Шифр «Захист інформації»

Наукова робота

«Захищений обмін інформацією в об’єднаних територіальних громадах на основі Smart – технології («Розумна громада»)

Зміст

Вступ

Актуальність дослідження. Інформатизація є важливою сферою суспільного життя тому, що охоплює коло поточних та перспективних проблем – економічних, організаційних, соціальних, правових, політичних, науково-технічних, виробничих, а також розвиток культури та освіти. Вона сприяє поліпшенню керованості економікою, інноваційним розвитком, задоволенню інформаційних потреб громадян, їх об'єднань, підприємств, організацій, установ, органів місцевого самоврядування та державної влади, зростанню продуктивності праці, вдосконаленню соціально-економічних відносин тощо. Цей процес передбачає використання інформаційних систем, мереж, ресурсів та інформаційних технологій, побудованих на основі застосування сучасної обчислюваної та комунікаційної техніки. Тому, питання захищеного обміну інформацією в об'єднаних територіальних громадах на основі Smart – технології, стає все більш актуальним та важливим для життя громади.

Аналіз наукових досліджень. Проблемою використання Smart-технологій у місцевому самоврядуванні на місцевому рівні займалися такі вітчизняні науковці,як: О. Андрєєва, В. Бабаєв, А. Балашов, В.Воронкова, В. Геєць, А. Гошко, В. Дзюндзюк, І. Жукович, К. Козак, А. Козирєв, Ю., М. Тарасенко, Л. Товажнянський, В. Уманця, А. Чухно, Ю. Шаров та інші. Вагомий внесок у дослідження питання розвитку та впровадження стратегії «розумних міст» здійснено як зарубіжними так і вітчизняними вченими, зокрема: М. Ангелідоу, М. Бойков, В. Дудикевич, В. Максимович, Г. Микитин, В. Хома, А. Грінфілд, І. Жукович, Р. Кітчін, П. Ломбарді, Д. Ніколаєва, Х. Тодосов, М. Салазкін, Р. Холландс, С. Чукут та ін. Попри це, на сьогодні недостатньо дослідженим залишається проблема використання Smart-технологій у процесі захисту обміном інформацією в об'єднаних територіальних громад.

Мета наукової роботи полягає в обґрунтуванні теоретичних та практичних засад впровадження захищеного обміну інформацією в об'єднаних територіальних громадах на основі Smart – технології.

Відповідно до мети дослідження були поставлені та вирішені наступні завдання:

- дослідити сутність, класифікацію засобів захисту інформації та можливість застосування Smart- технології в обєднаних територіальних громад;

- охарактеризувати інфраструктури інформатизації Софіївської ОТГ та особливості захисту інформації в громадах

- обґрунтувати інноваційні напрямки захищеного обміну інформацією в об'єднаних територіальних громадах, на прикладі Софіївської ОТГ

Об'єктом наукового дослідження є процес захищеного обміну інформацією в об'єднаних територіальних громадах на основі Smart – технології.

Предметом дослідження є теоретичні, методичні засади захищеного обміну інформацією в об'єднаних територіальних громадах на основі Smart - технології.

Методи дослідження. У науковій роботі використано методи: системний аналіз, та шифрування, за допомогою яких розроблено підхід до застосування криптографічного алгоритму шифрування даних AES в сенсорних мережах системи Smart – технології в об'єднаних територіальних громадах.

Законодавчо-нормативною, інформаційною та практичною базою дослідження є законодавчі акти, дані Державної служби статистики України, Кабінету Міністрів України, інформаційно-публіцистичні видання, монографії, наукові статті, результати власних досліджень і розрахунків.

Наукова новизна. Розроблено алгоритмічно-програмне забезпечення криптографічного захисту обміну інформацією в сенсорних мережах «розумного міста» (для використання в ОТГ) відповідно до алгоритму блокового шифрування даних AES та мови програмування C#.

РОЗДІЛ 1
ТЕОРЕТИЧНІ АСПЕКТИ ЗАХИЩЕНОГО ОБМІНУ ІНФОРМАЦІЄЮ В ОБ'ЄДНАНИХ ТЕРИТОРІАЛЬНИХ ГРОМАДАХ НА ОСНОВІ SMART – ТЕХНОЛОГІЇ

Захист інформації є однією з вічних проблем. Протягом історії людства способи розв'язання цієї проблеми визначались рівнем розвитку технологій. У сучасному інформаційному суспільстві технологія відіграє роль активатора цієї проблеми — комп'ютерні злочини стали характерною ознакою сьогодення.

