ТЕХНОЛОГІЇ ЯК ФАКТОР ЕКОНОМІЧНОГО ЗРОСТАННЯ

УДК 351:330.342.146
JEL Classification: D61, D89, L21
DOI: https://doi.org/10.20535/2307-5651.29.2024.308831

Горбаченко С. А.
доктор економічних наук, професор
ORCID ID: 0000-0001-8442-9581
Соколов А. В.
доктор технічних наук, доцент
ORCID ID: 0000-0003-0283-7229
Національний університет «Одеська юридична академія»
Клєвцєвич Н. А.
кандидат економічних наук, доцент,
старший науковий співробітник відділу розвитку підприємництва
ORCID ID: 0000-0002-2010-4814
Державна установа «Інститут ринку і економіко-екологічних досліджень Національної академії наук України»

Horbachenko Stanislav, Sokolov Artem
Odesa Law Academy National University,
Klievtsievych Nataliia
State Organization "Institute of Market and Economic&Ecological Researches of National Academy of Sciences of Ukraine"

РОЛЬ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ В ЗАБЕЗПЕЧЕННІ ЗАХИСТУ ІНФОРМАЦІЇ НА РІВНІ ТЕРИТОРІАЛЬНИХ ГРОМАД

THE ROLE OF INFORMATION AND COMMUNICATION TECHNOLOGIES IN ENSURING THE PROTECTION OF INFORMATION AT THE LEVEL OF TERRITORIAL COMMUNITIES

Метою даної роботи є обґрунтування теоретичних та практичних основ впровадження інструментів захисту інформації на рівні територіальної громади. У статті доведено, що ІКТ відіграють важливу роль у безпечному обміні інформацією на рівні територіальних громад. Визначені ІКТ що використовуються у розвитку ТГ. Систематизовано напрямки обміну інформацією на рівні ТГ. Зазначено, що використання розглянутих ІКТ при обміні інформацією на рівні ТГ відбувається за кількома напрямками. Обґрунтовано, важливість та необхідність захисту інформації на рівні ТГ. Розглянуті практичні застосування ІКТ у розвитку ТГ. Проведено групування засобів захисту інформації на рівні ТГ, зокрема виділено 5 таких груп (фізичні, комп'ютерні, організаційні, технологічні, соціально-психологічні). Зроблено висновок, що захист інформації на рівні територіальної громади є критично важливим як з погляду приватності та безпеки громадян, так і для забезпечення нормальної роботи адміністративних та соціальних служб, а також для запобігання потенційним кіберзагрозам та злочинам. Криптографічні засоби є одним з найважливіших інструментів, які використовуються для забезпечення захисту інформації, зокрема, у інформаційно-телекомунікаційних системах ТГ.

Ключові слова: *інформаційно-комунікативні технології, ІКТ, цифрові технології, цифрові рішення, територіальні громади, захист інформації, обмін інформацією.*

The theoretical basis of this scientific work consists of the best practices of safe exchange of information in territorial communities and protection of confidential data of citizens and municipal services from potential threats given in recent papers of a theoretical and practical nature. To carry out this scientific work and achieve the goal, the article uses methods of graphic interpretation of the results of analysis and generalization, methods of monographic analysis, and synthesis. It has been proven that ICT plays an important role in the secure exchange of information. The ICT used in the development of TC have been identified. Areas of information exchange at the TC level have been systematized. It is noted that the use of the considered ICT in the exchange of information at the TC level takes place in several directions: in the management of the TC directly; when interacting with other TC; when interacting with central authorities. It was noted that the use of digital technological solutions in the management of the TC is envisaged at several levels: at the level of the residents of the TC; at the level of the business environment; at the level of local authorities; at the level of TC as a whole. The importance and necessity of protecting information at the TC level is justified. Practical applications of ICT in the development of TC are considered. Grouping of methods of

information protection at the TC level was carried out, in particular, 5 such groups were selected (physical, computer, organizational, technological, socio-psychological). It was concluded that the protection of information at the level of the territorial community is critically important both from the point of view of privacy and security of citizens, and for ensuring the normal operation of administrative and social services, as well as for preventing potential cyber threats and crimes. Cryptographic means are one of the most important tools used to ensure information protection, in particular, in information and telecommunication systems of the TG.

Keywords: *information and communication technologies, ICT, digital technologies, digital solutions, territorial communities, information protection, information exchange.*

Постановка проблеми. В результаті впровадження територіально-адміністративної реформи в Україні територіальні громади (ТГ) отримали додаткові повноваження. Разом з тим зросла відповідальність за прийняття управлінських рішень щодо забезпечення соціально-економічного розвитку відповідних територій. Планування ефективного використання наявних ресурсів, зміцнення економічного потенціалу, створення комфортних умов проживання населення, надання необхідних адміністративних послуг є неповним переліком завдань, які наразі стоять перед громадами. В таких умовах інформаційно-комунікаційні технології (ІКТ) соціально-економічного розвитку суттєво поліпшують інформаційне забезпечення усіх зацікавлених сторін, забезпечують відкритість управління, підвищують ступінь обґрунтованості прийнятих рішень та сприяють кращому усвідомленню цілей розвитку громади. ІКТ відіграють важливу роль у безпечному обміні інформацією, забезпечуючи не лише ефективну комунікацію та обмін даними між відомствами та громадянами, але й захист конфіденційності, цілісності та доступності інформації, автоматизуючи процеси управління. Такі технології забезпечують засоби для моніторингу та аналізу даних, що створює можливості для місцевої влади вчасно виявляти проблеми, реагувати на них та приймати обґрунтовані управлінські рішення. З огляду на зазначене, забезпечення захисту інформації наразі є надважливим. Територіальні громади, особливо у великих містах, можуть стати об'єктом кібератак, спрямованих на викрадення чутливої інформації, паралізацію муніципальних служб або навіть шантажу. Захист інформації дозволяє реагувати швидко та координовано, забезпечуючи безпеку та захист населення, але сьогодні не існує універсальної методики забезпечення захисту, яка надавала б 100% гарантію безпеки. Відповідно, інформаційна система захисту потребує постійного вдосконалення і покращення. Адже, хакери і злочинні елементи безперервно вдосконалюють власні методики злому і несанкціонованого проникнення. Вище зазначене потребує розробки та впровадження певних інструментів та важелів забезпечення захисту інформації на рівні територіальних громад.

