DOI: https://doi.org/10.36910/6775-2524-0560-2021-43-37
УДК 342.721
Франков Олександр Сергійович, заступник начальника центру
https://orcid.org/0000-0003-3913-4420
Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України

МЕХАНІЗМИ ЗАХИСТУ ПЕРСОНАЛЬНОЇ ІНФОРМАЦІЇ У ЧАТІ

Франков О. С. Механізми захисту персональної інформації у чаті. У статті розкрито механізми захисту персональної інформації у чаті. Сформовано низку проблем, які є ключовими у забезпеченні безпечного інформаційного простору для спілкування. Запропоновано формальний опис глобальних комунікацій з використанням дискретних структур. Наголошено, що захист особистої інформації є важливою проблемою у розподілених сервісах і мережевих комунікаціях, включаючи хмарні сервіси. Тому слід застосовувати спеціальні технологічні та організаційні заходи щодо захисту персональних даних. Підкреслено призначення заходів захисту, як спеціально технічних так і організаційних. Обґрунтовано той факт, що права на конфіденційність пов'язані з особистою інформацією яку, безпосередньо, можна зібрати в процесі використання мережевих засобів спілкування. Позначено, що можна збирати і фіксувати будь-яку особисту інформацію без відома користувача, і, більш того, особисті дані можуть бути передані на законних підставах будь-якій третій особі. Сформовано модель здійснення комунікацій у мережі Інтернет, яка включає дві окремі групи: учасники / особи, визначені як сукупність користувачів, що мають можливість ініціалізації віддаленого доступу через Інтернет та інформаційне середовище, з конкретними технологічними компонентами для визначення конкретної структури і призначення простору, в тому числі модуль для попередньої реєстрації та збір даних у власній базі даних. Запропоновано графічну інтерпретацію життєвого циклу обробки персональних даних з детальним описом кожної окремої позиції. Структуровано всі можливі ланки зв'язку політики захисту даних із загальною структурою політики безпеки і структурними рівнями системи захисту персональних даних. Сформовано чотири основні механізми захисту персональної інформації у чаті та запропоновано у подальшому виконати формування єдиного підходу до реалізації системи захисту персональної інформації у соціальних мережах з урахуванням міжнародного досвіду.
Ключові слова: захист інформації, персональні дані, мережа Інтернет, чат, віртуальне спілкування, кібербезпека.

Франков А. С. Механизмы защиты персональной информации в чате. В статье раскрыты механизмы защиты персональной информации в чате. Сформирован ряд проблем, которые являются ключевыми в обеспечении безопасного информационного пространства для общения. Предложено формальное описание глобальных коммуникаций с использованием дискретных структур. Отмечено, что защита личной информации является важной проблемой в распределенных сервисах и сетевых коммуникациях, включая облачные сервисы. Поэтому следует применять специальные технологические и организационные меры по защите персональных данных. Подчеркнуто назначения мер защиты, как специально технических так и организационных. Обоснованно тот факт, что права на конфиденциальность связанные с личной информацией которую, непосредственно, можно собрать в процессе использования сетевых средств общения. Обозначены, что можно собирать и фиксировать любую личную информацию без ведома пользователя, и, более того, личные данные могут быть переданы на законных основаниях любому третьему лицу. Сформирована модель осуществления коммуникаций в сети Интернет, включая две отдельные группы: участники / лица, определенные как совокупность пользователей, имеющих возможность инициализации удаленного доступа через Интернет и информационная среда, с конкретными технологическими компонентами для определения конкретной структуры и назначения пространства, в том числе модуль для предварительной регистрации и сбор данных в собственной базе данных. Предложено графическую интерпретацию жизненного цикла обработки персональных данных с подробным описанием каждой отдельной позиции. Структурировано все возможные звена связи политики защиты данных с общей структурой политики безопасности и структурными уровнями системы защиты персональных данных. Сформированы четыре основные механизмы защиты персональной информации в чате и предложено в дальнейшем выполнить формирования единого подхода к реализации системы защиты персональной информации в социальных сетях с учетом международного опыта.
Ключевые слова: защита информации, персональные данные, сеть Интернет, чат, виртуальное общение, кибербезопасность.