Згідно із Законом України «Про захист інформації в автоматизованих системах» захист інформації — це сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією.

Залежно від можливих порушень у роботі системи та загроз несанкціонованого доступу до інформації численні види захисту можна об'єднати у групи, які представленні на рисунку 1.1 [1]

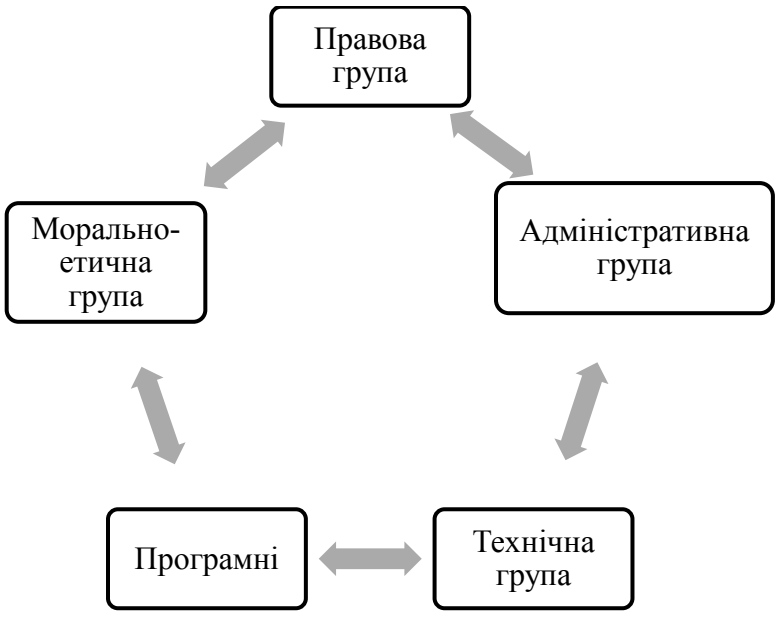

Рисунок 1.1 Класифікація засобів захисту інформації

Морально-етичні засоби. До цієї групи належать норми поведінки, які традиційно склались або складаються з поширенням ЕОМ, мереж і т. ін. Ці норми

здебільшого не є обов'язковими і не затверджені в законодавчому порядку, але їх невиконання часто призводить до падіння авторитету та престижу людини, групи осіб, організації або країни. Найбільш характерним прикладом є Кодекс професійної поведінки членів Асоціації користувачів ЕОМ США.

Правові засоби захисту — чинні закони, укази та інші нормативні акти, які регламентують правила користування інформацією і відповідальність за їх порушення, захищають авторські права програмістів та регулюють інші питання використання ІТ. Перехід до інформаційного суспільства вимагає удосконалення карного і цивільного законодавства, а також судочинства. Так, уже сьогодні у Гонконгу максимальним покаранням за такий злочин, якщо він призвів до виведення з ладу ІС або Web-сайту, є 10 років позбавлення волі. Для порівняння, у Кримінальному кодексі України незаконне втручання в роботу комп'ютерів та комп'ютерних мереж карається штрафом до сімдесяти неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або обмеженням волі на той самий строк [1].

Адміністративні (організаційні) засоби захисту інформації регламентують процеси функціонування ІС, використання її ресурсів, діяльність персоналу, а також порядок взаємодії користувачів із системою таким чином, щоб найбільшою мірою ускладнити або не допустити порушень безпеки. Адміністративні засоби є невід’ємною частиною захисту інформації, їх значення зумовлюється тим, що вони доступні і здатні доповнити законодавчі норми там, де це потрібно організації, а особливістю є те, що здебільшого вони передбачають застосування інших видів захисту (технічного, програмного) і тільки в такому разі забезпечують достатньо надійний захист.

Засоби фізичного (технічного) захисту інформації — це різного роду механічні, електро- або електронно-механічні пристрої, а також спорудження і матеріали, призначені для захисту від несанкціонованого доступу і викрадень

інформації та попередження її втрат у результаті порушення роботоздатності компонентів ІС, стихійних лих, саботажу, диверсій і т. ін. [1].