Аналіз останніх досліджень і публікацій. Аналіз останніх публікацій по проблемі дозволив нам розбити їх на 5 основних блоків. Перший присвячений кібербезпеці та кіберзаходам. Вагомий внесок у розробку цього наукового напрямку зробили Данильченко Ю. [1], Мальцева І., Черниш Ю., Штонда Р. [2]. Їх публікації акцентують увагу на необхідності удосконалення заходів кібербезпеки для запобігання кібератак та забезпечення безпечного обміну інформацією. Наступний блок присвячений питанням цифрової трансформації, публікації Квітка С., Новіченко Н., Гусаревич Н., Піскоха Н., Бардах О. Демошенко Г. [3], Литвин Н., Крупнова Л. [4] відзначають значення цифрової трансформації для територіальних громад і вказують на те, що ІКТ є основним каталізатором для створення ефективних систем обміну інформацією, які відповідають потребам сучасного суспільства. Третій напрямок – захист особистих даних. Тут відзначилися Гнатюк С. [5], Кардаш А. [6]. В своїх публікаціях вони звертають увагу на важливість захисту особистих даних громадян в контексті обміну інформацією та обов'язковість дотримання відповідних нормативно-правових актів. Інновації в розвитку електронних сервісів складають наступний блок, його представниками є Бакуменко В., Попов С. [7], Баштанник В. [8], Бодров В. [9], Грибко О. [10]. Їх дослідження висвітлюють інноваційні підходи та технології, що використовуються для розвитку електронних сервісів у муніципалітетах з метою забезпечення безпеки обміну інформацією та підвищення задоволення громадян. І останній напрямок – управління ризиками та надзвичайні ситуації, вагомими у цьому блоці є наробки Потій О., Лєншин А. [11], вони підкреслюють важливість попереднього планування та реагування на ризики та надзвичайні ситуації шляхом використання ІКТ для швидкого та координованого обміну інформацією.

Формулювання цілей статті. Метою даної роботи є обґрунтування теоретичних та практичних основ впровадження інструментів захисту інформації на рівні територіальної громади.

Виклад основного матеріалу.

ІКТ що використовуються у розвитку ТГ. Взаємодія місцевого самоврядування ТГ з громадськістю відбувається за допомогою інформаційних ресурсів, які є ключовим інструментом для побудови партнерських відносин та поліпшення діяльності самої місцевої влади. Це означає не лише надання інформації, але й обмін нею. Для цього потрібний відповідний рівень інформаційних технологій і їх доступність для всіх сторін, включаючи органи місцевої влади та широке коло громадськості.

Деякі з найбільш поширених ІКТ на цьому рівні включають такі технології.

Інтернет речей (IoT). Основна ідея полягає в тому, щоб створити мережу речей, яка була б здатна збирати інформацію, аналізувати її і діяти відповідно до отриманих даних. Інтернет речей (IoT) об'єднує різноманітні технології для створення зв'язаної мережі речей. Наприклад, бездротові технології, такі як Wi-Fi, Bluetooth, Zigbee, Z-Wave, LoRa, NB-IoT, дозволяють підключати різні пристрої до мережі без необхідності фізичного підключення за допомогою кабелів. Датчики збирають різні типи даних, такі як температура, вологість, рівень освітленості, рух, звук тощо [12]. Ці дані використовуються для моніторингу оточуючого середовища та збору інформації для подальшого аналізу.

Блокчейн технології. Блокчейн – це розподілена база даних, що складається з набору блоків, кожен з

яких містить певну кількість транзакцій. Кожен блок містить посилання на попередній блок, утворюючи таким чином ланцюжок блоків. Основні характеристики блокчейну включають децентралізацію, недоторканність даних і відкритість. Блокчейн використовує криптографію для забезпечення безпеки даних та підтвердження автентичності транзакцій. Для цього використовуються хеш-функції, цифрові підписи та інші методи шифрування [13]. Ця технологія працює на основі децентралізованої мережі, що означає, що дані зберігаються на кожному вузлі мережі, а не на централізованому сервері. Це забезпечує високу стійкість до вторгнень та відмовостійкість.

Штучний інтелект (AI). AI складається з двох основних складових: машинного навчання (Machine Learning, ML) та глибинного навчання (Deep Learning, DL). Машинне навчання – це підрозділ штучного інтелекту, який допомагає системам самостійно вчитися на даних без будь-якої явної участі людини. ML використовує різні алгоритми, які використовують дані, щоб з'ясувати, як поліпшити, спрогнозувати й описати дані [14]. Глибинне навчання – це різновид штучного інтелекту і метод машинного навчання, заснованого на концепції штучних нейронних мереж. Такі мережі допомагають машинам вчитися на даних, особливо на неструктурованих даних. Найчастіше використовується в комп'ютерному зорі, розпізнаванні зображень і мови.