Frankov Oleksandr. Defence mechanisms of the personal information in chat. The article reveals the mechanisms of personal information protection in chat. A number of problems have been identified that are key to providing a secure information space for communication. A formal description of global communications using discrete structures is proposed. It is emphasized that the protection of personal information is an important issue in distributed services and network communications, including cloud services. Therefore, special technological and organizational measures should be applied to protect personal data. The purpose of protection measures, both specially technical and organizational, is emphasized. The fact that the rights to confidentiality are related to personal information that can be directly collected in the process of using online means of communication is substantiated. It is stated that it is possible to collect and record any personal information without the knowledge of the user, and, moreover, personal data may be lawfully transferred to any third party. A model of communication on the Internet has been formed, which includes two separate groups: participants / persons defined as a set of users who have the ability to initialize remote access via the Internet and information environment, with specific technological components to determine the specific structure and purpose of space, including module for pre-registration and data collection in its own database. A graphical interpretation of the life cycle of personal data processing with a detailed description of each item is proposed. All possible links between the data protection policy and the general structure of the security policy and the structural levels of the personal data protection system are structured. Four main mechanisms for the protection

of personal information in the chat have been formed and it is proposed to further form a unified approach to the implementation of the system of personal information protection in social networks, taking into account international experience.

Keywords: information protection, personal data, Internet, chat, virtual communication, cybersecurity.

Вступ та постановка проблеми дослідження. Модернізація та вдосконалення інформаційного суспільства (ІС) визначають нові вимоги до сучасних інформаційно-комунікаційних технологій (ІКТ) для вирішення різних проблем глобалізації, віддаленого доступу до інформаційних ресурсів і хмарних обчислень, розподіленої інформації, обслуговування віртуального середовища і визначення адекватної політики інформаційної безпеки на підприємствах. Засоби віртуального спілкування у мережі Інтернет також повинні бути включені в цю групу, тому що сучасні ІКТ дозволяють розширювати соціальні відносини і підтверджувати область «соціальних обчислень», пов'язану з побудовою мереж веб-сайтів. Інформаційне суспільство створило різні можливості для віддаленого доступу до розподілених інформаційних ресурсів і зв'язку між користувачами (віртуальні середовища, хмарні сервіси, соціальні мережі, чати і т. д.). Всі ці аспекти глобалізації змушують користувачів створювати свої власні профілі з особистими даними і публікувати персональну інформацію. Саме тому, питання захисту персональної інформації стало одним з пріоритетних завдань сьогодення.

Аналіз останніх досліджень і публікацій. Проблемам захисту персональної інформації у мережі Інтернет присвячено чимало робіт як теоретичної так і практичної направленості.

О. В. Гронь та А. К. Погореленко [1]розкрили проблеми захисту персональних даних у контексті сучасної комунікації. У статті проаналізовано європейські законодавчі основи та принципи захисту персональних даних, які становлять основу сучасної практики в цій сфері. Викладено базові положення української системи правового захисту персональних даних. Визначено правові підстави для реалізації та захисту інтересів суб'єкта персональних даних.

Стандарти захисту персональних даних в соціальній сфері запропонували М. В. Бем, І. М. Городиський[2]. В свою чергу, Н. В. Камінська [3] підійшла до проблеми з правового аспекту. Авторка розглянула питання захисту персональних даних відповідно до чинного законодавства України, що зумовило появу проблем як теоретичного, так і практичного характеру. Зокрема, важливим є здійснення аналізу правової основи процесу захисту персональних даних, узагальнення норм міжнародного і наднаціонального права, зарубіжного досвіду в цій сфері. Це дозволяє з'ясувати відповідність національного законодавства існуючим міжнародним стандартам, визначити шляхи підвищення його ефективності, усунення суперечностей та прогалин.

І. М. Сопілко [4] розкрив механізми захисту персональних даних, визначив проблеми та перспективи. Аспекти держаного регулювання окреслила Т. І. Обуховська[5]. У дисертації здійснено теоретичне обґрунтування державних механізмів забезпечення захисту персональних даних в Україні, визначені перспективні напрямки їхнього розвитку та здійснено розробку науково-практичних рекомендацій органам влади в умовах трансформації державного управління в Україні.

Із зарубіжних варто рів варто відзначити такі роботи як: Subramanian, A., Kessler, M.[6], Weichert, T. [7], Lam, S. K., Riedl, J. [8], Bennett, C. J. [9], Romansky, R. [10], Duggan, M., Smith, A. [11]та інші.

Проте, враховуючи описані наукові набутки, за темою, питання захисту персональної інформації у чаті залишається відкритим та потребує детального опрацювання.

