службою детальних планів захисту інформації в сфері її компетенції з урахуванням загальної мети організації;
- цілеспрямованим. Захищається те, що має захищатися в інтересах конкретної мети, а не вся інформація;
- конкретним. Захисту підлягають конкретні дані, що об'єктивно підлягають охороні, втрата яких може заподіяти організації певної шкоди;



- активним. Захищати інформацію необхідно з достатнім ступенем наполегливості;
- надійним. Методи і форми захисту повинні надійно перекривати можливі шляхи неправомірного доступу до охоронюваних компонентів, незалежно від форми їх подання, мови вираження і виду фізичного носія, на якому вони закріплені;
- універсальним. Вважається, що в залежності від виду каналу витоку або способу несанкціонованого доступу його необхідно перекривати, де б він не виявився, розумними і достатніми засобами, незалежно від характеру, форми і виду інформації;
- комплексним. Для захисту інформації у всьому різноманітті структурних елементів повинні застосовуватися всі види і форми захисту в повному обсязі. Неприпустимо застосовувати лише окремі форми або технічні засоби. Комплексний характер захисту виникає з того, що захист – це специфічне явище, що представляє собою складну систему нерозривно взаємопов'язаних і взаємозалежних процесів, кожен з яких в свою чергу має безліч різних взаємообслуговуваних один одного сторін, властивостей, тенденцій [23, с. 183].

Зарубіжний і вітчизняний досвід показує, що для забезпечення виконання настільки багатогранних вимог безпеки система захисту інформації повинна відповідати певним умовам:

- охоплювати весь технологічний комплекс інформаційної діяльності;
- бути різноманітною щодо використовуваних засобів, багаторівневою з ієрархічною послідовністю доступу;
- бути відкритою для зміни і доповнення заходів забезпечення безпеки інформації;
- бути нестандартною, різноманітною. При виборі засобів захисту не можна розраховувати на непоінформованість зловмисників щодо її можливостей;

- бути простою для технічного обслуговування і зручною для експлуатації користувачами;
- бути надійною. Будь-які поломки технічних засобів є причиною появи неконтрольованих каналів витоку інформації;
- бути комплексною, володіти цілісністю, це означає, що жодна її частина не може бути вилучена без шкоди для всієї системи.

До системи безпеки інформації пред'являються також певні вимоги:

- чіткість визначення повноважень і прав користувачів на доступ до певних видів інформації;
- надання користувачу мінімальних повноважень, необхідних йому для виконання дорученої роботи;
- зведення до мінімуму числа загальних для деяких користувачів засобів захисту;
- облік випадків і спроб несанкціонованого доступу до конфіденційної інформації;
- забезпечення оцінки ступеня конфіденційної інформації;
- забезпечення контролю цілісності засобів захисту і негайне реагування на їх вихід з ладу [21, с. 82].

Порушення безпеки інформації в кінцевому підсумку може зашкодити її власнику. Тому для того, щоб встановити, що захищати, в чийх інтересах захищати, як і чим захищати, введена система понять в області захисту інформації, що включає в себе:

- поняття, пов'язані з визначенням інформації, її правового режиму, правами власності та доступу до інформації, що захищається (правові поняття в області інформаційних відносин);
- поняття, пов'язані безпосередньо з предметною областю захисту інформації.

Поняття першої групи використовуються в правових документах, поняття другої – в нормативних.

Інформація, що захищається – інформація, яка є предметом власності і підлягає захисту відповідно до вимог правових документів або до вимог, встановлених власником інформації. Власником інформації може бути: держава, юридична особа, група фізичних осіб, окрема фізична особа.

Захист інформації – прийняття правових, організаційних і технічних заходів, спрямованих на [19, с. 218]:

- 1) забезпечення захисту інформації від незаконного втручання, знищення, модифікування, блокування, копіювання, надання, поширення, а також від інших неправомірних дій у відношенні такої інформації;
- 2) дотримання конфіденційності інформації обмеженого доступу;
- 3) реалізацію права на доступ до інформації.

Захист інформації від витоку – діяльність, спрямована на запобігання неконтрольованого розповсюдження інформації, що захищається в результаті її розголошення, несанкціонованого доступу до інформації та отримання інформації, що захищається розвідками. Захист інформації від несанкціонованого впливу – діяльність, спрямована на запобігання впливу на захищає інформацію з порушенням встановлених прав і (або) правил на зміну інформації, що призводить до її спотворення, знищення, блокування доступу до інформації, а також до втрати, знищення або збою функціонування носія інформації.

Захист інформації від ненавмисного впливу – діяльність, спрямована на запобігання впливу на інформацію, що захищається, помилок її користувача, збою технічних і програмних засобів інформаційних систем, природних чи інших явищ, які не цілеспрямовано впливають на зміну інформації, що призводять до спотворення, знищення, копіювання, блокування доступу до інформації, а також до втрати, знищення або збою функціонування носія інформації.

Захист інформації від розголошення – діяльність, спрямована на запобігання несанкціонованого доведення інформації, що захищається, до споживачів, які не мають права доступу до цієї інформації. Захист інформації



від несанкціонованого доступу – діяльність, спрямована на запобігання отримання інформації, що захищається, зацікавленим суб'єктом з порушенням встановлених правовими документами чи власником інформації прав або правил доступу до інформації, що захищається.

Зацікавленим суб'єктом, що здійснює несанкціонований доступ до інформації, що захищається, може бути: держава; юридична особа; група фізичних осіб, в тому числі громадська організація; окрема фізична особа. Захист інформації від розвідки – діяльність, спрямована на запобігання отримання інформації, що захищається розвідкою [20, с. 26].

Ефективне забезпечення захисту інформації можливе тільки на основі комплексного використання всіх відомих методів і підходів до вирішення даної проблеми. До концепції комплексного захисту пред'являється ряд вимог [20]:

1. Розробка і доведення до рівня регулярного використання всіх необхідних механізмів гарантованого забезпечення необхідного рівня захищеності інформації;
2. Існування механізмів практичної реалізації необхідного рівня захищеності;
3. Наявність засобів раціональної реалізації всіх необхідних заходів щодо захисту інформації на базі досягнутого рівня розвитку науки і техніки;
4. Розробка способів оптимальної організації та забезпечення проведення всіх заходів щодо захисту в процесі обробки інформації. З метою побудови концепції, що задовольняє всієї сукупності вимог, останнім часом активно розробляється теорія захисту інформації, що включає поняття завдання захисту, засобів захисту, системи захисту. Функція захисту – сукупність однорідних в функціональному відношенні заходів, регулярно здійснюваних в інформаційній системі різними засобами і методами з метою створення, підтримки і забезпечення умов, об'єктивно необхідних для надійного захисту інформації. Повний безліч функцій захисту:



- попередження виникнення умов, що сприяють появі дестабілізуючих чинників;
- попередження безпосереднім виявленням дестабілізуючих чинників;
- виявлення дестабілізуючих чинників, які проявилися;
- попередження впливу на інформацію проявилися дестабілізуючих чинників, які проявилися;
- виявлення впливу дестабілізуючих чинників;
- локалізація впливу дестабілізуючих чинників;
- ліквідація наслідків локалізованого впливу дестабілізуючих факторів.

Всі засоби захисту діляться на формальні (виконують захисні функції строго за заздалегідь передбаченою процедурою без безпосередньої участі людини) і неформальні (визначаються цілеспрямованою діяльністю людини або регламентують цю діяльність). Технічні засоби реалізуються у вигляді електричних, електромеханічних і електронних пристроїв. Вся сукупність технічних засобів поділяється на апаратні і фізичні.

Під апаратними технічними засобами прийнято розуміти пристрої, що вбудовуються безпосередньо в телекомунікаційну апаратуру, або пристрої, які сполучаються з подібною апаратурою по стандартному інтерфейсу. З найбільш відомих апаратних засобів можна відзначити схеми контролю інформації по парності, схеми захисту полів пам'яті – по ключу і т. д.

Фізичні засоби реалізуються у вигляді автономних пристроїв і систем. Це можуть бути, наприклад, замки на дверях приміщень, де розміщена апаратура, решітки на вікнах, електронно-механічне обладнання охоронної сигналізації. Програмні засоби являють собою програмне забезпечення, розроблене спеціально для виконання функцій захисту інформації. Зазначені вище засоби і становили основу механізмів захисту на першій фазі розвитку технології забезпечення безпеки зв'язку в каналах телекомунікацій. При цьому вважалося, що основними засобами захисту є програмні [11, с. 93].

Організаційні засоби захисту являють собою організаційно-технічні та організаційно-правові заходи, здійснювані в процесі створення і експлуатації апаратури телекомунікацій для забезпечення захисту інформації. Організаційні заходи охоплюють всі структурні елементи системи на всіх етапах їх життєвого циклу (будівництво приміщень, проектування системи, монтаж і налагодження обладнання, випробування та експлуатація).

Законодавчі засоби захисту визначаються законодавчими актами країни, якими регламентуються правила використання, обробки та передачі інформації обмеженого доступу і встановлюються міри відповідальності за порушення цих правил [13, с. 59].

Морально-етичні засоби захисту реалізуються у вигляді всіляких норм, які склалися традиційно або складаються в міру поширення обчислювальної техніки і засобів зв'язку в певній країні або суспільстві. Ці норми здебільшого не є обов'язковими, як законодавчі заходи, проте недотримання їх веде зазвичай до втрати авторитету і престижу людини [13, с. 60].

Отже, викладену інформацію в цьому підрозділі можна коротко сформулювати таким чином. Інформація – це ресурс. Втрата конфіденційної інформації приносить моральної чи матеріальної шкоди. Умови, що сприяють неправомірному оволодінню конфіденційною інформацією, зводяться до її розголошення, витоку і несанкціонованого доступу до її джерел. У сучасних умовах безпека інформаційних ресурсів може бути забезпечена тільки комплексною системою захисту інформації. Комплексна система захисту інформації повинна бути: безперервною, плановою, цілеспрямованою, конкретною, активною, надійною. Система захисту інформації повинна спиратися на систему видів власного забезпечення, здатного реалізувати її функціонування не тільки в повсякденних умовах, але і в критичних ситуаціях.

## 1.2. Напрями забезпечення інформаційної безпеки

Напрями забезпечення безпеки взагалі розглядаються як нормативно-правові категорії, що визначають комплексні заходи захисту інформації на державному рівні, на рівні підприємства і організації, на рівні окремої особистості. З урахуванням сформованої практики забезпечення інформаційної безпеки виділяють наступні напрямки захисту інформації:

- правовий захист – це спеціальні закони, інші нормативні акти, правила, процедури та заходи, що забезпечують захист інформації на правовій основі;
- організаційний захист – це регламентація виробничої діяльності та взаємовідносин виконавців на нормативно-правовій основі, що виключає або послаблює нанесення якого-небудь збитку виконавцям;
- інженерно-технічний захист – це використання різних технічних засобів, що перешкоджають нанесенню шкоди комерційної діяльності [29, с. 294].

Крім цього, захисні дії, орієнтовані на забезпечення інформаційної безпеки, можуть бути охарактеризовані цілим рядом параметрів, що відбивають, крім напрямків, орієнтацію на об'єкти захисту, характер загроз, способи дій, їх поширеність, охоплення і масштабність.

Так, за характером загроз захисні дії орієнтовані на захист інформації від розголошення, витоку і несанкціонованого доступу.

Правовий захист інформації як ресурсу визнаний на міжнародному, державному рівні і визначається міждержавними договорами, конвенціями, деклараціями і реалізується патентами, авторським правом і ліцензіями на їх захист. На державному рівні правовий захист регулюється державними та відомчими актами.

Вимоги інформаційної безпеки повинні органічно включатися в усі рівні законодавства, в тому числі і в конституційне законодавство, основні загальні закони, закони по організації державної системи управління, спеціальні



закони, відомчі правові акти та інші. У літературі наводиться така структура правових актів, орієнтованих на правовий захист інформації.