До цієї групи відносять [2]: засоби захисту кабельної системи; засоби захисту системи електроживлення; засоби архівації та дублювання інформації; засоби захисту від відпливу інформації по різних фізичних полях, що виникають під час роботи технічних засобів; засоби виявлення прослуховувальної апаратури; електромагнітне екранування пристроїв або приміщень; активне радіотехнічне маскування з використанням широкосмугових генераторів шумів. Найчастіше технічні засоби захисту реалізуються в поєднанні з програмними.

Програмні засоби захисту забезпечують ідентифікацію та аутентифікацію користувачів, розмежування доступу до ресурсів згідно з повноваженнями користувачів, реєстрацію подій в ІС, криптографічний захист інформації, захист від комп'ютерних вірусів тощо.

Розглядаючи програмні засоби захисту, доцільно спинитись на криптографічному захисту (шифрування) інформації.

Криптографічний захист (шифрування) інформації - це вид захисту, який реалізується за допомогою перетворень інформації з використанням спеціальних (ключових) даних з метою приховування змісту інформації, підтвердження її справжності, цілісності, авторства тощо. На відміну від тайнопису, яке приховує сам факт передавання повідомлення, зашифровані повідомлення передаються відкрито, приховується їхній зміст.

Методи криптографії поділяють на дві групи — підставлення (заміни) і переставлення. Підстановчний метод передбачає, що кожна літера та цифра повідомлення замінюється за певним правилом на інший символ. Зокрема, для визначення порядку підставлення може використовуватись певне слово або фраза — ключ. У загальному випадку у криптографії ключ — це послідовність бітів, що використовуються для шифрування та розшифрування даних [3].

Сьогодні існує достатня кількість криптографічних алгоритмів. Найбільш поширеними з них є стандарт шифрування даних DES, AES та RSA. Ступінь захищеності під час використання цих алгоритмів прямо залежить від довжини ключа, що застосовується.

Криптографічні алгоритми використовуються як для шифрування повідомлень, так і для створення електронних (цифрових) підписів (ЦП) — сукупностей даних, які дають змогу підтвердити цілісність електронного документа та ідентифікувати особу, що його підписала.

XXI століття можна охарактеризувати, як інформаційне століття тому, що саме з початку цього століття почалась здійснюватися інформатизація всіх галузей науки і освіти. Інформатизація суспільства - це глобальний соціальний процес, особливість якого полягає в тому, що домінуючим видом діяльності в сфері суспільного виробництва є збирання, нагромадження, продукування, оброблення, зберігання, передавання та використання інформації. Ці процеси здійснюються на основі сучасних засобів процесорної та обчислювальної техніки, а також на базі різноманітних засобів інформаційного обміну [4].

Взаємодія органів місцевого самоврядування ОТГ з громадськістю відбуваються через інформаційні ресурси, які є важливим інструментом налагодження партнерських стосунків між ними, покращення діяльності самої місцевої влади. Це передбачає не тільки надання, а й обмін інформацією. Для реалізації цього необхідний відповідний рівень інформаційних технологій та забезпечення ними всіх задіяних сторін: як органів місцевої влади, так і широкого кола громадськості.

Виникнення та розвиток інформаційного суспільства припускає широке застосування Smart-технологій в усіх сфера життя, що визначається багатьма чинниками. Smart-технології – засоби, пов'язані зі створенням, збереженням, передачею, обробкою і управлінням інформації. Цей термін включає в себе всі технології, що використовуються для спілкування та роботи з інформацією[5].

Пітер Ферндинанд Друкер – американський вчений австрійського походження; економіст, публіцист, педагог, один з найвпливовіших теоретиків менеджменту XX століття. Саме він в 1954 році ввів абревіатуру SMART. Термін - Smart (англ. Smart) українською перекладають як - розумний або - інтелектуальний. Ці терміни не є тотожними: вони взаємопов‘язані (навіть взаємозумовлені) і певним чином співвідносяться між собою. Також, цікавим, на перший погляд, є тлумачення абревіатури Smart: S - самокерований; M - мотивований; A - адаптивний; R - ресурсозбагачений; T - технологічний [6].

Основою концепції «Розумне місто» (Smart-місто) виступає цілий спектр найрізноманітніших рішень та розробок, які реалізуються за допомогою впровадження різнопланових розумних та сучасних технологій. Це можуть бути як альтернативні підходи до енергозабезпечення та раціональне водокористування, так і можливість переробляти морську солону воду в прісну, використання сучасних розумних систем із сортування та переробки сміття, розміщення в містах широкої мережі відеоспостереження [7].