Основна ***мета*** цієї статті – обговорити проблеми захисту персональної інформації віртуального спілкування як компоненти конфіденційності. З цієї причини запропоновано формальний опис глобальних комунікацій з використанням дискретних структур.

Викладення основного матеріалу дослідження.Новітні ІКТ і розподілені середовища змушують користувачів створювати свої власні профілі з особистими даними і публікувати особисту інформацію, доступну іншим користувачам через глобальну мережу. Це можливість розширити соціальні контакти, але це може надати небажаний вплив на конфіденційність зареєстрованого користувача [6]. В цьому відношенні захист особистої інформації є важливою проблемою у розподілених сервісах і мережевих комунікаціях, включаючи хмарні сервіси. Тому слід застосовувати спеціальні технологічні та організаційні заходи щодо захисту персональних даних. Ці заходи повинні захищати профіль кожного користувача з особистими даними від незаконного доступу, поширення та використання інформації для інших цілей, відмінних від визначених. Необхідно сформулювати нову точку зору на правила авторизації і аутентифікації в соціальних середовищах.

Необхідність захисту персональних даних визначається тим фактом, що конфіденційність є важливим правом людини, яке поєднує в собі комплекс окремих індивідуальних прав –точну і адекватну обробку особистих даних, різні форми особистого спілкування (поштою, через Інтернет і т. д.), безпечну підтримку особистих профілів на форумах і в соціальних мережах і т. д. Традиційне визначення терміна «конфіденційність» - це «право бути на самоті», і цей сенс повинен зберігатися у всіх соціальних контактах через глобальну мережу. Це може бути реалізовано на основі суворої політики безпеки, визначеної для кожної конкретної мети особистого спілкування і підтримки профілів людей, оскільки використання сучасних ІКТ висуває нові вимоги до політики захисту персональних даних і змінює розуміння конфіденційності в глобальному суспільстві. Ця політика повинна підвищити ефективність засобів і інструментів захисту персональних даних в новому мережевому суспільстві і, зокрема, в соціальних мережах і мережах персонального спілкування. Основна проблема полягає в тому, що існуючі процедури захисту персональних данихне відповідають реальним комунікацій в глобальному суспільстві і їх необхідно актуалізувати.

Права на конфіденційність пов'язані з особистою інформацією що можна було зібрати в процесі використання мережевих засобів спілкування. Можна збирати і фіксувати будь-яку особисту інформацію без відома користувача, і, більш того, особисті дані можуть бути передані на законних підставах будь-якій третій особі.

Комунікації в глобальному середовищі (особливо у веб-просторі) можуть бути описані за допомогою дискретної структури елементів (вузлів) $V = \{V_1, \dots, V_n\}, V \neq \emptyset$ і відносини між ними $R_{ij}: V_i \to V_j$. Кожен вузол V_i представляє фізичного учасника глобальної комунікації, і його можна розглядати як незалежний розподілений блок з власною внутрішньою функціональністю. Модель, побудована на основі цієї концепції, представлена на рис.1.