Базові засади інформаційної безпеки нашої держави закладено у статтях 17, 19, 31, 32, 34, 50, 57 та 64 Конституції України. Закон України «Про інформацію» закріплює право громадян України на інформацію, закладає правові основи інформаційної діяльності [22]. Закон стверджує інформаційний суверенітет України і визначає правові форми міжнародного співробітництва в галузі інформації, встановлює загальні правові основи одержання, використання, поширення та зберігання інформації, закріплює право особи на інформацію в усіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначає статус учасників інформаційних відносин, регулює доступ до інформації та забезпечує її охорону, захищає особу та суспільство від неправдивої інформації.

У ст. 1 закону інформація визначається як документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі. Державну інформаційну політику розробляють і здійснюють органи державної влади загальної компетенції, а також відповідні органи спеціальної компетенції [22].

Кожному громадянину забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законами України. Державний контроль за додержанням встановленого режиму здійснюється спеціальними органами, які визначають Верховна Рада України і Кабінет Міністрів України. Доступ до відкритої інформації забезпечується шляхом: систематичної публікації її в офіційних друкованих виданнях (бюлетенях, збірниках); поширення її засобами масової комунікації; безпосереднього її надання заінтересованим громадянам, державним органам та юридичним особам.

Організаційний захист – це регламентація виробничої діяльності та взаємовідносин виконавців на нормативно-правовій основі, що виключає або



суттєво ускладнює неправомірне заволодіння конфіденційною інформацією і прояв внутрішніх і зовнішніх загроз. Організаційний захист забезпечує:

- організацію охорони, режиму, роботу з кадрами, з документами;
- використання технічних засобів безпеки та інформаційно-аналітичну діяльність з виявлення внутрішніх і зовнішніх загроз підприємницької діяльності [26, с. 84].

Організаційні заходи відіграють істотну роль у створенні надійного механізму захисту інформації, оскільки можливості несанкціонованого використання конфіденційних відомостей в значній мірі обумовлюються не технічними аспектами, а зловмисними діями, недбалістю і халатністю користувачів або персоналу захисту. Впливу цих аспектів практично неможливо уникнути за допомогою технічних засобів.

Для цього необхідна сукупність організаційно-правових та організаційно-технічних заходів, які виключали б (або, принаймні, зводили б до мінімуму) можливість виникнення небезпеки конфіденційної інформації.

До основних організаційних заходів можна віднести:

- організацію режиму і охорони. Їх мета – виключення можливості таємного проникнення на територію і в приміщення сторонніх осіб; забезпечення зручності контролю проходу і переміщення співробітників і відвідувачів; створення окремих виробничих зон по типу конфіденційних робіт з самостійними системами доступу; контроль і дотримання тимчасового режиму праці та перебування на території персоналу фірми; організація і підтримка надійного пропускового режиму і контролю співробітників і відвідувачів та ін.;

- організацію роботи зі співробітниками, яка передбачає підбір і розстановку персоналу, включаючи ознайомлення зі співробітниками, їх вивчення, навчання правилам роботи з конфіденційною інформацією, ознайомлення з заходами відповідальності за порушення правил захисту інформації та ін.;

- організацію роботи з документами і документованою інформацією, включаючи організацію розробки і використання документів та носіїв конфіденційної інформації, їх облік, виконання, повернення, зберігання і знищення;
- організацію використання технічних засобів збору, обробки, накопичення і зберігання конфіденційної інформації;
- організацію роботи з аналізу внутрішніх і зовнішніх загроз конфіденційної інформації і розробка заходів щодо забезпечення її захисту;
- організацію роботи з проведення систематичного контролю за роботою персоналу з конфіденційною інформацією, порядком обліку, зберігання і знищення документів і технічних носіїв [38, с. 12].

Інженерно-технічний захист (ІТЗ) за визначенням – це сукупність спеціальних органів, технічних засобів і заходів щодо їх використання в інтересах захисту конфіденційної інформації. Різноманіття цілей, завдань, об'єктів захисту і заходів, що проводяться, передбачає розгляд певної системи класифікації засобів за видом, орієнтацією та іншими характеристиками. Наприклад, кошти інженерно-технічного захисту можна розглядати за об'єктами їх впливу. В цьому плані вони можуть застосовуватися для захисту людей, матеріальних засобів, фінансів, інформації.

За функціональним призначенням засоби інженерно-технічного захисту діляться на такі групи:

- матеріальні ресурси, що включають різні засоби і споруди, що перешкоджають фізичному проникненню (або доступу) зловмисників на об'єкти захисту і до матеріальних носіїв конфіденційної інформації і здійснюють захист персоналу, матеріальних засобів, фінансів та інформації від протиправних дій;
- апаратні засоби. Сюди входять прилади, пристрої, пристосування і інші технічні рішення, які використовуються в інтересах захисту інформації. У практиці діяльності підприємства знаходить широке застосування найрізноманітніша апаратура, починаючи з телефонного апарату до

бездоганних автоматизованих систем, що забезпечують виробничу діяльність. Основне завдання апаратних засобів – забезпечення стійкого захисту інформації від розголошення, витоку і несанкціонованого доступу через технічні засоби забезпечення виробничої діяльності;

- програмні засоби, що охоплюють спеціальні програми, програмні комплекси і системи захисту інформації в інформаційних системах різного призначення і засобах обробки (збирання, накопичення, зберігання, обробки і передачі) даних;

- криптографічні засоби – це спеціальні математичні та алгоритмічні засоби захисту інформації, переданої по системам і мережам зв'язку, зберігається та обробляється на електронно-обчислювальних машинах з використанням різноманітних методів шифрування [40, с. 164].

Апаратні засоби та методи захисту поширені досить широко. Однак через те, що вони не володіють достатньою гнучкістю, часто втрачають свої захисні властивості при розкритті їх принципів дії і в подальшому не можуть бути використані.

Програмні засоби і методи захисту надійні і період їх гарантованого використання без перепрограмування значно більший, ніж апаратних. Криптографічні методи займають важливе місце і виступають надійним засобом забезпечення захисту інформації на тривалі періоди. Очевидно, що такий розподіл засобів захисту інформації є досить умовним, оскільки на практиці дуже часто вони і взаємодіють, і реалізуються в комплексі у вигляді програмно-апаратних модулів з широким використанням алгоритмів закриття інформації.

Найпростіший і найпоширеніший метод ідентифікації використовує різні карти і картки, на яких поміщається кодована або відкрита інформація про власника, його повноваження та інше. Зазвичай це пластикові карти типу пропусків або жетонів. Карти вводяться в пристрій, здатний читати кожен раз, коли потрібно увійти або вийти з приміщення, що охороняється, або отримати доступ до чого-небудь (сейфу, камери, терміналу) [43, с. 63].



Існує багато різновидів пристроїв розпізнавання та ідентифікації особистості, що використовують подібні карти. Одні з них оптичним шляхом звіряють фотографії та інші ідентифікаційні елементи, інші – магнітні поля.

1. Системи розпізнавання за відбитками пальців. В основу ідентифікації покладено порівняння відносного положення закінчень і розгалужень ліній відбитка. Пошукова система шукає на поточному зображенні контрольні елементи, визначені при дослідженні еталонного зразка. Для ідентифікації однієї людини вважається достатнім визначення координат 12 точок. Ці системи, природньо, дуже складні і рекомендуються до використання на об'єктах, що вимагають надійного захисту.

2. Системи розпізнавання по голосу. Існує декілька способів виділення характерних ознак мови людини: аналіз короткочасних сегментів, контрольний аналіз, виділення статистичних характеристик.

3. Системи розпізнавання по почерку вважаються найбільш зручними для користувача. Основним принципом ідентифікації за почерком є сталість підпису кожного індивідуума, хоча абсолютного збігу не буває.

4. Система розпізнавання по геометрії рук. Для ідентифікації застосовують аналіз комбінації ліній згинів пальців і долоні, ліній складок, довжини і товщини пальців тощо [49].

Для захисту від чужого вторгнення обов'язково передбачаються певні заходи безпеки. Основні функції, які повинні здійснюватися програмними засобами, це:

- ідентифікація суб'єктів і об'єктів;
- розмежування (іноді і повна ізоляція) доступу до обчислювальних ресурсів та інформації;
- контроль і реєстрація дій з інформацією і програмами.

Процедура ідентифікації і підтвердження автентичності передбачає перевірку, чи є суб'єкт, який здійснює доступ (або об'єкт, до якого здійснюється доступ), тим, за кого себе видає. Подібні перевірки можуть бути



одноразовими або періодичними (особливо у випадках тривалих сеансів роботи). У процедурах ідентифікації використовуються різні методи:

- прості, складні або одноразові паролі;
- обмін питаннями і відповідями з адміністратором;
- ключі, магнітні карти, значки, жетони;
- засоби аналізу індивідуальних характеристик (голоси, відбитки пальців, геометричні параметри рук, обличчя);
- спеціальні ідентифікатори або контрольні суми для апаратури, програм, даних [12, с. 482].

Найбільш поширеним методом ідентифікації є парольна ідентифікація. Практика показала, що парольний захист даних є слабкою ланкою, оскільки пароль можна підслухати або підглядіти, пароль можна перехопити, а то і просто розгадати.

Для захисту самого пароля вироблені певні рекомендації, як зробити пароль надійним:

- пароль повинен містити принаймні вісім символів. Чим менше символів містить пароль, тим легше його розгадати;
- не слід використовувати в якості пароля очевидний набір символів, наприклад ім'я, дату народження, імена близьких або найменування програм. Найкраще використовувати для цих цілей невідому формулу або цитату;
- якщо криптографічна програма дозволяє, слід ввести в пароль принаймні один пробіл, небуквений символ або прописну букву, не слід називати пароль нікому, не варто записувати його на видному місці;
- частіше слід змінювати пароль;
- не слід вводити пароль в процедуру встановлення діалогу або макрокоманду [9].

Таким чином, комплексна безпека інформаційних ресурсів досягається використанням правових актів державного та відомчого рівня, організаційних заходів і технічних засобів захисту інформації від різних внутрішніх і

зовнішніх загроз. Правові заходи забезпечення безпеки та захисту інформації є основою порядку діяльності і поведінки співробітників всіх рівнів і ступеня їх відповідальності за порушення встановлених норм і правил роботи із забезпечення збереження комерційних секретів. Організаційні заходи є вирішальною ланкою у формуванні та реалізації комплексних заходів захисту інформації. Вони, в першу чергу, виражаються в створенні служби безпеки організації і забезпеченні її нормального функціонування.



## **РОЗДІЛ 2. АНАЛІЗ ПРОГРАМИ «ДІЙ ВДОМА», ЇЇ ПЕРЕВАГ, НЕДОЛІКІВ ТА БЕЗПЕКИ ОСОБИСТИХ ДАНИХ**

### **2.1. Особливості роботи додатку «Дій вдома»**

Міністерство цифрової трансформації повідомило про запуск мобільної програми «Дій вдома» для моніторингу режиму обов'язкової самоізоляції, на якій повинні знаходитися громадяни, які прибули з-за кордону, з підтвердженням або підозрою на зараження COVID-19 [17].

Як пояснив міністр з питань цифрової трансформації Михайло Федоров, «протягом двох тижнів користувач програми буде отримувати 10 push-повідомлень на день. Людина на самоізоляції чи на карантині повинна сфотографуватися, і пристрій автоматично включить геолокацію. Дані з додатка будуть передаватися до поліції» [18].

Цільова аудиторія програми: люди, які повернулися з-за кордону і підлягають обсервації; хворі, що знаходяться на домашньому лікуванні, а також особи з підозрою коронавірусної хвороби.

Про рішення пройти самоізоляцію з додатком «Дій вдома» потрібно повідомити під час паспортного контролю. Потрібно сказати свій номер телефону та адресу місця, в якому людина має намір пройти самоізоляцію. Потім потрібно показати співробітнику прикордонної служби вікно керування [16].