Обробка даних та аналітика – це комплексний набір програмних та технічних засобів, які використовуються для збору, обробки, аналізу та інтерпретації даних з метою виявлення корисної інформації, тенденцій, закономірностей та залежностей, які можуть бути використані для прийняття рішень [15]. Для ефективного функціонування системи аналізу даних важливо мати високоякісні та надійні дані, а також використовувати відповідні методи та техніки аналізу даних, залежно від поставлених завдань та цілей.

Платформи обміну ресурсами. Платформи обміну ресурсами можуть бути корисним інструментом для сприяння економічному розвитку та ефективному використанню ресурсів. Існують різні види таких платформ: організаційні платформи, муніципальні платформи, індустріальні маркетплейси [16]. Вони можуть забезпечувати можливість знаходження потенційних партнерів для спільних проєктів або обміну ресурсами.

Напрямки обміну інформацією на рівні ТГ. Використання наведених вище ІКТ при обміні інформацією на рівні ТГ відбувається за кількома напрямками:

1) в управлінні ТГ безпосередньо;
2) при взаємодії з іншими ТГ;
3) при взаємодії з центральними органами влади.

В управлінні ТГ використання цифрових технологічних рішень передбачається на декількох рівнях (рис. 1):

На рівні мешканців громади.

Для мешканців громади використання широкого арсеналу цифрових рішень описаних вище забезпечує можливість зручно і швидко отримувати корисну інформацію про різні сфери життєдіяльності громади (наприклад, сфери ЖКГ, громадського транспорту, заклади освіти та охорони здоров'я), а також можливість співпрацювати з місцевою владою (наприклад, сервіс петицій, доступ до електронних приймалень голови, його заступників, депутатів тощо). Цифрові інструменти відкривають можливість передачі інформації про будь-яку проблему, пов'язану з безпекою, благоустроєм громади тощо.

На рівні підприємницького середовища.

Наразі ЦНАПи мають веб-портали або спеціалізовані онлайн-системи, через які громадяни можуть подавати заяви, заповнювати форми, записуватися на прийом та отримувати інформацію про надання послуг. Ці системи зазвичай забезпечують можливість взаємодії з ЦНАПом без необхідності особистого візиту. Громадяни можуть надсилати свої запити, заяви або документи через електронну пошту ЦНАПу. Це забезпечує

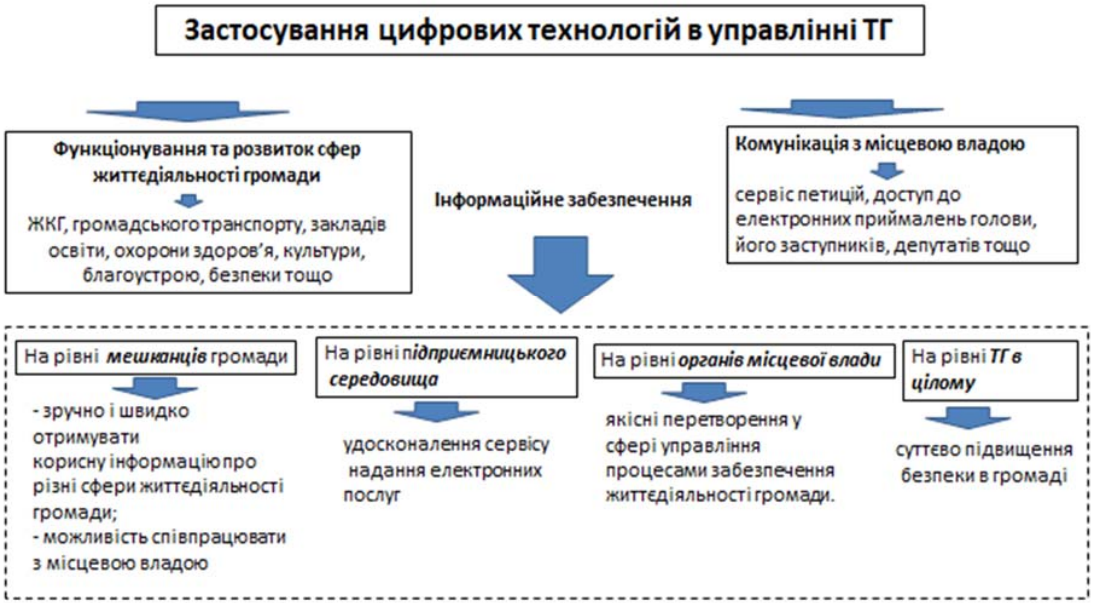

Рис. 1. Напрямки обміну інформацією на рівні ТГ

Джерело: складено авторами [8–10]

швидку та ефективну комунікацію в реальному часі. Інформаційні системи ЦНАПів можуть бути пов'язані з електронними базами даних, які забезпечують можливість швидкого доступу до інформації про громадян, їхні заяви та інші документи.

На рівні органів місцевої влади.

Представники місцевої влади отримають механізм якісних перетворень у сфері управління процесами забезпечення життєдіяльності громади. Це стосується, як системи управління та контролю за виконанням доручень, так і системами контролю за діючою інфраструктурою за допомогою новітніх технологій. Внаслідок застосування цифрових рішень під контроль беруться принципи роботи органів місцевого самоврядування та їх підрозділів. Тому серед пріоритетів – підвищення безпеки зберігання даних, стандартизація та регламентація процесів на всіх етапах виконання завдань.