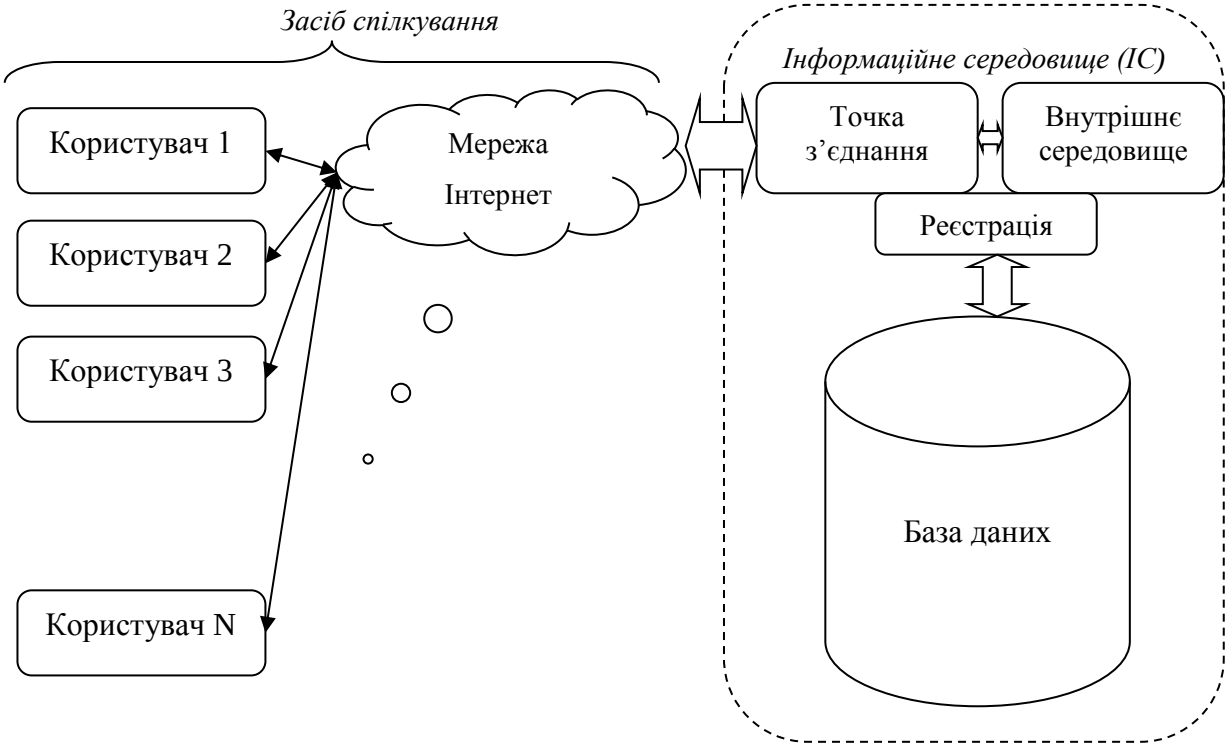

Рис. 1. Модель здійснення комунікацій у мережі Інтернет

Учасники комунікацій утворюють дві групи: це учасники / особи, визначені як сукупність користувачів $U = \{U_1, U_2, \dots, U_N\}, U \neq \emptyset$, що мають можливість ініціалізації віддаленого доступу через Інтернет; це інформаційне середовище $IE = \{IE_1, \dots, IE_M\}, IE \neq \emptyset$, з конкретними технологічними компонентами для визначення конкретної структури і призначення простору, в тому числі модуль для попередньоїреєстрації та збір даних у власній базі даних.

Організація всіх процесів глобального зв'язку здійснюється ресурсами «комунікаційного середовища», які можна описати як передавачі$T = \{T_1, \dots, T_K\}, T \neq \emptyset$. Кожен передавач складається з апаратних і програмних засобів для розподілу запитів на доступ до інформаційних об'єктів $req: \{U\} \to \{IE\}$ і повернення інформаційного змісту $inf: \{IE\} \to \{U\}$ клієнтам.

Формалізація дозволяє описувати елементи глобальних комунікацій упорядкованим триплетом (U, IE, T) з двома типами відносин $req: \{U\} \to \{IE\}$ та $inf: \{IE\} \to \{U\}$ для $\forall U_i \in U; \forall IE_j \in IE$.

Давайте визначимо відстань $d_{ij} (i \neq j; i, j \in \{1 \div n\})$ між кожною парою вузлів (V_i, V_j). Це дозволяє побудувати матрицю відстаней DM з розмірністю n та елементами $d_{ii} = 0\ (i = 1, \ldots, n)$ та визначити мінімальну довжину шляхів між вузлами в структурі.

Представимо два бінарні параметри $u_{ik} \in \{0,1\}$ (розташування користувача $U_i \in U$ у вузлі $V_k \in V$) та $r_{jk} \in \{0,1\}$ (розташування середовища $IE_j \in IE$ у вузлі $V_k \in V$):

$$u_{ik} = \begin{cases} 1, \text{якщо користувач } U_i \in U \text{ знаходиться у вузлі } V_k \in V \\ 0, \text{інакше} \end{cases}$$

У загальному випадку можливо, що два учасники з різного типу (користувач та інформаційне середовище) фізично розподіляються разом у загальному вузлі V_k, і це можна описати виразами (рис. 2):

$$(\text{перший учасник}) \exists V_k \in V \Rightarrow (V_k \in V)(V_k \in IE)$$
$$(\text{другий учасник}) \exists V_k \in V \Rightarrow [(V_k \in V)(V_k \notin IE)] \text{або} [(V_k \notin U)(V_k \in IE)]$$