Працює програма «Дій вдома» за такими принципами:

1. Передбачається 24 години для прибуття на місце ізоляції. Після цього людина робить перші зразки фото з геолокації, за яким людину будуть ідентифікувати в подальшому;
2. Коли людина прибула на місце ізоляції, починається відлік днів. Додаток відраховує, скільки ще залишилося пробути на особистому карантині;
3. Кілька разів в день надходить повідомлення з проханням зробити фото з включеною на смартфоні геолокацією. Автоматично включається

фронтальна камера і потрібно зробити знімок, в форматі селфі, який, до речі, можуть не прийняти з першого разу;

4. Якщо проігнорувати сповіщення, то прийде нове, і так п'ять разів;

5. Інтервал надходження повідомлень мимовільний, але розробники запевняють, що вночі не будуть турбувати повідомленнями. За спостереженнями користувачів, повідомлення не приходять з 21.00 до 9.00;

6. Коли людина закінчує 14-денну ізоляцію, в додатку активується кнопка «Вийти»: так можна вийти і видалити додаток.

7. Крім основного функціоналу, в програмі є розділ з питаннями і відповідями і можливість здійснити екстрений дзвінок на гарячу лінію Міністерства охорони здоров'я.

8. Ввести в оману додаток неможливо, не рекомендується навіть робити такі спроби. Слід пам'ятати, що за порушення самоізоляції передбачені штрафи від 17 000 грн, домашній режим можуть змінити на проживання в медичному ізоляторі – в обсервації [7].

Також користувача можуть застати зненацька при першій же спробі порушити режим самоізоляції. Після п'яти пропущених підряд сповіщень на телефон приходить повідомлення на червоному тлі, яке ще дає можливість зробити фото, але попереджає, що зволікати не варто. Після такого оповіщення, швидше за все, до людини навідається дільничний або патрульна поліція з перевіркою.

Офіційно поліція не має права виписати штрафи за відсутність відповідей на push-повідомлення або некоректну геолокацію. Але насправді норми дуже неоднозначні, а підставою для штрафу можуть стати результати оперативної перевірки за місцем проживання користувача.

Як заявив Євген Горбачов — керівник Департаменту з розробки програмного забезпечення Міністерства цифрової трансформації: «Ми не маємо права будити людину вночі й робити перевірки. І, звичайно, людина має бути також самоорганізована і відповідальна за те, що вона робить. Ми не робимо браслети, які контролюють. «Дій вдома» не трекає геолокацію



постійно. Ми лише беремо геолокацію в момент, коли робиться фото. І все. Постійної інформації про те, куди людина переміщується у нас нема. Тобто, коли людина робить фото, потім перейде 30 метрів праворуч і ще раз зробить фото, – ми бачимо геолокацію. Де вона була між двома точками – ми не знаємо» [6].

Пандемія коронавірусу поставила під загрозу захист персональних даних, пов'язаних зі здоров'ям. Вони можуть підлягати обробці в випадках, коли ставлять під загрозу, зокрема, інтереси суспільства щодо охорони здоров'я, запобігання поширенню коронавірусної інфекції тощо. Зокрема, «Загальний регламент з захисту даних» дозволяє це робити для наукових досліджень, хоча тільки після згоди людини. По можливості такі дані повинні бути анонімізувати і зберігатися певний час під контролем і відповідальністю тих, хто має до них доступ [6].

У свою чергу, в Україні парламент прийняв зміни до Закону «Про захист населення від інфекційних хвороб» в середині квітня 2020 року, яким тимчасово (на період карантину та до 30 днів після його відміни) дозволяється обробка персональних даних громадян, які захворіли на COVID-19, без їх згоди.

Зокрема, дозволяється обробка даних, що стосуються стану здоров'я, місця госпіталізації або самоізоляції, прізвища, імені, по батькові, дати народження, місця проживання, роботи (навчання) ... «за умови використання таких даних виключно з метою здійснення протиепідемічних заходів».

Протягом 30 днів після закінчення карантину такі дані підлягають знеособленню, а в разі неможливості – знищенню.

Ці норми застосовуються і для використання мобільного додатку «Дій вдома» для моніторингу дотримання самоізоляції чи обсервації громадянами, які прибули з-за кордону, з підтвердженням або підозрою на COVID-19 [17].

Станом на початок травня 2020 року, цим додатком скористалися понад 32 000 фізичних осіб, повідомляє Міністерство цифровий трансформації. За словами експерта Олега Заярного, Міністерство повинно було затвердити

окремий порядок обробки персональних даних у додатку «Дій вдома», попередньо погодивши його з Уповноваженим. Крім того, залишається відкритим питання, що буде з персональними даними тих, хто користувався додатком, після оприлюднення офіційного рішення про скасування карантину. Оскільки в вищезгаданому законі йдеться, що дані можуть бути або знищені, або знеособлені [17].

На рис. 2.1 наведений алгоритм припинення самоізоляції через сервіс «Дій вдома».

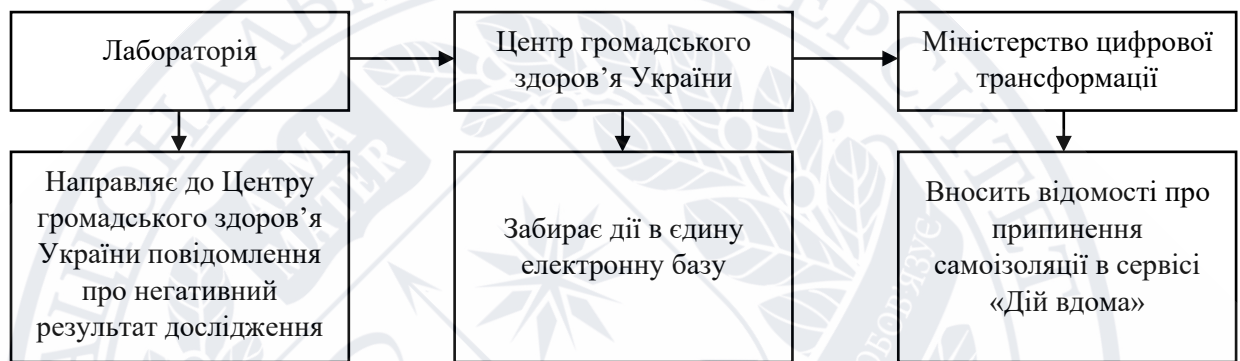


Рисунок 2.1 – Алгоритм припинення самоізоляції через сервіс «Дій вдома» [6]

Знеособлення, тобто виключення ідентифікуючої інформації з даних про місцезнаходження користувача мобільного зв'язку, прийнято вважати однією з гарантій захисту приватності, проте на сьогоднішній день вже добре відомо, що зіставлення знеособлених даних з персональною і загальнодоступною інформацією дозволяє ідентифікувати особу. Щоб виключити таку можливість, урядам потрібно вводити пряму заборону на зіставлення знеособлених даних з іншими персональними даними. Це стало серйозною проблемою в Південній Кореї, де ступінь деталізації історії пересувань осіб з підтвердженням коронавірусом в розісланих SMS-повідомленнях дозволяла «обчислювати» координати конкретної людини. Повідомлялося, що деякі люди, яких на підставі таких повідомлень запідозрили як носіїв вірусу, ставали мішенню ненависницьких висловлювань або утисків. В інших випадках інформація в повідомленнях давала привід для спекуляцій про подружню

невірність і соціальну стигматизацію. Національна комісія з прав людини розкритикувала владу за розголошення більшого обсягу інформації, ніж це необхідно в протиепідемічних цілях, і, відповідно, порушення приватності і прав інфікованої особи, включаючи «вторинні наслідки, коли пацієнт стає об'єктом критики, образ і ненависті в інтернеті». Комісія рекомендувала оприлюднювати тільки час появи носія вірусу в тому чи іншому громадському місці, але не всю історію його пересувань [17].

На думку Ірини Кушнір, навіть в умовах протидії поширенню COVID-19 важливо, щоб оприлюднені дані хворих в сукупності не призводили до можливості їх ідентифікації.

«Є окремі дані, оприлюднивши які принаймні вузькому колу осіб, можна ідентифікувати людину. Якщо повідомляють, наприклад, що в Дарницькому районі захворіло стільки-то людей, то ідентифікації не відбулося. У цьому районі проживає багато людей. Втім, якщо говорять про маленьке містечко, де називають конкретну адресу і ще й дату народження або професію, то його мешканці дізнаються, про кого йде мова», – пояснює вона, відзначаючи, що в такому випадку мова йде про поширення персональних даних [18].

На її думку, щоб дотримуватися принаймні чинного законодавства щодо захисту персональних даних, потрібно притягати до відповідальності тих, хто його порушує. «Інакше не буде забезпечено стримуючого ефекту. Всі будуть знати, що дані можуть розголосити або продати, і ніхто не понесе відповідальності за це», – додає вона [18].

Незалежно від того, ставив користувач додаток чи ні, дані про нього зберігаються в системі «Дій вдома». Нещодавно прийнятий закон дозволив збір та обробку персональних даних користувачів без їх згоди в разі, якщо це стосується боротьби з епідемією. У постанові Кабміну органам влади дозволяється обробляти в системі «Дій вдома» такі дані (табл. 2.1).



Таблиця 2.1 – Дані у системі «Дій вдома», які у постанові Кабміну органам влади дозволяється обробляти

	Медичні працівники	Центр громадянського здоров'я, епідеміологічні установи МОЗ	Мінцифри	Національна поліція Національна гвардія	Органи соціального захисту
ПІБ	+	+	+	+	+
Дата народження	+	+	+	+	+
Місце самоізоляції	+	+	+	+	+
Місце реєстрації	+	+	+	+	+
Місце проживання	+	+	+	+	+
Номер телефону	+	+	+	+	+
Місце роботи/навчання	+	+	+		
Стан здоров'я	+	«короткі відомості»*	«короткі відомості»*		
Стать	+				+
Необхідність піклування (соціального супроводу)	+			+ (за наявності в системі)	За згодою
Контактні особи	+ (за наявності)	+			

Джерело: складено за даними [18]

Тут потрібно уточнити два моменти:

Система «Дій вдома» – це щось на зразок електронного реєстру, куди вносять дані людей, які контактували з хворими, які повернулися з-за кордону, які хворіють в легкій формі і т. д. Додаток «Дій вдома» – один з каналів роботи з цим реєстром, з можливістю перевіряти, чи дійсно конкретний користувач перебуває вдома.

Особи старше 60 років не зобов'язані ставити додаток, якщо тільки немає підозри, що вони могли захворіти. Але вони повинні дотримуватися самоізоляції. Як пояснює юрист «Лабораторії цифрової безпеки» Віта Володовська, дані про осіб старше 60 років не вносять в систему «Дій вдома» автоматично.

«У систему «Дій вдома» вносять дані тільки про осіб, які повернулися з-за кордону, контактували з хворим або хворіють на Covid-19 в легкій формі.

Відповідно, всі особи старше 60 років в Україні не зобов'язані встановлювати цей додаток. Але цей пункт Правил означає в той же час, що поліція має право зупиняти їх на вулиці і уточнювати мету», – пояснює юрист.

Важливий пункт у Порядку, який стосується штрафів за невикористання цього додатка: повідомлення в додатку «не можуть бути окремою підставою для притягнення особи до адміністративної відповідальності за порушення правил карантину». Тобто, якщо користувач не встиг зробити і вислати селфі, або у нього не збіглася геолокація, поліція має право приїхати перевірити, чи сидить він удома, але не має права виписати штраф (п. 13 Порядку). Але цей пункт сформульований не надто чітко, і 100% бути впевненим в тому, що відповідальності за «неправильну геолокацію» не буде – не можна [39].

Міжнародні норми про права людини передбачають, що навіть коли держава в умовах надзвичайного стану обмежує права і свободи в інтересах охорони здоров'я населення, то такі обмеження повинні бути законними, необхідними і пропорційними. Надзвичайний стан має бути обмежений за часом, а будь-які обмеження прав людини повинні враховувати непропорційні наслідки для окремих категорій населення або маргіналізованих груп [47].