На рівні ТГ в цілому.

Застосування ІКТ, дозволить суттєво підвищити безпеку у громаді за рахунок встановлення камер зовнішнього відеоспостереження і системи контролю та аналізу даних. Впровадження технології Інтернету речей, наприклад, дозволить швидко відслідковувати аварії на мережах електропостачання, теплопостачання, постачання холодної та гарячої води.

Таким чином, в межах самої громади важлива різноманітна інформація яка охоплює різні аспекти, що допомагають громаді взаємодіяти, приймати рішення та розвиватися, а саме: громадська активність; бюджет та фінансова інформація; інфраструктура та комунальні послуги; соціальні програми; екологічні аспекти; місцева економіка та підприємництво; безпека та правопорядок.

Цифрові рішення при взаємодії з іншими громадами грають ключову роль у покращенні комунікацій, обміну інформацією, оптимізації процесів та спільного вирішення проблем. В міжмуніципальному співробітництві важлива різноманітна інформація, яка допомагає управлінцям приймати обґрунтовані рішення, планувати та координувати спільні проєкти та забезпечує ефективну комунікацію між різними ТГ.

Ця інформація допомагає муніципалітетам краще розуміти потреби та можливості один одного, планувати спільні дії, ефективно використовувати ресурси та розвивати територіальні громади в цілому. Застосування цифрових технологій для обробки та обміну цією інформацією може значно полегшити співпрацю між муніципалітетами. Такі рішення сприяють підвищенню ефективності та забезпеченню більш взаємовигідних відносин між муніципалітетами. Основні з них такі: електронний документообіг та архівація; електронні платформи для спільного планування; системи управління ресурсами; геопросторові технології для планування розвитку; електронні системи обліку та фінансового планування, спільні портали для громадян; цифрові інструменти для моніторингу та звітності; застосування цифрових систем для відстеження прогресу спільних проєктів, вирішення питань та підготовки звітів.

Ці цифрові інструменти сприяють вдосконаленню співпраці між муніципалітетами, роблять процеси управління більш прозорими та ефективними, і сприяють спільному розвитку територіальних громад.

Цифрові рішення для взаємодії територіальних громад з органами центральної влади важливі для забезпечення ефективної комунікації, обміну інформацією та координації заходів на різних рівнях управління. Такі рішення допомагають зробити владу більш прозорою, забезпечують оперативну реакцію на потреби громад та сприяють їх розвитку. Насамперед мова йде про: електронне урядування (E-Government); системи обліку та звітності; геопросторові технології; системи управління проєктами; електронні системи безпеки.

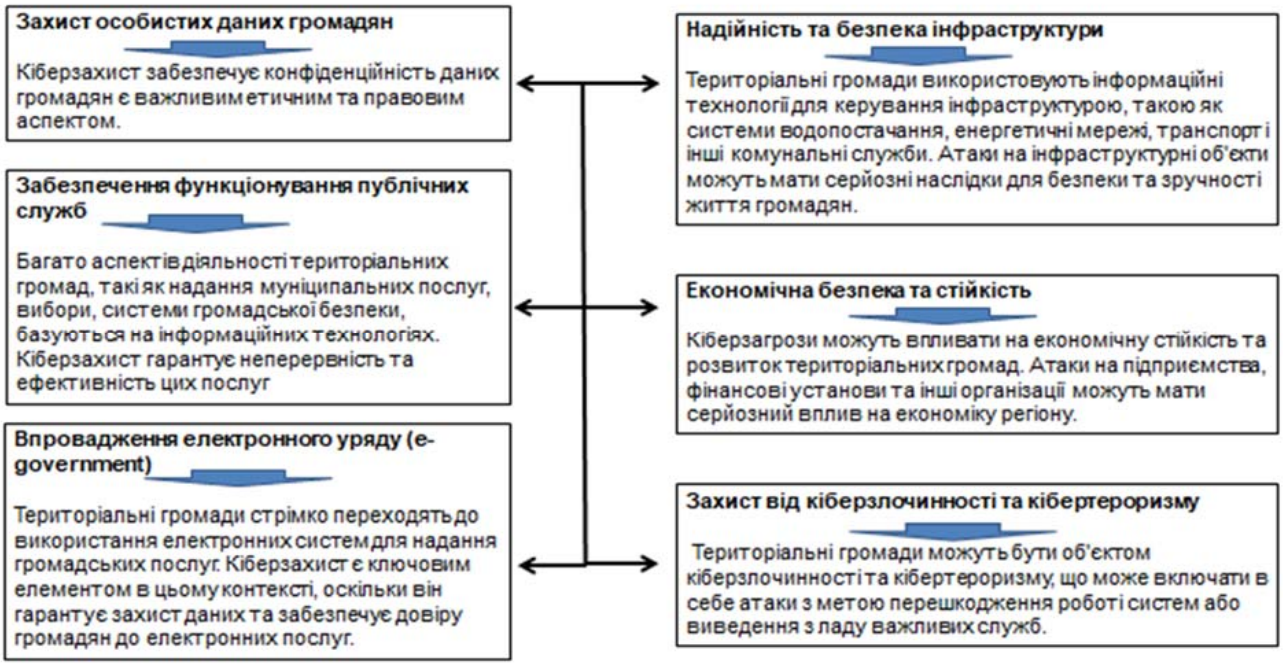

Рис. 2. Важливість та необхідність захисту інформації на рівні територіальної громади