Згідно концепції, структура «розумного міста» містить такі складові [7]:

− «smart economy» (розумна економіка) – складається з електронного бізнесу та електронної торгівлі, такій економіці характерне: зростання продуктивності, інноваційно-технологічне виробництво товарів та швидка доставка послуг;

− «smart mobility» (розумне переміщення) – являє собою транспортні та логістичні системи, основою для них є інформаційно-комунікаційні технології, які б дозволяли використовувати максимум два види екологічно чистого транспорту для переміщення у будь-яку точку міста;

− «smart people» (розумні люди) – тобто це розвиток електронних навичок населення, підвищення їхнього рівня освіченості, кваліфікації та розвиток креативності;

− «smart living» (розумне життя) – в основі цієї складової лежить цифрова інфраструктура в квартирах, яка дає змогу дистанційно керувати різними

приладами в житлі, отримувати сповіщення про пожежу в вашій квартирі та набагато раціональніше використовувати ресурси (вода, газ, електрика).

− «smart governance» (розумне врядування) – передбачає застосування інформаційних технологій для надання державних послуг населенню і дозволяє оптимізувати роботи різних департаментів.

– «smart environment» (розумне довкілля) – ця складова має тісний зв'язок із енергетикою та енергозбереженням, адже в «розумному довкіллі» увага акцентується на запровадженні принципів енергоефективності, доцільному використанні ресурсів та зменшенні викидів парникових газів за рахунок запровадження замкнутих енергетичних мереж та розумних енергосистем.

Теоретично, будь-яка сфера управління чи то містом, чи громадою може бути включена в ініціативу Smart-технології («розумного міста»/«розумна громада»). На нашу думку, до основних технологій Smart-технології слід віднести наступні технології: автоматизацію, машинне навчання (штучні нейронні мережі) та Інтернет речей.

Автоматизація. Під автоматизацією розглядають організацію і управління процесами без участі людини, за допомогою якого-небудь пристрою і алгоритму. Автоматизація охоплює багато складних процесів, тому окремі вирішення завдань засобами автоматизації – інформаційні системи, зокрема такими, як [8]: автоматизована система управління; інформаційно-аналітична система; система підтримки прийняття рішень; експертна система; вимірювальна інформаційна система. Задля автоматизації процесу використовують такі засоби, як: ANN – штучна нейронна мережа, DCS – розподілена система керування, HMI – Human Machine Interface, SCADA – диспетчерське керування та збір даних, PLC – програмований логічний контролер, вимірювальні прилади, робототехніка.

Машинне навчання. Іншою складовою «розумної громади» є машинне навчання, яке прискорює роботу бізнесу, робить її ефективнішою, потужнішою, виводить на новий рівень. Із цим інструментом менеджери можуть вирішувати

надскладні проблеми, які вимагають нетрадиційних підходів до їх вирішення. Машинне навчання на основі штучних нейронних мереж допомагає автоматизувати системні операції, стежити за ефективністю міста (підприємства) і швидше виявляти проблеми та надзвичайні ситуації[8].

Інтернет речей. Найбільш важливою та значущою технологією «розумної громади» є саме інтернет речей, адже він складається з усіх підключених до інтернету пристроїв, які збирають інформацію та обмінюються нею. Завдяки процесорам і бездротовим мережам в IoT можна перетворити, що завгодно — від автомобіля, який сповіщає водія про низький тиск у шинах, до свійських тварин з біочіпом. Головне завдання цієї технології — підвищити комфорт життя населення і полегшити прийняття правильних рішень управлінцями. Маючи на меті збір та аналіз інформації, розумні пристрої, які є складовою інтернет речей, використовують вбудовані процесори, давачі та комунікаційне обладнання. IoT-пристрої виконують надсилання даних використовуючи хмарне сховище або обмінюються ними напряму [8].

Отже, зміст Smart-технологій можна визначити як сукупність різноманітних технологічних інструментів і ресурсів, які використовуються для забезпечення процесу комунікації та створення, поширення, збереження та управління інформацією. Використовуючи Smart-технологій спроможні територіальні громади мають стати такими собі компактними територіями, з доступними для всіх мешканців можливостями участі у самоврядуванні, отримання послуг та сервісів у режимі он-лайн.