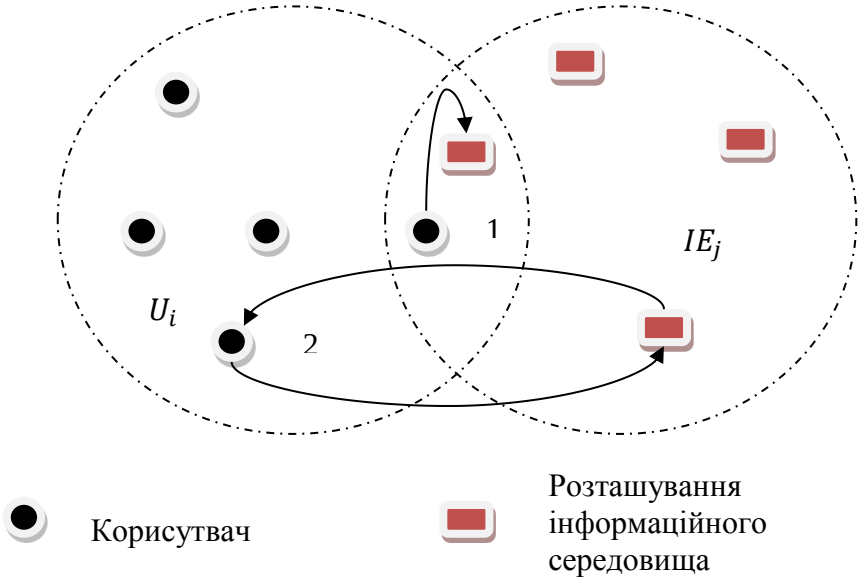

Рис. 2. Можливі типи спілкування

Це припущення визначає потужність (кількість елементів) $n \leq N + M$ набору V. Дві двійкові матриці з компонентами $u_{ik}(N \times n)$ та $r_{jk}(M \times n)$ можуть бути побудовані для дослідження фізичного розподілу учасників глобальних комунікацій. Логічна обробка на основі

$$IF \left\{ \sum_{i=1}^{N} UL[i,k] \geq 1 \right\} \left\{ \sum_{i=1}^{M} RL[j,k] \geq 1 \right\} \text{ тоді } v_k = 1 \text{ інакше } v_k = 0$$

$(\text{для } k = 1 \div n)$визначить новий вектор для визначення загальних вузлів розподілу учасників з різним типом. Ця формалізація дозволяє зробити детермінований опис комунікацій парами двох елементів (перший з U, другий з IE) та провести дослідження процесів у глобальному середовищі.

Графічна інтерпретація життєвого циклу обробки персональних даних запропонована на рис. 3. Дана модель життєвого циклу описує традиційну обробку персональних даних з послідовністю етапів, починаючи від надання персональних даних фізичною особою і закінчуючи знищенням персональних даних (контролером даних) після реалізації мети.