Джерело: складено авторами [17]

Важливість та необхідність захисту інформації на рівні ТГ. Таким чином, описаний вище процес передбачає використання інформаційних систем, мереж, ресурсів та ІКТ, побудованих на основі застосування сучасної обчислюваної та комунікаційної техніки. Питання захищеного обміну інформацією на рівні територіальних громадах, у зв'язку з цим, стає все більш актуальним та важливим для життя громади. Захист всього цього комплексу інформації є надзвичайно важливим для забезпечення безпеки та ефективності функціонування адміністративних та інших процесів. На рис. 2 наведено деякі ключові аспекти, які підкреслюють важливість та необхідність захисту інформації на цьому рівні.

В територіальних громадах обробляється велика кількість конфіденційної інформації, такої як особисті дані громадян, фінансова інформація, а також документи, пов'язані з внутрішньою діяльністю громади. Кіберзахист є необхідним для збереження конфіденційності цієї інформації та запобігання її несанкціонованому доступу.

Практичні застосування ІКТ у розвитку ТГ. Проаналізувавши дані, які є у відкритому доступі щодо можливостей застосування ІКТ при обміні інформацією на рівні ТГ [18], автори дійшли висновку, що інформатизація ТГ України характеризується наступними основними моментами табл. 1.

Отже, розгляд як сильних сторін, так і слабких сторін, а також можливостей та загроз інформатизації ТГ, наразі є важливим, його результати нададуть можливість розробити ефективні стратегії впровадження та захисту від потенційних загроз ТГ для забезпечення її інформаційної безпеки.

Засоби захисту інформації на рівні ТГ. Існуючі сьогодні засоби захисту інформації можуть бути розділені на такі основні групи.

Фізичні засоби захисту. Вони включають заходи для фізичного захисту інформації, такі як захищені приміщення, контроль доступу до пристроїв і обладнання, використання замків, кейсів та інших засобів.

Комп'ютерні засоби захисту. Ці засоби включають в себе використання криптографії, аутентифікації, авто-

Таблиця 1

SWOT- аналіз інформатизації ТГ України

Сильні сторони	Можливості
1. Покращення доступності послуг для громадян: електронні сервіси та платформи дозволяють громадянам зручно та швидко отримувати необхідні послуги, такі як подання заяв, отримання документів чи сплату податків, без необхідності відвідування офісів влади. **2. Зростання ефективності громадських послуг:** впровадження цифрових технологій дозволяє оптимізувати надання громадських послуг, таких як освіта, охорона здоров'я та соціальна підтримка, покращуючи якість життя громадян. **3. Підвищення транспарентності та відкритості влади:** інформаційні технології допомагають забезпечувати доступ до публічної інформації, підвищуючи транспарентність роботи місцевих органів влади та зменшуючи ризики корупції. **4. Розвиток людського капіталу:** Впровадження інформатизації вимагає кваліфікованих кадрів, що сприяє розвитку інформаційних технологій та підвищує рівень компетентності населення.	**1. Підвищення ефективності управління**: запровадження цифрових технологій дозволяє оптимізувати роботу ОМС, забезпечуючи швидку і точну обробку даних, автоматизацію бізнес-процесів та зменшення бюрократичних перешкод. **2. Розвиток інноваційного середовища:** інформатизація створює умови для розвитку інноваційного середовища, стимулюючи виникнення стартапів, технологічних компаній та нових видів бізнесу, що сприяє економічному зростанню та залученню інвестицій. **3. Підвищення рівня технічної компетентності:** інформатизація сприяє підвищенню рівня технічної компетентності населення та розвитку ІТ-галузі, що створює нові можливості для робочих місць та освіти. **4. Покращення роботи інфраструктури:** застосування ІКТ допомагає вдосконалювати системи управління транспортними потоками, енергоефективності та екологічної безпеки, що сприяє створенню зручного та екологічного середовища для проживання.
Слабкі сторони	**Загрози**
1. Нерівномірний доступ до технологій: У деяких регіонах може бути обмежений доступ до технологій через відсутність інфраструктури або фінансові обмеження, що призводить до цифрового відчуження та нерівності. **2. Недостатня компетентність персоналу:** недостатній рівень навичок та обізнаності персоналу у галузі інформаційних технологій може ускладнювати ефективне впровадження та управління цифровими системами. **3. Ризик втрати даних:** недостатнє резервне копіювання та захист даних може призвести до втрати важливої інформації, що може мати серйозні наслідки для функціонування та діяльності громади. **4. Недостатня здатність до адаптації:** Швидкий темп змін у технологічній сфері може ускладнювати здатність громад до адаптації до нових цифрових рішень та технологій. **5. Соціальні аспекти:** Інформатизація може призвести до виключення певних груп населення, таких як люди похилого віку або особи з обмеженими можливостями, через відсутність доступу або навичок у користуванні цифровими технологіями.	**1. Відсутність адекватної інфраструктури**: у багатьох регіонах може бути обмежений доступ до сучасних технологій через відсутність високошвидкісного Інтернету, погану якість зв'язку та інші технічні обмеження. **2. Недостатня кібергігієна**: відсутність належної освіти та навичок у галузі кібербезпеки серед населення може призвести до неправильного використання цифрових технологій та збільшення ризику кібератак. **3. Залежність від технологій:** збільшення залежності від інформаційних технологій може призвести до вразливості громад в разі відмови або порушення роботи систем. **4. Проблеми з конфіденційністю даних**: збільшення обсягів збирання та обробки особистих даних може призвести до проблем з приватністю даних та порушення прав людини. **5. Економічні виклики:** впровадження нових технологій може потребувати значних витрат на покупку та підтримку обладнання, а також навчання персоналу, що може бути складно для бюджетів територіальних громад.