Ці принципи застосовні і до заходів реагування на COVID-19 з використанням даних про місцеперебування користувачів мобільного зв'язку. В ході збору і аналізу таких даних може бути отримана інформація про особу, пересування і контакти користувачів, що загрожує обмеженням права на недоторканність приватного життя. Стаття 17 Міжнародного пакту про громадянські і політичні права, заснована на статті 12 Загальної декларації прав людини свідчить, що «ніхто не може зазнавати безпідставного чи незаконного втручання в його особисте і сімейне життя, свавільних чи незаконних посягань на недоторканність його житла, таємниці його кореспонденції». Комітет з прав людини в своєму зауваженні загального порядку за цією статтею вказує, що втручання в право на особисте життя «взагалі не може мати місця за винятком випадків, передбачених законом».

При цьому обмеження повинні бути пропорційними щодо шуканої мети і необхідними з урахуванням гостроти ситуації [39].

Human Rights Watch і ще понад 100 неурядових організацій закликали уряди поважати приватність і права людини при використанні цифрових технологій для стримування пандемії [47].

На нашу думку, при цьому повинні дотримуватися як мінімум такі умови:

- повинні бути законними, необхідними, пропорційними, прозорими і виправданими з точки зору законної мети в галузі охорони здоров'я населення;
- повинні бути обмежені за часом і діяти тільки на період, необхідний для боротьби з пандемією;
- повинні бути обмежені за масштабами і прийматися виключно в цілях боротьби з пандемією;
- повинні забезпечувати достатній рівень захисту будь-яких збираються персональних даних;
- повинні враховувати ризики дискримінації та інших порушень прав людини щодо маргіналізованих груп населення;
- повинні забезпечувати прозорість будь-яких домовленостей про обмін даними з іншими державними і приватними діями;
- повинні включати гарантії недопущення неправомірного стеження і забезпечення доступу до ефективних засобів правового захисту;
- повинні включати механізми вільної, активної і змістовної участі зацікавлених сторін.

## **2.2. Переваги та недоліки додатку «Дій вдома», особливості системи захисту інформації додатку**

З початку режиму «Дій вдома» веде звіт. Основне вікно показує, скільки днів залишається до завершення самоізоляції. Під час використання програми,



кілька разів користувачі мають право отримати повідомлення з вимогою зробити селфі для підтвердження свого місцезнаходження. Всі push-повідомлення приходять в різний період, і часто без звуку. На жаль, не завжди всі бачать його своєчасно і встигають протягом 15 хвилин зробити своє фото. Тому тільки за один місяць правоохоронці отримали з додатка більше 1000 повідомлень про порушення самоізоляції. Якщо користувач не встиг підтвердити своє селфі, поліція має право виїхати до нього додому, щоб упевнитися про його місцезнаходження.

До роботи додатка багато зауважень. Він активується з українського номеру телефону з підтвердженням по SMS. Потім на кордоні цей номер повинні ввести в систему прикордонної служби. Але програма не має ніякого захисту. Безліч людей активували додаток в літаку або ще за кордоном, і тепер у них неправильна геолокація і додаток не працює [46].

Якщо користувач приїхав додому, активував додаток, але в цей момент геолокація збилася (наприклад, неправильно визначена оператором), додаток запам'ятає саме її назавжди, без можливості виправити. Що би людина не робила – авторизація буде неуспішною через розбіжність геолокації.

Якщо користувач авторизувався по мобільному інтернету, а потім перейшов на Wi-Fi, геолокація по провайдеру першого і другого може бути різною, і знову нічого може не працювати.

Користувачеві приходять push-повідомлення, щоб він робив селфі і відправляв їх на сервер разом з даними геолокації. Проблема в тому, що в 90% телефонів push-повідомлення за замовчуванням відключені у фоновому режимі, щоб не розряджати батарею. Тобто, поки людина не розблокує телефон, вона не дізнається, що прийшло push-повідомлення, а коли побачить його – буде пізно, оскільки «вже було здійснено порушення».

Найбільша проблема додатку – це те, що користувач може випадково зробити дію, яку потім ніяк не виправити, і яка заблокує нормальну роботу програми назавжди. Це – кричущий прорахунок для такого сервісу, адже ним користуються люди, які взагалі не розбираються в техніці [46].

Також є претензії до додатка і в українських правознавців. Юрист «Ader Haber Law Firm» Володимир Бабичев зазначив, що українці при установці додатка повинні враховувати такі особливості: у випадку збоїв в роботі карт або додатку людину можуть притягнути до відповідальності за надання неправдивих відомостей, які стосуються самоізоляції. Маються на увазі випадки, коли фактична геолокація (наприклад, будівлі) не збігається з реальною на карті.

Поліція отримує і наповнює базу даних про людину, не дивлячись на те, що раніше така можливість була передбачена тільки щодо затриманих за підозрою у правопорушеннях за ч.2 ст.26 та п.7 ч.1 ст.26 Закону «Про національну поліцію». Поліція отримує ще одну можливість збирати інформацію про соціальні зв'язки людини не в порядку, передбаченому законом.

Фото користувача може з'явитися в протоколі розпізнавання особи по фотографії в рамках кримінального провадження (за порушення режиму самоізоляції, які призвели до тяжких наслідків, в тому числі – до смерті третіх осіб передбачена кримінальна відповідальність).

Проблеми з роботою GPS, неможливість увійти в додаток, багато проблем, пов'язаних з відправкою фото і їх верифікацією – до таких умов карантину варто готуватися українцям, які виявлять бажання самоізолюватись вдома.

Заступник міністра охорони здоров'я з питань цифрового розвитку Руслан Кучер розповів про поліпшення та нововведення додатку «Дій вдома» 2 грудня 2020 року [7].

Відзначається, що тепер в додатку «Дій вдома» збільшений термін верифікації особистості – з 15 хвилин до 20 хвилин. Стільки часу дається на те, щоб зробити фотографію. Нагадування приходять кожні 4 хвилини, поки людина на ізоляції не сфотографується. Також розробники додали можливість вказати перелік контактних осіб.

Серед інших нововведень Руслан Кучер назвав:

- Таймер на 24 години для досягнення місця самоізоляції.
- З'явилася дія «Залишення місця самоізоляції». Це можна зробити, наприклад, щоб вийти на прогулянку з собакою, піти в аптеку або поїхати на тестування.
- З'явилася функція перевірки симптомів на прикладі питання-відповіді.

Тепер в додаток приходить офіційне оприлюднення при отриманні негативних результатів ПЛР-тестів [7].

Також використання додатку несе певні ризики, з якими може зіткнутися користувач в аспекті захисту інформації. По-перше, такі ризики включають несанкціонований доступ до даних, що генеруються у мобільних додатках, анонімізацію самоізолюваних або відстежуваних осіб, невиправданий контроль їх руху шляхом відстеження геолокації конкретних осіб, особисті дані для використання таких даних як публічних, оброблення інформації про фізичних осіб поза встановлені національним законодавством строки, а також несанкціоноване втручання в роботу мобільних пристроїв, в яких встановлені мобільні додатки тощо.

Як заявляє Євген Горбачов: «Щодо того, що додаток не впізнає людину. Поясню, як це працює. Спочатку ми забираємо фотографію, потім в серверній частині обробляється фотографія еталонна, яка робилась перший раз, коли людина прибула. Береться це фото і звіряється по точках, там дуже тонка технологія. І якщо на тій фотографії, яку ви зробили, буде засвіт, тобто, якщо ви будете стояти, за вами вікно і світить яскраво сонце, й у вас може бути засвіт однієї частини обличчя, то, звичайно, буде помилка розпізнавання. Або часто люди роблять фото чомусь знизу. І, звичайно, коли людина лежить, в неї трохи змінюється обличчя. Тому можуть бути історії, коли буде запит на ще одне розпізнавання. Щодо сповіщень про відсутність інтернету або некоректного розпізнавання геолокації – таке буває, коли людина приховує GPS або використовує VPN» [6].



Щоб захистити свої персональні дані під час користування додатком «Дій вдома», необхідно здійснити такі дії:

- не надавати (не завантажувати) більше персональних даних про себе, ніж це встановлено підпунктом 1 пункту 2 розділу II «Прикінцеві та перехідні положення» Закону № 555-IX;

- якщо через тридцять днів з дати офіційного завершення карантину та пов'язаних з цим епідеміологічних заходів на ім'я суб'єкта персональних даних користувач мобільного додатку «Дій вдома» не отримує повідомлення про видалення, варто звернутися з відповідним клопотанням до розпорядника мобільного застосунку «Дій вдома» – Міністерства цифрової трансформації України;

- якщо Міністерство цифрової трансформації України не вживає необхідних заходів після припинення мети та умов обробки персональних даних у мобільному додатку «Дій вдома», а саме – видалення персональних даних, що обробляються з використанням додатку «Дій вдома» або особи, персоналізація, обробка персональних даних якої буде продовжуватися, вона має право звернутися до Верховної Ради України з прав людини з приводу незаконних дій держателя порталу «Дій вдома»;

- оскаржити незаконні рішення, дії чи бездіяльність Міністерства цифрової трансформації України позовом безпосередньо до Київського окружного адміністративного суду як щодо власника персональних даних, які обробляються у мобільному додатку «Дій вдома» [17].

З одного боку, особисті дані не можуть оброблятися більше 30 днів після закінчення карантинних заходів, а з іншого боку, персональні дані, що обробляються відповідно до Закону № 555-IX, повинні бути знищені, якщо це неможливо – знеособленими. Тому питання, що буде з персональними даними після оголошення офіційного рішення про скасування карантину, залишається відкритим.

Згідно з одним із офіційних ресурсів Кабінету Міністрів України, мобільний додаток «Дій вдома» базується на зарубіжному досвіді країн, які

використовують цифрові пристрої для забезпечення безпеки громадян під час пандемії. За своїми принципами роботи, IT-архітектурою та функціями мобільний додаток «Дій вдома» подібний до польської Kwarantanna Domowa.

Однак офіційні дані про IT-архітектуру мобільного додатку «Дій вдома», на основі якого здійснюється обмін інформацією, офіційні джерела інформації про умови технічного захисту інформації в цьому мобільному додатку не дають чіткого переліку стандартів, якими керуються замовники (Міністерство цифрової трансформації України) [17].

Крім того, з урахуванням положень частини 10 статті 6 Закону України «Про захист персональних даних» від 01 червня 2010 року № 2297-VI та підпунктів 1.1. та 1.2. Типового порядку обробки персональних даних, затвердженого Наказом Уповноваженого Верховної Ради України з прав людини від 08 січня 2014 року № 1/02-14, Міністерство цифрової трансформації України мало узгодити з уповноваженим Верховної Ради з прав людини окремий порядок обробки персональних даних у мобільному додатку «Дій вдома». Однак наразі такого порядку немає [16].

У будь-якому випадку, для забезпечення законності транзакцій, пов'язаних з використанням мобільного додатку «Дій вдома», цей додаток повинен базуватися на стандартах прав людини для захисту персональних даних, а не для втручання в особисте та сімейне життя, здійснювати їх автоматизовану обробку, як визначено в актах Ради Європи.

Сюди входять, зокрема, вимоги статті 8, частини 1 статті 3 Конвенції про захист прав людини та основоположних свобод та статей 5-9 Конвенції Ради Європи № 108 Про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних.