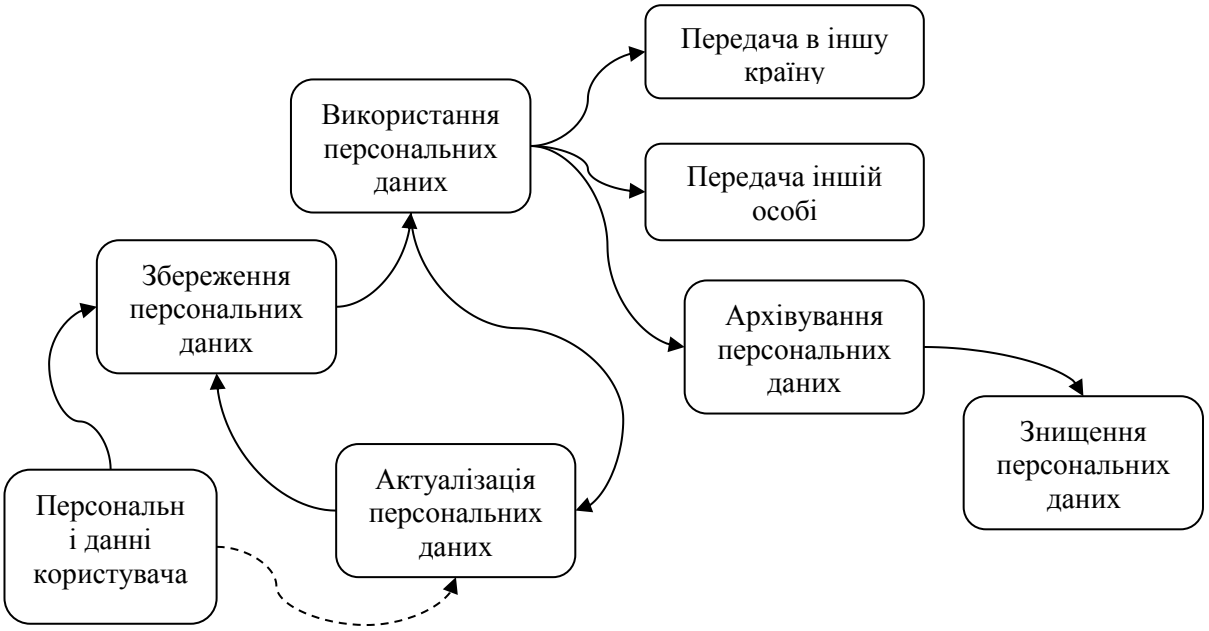

Рис. 3. Графічна інтерпретація життєвого циклу обробки персональних даних

Фази здійснення обробки:

– збір особистих даних повинен здійснюватися тільки на законних підставах і за згодою фізичної особи;

– збереження зібраних даних повинно здійснюватися в регістрах на основі попередньо визначеної мети і критеріїв;

– використання повинно здійснюватися законними особами на основі принципів інформаційної безпеки: аутентифікація (з використанням імені користувача, пароля, цифрового сертифікату, особистого ідентифікаційного номера та біометричних засобів); авторизація (на основі розробленої системи управління цифровими правами); підзвітність (персоналізація доступу до структур даних і реєстрація дій користувачів);

– актуалізація – персональні дані повинні бути вірними, повними і актуальними;

– передача в іншу країну і передача іншій особі повинні бути здійснені. тільки на підставі чинного законодавства;

– архівування може бути здійснено, якщо це потрібно за законом, але тільки на обмежений період;

– знищення особистих даних має бути здійснене після досягнення мети.

У світі існує кілька різних моделей захисту персональної інформації – модель централізованого законодавства, модель спільного регулювання, модель галузевого законодавства, модель саморегулювання і модель особистого (індивідуального) захисту. Остання модель показує, що більшість користувачів інформаційних сервісів через глобальну мережу не довіряють політиці інформаційної безпеки і захисту персональної інформації при розподіленому обслуговуванні інформації. Це вимагає, щоб політика захисту персональної інформації була узгоджена із заходами політики безпеки в рамках загальної політики безпеки (рис. 4).

Користувачі чату надають свої особисті дані для реєстрації та завантаження персональної інформації про особисте життя. Ця інформація доступна і може використовуватися іншими особами (в тому числі для передачі третім особам) без згоди власника. Це вимагає загальної гармонізації захисту даних.

Система захисту персональних даних – це набір технічних і організаційних засобів і інструментів для реалізації захисту структур персональних даних контролером даних. Всі процедури обробки персональних даних з використанням інструментів ІКТ повинні бути детально проаналізовані при визначенні політики захисту даних для мереж спілкування і захисту персональних даних.

Конфіденційність в чаті стосується захисту інформації користувача і захисту прав користувача. Носій повинен бути базою для запобігання різних інцидентів з даними користувача, таких як несанкціонований доступ, віруси, незаконна передача третім особам і т. д.