Джерело: складено авторами на основі [18]

ризації, встановлення політик доступу, антивірусного програмного забезпечення, фаєрволів та інших технологій для захисту інформації на рівні комп'ютерних систем і мереж.

Організаційні засоби захисту. Вони охоплюють створення політик безпеки, розробку процедур безпеки, проведення навчання та свідомості з питань безпеки серед персоналу, а також введення механізмів аудиту безпеки та внутрішнього контролю.

Технологічні засоби захисту. Ці засоби включають в себе застосування спеціалізованих технологій, таких як біометричні системи, системи виявлення вторгнень, шифрування даних та інші технічні засоби безпеки.

Соціально-психологічні засоби захисту. Ці засоби враховують фактори людського впливу, такі як соціальна інженерія, психологічні техніки управління вразливістю та поведінка користувачів.

Ці групування можуть перетинатися, оскільки багато засобів захисту інформації використовують комбінації різних підходів для досягнення максимального рівня безпеки.

Криптографічні засоби. Ці засоби є одним з найважливіших інструментів, які використовуються для забезпечення захисту інформації, зокрема, у інформаційно-телекомунікаційних системах ТГ. Тим не менш, зростання частки мультимедійної інформації у загальному трафіку, що генерується, передається та зберігається у інформаційно-телекомунікаційних системах ТГ призводить до зростання ролі стеганографічних засобів, а також дуже перспективною є ідею поєднання криптографічних та стеганографічних засобів у єдину крипто-стеганографічну систему [19]. Такий підхід потребує проведення подальших досліджень задля розробки та адаптації існуючих знань щодо побудови крипто-стеганографічних систем які були б адаптованими для вирішення потреб саме ТГ.

Висновки. Проведене в рамках даної статті дослідження дозволило зробити наступні висновки. Територіальна громада є важливим центром діяльності громадян, де збирається та обробляється значна кількість конфіденційних даних, включаючи особисту інформацію мешканців, фінансові дані та іншу чутливу інформацію. Тому захист цих даних є важливим завданням для забезпечення приватності та безпеки громадян. Крім того, територіальні громади здійснюють різноманітні адміністративні та соціальні функції, велика частина яких базується на обміні та зберіганні інформації, тому вразливість системи може призвести до порушення роботи та непередбачених наслідків для громадян. В сучасному цифровому світі територіальні громади стають мішенню для кіберзлочинців, які можуть намагатися зламати системи та отримати доступ до конфіденційної інформації з метою вчинення шкідливих або злочинних дій. Тому важливо мати належні заходи захисту для запобігання таким загрозам та збереження довіри та стабільності в громаді. Отже, захист інформації на рівні територіальної громади є критично важливим як з погляду приватності та безпеки громадян, так і для забезпечення нормальної роботи адміністративних та соціальних служб, а також для запобігання потенційним кіберзагрозам та злочинам. Інформаційно-комунікаційні технології відіграють ключову роль у забезпеченні такого захисту, надаючи ефективні технічні засоби захисту, розвиваючи системи моніторингу та реагування на загрози, а також підвищуючи обізнаність персоналу з питань кібербезпеки. Криптографічні засоби є одним з найважливіших інструментів, які використовуються для забезпечення захисту інформації, зокрема, у інформаційно-телекомунікаційних системах ТГ. Такий підхід потребує проведення подальших досліджень задля розробки та адаптації існуючих знань щодо побудови крипто-стеганографічних систем які були б адаптованими для вирішення потреб саме ТГ.

Література:

1. Данильченко Ю.Б. Проблеми протидії кібертераризму в контексті збройної агресії: кримінально-правовий вимір. «Кібербезпека в Україні: правові та організаційні питання», матеріали міжнародної науково-практичної конференції (Одеса, 17 листопада 2023 р.) Одеса: ОДУВС, 169 с. URL: https://dspace.oduvs.edu.ua/server/api/core/bitstreams/59353573-4db8-41ee-805a-c951e1a2b9ce/content

2. Мальцева І.Р., Черниш Ю.О., Штонда Р.М. Аналіз деяких кіберзагроз в умовах війни. *Кібербезпека: освіта, наука, техніка*. 2022. № 4(16). URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/362/300

3. Квітка С., Новіченко Н., Гусаревич Н., Піскоха Н., Бардах О. Демошенко Г. Перспективні напрямки цифрової трансформації публічного управління. *Аспекти публічного управління*. 2020. № 8(4). С. 129–146.

4. Литвин Н.А., Крупнова Л.В. Діджиталізація як засіб підвищення відкритості, прозорості та ефективності діяльності органів державної влади та органів місцевого самоврядування щодо надання електронних послуг. *Ірпінський юридичний часопис: науковий журнал*. 2020. №. (2). С. 69–75.