Як вважає Павло Белоусов, експерт Школи цифрової безпеки DSS380: «Що з цими даними буде робити поліція та чи будуть вони використовуватися тільки для тих цілей, які позначені, ми не дізнаємося. В угоді зазначено, що з даними може відбуватися, а саме: збирання, реєстрація, накопичення, зберігання, адаптація, зміна, поновлення, використання і

поширення (розповсюдження, реалізація, передача), знеособлення, знищення. Це може мати негативні наслідки. Та й проблема не тільки в тому, що ці дані будуть зібрані, а й в тому, що держава не зупиниться і буде прагнути до того, щоб контролювати людей не тільки під час епідемії, а й всі 365 днів в році. Справа не лише у контролі, але й у здатності держави зберігати дані українців захищеними. Український уряд не здатний убезпечити персональні дані своїх громадян, які потенційно є уразливою групою пацієнтів з підозрою на COVID-19» [18].

Як наголошує керівник програм нових медіа ГО «Інтерньюз-Україна» Віталій Мороз: «Витоки даних нерідко стаються з вини чиновників. Якою може бути реакція на плани уряду контролювати поведінку цієї уразливої групи через розроблений додаток? Це стане черговим порушенням базових прав людини у ситуації низької довіри до дій уряду. Більше того, за цією логікою уряд має зобов'язати усіх користуватися смартфоном, передплачувати послуги з інтернету, встановлювати якісь додатки. Це поза будь-якою логікою здорового глузду під гаслом спільної турботи про здоров'я» [18].

Отже, додаток має велику кількість недопрацювань, серед яких – запізніла ідентифікація, проблеми з визначенням реальної геолокації, нерівномірні в часі сповіщення, загрози розголошення даних з огляду на законодавчо-правові проблеми в цьому питанні. Слід також зазначити, що сьогодні в Україні немає необхідності встановлювати та використовувати мобільний додаток «Дій вдома», щоб контролювати дотримання процедури самоізоляції. Самоізоляція або спостереження можуть також здійснюватися спеціальними спостерігачами.



### **РОЗДІЛ 3. ЗАРУБІЖНИЙ ДОСВІД ВИКОРИСТАННЯ ДОДАТКІВ ДЛЯ КОНТРОЛЮ ЗА САМОІЗОЛЯЦІЄЮ ТА НАПРЯМКИ ВДОСКОНАЛЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ ДОДАТКУ «ДІЙ ВДОМА»**

#### **3.1. Особливості використання додатків для контролю за самоізоляцією в іноземних країнах**

Зростаюче використання урядами даних про місцеперебування користувачів мобільного зв'язку для боротьби з поширенням Covid-19 пояснюється цілком зрозумілими міркуваннями охорони здоров'я населення, оскільки будь-яка вірусна інфекція – це перш за все контакти між людьми. Базована в Лондоні організація Privacy International веде моніторинг відповідних практик урядів, технологічних компаній і міжнародних організацій. Нижче наведемо деякі приклади.

Влада може отримувати доступ до даних мобільних мереж. В Ізраїлі уряд 17 березня 2020 р. надав службі контррозвідки і внутрішньої безпеки «Шин-Бет» право запитувати у мобільних операторів та обробляти «технічні дані», включаючи місце розташування абонентів, без згоди останніх з метою виявлення кола осіб, які контактували з носієм вірусу. В рамках цієї програми міністерство охорони здоров'я розсилає на відповідні номери попередження про необхідність самоізоляції. Дане рішення було прийнято кабінетом в обхід парламенту, і верховний суд згодом постановив, що уряд повинен провести закон, який «забезпечує дотримання принципів захисту приватності», в іншому випадку програма повинна бути зупинена. 23 березня 2020 р. міністерство охорони здоров'я випустило спеціальний додаток, який встановлюється добровільно і попереджає користувача, якщо він контактував з інфікованою людиною [47].

У Вірменії парламент 31 березня надав владі гранично широкі повноваження щодо стеження за громадянами, зобов'язавши мобільних

операторів надавати відомості по всім абонентам, включаючи номер і місце розташування телефону, дату і час кожного дзвінка і SMS-повідомлення. Влада може використовувати цю інформацію для виявлення інфікованих осіб, котрі підлягають ізоляції та самоізоляції, близько контактували з інфікованими, а також для моніторингу дотримання карантинних заходів.

У Росії прем'єр-міністр 20 березня 2020 р. доручив Мінкомзв'язку розробити на основі даних мобільних операторів загальнонаціональну систему відстеження осіб, які контактували з хворими на COVID-19. 1 квітня 2020 р міністерство відзвітувало про виконання. Воно запросило у регіональних органів влади знеособлені списки мобільних номерів носіїв коронавірусу і людей, що знаходяться на самоізоляції після повернення з-за кордону або контактів з підтвердженими носіями [47].

В Еквадорі президент 16 березня 2020 р. своїм надзвичайним указом дозволив уряду використовувати дані супутникового та мобільного зв'язку для моніторингу людей, у яких виявлено коронавірус, які близько контактували з хворими, а також тих, у кого є характерні симптоми або хто знаходиться на обов'язковій самоізоляції після повернення з-за кордону.

Лідерами по впровадженню систем очікувано виявилися держави Азії. Справа тут, мабуть, не тільки в технічному розвитку (наївно припускати, що найрозвиненіші європейські країни не володіють технологіями для впровадження аналогічних систем), але й у відносно спокійному ставленні населення до контролю держави за пересуванням жителів. Країни Європи також фігурують в списку держав, де системи цифрового контролю присутні, але, по-перше, таких країн небагато, а по-друге – системи там в основному стосуються контролю саме інфікованих людей, що знаходяться на суворому карантині, а не всіх громадян [42].

Однією з перших країн, де населення стали контролювати, очікувано став Китай. Одна з варіацій на тему «карантинного IT» була введена на батьківщині нового коронавірусу ще в лютому 2020 р. Йдеться про програму Alipay Health Code, розроблену «дочкою» Alibaba за підтримки влади

Піднебесної. Запущена вона було 11 лютого 2020 р. в столиці провінції Чжецзян – в місті Ханчжоу, широкого поширення програма набула в березні.

Кожен зареєстрований в системі користувач отримує колірний код. Зелений дозволяє вільно пересуватися, при жовтому коді користувача можуть попросити залишитися вдома на тиждень, при червоному – обов’язковий карантин на два тижні. QR-код генерується на підставі анкети, в якій вказується інформація, наприклад, про те, чи хворів користувач або хтось із його родичів, а також дані про поїздки всередині країни або за кордон. За даними The New York Times, додаток ділиться інформацією з поліцією.

У Тайвані, що знаходиться неподалік від провінції Хубей, звідки почав поширення COVID-19, діє інша система, відома там як «електронний паркан». Система призначається для жителів, які повинні бути на карантині. «Електронний паркан» стежить за активністю телефону знаходиться на карантині людини і отримує повідомлення, якщо пристрій не подає сигналів більше 15 хвилин, – і викликає інтерес представників органів влади до місцезнаходження телефону і, що важливіше, його власника. Крім цього, Тайвань використовує і систему цифрового відстеження, схожі застосовуються і в інших азіатських країнах – наприклад, в Південній Кореї та Сінгапурі [42].

В острівній місті-державі жителям пропонують встановити додаток TraceTogether. Інформації про те, наскільки пропозиція установки наполеглива, виявити не вдалося. Основна суть сінгапурської програми, як і в додатках з багатьох інших країн (про них буде розказано нижче), у виявленні контактів хворих. Програма фіксує взаємодії між усіма користувачами через Bluetooth – наприклад, коли вони проходять повз один одного. При зближенні з людиною, у якої був позитивний тест на коронавірус, додаток сигналізує про це і пропонує зв’язатися з владою для організації тесту на COVID-19. У використанні Bluetooth, до речі, основна відмінність TraceTogether від програм з інших країн – зазвичай для виявлення контакту використовуються дані про місцезнаходження в поєднанні з інформацією про місцезнаходження людей,



які заразилися – тут же телефони постійно шукають один одного, забезпечуючи інформацію про соціальні контакти.

Схожа за своєю суттю система діє і в Ізраїлі. Додаток «Ха-Маген» (в перекладі з івриту – «Щит») від Міністерства охорони здоров'я дозволяє дізнатися, чи перебував користувач поруч з хворим на коронавірус. При необхідності «Ха-Маген» може і надіслати повідомлення про це. Як окремо зазначає МОЗ, інформація про місцезнаходження зберігається тільки на пристрої користувача і не передається далі. Ізраїльське відомство стверджує, що додаток «заснований на відкритому вихідному коді і цінностях солідарності». Інформація про контакти з хворими береться з постійно оновлюваних даних МОЗ. Втім, судячи з відгуків, додаток часто спрацьовує помилково: досить багато повідомлень про те, що додаток попереджає про недавні контакти в тих місцях, де користувач не був [42].

У Південній Кореї, де не був оголошений загальний карантин, влада отримувала інформацію про переміщення жителів з даних GPS, а також з даних про транзакції по банківських картах. Стосується це, щоправда, тільки людей, що знаходяться на карантині (найчастіше це люди, які приїхали з інших країн, і які контактували з хворими, або люди з підтвердженням COVID-19). При цьому, деякі порушники залишають смартфони в будинку або відключають функцію GPS – в результаті влада обговорює можливість контролю за пересуванням мешканців за допомогою електронних браслетів. Також у Південній Кореї влада на додаток до відстеження носіїв вірусу по мобільному трекінгу, камер зовнішнього спостереження і використання інформації про використання банкоматів і банківських карт розробила на основі агрегованих даних публічну карту випадків зараження, яка дозволяє громадянам перевірити вірогідність контактів. Ця карта була офіційно запущена 26 березня 2020 р. Органи охорони здоров'я також розсилають користувачам мобільних телефонів докладні повідомлення з інформацією про підтверджені випадки, включаючи вік, стать і пересування людини за дві доби. Це робиться для того, щоб ті, хто випадково контактували з хворими особи

(наприклад, відвідувачі того самого ресторану в той же час) були готові до того, що і у них може виявитися коронавірус [42].

Стежать за інфікованими на коронавірус за допомогою телефону і в Туреччині. Використовуються для цього дані мобільних мереж. МОЗ розробило програму з метою спостереження за тими, хто був заражений COVID-19. Вона повинна відстежувати пересування і при виході на вулицю – надсилати попередження. Людям, що знаходяться на карантині, також надійде телефонний дзвінок, в якому нагадають про необхідність дотримання ізоляції.

А ось в більшості країн Європи ситуація з «технологічними» рішеннями, пов'язаними з коронавірусом, відрізняється від азіатської. Навряд чи це можна пояснити рівнем розвитку цифрових технологій – справа швидше в ставленні до самого стеження за громадянами. Ті нечисленні рішення, які є, передбачають прямий і постійний моніторинг місця розташування людини, хоча деякі з них і можуть періодично отримувати дані геолокації.

Наприклад, в Польщі уряд розробив додаток під промовистою назвою Home Quarantine («Домашній карантин»). Призначений він для людей, які повинні знаходитися на карантині протягом 14 днів після повернення з-за кордону. Користувач сервісу повинен після реєстрації відправляти селфі з геолокаційні даними за запитом. Якщо протягом 20 хвилин запит залишився без відповіді – поліція отримує попередження про порушення. Представник прес-служби міністерства впровадження цифрових технологій Польщі каже, що «у людей на карантині є вибір: або несподіваний візит поліції, або завантаження програми і виконання її вимог» [47].

В одній з країн Західної Європи, яка сильно постраждала від коронавірусу, – Франції – додатково до друкованого формуляру, необхідного для виходу з дому, ввели можливість отримання QR-коду. Онлайн-форма, яку потрібно заповнити на сайті уряду для отримання коду, не дозволяє владі зберігати дані французів: QR-код генерується на пристрої користувача, що має виключити витік інформації. По суті, за QR-кодом ховається все той же заповнений бланк, необхідний у Франції для виходу з дому ще з 16 березня,

тільки тепер його не потрібно носити в паперовому вигляді. У бланку повинні бути вказані ім'я, дата народження, адреса проживання і причина виходу з дому.