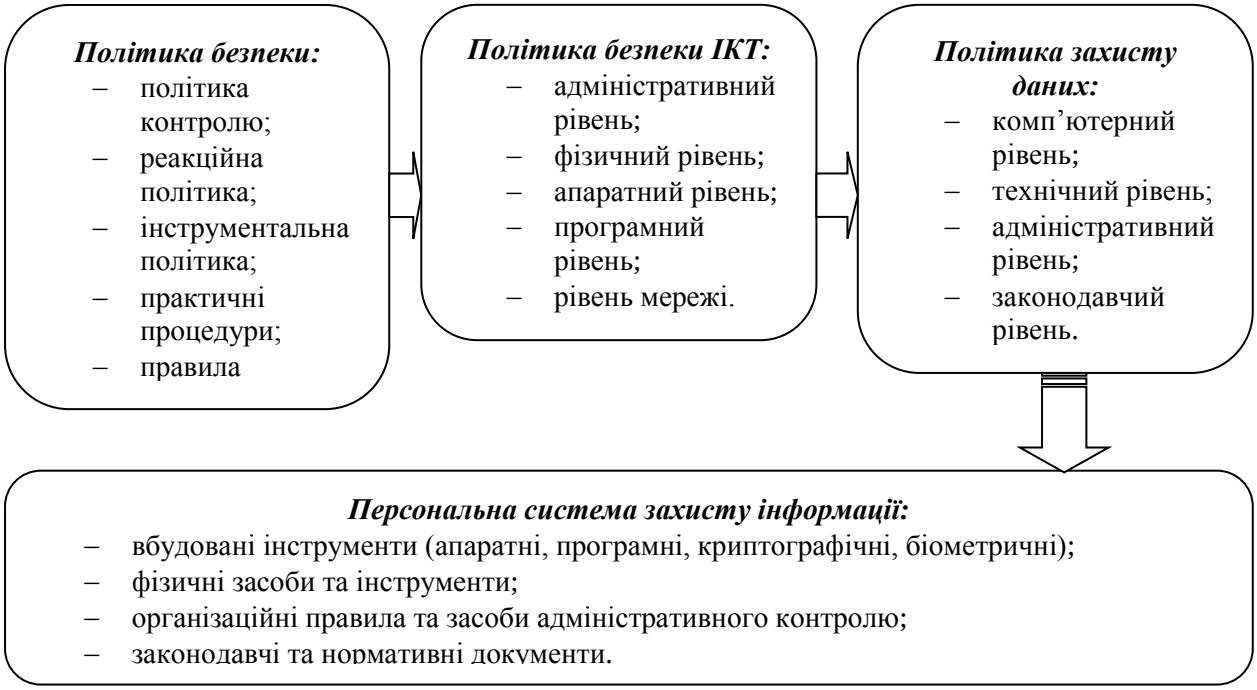

Рис. 4. Зв'язок політики захисту даних із загальною структурою політики безпеки і структурними рівнями системи захисту персональних даних

Важливим обов'язком диспетчерів даних є створення надійної системи захисту персональної інформації для реалізації принципів всіх структурних рівніві чіткого, зрозумілого і прозорого інформування кожного користувача про використання особистих даних. Для цього необхідно в якості початкового кроку визначити ролі «контролера даних», «обробника даних» і «суб'єкта даних» в соціальних мережах і визначити відповідальність за процедури захисту даних (правила, заходи, конфіденційність і права суб'єктів даних). Згідно з визначеннями регламенту європейського парламенту і ради 2016/679, контролер даних визначає цілі і засоби обробки персональних даних. Проблема в чаті полягає в тому, що функції покупця, продавця та постачальника і відносини між ними можуть бути визначені тільки для конкретного випадку. Постачальники послуг не мають юридичних зобов'язань щодо захисту особистих даних, якщо вони не визначені як контролери або обробники. Різні можливості визначення статусу провайдера (і можливість його зміни) дуже ускладнюють вирішення цієї проблеми. Ця характеристика дозволить ігнорувати зобов'язання щодо захисту даних у випадках, коли особисті дані передаються на аутсорсинг або передаються третій стороні для обробки. Ще одна проблема, яку можна визначити в чаті, - це право суб'єкта даних на отримання інформації. Це комплексна проблема, тому що при обробці персональних даних люди мають різні права. По-перше, існує ризик для конфіденційності користувача під час реєстрації (може знадобитися більше особистих даних для реєстрації та ідентифікації) і використання ресурсів чату.

Обов'язок контролерів – гарантувати легкий доступ до особистих даних користувачів. Це дозволить реалізувати права користувача на зміну, доступ, блокування або видалення своїх особистих даних в профілі (що є основним правом, гарантованим законами про захист даних). Іншою стороною проблеми є доступ до інформації в профілі – контролер повинен гарантувати, що кожен користувач може встановити обмеження для доступу до власного профілю. Це попередить несанкціонований доступ і неправильне поширення особистої інформації. Цю дію можна реалізувати, зробивши профіль закритим для користувачів, вибравши тих, хто може відвідувати сторінку. Традиційний спосіб аутентифікації при доступі до профілю – по імені користувача і паролю, і при цьому ігноруються будь-які операції зі збереженою інформацією (додавання, видалення, зміна). В цьому випадку користувачеві буде забезпечена конфіденційність в чаті.

Міжнародну передачу даних можна визначити як наступну можливу проблему конфіденційності в соціальних мережах. Згідно з основними принципами захисту персональної інформації персональні дані можуть бути передані в іншу країну, якщо їх рівень захисту є адекватним.