5. Гнатюк С.Л. Особливості захисту персональних даних в сучасному кіберпросторі: норматив-но-правовий досвід ЄС. Проблеми захисту прав людини в інформаційному суспільстві, матеріали наук.-практ. конф. / 1 квітня 2016 р., м. Київ / Упорядн.: В.М. Фурашев, С.Ю. Петряєв. Київ : НДІІП НАПрН України, Національний інститут страте-гічних досліджень, Секретаріат Уповноважено-го Верховної Ради України з прав людини, НТУУ «КПІ» Вид-во «Політехніка», 2016. С. 88–96.

6. Кардаш А.В. Конституційно-правовий захист інформації про особу (порівняльно-правовий аспект): дис. канд. юрид. наук; спец: 12.00.02. Харків, 2019. 228 с.

7. Бакуменко В. Парадигма інноваційного розвитку суспільства : сучасні концепції реформування публічного управління. *Ефективність державного управління : зб. наук. пр*. 2015. Вип. 43. URL: http://www.lvivacademy.com/vidavnitstvo_1/edu_43/fail/4.pdf

8. Баштанник В. Інноваційні механізми регіонального розвитку. *Державне управління та місцеве самоврядування* : *зб. наук. пр*. 2012. Вип. 4(15). URL: http://www.dbuapa.dp.ua/vidavnictvo/2012/2012_04(15)/12bvvurr.pdf

9. Бодров В.Г. Інноваційні механізми державного управління процесами модернізації національної економіки. Інновації в державному управлінні: системна інтеграція освіти, науки, практики, матеріали наук.-практ. конф. за міжнар. участю, (Київ, 27 травня, 2011 р.) : у 2 т. Київ : НАДУ, 2011. Т. 1. С. 331–334.

10. Грибко О.В. Використання інноваційних підходів в державному управлінні. *Публічне управління: виклики XXI ст*., матеріали XIII Міжнародного наукового конгресу. 2023. URL: https://docs.google.com/file/d/0B5PLeqrlVLsIdk5TRS0zd2E0akU/edit

11. Потій О.В., Лєншин А.В. Дослідження методів оцінки ризиків безпеці інформації та розробка пропозицій з їх вдосконалення на основі системного підходу. *Зб. наук. праць ХУПС*. 2010. Вип. 2(24). С. 85–91.

12. Що таке Інтернет речей. URL: Освітня програма «Internet of things». 2022. URL: http://iot.lviv.ua

13. Що таке блокчейн і як він працює? 2021. Academy.binance. URL: https://academy.binance.com/uk/articles/what-is-blockchain-and-how-does-it-work

14. Що таке Artificial Intelligence (AI)? 2021. Qagroup. URL: https://qagroup.com.ua/publications/shcho-take-artificial-intelligence-ai/

15. Обробка та аналіз даних. Центр прикладних досліджень. 2020. URL: https://cpd.com.ua/uk/obrobka-danyh/

16. Революція платформ. Як мережеві ринки змінюють економіку – і як змусити їх працювати на вас. 2022. URL: https://hub.kyivstar.ua/reviews/revolyucziya-platform-yak-merezhevi-rinki-zminyuyut-ekonomiku-i-yak-zmusiti-yih-praczyuvati-na-vas

17. Кібербезпека в Україні: шляхи розвитку та можливості. Укрінформ. 2023. URL: https://www.ukrinform.ua/rubric-technology/3704093-kiberbezpeka-v-ukraini-slahi-rozvitku-ta-mozlivosti.html

18. Індекс цифрової трансформації регіонів України. Підсумки 2023 року. Міністерство цифрової трансформації України. URL: https://thedigital.gov.ua/storage/uploads/files/page/community/reports/.pdf

19. Задирака В.К. Сучасні методи розв'язання задач інформаційної безпеки. *Вісник НАН України*. 2014. № 5. С. 65–69.

References:

1. Danylchenko Yu. B. (November 17, 2023) Problemy protydii kiberteraryzmu v konteksti zbroinoi ahresii: kryminalno-pravovyi vymir. [Problems of combating cyber-terrorism in the context of armed aggression: criminal-legal dimension]. «Kiberbezpeka v Ukraini: pravovi ta orhanizatsiini pytannia», materialy mizhnarodnoi naukovo-praktychnoi konferentsii. Odesa: ODUVS, 169 p. Available at: https://dspace.oduvs.edu.ua/server/api/core/bitstreams/59353573-4db8-41ee-805a-c951e1a2b9ce/content

2. Maltseva I. R., Chernysh Yu. O., Shtonda R. M. (2022) Analiz deiakykh kiberzahroz v umovakh viiny. [Analysis of some cyber threats in the conditions of war]. *Kiberbezpeka: osvita, nauka, tekhnika*, no. 4(16). Available at: https://csecurity.kubg.edu.ua/index.php/journal/article/view/362/300

3. Kvitka S., Novichenko N., Husarevych N., Piskokha N., Bardakh O. Demoshenko H. (2020) Perspektyvni napriamky tsyfrovoi transformatsii publichnoho upravlinnia. [Promising directions of digital transformation of public administration]. *Aspekty publichnoho upravlinnia*, no. 8(4), pp. 129–146.

4. Lytvyn N. A., Krupnova L. V. (2020) Didzhytalizatsiia yak zasib pidvyshchennia vidkrytosti, prozorosti ta efektyvnosti diialnosti orhaniv derzhavnoi vlady ta orhaniv mistsevoho samovriaduvannia shchodo nadannia elektronnykh posluh. [Digitization as a means of increasing the openness, transparency and efficiency of the activities of state authorities and local self-government bodies in the provision of electronic services]. *Irpinskyi yurydychnyi chasopys: naukovyi zhurnal*, no. 2, pp. 69–75.