Нарешті, ще в одній з європейських країн, Чехії, планується ввести так званий «розумний карантин». Система поки не запущена, але прем'єр-міністр країни Андрей Бабіш заявляв, що вона повинна бути альтернативою жорсткого карантину. Матися на увазі під «розумним карантинном» буде відстеження переміщення інфікованих за допомогою обробки даних телефону і банківських карт з подальшою ізоляцією і тестуванням всіх людей, які вступали в контакт з носієм COVID-19 [47].

Дані про місцезнаходження користувача мобільного зв'язку можуть бути отримані різними способами, включаючи базові станції, GPS-сигнал і Bluetooth-маячки:

Позиціонування по базовим станціям. Зв'язок між користувачами і підключення до інтернету здійснюється через базові станції в центрі кожної «соти». У міру руху власника пристрою він зв'язується з різними базовими станціями, і ця інформація зберігається у оператора мобільного зв'язку. По трьом базовим станціям методом «триангуляції» можна досить точно встановити місце розташування мобільного пристрою. Уряди можуть вимагати від оператора мобільного зв'язку надавати такі відомості як за поточними, так і за минулими пересуваннями.

GPS-сигнал. Вбудована в мобільний телефон функція геолокації по GPS-сигналу дозволяє визначити його місце розташування з точністю від 1,5 до 3 метрів. Ця функція використовується безліччю мобільних додатків (карти, соцмережі, ігри, шопінг, службові програми), і журнал завантажень даних геолокації може виявитися доступним владі і компаніям, які займаються комерціалізацією даних. Серед останніх є як великі, так і маловідомі компанії, що збирають дані про потенційних споживачів і потім продають їх безпосередньо або засновану на них аналітику на вільному ринку. На сьогоднішній день з'явилося вже безліч GPS-додатків для відстеження



контактів і дотримання карантину. Крім цього, знеособлені дані геолокації можуть використовуватися для моделювання потоків людей як в минулому, так і в режимі реального часу.

Bluetooth-маячки. Bluetooth являє собою технологію малопотужного бездротового зв'язку на короткій відстані (в межах близько 10 метрів), яка переважно використовується для прямого з'єднання пристроїв один з одним. Для цілей відстеження контактів людині буде запропоновано використовувати спеціальний додаток, який за сигналом Bluetooth здатний з відносно високою точністю встановити факт знаходження мобільного телефону поруч з іншими пристроями. В силу цього даний метод можна найпростіше охарактеризувати як трекінг контактів [47].

Методи застосування у всіх додатках різні. В Азії, хоча смартфони та геолокація використовуються для виявлення та повідомлення про контакт людей із носіями коронавірусу, держави-члени Ради Європи використовують таку технологію, щоб перевірити, чи ізолюються громадяни від безпосереднього контакту з пацієнтами, які хворіють. В даний час ЄС веде переговори з операторами зв'язку щодо активного підписання колекції конфіденційної інформації про місцезнаходження та розробку єдиного мобільного додатку, який допоможе запобігти поширенню коронавірусу [14].

Проаналізувавши зарубіжний досвід використання таких додатків, погоджуємося з думкою, що «відмінність України в тому, що через слабкі державні інститути, схильність можновладців до популізму й високий запит на «сильну руку» нинішні обмежувальні заходи можуть стати лише початком для подальшого посилення наступу на права людини і її приватність під приводом антивірусної боротьби».

### **3.2. Напрями вдосконалення додатку «Дій вдома» та підвищення захисту інформації додатку**

Рада Європи узагальнила рекомендації у Спільній заяві про контроль цифрових комунікацій. Умовно їх можна звести до:

1. Встановлення мобільних додатків для цифрового контролю зв'язку повинне бути добровільним та прозорим.

2. Метою цифрової системи спостереження за COVID-19 є виявлення людей, яким загрожує зараження. Це повністю виключає подальшу обробку даних для не пов'язаних цілей, таких як комерційні або правоохоронні цілі.

3. Враховуючи унікальний характер інформації про місцезнаходження та близькість людей, яку можна визначити, не визначаючи їх місцезнаходження, моніторинг цифрового зв'язку повинен базуватися на записах зв'язку між пристроями (наприклад, дані, що генеруються GPS, а не на даних про місцезнаходження).

4. Дуже важливо забезпечити якість та точність інформації, оскільки люди, визначені потенційними контактуючими з зараженою людиною, можуть спричиняти серйозні наслідки (самоізоляція, тестування).

5. Дані, розроблені з метою управління цифровим зв'язком, повинні бути мінімальними. Незв'язані та небажані дані не можуть збиратися для цілей відстеження.

6. Не повинно бути прямої ідентифікації користувачів системи управління даними, такі системи повинні використовувати лише як унікальні та безособові ідентифікатори, створені та властиві системі. Ці ідентифікатори повинні постійно оновлюватися та бути криптографічно стабільними.

7. Системи управління цифровими комунікаціями повинні базуватися на архітектурі, яка максимально покладається на обробку та зберігання даних на окремі користувацькі пристрої.

8. Дані, що використовуються для моніторингу цифрових комунікацій, слід зберігати лише під час пандемії COVID-19. Беручи до уваги

епідеміологічне значення (наприклад, інкубаційний період вірусу), необхідно встановити часові обмеження для зберігання даних [17].

Для удосконалення додаток вимагає чимало доробок. За багатьма відгуками користувачів беззвучні push-повідомлення – це не найкращий варіант в порівнянні зі звичайним SMS. Інші скаржилися на несвоєчасну верифікацію особистості користувача.

Знеособлення і безпечне зберігання даних – це важливі аспекти розробки, що вимагають пильного контролю в додатку «Дій вдома». Зібрані дані повинні знеособлюватися в максимально можливій мірі, а ризики зворотної ідентифікації – доводитися до користувачів в максимально зрозумілій і доступній формі. Розробники також повинні розкривати інформацію про те, яким чином зібрані дані захищаються від спроб третіх сторін отримати до них несанкціонований доступ або змінити їх. Наприклад, можна поставити питання: чи використовуються в програмі надійні методи інформаційної безпеки (такі як кінцеве шифрування) і підлягають ці методи регулярної перевірки.

Програма повинна перевірятися на відповідність перерахованим вище стандартам. Розробники повинні відстежувати соціально-політичний контекст і забезпечувати наявність механізмів і протоколів захисту від недобросовісного використання.

Також прем'єр-міністр України Денис Шмигаль заявив, що додаток чекає 5 основних цифрових рішень, які вдосконалять його роботу. «Сьогодні хочу представити 5 основних цифрових рішень, які мають допомогти приборкати пандемію в Україні й які будуть запроваджені найближчим часом. Вони розробляються і ми представимо їх:

- цифровізація й централізація збору інформації про факти підозри та випадків інфекційних захворювань;
- вдосконалення мобільного додатку «Дій вдома» із впровадженням автоматичних штрафів за порушення режиму самоізоляції;



- запуск електронного рецепту на ліки, антибіотики та розширення програми «Доступні ліки» на антибіотики, необхідні для боротьби з COVID в додатку «Дій вдома»;
- запровадження електронного направлення на ПЛР (тестування), що дасть можливість відслідковувати черги і не утворювати їх у режимі реального часу;
- QR-коди для публічних місць, які централізовано генерують і розміщують самі заклади.

Подібна система (QR-кодів) діє у Великій Британії, це єдина країна. Ми будемо швидко рухатися і будемо другою країною, яка запровадить подібні заходи» [16].

Для того, щоб в наочному вигляді оцінити те, що не вистачає користувачам додатку «Дій вдома», було проведене опитування, в якому в інтернет-режимі було опитано 50 осіб, які користувалися додатком. Результати опитування (відповіді на питання «Що саме не вистачає додатку «Дій вдома», на вашу думку?») наведені на рис. 3.1.



Рисунок 3.1 – Результати опитування щодо напрямків вдосконалення додатку «Дій вдома»

Таким чином, як відзначають самі користувачі, найбільша кількість незадоволених та занепокоєних ситуацією з тим, що в додатку немає функції анонімізації користувачів, які захворіли, а також користувачам не вистачає впевненості про те, що дані будуть видалені після закінчення самоізоляції.

Для вирішення даних незручностей для користувачів рекомендується встановити на початку використання та наприкінці інтерактивне вікно щодо того, які саме дані про користувача будуть використовуватися, куди вони будуть спрямовуватися, та в якому саме порядку вони будуть видалятися з бази даних. Також в додатку слід автоматично видаляти всі дані людей, які пробули на самоізоляції встановлений термін, та які були вже використані для ведення обліку та контролю людини. Для цього слід розробити більш синхронний зв'язок з базою даних Міністерства цифрової трансформації України, щоб дані, які вже не використовуються додатком, відразу видалялися у Міністерстві цифрової трансформації України.

Крім того, пропонується для анонімізації в додатку використовувати технологію визначення місця розташування, яка базувалась би на використанні даних з браузера та інших додатках в телефоні користувача, фактично не порушуючи принципи захисту особистої інформації в інтернеті. Зокрема, можна використовувати Cookies браузера, не використовуючи персональних даних людини, а використовуючи такі самі алгоритми, як використовує Google, щоб пропонувати потім контекстну рекламу на сайті пошукової системи. В цьому випадку за допомогою додатку «Дія вдома» буде змога фіксувати навіть такі дані, як геолокація, з огляду на те, де людина найчастіше перебувала ввечері, перед сном (коли з телефоном відбувалося найменше дій). Це дозволить більш ефективно використовувати даний додаток.

Таким чином, дані нововведення, на нашу думку, дозволять, по-перше, краще забезпечити людей контролем за самоізоляцією, і, по-друге, краще забезпечити персональні дані людей, оскільки їх використовуватиметься менше, і вони будуть більш анонімними.

## ВИСНОВКИ

Проведене дослідження дозволило зробити такі висновки.

1. Інформаційна безпека – стан захищеності інформаційних ресурсів (інформаційного середовища) від внутрішніх і зовнішніх загроз, які могли б зашкодити інтересам особистості, суспільства, держави (національним інтересам). Втрата конфіденційної інформації приносить моральної чи матеріальної шкоди. Умови, що сприяють неправомірному оволодінню конфіденційною інформацією, зводяться до її розголошення, витоку і несанкціонованого доступу до її джерел. У сучасних умовах безпека інформаційних ресурсів може бути забезпечена тільки комплексною системою захисту інформації. Комплексна система захисту інформації повинна бути: безперервною, плановою, цілеспрямованою, конкретною, активною, надійною. Система захисту інформації повинна спиратися на систему видів власного забезпечення, здатного реалізувати її функціонування не тільки в повсякденних умовах, але і в критичних ситуаціях.

2. Комплексна безпека інформаційних ресурсів досягається використанням правових актів державного та відомчого рівня, організаційних заходів і технічних засобів захисту інформації від різних внутрішніх і зовнішніх загроз. Правові заходи забезпечення безпеки та захисту інформації є основою порядку діяльності і поведінки співробітників всіх рівнів і ступеня їх відповідальності за порушення встановлених норм і правил роботи із забезпечення збереження комерційних секретів. Організаційні заходи є вирішальною ланкою у формуванні та реалізації комплексних заходів захисту інформації. Вони, в першу чергу, виражаються в створенні служби безпеки організації і забезпеченні її нормального функціонування.

3. Пандемія коронавірусу поставила під загрозу захист персональних даних, пов'язаних зі здоров'ям. Вони можуть підлягати обробці в випадках, коли ставлять під загрозу, зокрема, інтереси суспільства щодо охорони здоров'я, запобігання поширенню коронавірусної інфекції тощо.