РОЗДІЛ 2
ЗАГАЛЬНА ХАРАКТЕРИСТИКА ІНФРАСТРУКТУРИ ІНФОРМАТИЗАЦІЇ СОФІЇВСЬКОЇ ОТГ ТА ОСОБЛИВОСТІ ЗАХИСТУ ІНФОРМАЦІ В ГРОМАДАХ

Слобожанська селищна об'єднана територіальна громада – конкурентоспроможна, фінансово незалежна громада з розвинутою промисловою зоною, сучасними логістичними центрами, з інвестиційними можливостями, що ефективно використовує природні ресурси для розвитку фермерства та агропромислового комплексу. Вона ініціативна, активна громада, яка забезпечує власний розвиток та місцеве самоврядування, це сучасні дошкільні заклади і школи з використанням інноваційних освітніх технологій, що сприяють культурному розвитку особистості, служать людям духовним центром.

Громада довгий час знаходилась в інформаційному вакуумі: там була лише одна районна газета і та мала попит тільки серед старшого покоління. Не було інформаційних майданчиків, через які можна було б інформувати всіх мешканців громади — студентів, учнів, підприємців.

Аналіз стану інформатизації громади характеризується наступними показниками наведеними на рисунку 2.1 [9].

У громаді громадяни у віці понад 15 років користуються Інтернетом через персональні комп’ютери та мобільні телефони. Користувачі мобільних телефонів саме завдяки впроваджуваній в Україні технології передачі даних 3G є активними абонентами Інтернету.

На основі проведеного SWOT-аналізу інформатизації Софіївської ОТГ(табл..2.1), було виокремлено її сильні та слабкі сторони.

Дослідивши слабкі сторони та загрози, нами виділено основні проблеми інформатизації Софіївська ОТГ, що потребують вирішення:

- недостатня забезпеченість сучасною комп’ютерною технікою відділів виконавчого комітету селищної ради та установ;