5. Hnatiuk S. L. (April 1, 2016) Osoblyvosti zakhystu personalnykh danykh v suchasnomu kiberprostori: normatyv-no-pravovyi dosvid YeS. [Peculiarities of personal data protection in modern cyberspace: regulatory and legal experience of the EU]. Problemy zakhystu prav liudyny v informatsiinomu suspilstvi, materialy nauk.-prakt. konf. / Uporiadn.: V. M. Furashev, S. Iu. Petriaiev. Kyiv : NDIIP NAPrN Ukrainy, Natsionalnyi instytut strate-hichnykh doslidzhen, Sekretariat Upovnovazheno-ho Verkhovnoi Rady Ukrainy z prav liudyny, NTUU «KPI» Vyd-vo «Politekhnika», pp. 88–96.

6. Kardash A. V. (2019) Konstytutsiino-pravovyi zakhyst informatsii pro osobu (porivnialno-pravovyi aspekt) [Constitutional and legal protection of personal information (comparative and legal aspect)]: dys. kand. yuryd. nauk; spets: 12.00.02. Kharkiv. 228 p.

7. Bakumenko V. (2015) Paradyhma innovatsiinoho rozvytku suspilstva : suchasni kontseptsii reformuvannia publichnoho upravlinnia. [The paradigm of innovative development of society: modern concepts of reforming public administration]. *Efektyvnist derzhavnoho upravlinnia : zb. nauk. pr*., is. 43. Available at: http://www.lvivacademy.com/vidavnitstvo_1/edu_43/fail/4.pdf

8. Bashtannyk V. (2012) Innovatsiini mekhanizmy rehionalnoho rozvytku. [Innovative mechanisms of regional development]. *Derzhavne upravlinnia ta mistseve samovriaduvannia : zb. nauk. pr.,* is. 4(15). Available at: http://www.dbuapa.dp.ua/vidavnictvo/2012/2012_04(15)/12bvvurr.pdf

9. Bodrov V. H. (May 27, 2011) Innovatsiini mekhanizmy derzhavnoho upravlinnia protsesamy modernizatsii natsionalnoi ekonomiky. [Innovative mechanisms of state management of modernization processes of the national economy]. Innovatsii v derzhavnomu upravlinni: systemna intehratsiia osvity, nauky, praktyky, materialy nauk.-prakt. konf. za mizhnar. uchastiu: u 2 t. Kyiv : NADU. Vol. 1, pp. 331–334.

10. Hrybko O. V. (2023) Vykorystannia innovatsiinykh pidkhodiv v derzhavnomu upravlinni. [Use of innovative approaches in public administration]. Publichne upravlinnia: vyklyky KhKhI st., materialy KhIII Mizhnarodnoho naukovoho konhresu. Available at: https://docs.google.com/file/d/0B5PLeqrlVLsIdk5TRS0zd2E0akU/edit

11. Potii O. V., Lienshyn A. V. (2010) Doslidzhennia metodiv otsinky ryzykiv bezpetsi informatsii ta rozrobka propozytsii z yikh vdoskonalennia na osnovi systemnoho pidkhodu. [Researching information security risk assessment methods and developing proposals for their improvement based on a systematic approach]. *Zb. nauk. prats KhUPS*, is. 2(24), pp. 85–91.

12. Shcho take Internet rechei (2022). [What is the Internet of Things]. Osvitnia prohrama «Internet of things». Available at: http://iot.lviv.ua

13. Shcho take blokchein i yak vin pratsiuie? (2021). [What is blockchain and how does it work?]. Academy.binance. Available at: https://academy.binance.com/uk/articles/what-is-blockchain-and-how-does-it-work

14. Shcho take Artificial Intelligence (AI)? (2021). [What is Artificial Intelligence (AI)?]. Qagroup. Available at: https://qagroup.com.ua/publications/shcho-take-artificial-intelligence-ai/

15. Obrobka ta analiz danykh (2020). [Data processing and analysis]. Tsentr prykladnykh doslidzhen. Available at: https://cpd.com.ua/uk/obrobka-danyh/

16. Revoliutsiia platform. Yak merezhevi rynky zminiuiut ekonomiku – i yak zmusyty yikh pratsiuvaty na vas (2022). [Revolution of platforms. How network markets are changing the economy – and how to make them work for you.]. hub.kyivstar.ua. Available

at: https://hub.kyivstar.ua/reviews/revolyucziya-platform-yak-merezhevi-rinki-zminyuyut-ekonomiku-i-yak-zmusiti-yih-praczyuvati-na-vas

17. Kiberbezpeka v Ukraini: shliakhy rozvytku ta mozhlyvosti (2023). [Cyber security in Ukraine: ways of development and opportunities]. Ukrinform. Available at: https://www.ukrinform.ua/rubric-technology/3704093-kiberbezpeka-v-ukraini-slahi-rozvitku-ta-mozlivosti.html

18. Indeks tsyfrovoi transformatsii rehioniv Ukrainy. Pidsumky 2023 roku (2023). [Index of digital transformation of regions of Ukraine. Results of 2023]. Ministerstvo tsyfrovoi transformatsii Ukrainy. Available at: https://thedigital.gov.ua/storage/uploads/files/page/community/reports/.pdf

19. Zadyraka V. K. (2014) Suchasni metody rozviazannia zadach informatsiinoi bezpeky. [Modern methods of solving information security problems]. *Visnyk NAN Ukrainy*, no. 5. pp. 65–69.