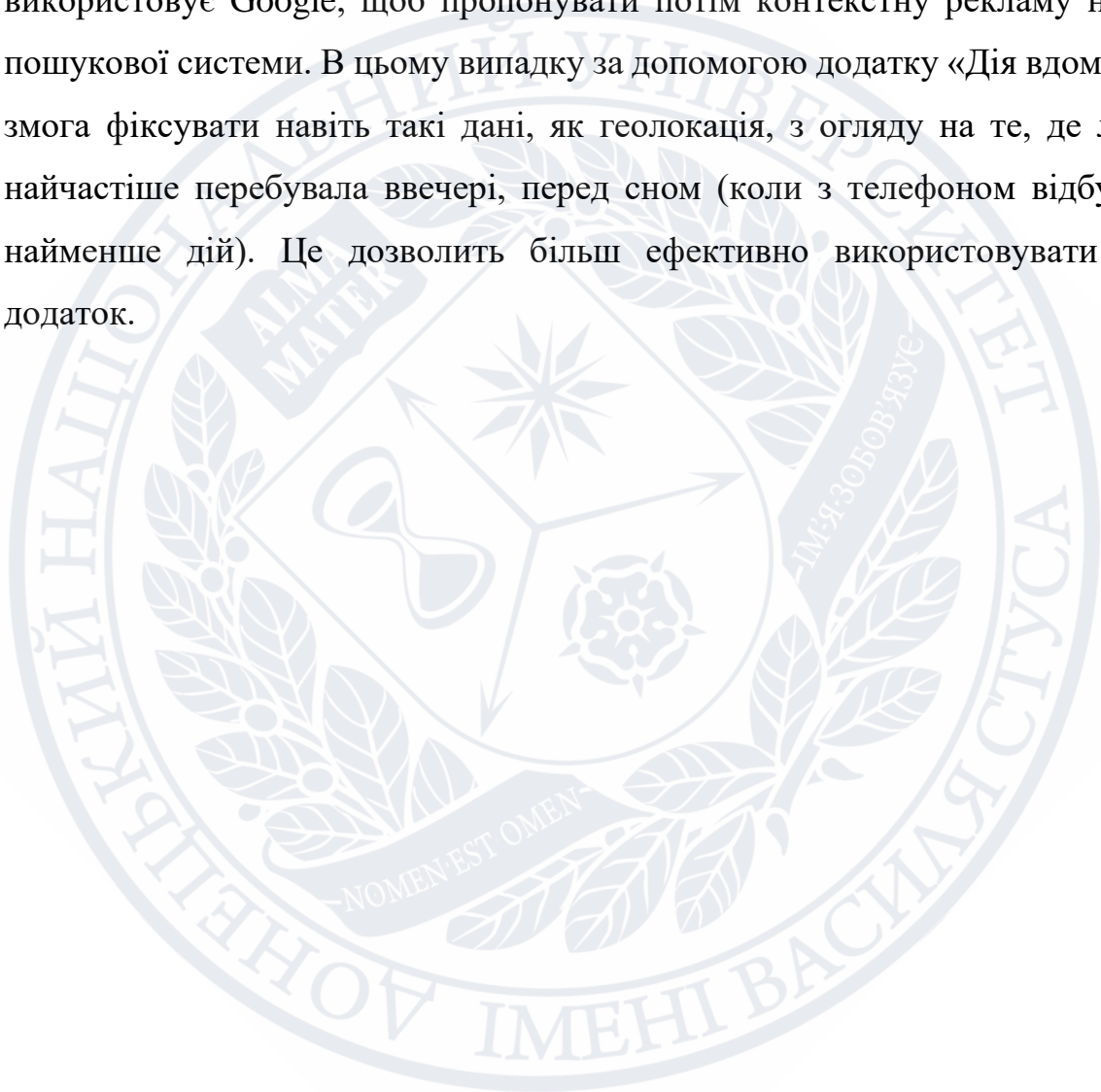


4. «Дій вдома» – це додаток для контакту з особою та контролю за дотриманням обов'язкової самоізоляції на час карантину. В основі – зарубіжний досвід країн, які використовують цифрові інструменти для забезпечення безпеки громадян в період пандемії. Застосунок надає переваги на час самоізоляції, але його встановлення є добровільним.

5. Додаток має велику кількість недопрацювань, серед яких – запізніла ідентифікація, проблеми з визначенням реальної геолокації, нерівномірні в часі сповіщення, загрози розголошення даних з огляду на законодавчо-правові проблеми в цьому питанні. В Україні немає необхідності встановлювати та використовувати мобільний додаток «Дій вдома», щоб контролювати дотримання процедури самоізоляції. Для забезпечення законності транзакцій, пов'язаних з використанням мобільного додатку «Дій вдома», цей додаток повинен базуватися на стандартах прав людини для захисту персональних даних, а не для втручання в особисте та сімейне життя, здійснювати їх автоматизовану обробку, як визначено в актах Ради Європи.

6. Важливим моментом має стати надання користувачам контролю за інформацією, що виходить від них, і можливістю припинення її надання. Стосовно додатків, відстеження контактів важливе, щоб зібрані, агреговані, та аналізовані відомості про контакти і здоров'я людей не були централізовані в рамках єдиної державної структури, наприклад, міністерства. Якщо дані, які збираються програмою, використовуються для аналізу ризиків зараження і оповіщення відповідної особи, то людині повинні пояснюватися ступінь надійності аналізу і можливості використання ресурсів охорони здоров'я, таких як державні інформаційні сервіси. В багатьох розвинених країнах та країнах, що розвиваються, існують додатки, які слідкують за дотриманням режиму самоізоляції людей, що захворіли на COVID-19, або ж контактували з хворим. Дані про місцезнаходження користувача мобільного зв'язку, з огляду на іноземний досвід, можуть бути отримані різними способами, включаючи базові станції, GPS-сигнал і Bluetooth-маячки.

7. Пропонується для анонізації в додатку використовувати технологію визначення місця розташування, яка базувалась би на використанні даних з браузера та інших додатках в телефоні користувача, фактично не порушуючи принципи захисту особистої інформації в інтернеті. Зокрема, можна використовувати Cookies браузеру, не використовуючи персональних даних людини, а використовуючи такі самі алгоритми, як використовує Google, щоб пропонувати потім контекстну рекламу на сайті пошукової системи. В цьому випадку за допомогою додатку «Дія вдома» буде змога фіксувати навіть такі дані, як геолокація, з огляду на те, де людина найчастіше перебувала ввечері, перед сном (коли з телефоном відбувалося найменше дій). Це дозволить більш ефективно використовувати даний додаток.



## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Антоненко В. М. Сучасні інформаційні системи і технології. Навчальний посібник / В. М. Антоненко, Ю. В. Ратушна. Київ: КСУМГІ. 2015. 131 с.
2. Безуглий Д., Інформаційна безпека України: огляд останніх тенденцій. Фізико-математична освіта. 2018. Вип. 2(16). С. 13–17.
3. Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: наук.-практ. посіб. Київ: К.І.С, 2015. 220 с.
4. Бурячок В. Л., Толюпа С. В., Семко В. В. Інформаційний та кіберпростори. Проблеми безпеки, методи та засоби боротьби: навч. посіб. Київ: Наш формат, 2016. 176 с.
5. Вирус победим, а слежку – нет. Коммерсантъ. URL: <https://www.kommersant.ru/doc/4322794>
6. «Вийшов з душі й очікував на поліцію»: що не так з додатком «Дій вдома»? Hromadske.ua. URL: <https://hromadske.ua/posts/vijshov-z-dushu-j-ochikuvav-na-policiyu-sho-ne-tak-z-dodatkom-dij-vdoma>
7. В улучшенном приложении «Дій вдома» на 5 минут увеличен срок верификации и появилась возможность покинуть место самоизоляции. ІТС.ua. URL: <https://itc.ua/news/v-uluchshennom-prilozhenii-dij-vdoma-na-5-minut-uvelichen-srok-verifikaczii-i-poyavilas-vozmozhnost-pokinut-mesto-samoizolyaczii/>
8. Вострецова Е. В. Основы информационной безопасности : учеб. пособ. / Е. В. Вострецова. Екатеринбург : Изд-во Урал.ун-та, 2019. 204 с.
9. Галицкий А. В. Защита информации в сети – анализ технологий и синтез решений / А. В. Галицкий, С. Д. Рябко, В. Ф. Шаньгин. Москва : ДМК Пресс, 2009. 616 с.



10. Годин В. В., Корнеев И. К. Информационное обеспечение управленческой деятельности: учеб. / В. В. Годин, И.К. Корнеев. Москва: Мастерство; Высшая школа, 2011. 240 с.
11. Горбенко І. Д. Гриненко Т. О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч. 1. Криптографічний захист інформації. Харків: ХНУРЕ, 2004 368 с.
12. Грайворонський М. В. Безпека інформаційно-комунікаційних систем [Текст] / М. В. Грайворонський, О. М. Новіков. Київ: Видавнича група BHV, 2009. 608 с.
13. Гундарь К. Ю. Защита информации в компьютерных системах / К. Ю. Гундарь, А. Ю. Гундарь, Д. А. Янишевский. Киев: «Корнійчук», 2000. 152 с.
14. «Держава в смартфоні» під час карантину: тимчасово чи назавжди? «Держава в смартфоні» під час карантину: тимчасово чи назавжди? LexInform. URL: <https://lexinform.com.ua/dumka-eksperta/derzhava-v-smartfoni-pid-chas-karantynu-tymchasovo-chy-nazavzhdy/>
15. Дешко Л. М., Бондарєва К. Д. Кібербезпека в Україні: національна стратегія та міжнародне співробітництво. Електронне наукове фахове видання «Порівняльно-аналітичне право». 2018. № 2. С. 379–382.
16. Диджиталізація проти COVID: влада планує автоматичні штрафи, QR-коди і не лише. Економічна правда. URL: <https://www.epravda.com.ua/news/2020/11/17/668082/>
17. Додаток «Дій вдома» і стандарти захисту персональних даних – коментар експерта Ради Європи. Громадський простір. URL: <https://www.prostir.ua/?news=chy-vidpovidaje-dodatok-dij-vdoma-standartam-zahystu-personalnyh-danyh-komentar-eksperta-rady-evropy>
18. Додаток «Дій вдома»: як уряд намагається контролювати українців під час поширення COVID-19. Інтернет свобода. URL: <https://netfreedom.org.ua/article/dodatok-dij-vdoma-yak-uryad-namagayetsya-kontrolyuvati-ukrayinciv-pid-chas-poshirennya-covid-19>

19. Домарев В. В. Безпека інформаційних технологій. Методологія створення систем захисту Видавництво: ТИД Діа Софт, 2014. С. 414.
20. Дорошенко А. Н. Информационная безопасность. Методы и средства защиты информации в компьютерных системах : учебн. пособ. / А. Н. Дорошенко, Л. Л. Ткачев. Москва: МГУПИ, 2006. 143 с.
21. Дорошенко А. Н. Кибербезопасность. Санкт-Петербург: Кибер-издание, 2008. 219 с.
22. Закон України «Про інформацію». Відомості Верховної Ради, 1992, № 48, с. 650 – 651.
23. Козирев А. А. Інформаційні технології в економіці і управлінні: підручник / А. А. Козирев. Санкт-Петербург.: Вид-во Михайлова Ст. А., 2000. 360 с.
24. Конах В. К. Нормативно-правові засади державної політики України у сфері інформаційно-психологічної безпеки. Стратегічні пріоритети. 2012. № 3(24). С. 15.
25. Круглов В. В. Державно-приватне партнерство у сфері кібербезпеки. URL: [http://www.pubadm.vernadskyjournals.in.ua/journals/2018/3\\_2018/13.pdf](http://www.pubadm.vernadskyjournals.in.ua/journals/2018/3_2018/13.pdf)
26. Ляшенко І. О. Європейські критерії безпеки інформаційних технологій. Сучасні інформаційні технології у сфері безпеки та оборони. 2012. № 1 (13). С. 84–86.
27. Мінцифри не порушує законодавство у сфері персональних даних. Galinfo. URL: [https://galinfo.com.ua/news/mintsyfry\\_ne\\_porushuie\\_zakonodavstvo\\_u\\_sferi\\_personalnyh\\_danyh\\_345760.html](https://galinfo.com.ua/news/mintsyfry_ne_porushuie_zakonodavstvo_u_sferi_personalnyh_danyh_345760.html)
28. Омбудсман підтвердила безпеку сервісів Мінцифри. Міністерство та Комітет цифрової трансформації України. URL: <https://thedigital.gov.ua/news/ombudsman-pidtvverdila-bezpeku-servisiv-mintsifri>
29. Основи інформаційної безпеки / С. В. Кавун, О. А. Смірнов, В. Ф. Столбов. Кіровоград: Вид. КНТУ, 2012. 414 с.