Передача даних між різними постачальниками послуг є типовою процедурою в соціальних мережах, оскільки вузли (сервери, клієнти, сховища і т. д.) можуть бути розташовані в будь-якій точці світу. Якщо будь-яка особиста інформація завантажується в соціальні мережі, вона повинна бути захищена відповідно до правил персонального захисту особистої інформації, і людина (користувач часу) повинна бути поінформована про всі види передач своїх даних від одного постачальника послуг іншому в рамках країни або за її межами.

Всі інформаційні ресурси можуть бути доступні з різних точок світу. Це провокує традиційні небезпеки в глобальній мережі (втрата даних, порушення цілісності, проблеми з підзвітністю, хакерські атаки і т. д.). Кожен користувач завантажує інформацію, яка буде спільно використовуватися безліччю користувачів чату, і її можна буде поширити в різних місцях. У цьому випадку суб'єкт даних не знає, яка політика і заходи використовуються для протидії можливим атакам. Постачальники послуг повинні гарантувати ефективний захист цілісності і доступності даних. Відомо, що додаткові заходи безпеки даних підвищать вартість процедур захисту персональних даних, і це буде причиною ігнорування деяких заходів захисту.

Висновки та перспективи подальших досліджень.У роботі дослідженомеханізми захисту персональної інформації у чаті.Конфіденційність в чаті може бути порушена багатьма факторами, обумовленими некоректним використанням особистих даних. Подальший розвиток і використання кіберпростору неможливо здійснити без адекватного і надійного захисту прав окремих користувачів. Головними механізмами захисту персональної інформації у чаті визначено: формування єдиного контенту повинно буди урегульовано єдиним законом (приватний, державний рівні); жорстке регулювання європейської цифрової індустрії; право на видалення – це право людини видалити свої особисті дані з системи, якщо він / вона більше не хоче використовувати онлайн-сервіси та зберігати свої персональні дані у онлайн-системі; єдине вікно для підприємств і громадян – регулювання обробки персональних даних контролером або процесором, встановленим в країнах Європейського Союзу.

Нові механізми захисту персональної інформації у чаті повинні розширити рамки захисту у відповідності до міжнародних регламентів і запропонувати адекватні рішення для всіх проблем захисту персональної інформації в соціальному середовищі.

Перспективи подільних досліджень ґрунтуються на формуванні єдиного підходу до реалізації системи захисту персональної інформації у соціальних мережах з урахуванням міжнародного досвіду.

Список бібліографічного опису.

1. Гронь, О. В., & Погореленко, А. К. (2018). Проблеми захисту персональних даних у контексті сучасної комунікації. *Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство*, (19 (1)), 102-108.
2. Бем, М. В, Городиський, І. М.. (2018). Стандарти захисту персональних даних в соціальній сфері Львів: б.в.
3. Камінська Н. В. (2015). Захист персональних даних: проблеми внутрішньодержавного, наднаціонального і міжнародно-правового регулювання. *Науковий вісник Національної академії внутрішніх справ*, *96*(3), 106-114.
4. Сопілко, І. М. (2013). Механізм захисту персональних даних: проблеми та перспективи. *Юридичний вісник. Повітряне і космічне право*, (2), 66-70.
5. Обуховська Т. І.(2016.). Державні механізми забезпечення захисту персональних даних в Україні [Текст] : дис. ... канд. наук з держ. упр. : 25.00.02 ; Нац. акад. держ. упр. при Президентові України. Київ.

References.

1. Subramanian, A., & Kessler, M. (2013). The hyperglobalization of trade and its future.
2. Weichert, T. (2013). Current Data Protection Challenges in Social Networks. In *Annual Conference on EU Data Protection Law 2013*.
3. Lam, S. K., Riedl, J. (2012), Are Our Online „Friend" Really Friends? Computer, January, 91-93.
4. Bennett, C. J. (2011). Privacy advocacy from the inside and the outside: Implications for the politics of personal data protection in networked societies. *Journal of Comparative Policy Analysis*, *13*(2), 125-141.
5. Romansky, R. (2013). Distributed Information Servicing and Personal Data Protection. *Bulgarian Science (in Bulgarian)*, (59), 86-98.
6. Madden, M., Lenhart, A., Cortesi, S., Gasser, U., Duggan, M., Smith, A., & Beaton, M. (2013). Teens, social media, and privacy. *Pew Research Center*, *21*(1055), 2-86.