30. Петров О. С. Основи безпеки інформаційних систем. Луганськ: Вид-во СНУ ім. В. Даля, 2004. 148 с.
31. Поповский В. В. Основы криптографической защиты информации в телекоммуникационных системах. Ч. 1 / В. В. Поповский, А. В. Персиков. Харьков: Компания СМІТ, 2010. 352 с.
32. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. № 2163-VIII. Режим доступу: <https://zakon.rada.gov.ua/laws/show/2163-19>
33. Рябко Б. Я., Фионов А. Н. Криптографические методы защиты информации. Москва: Горячая линия – Телеком, 2005. 229 с.
34. Сенів М. М. Безпека програм та даних: навч. посібник / М.М. Сенів, В.С. Яковина. Львів : Видавництво Львівської політехніки, 2015. 256 с.
35. Смалько О. А. Захист інформаційних ресурсів: Монографія. Кам'янець-Подільський: ПП Буйницький О. А., 2011. 704 с.
36. Столингс В. Криптография и защита сетей. Принципы и практика. М.: Вильямс, 2014. 672 с.
37. Тарнавський Ю. А. Технології захисту інформації : підручник для студ. спеціальності 122 «Комп'ютерні науки»; КПІ ім. Ігоря Сікорського. Київ : КПІ ім. Ігоря Сікорського, 2018. 162 с.
38. Толюпа С. В., Власов О. М. Комплексний підхід оцінки ефективності систем захисту інформації в інфокомунікаційних мережах нового покоління. Наукові записки УНДІЗ. 2011. №3(19). С. 10-14.
39. У Денісової перевірили мобільний застосунок «Дій вдома», порушень не знайшли. Укрінформ. URL: <https://www.ukrinform.ua/rubric-society/3222667-u-denisovoi-perevirili-mobilnij-zastosunok-dij-vdoma-porusen-ne-znajsl.html>
40. Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. Інформація і право. 2012. № 2. С. 162–169.



41. Хорошко В. О. Основи інформаційної безпеки: підручник / В. О. Хорошко, В. С. Чередниченко, М. Є. Шелест; за ред. В. О. Хорошка. Київ: ДУІКТ, 2008. 186 с.
42. Цифровой карантин: как в разных странах следят за перемещениями жителей в условиях пандемии. Реальное время. URL: <https://realnoevremya.ru/articles/171840-tehnologii-karantina-vo-vremya-koronavirusa>
43. Цюцюра М. І., Моспан О. В. Інформаційна безпека та її забезпечення у соціальних мережах. Безпека соціально-економічних процесів в кіберпросторі: матеріали Всеукр. наук.- практ. конф. (Київ, 27 берез. 2019 р.). Київ: Київ. нац. торг.-екон. ун-т, 2019. С. 63–64.
44. Чи відповідає додаток «Дій вдома» стандартам захисту персональних даних – коментар експерта Ради Європи. Офіс Ради Європи в Україні. URL: <https://www.coe.int/uk/web/kyiv/-/does-the-act-at-home-ukrainian-mobile-app-meet-data-protection-standards-comment-of-the-council-of-europe-expert>
45. Чи загрожує використання «Дій вдома» цифровим правам? Digital Security Lab. URL: <https://dslua.org/publications/chy-zahrozhuie-vykorystannia-diy-vdoma-tsyfrovym-pravam/>
46. Як працює застосунок «Дій вдома». Департамент комунікацій Секретаріату Кабінету Міністрів України. URL: <https://www.kmu.gov.ua/news/yak-pracyuye-zastosunok-dij-vdoma>
47. Covid-19 и мобильный трекинг в вопросах и ответах. Human Right Watch. URL: <https://www.hrw.org/ru/news/2020/05/18/375128>
48. COVID-1984: отчёт о слежке во всём мире во время пандемии. Роскомсвобода. URL: <https://roskomsvoboda.org/post/covid-1984-otchyot-o-slezhke-vo-vsyom-mire-vo-vremya-p/>
49. Lakhno V. A., Hrabariev A. V., Petrov O. S., Ivanchenko Y. V., & Beketova G. S. Improving of information transport security under the conditions of

destructive influence on the information-communication system. Journal of theoretical and applied information technology. 2016. № 89(2). PP. 352–361.



## ДОДАТКИ

## ДОДАТОК А

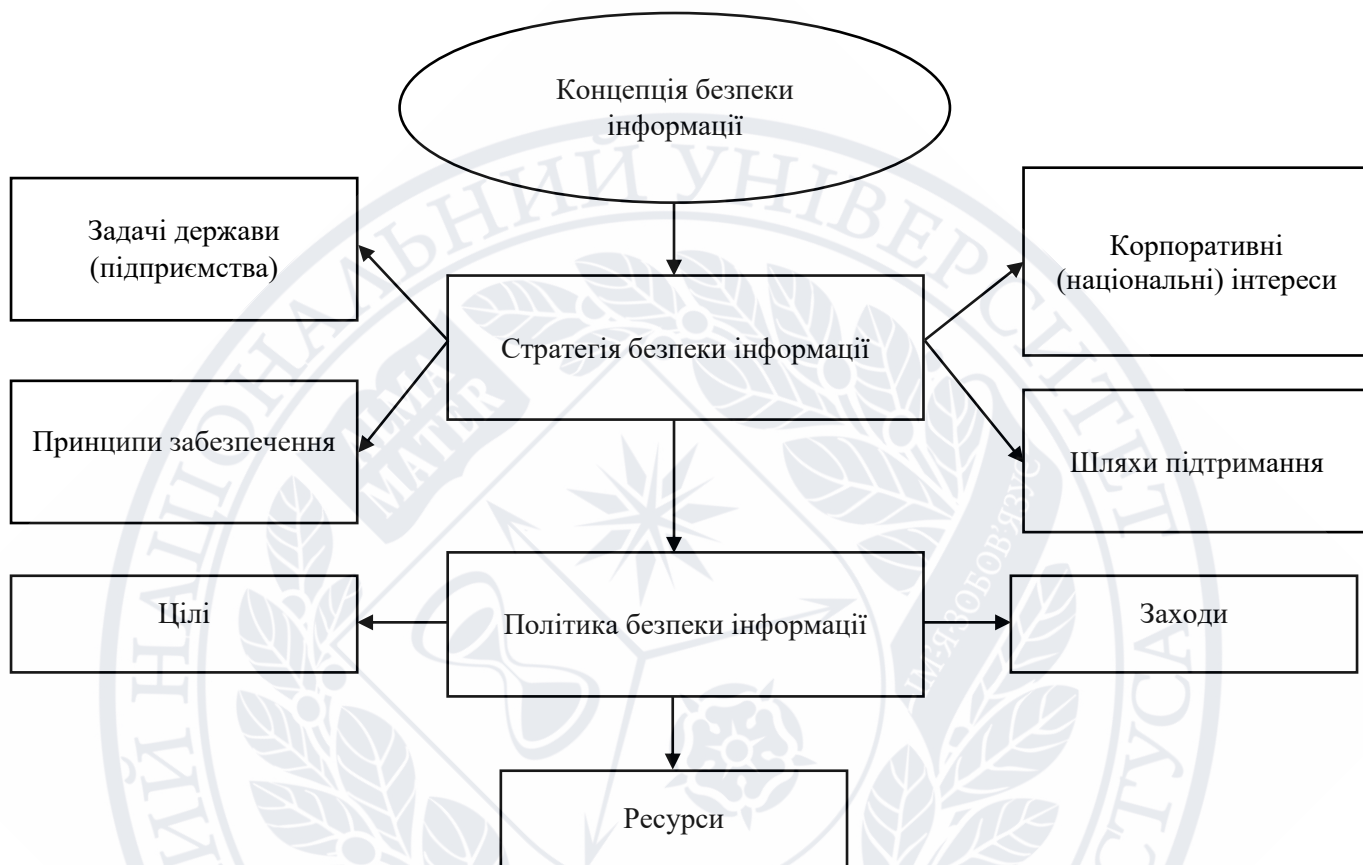


Рисунок А.1 – Ієрархічний підхід до забезпечення безпеки інформації [12]



## ДОДАТОК Б

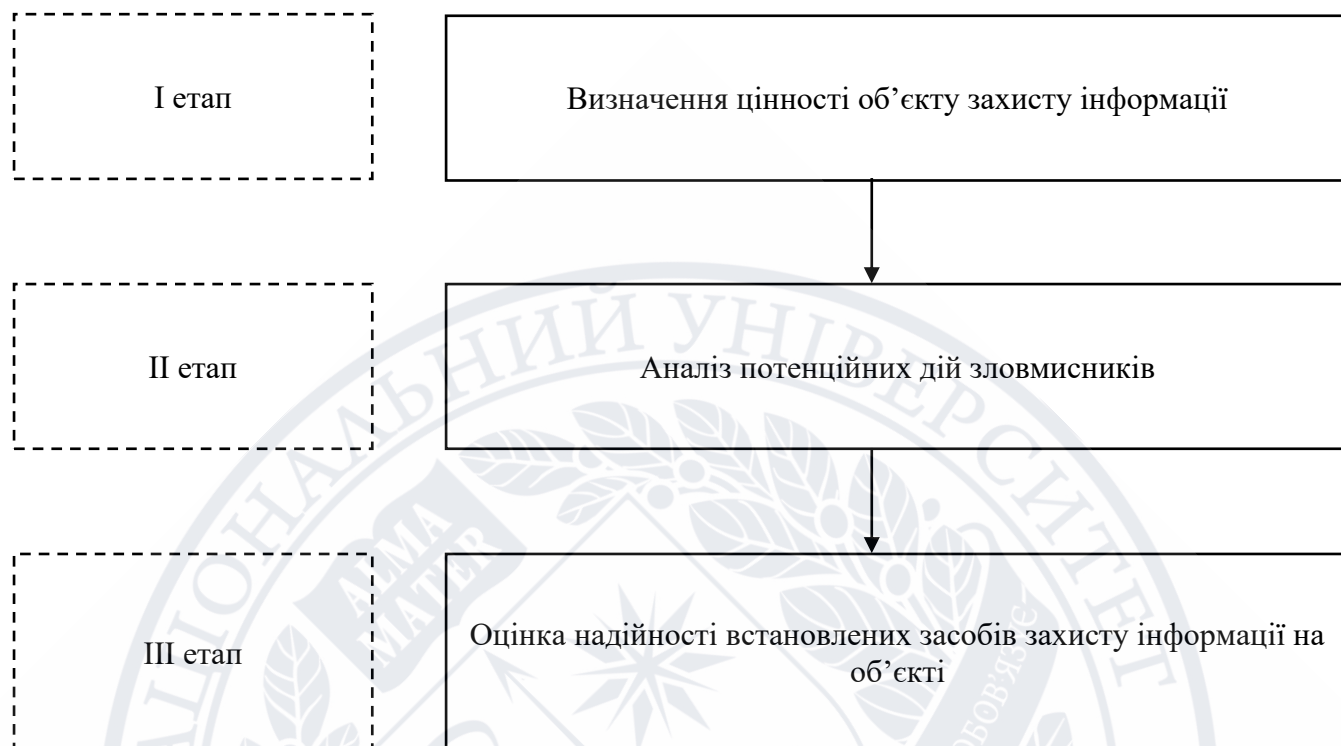


Рисунок Б.1 – Етапи розробки концепції захисту інформації [19]

## ДОДАТОК В



Рисунок В.1 – Правове забезпечення безпеки інформації [24]