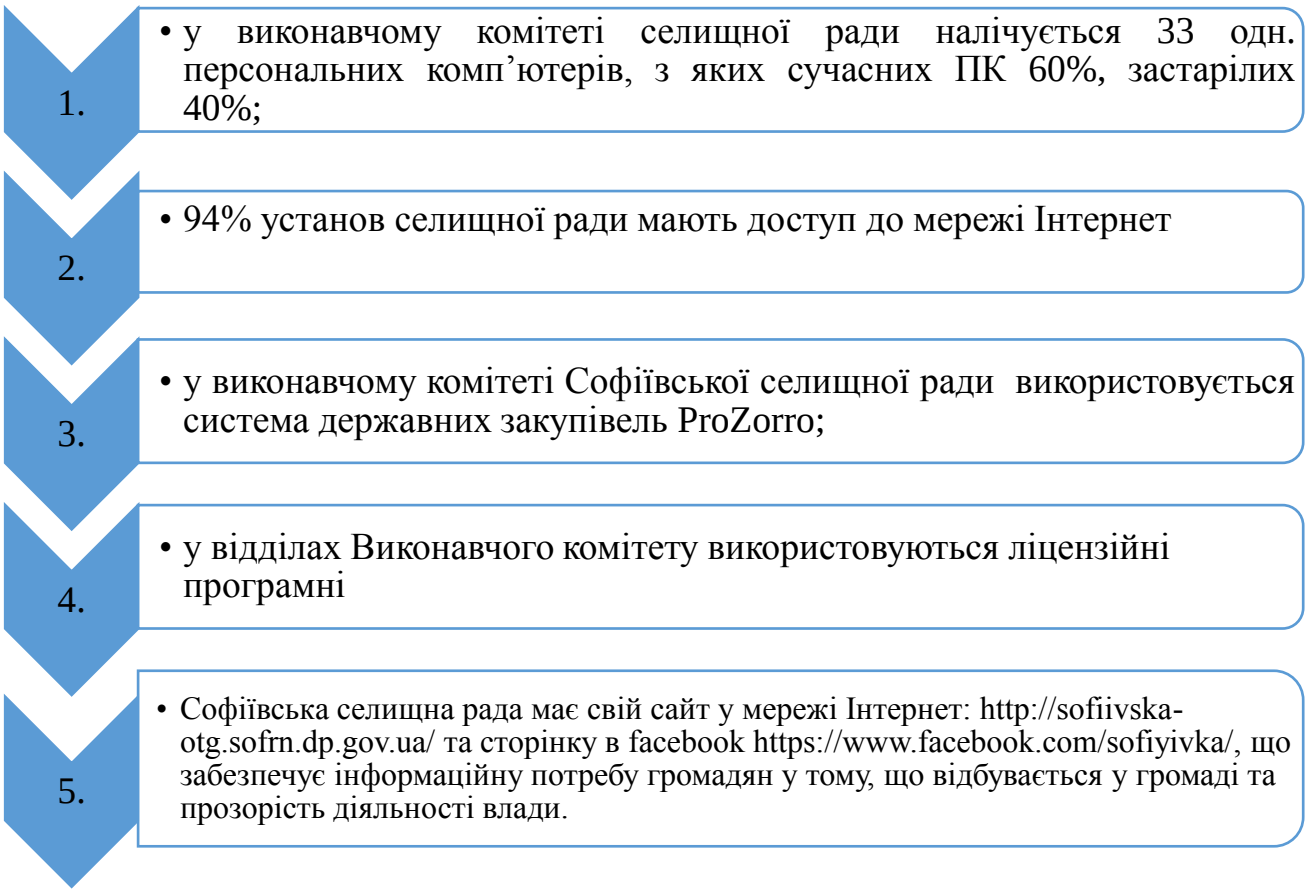

Рисунок 2.1 Стан інформатизації Софіївської об'єднаної територіальної громади [9].

- низький рівень ліцензійного програмного забезпечення у відділах виконавчого комітету Софіївської селищної ради;

- недостатня компетентність службовців та посадових осіб з питань електронного врядування та інформаційних технологій: володіння інформаційно-комп'ютерними технологіями, використання технологій е-урядування та е-демократії; - недостатня кількість зон безкоштовного доступу до wi-fi громадян; - низький рівень доступу громадян у сільських місцевостях до електронної інформації про діяльність громади.

Але поряд з тим Софіївська ОТГ намагається активно розвивається в ІТ сфері. Протягом останніх років в громаду зайшли декілька нових провайдерів, які постійно збільшують зону покриття громади високошвидкісним оптоволоконним Інтернетом.

Таблиця 2.2 SWOT-аналізу інформатизації Софіївської ОТГ

Сильні сторони	Можливості
✓ Відділ економічного розвитку, інвестицій та комунікаційних технологій ✓ Наявність та конкуренція провайдерів ✓ Зона покриття Інтернет (оптоволоконний, 3G, 4G) ✓ Сайт громади з електронними сервісами ✓ Всі працівники апарату забезпечені сучасними ПК ✓ Гнучкий бюджет ✓ Соціальні мережі ✓ Комунікаційна стратегія	✓ Розширення зони покриття оптоволоконного Інтернету ✓ Розширення зони покриття мобільного інтернету ✓ Автоматизація діяльності ЦНАП ✓ Автоматизація діяльності апарату (електронний документообіг) ✓ Донорські програми
Слабкі сторони	**Загрози**
✓ Брак ресурсів (фінансування, кваліфіковані кадри) ✓ Нерозуміння важливості впровадження ІТ технологій у різних сферах ✓ Непридатна для використання система електронного документообігу ✓ Не впроваджена процедура бекапу	✓ Примусове доєднання територій (додаткові видатки)

Мобільні оператори покривають більшість території громади, в центрі громади запущено 4G. В громаді активно використовується сайт громади та соціальні мережі у сфері інформування та взаємодії між мешканцями та органами місцевого самоврядування В громаді працюють декілька приватних підприємців у сфері продажу та обслуговування ПК та оргтехніки [9].

Веб-сайт є офіційним джерелом інформації, що забезпечує висвітлення діяльності територіальної громади чи ОТГ: її органів, виконавчого комітету, постійних комісій, депутатських груп, депутатів ради, інформаційної взаємодії з громадськістю, надання інформаційних та інших послуг громадськості, взаємний обмін інформацією з іншими громадськими організаціями, органами державної влади та органами місцевого самоврядування, підприємствами, установами, організаціями з питань, пов’язаних з діяльністю громади, з метою забезпечення

впливу громадськості на процеси, що відбуваються у державі та на території громади.

Поряд з цим, в Софіївській ОТГ розпочато ведення електронного документообігу. Якщо в режимі офлайн для них потрібні стіл або шафа, теки та файли, то для онлайну є інші поради. Аби база документів не нагадувала захаращений балкон, тримайте їх гарно структурованими. Як саме — розглянемо на прикладі сайту Софіївської ОТГ (рис. 2.2).

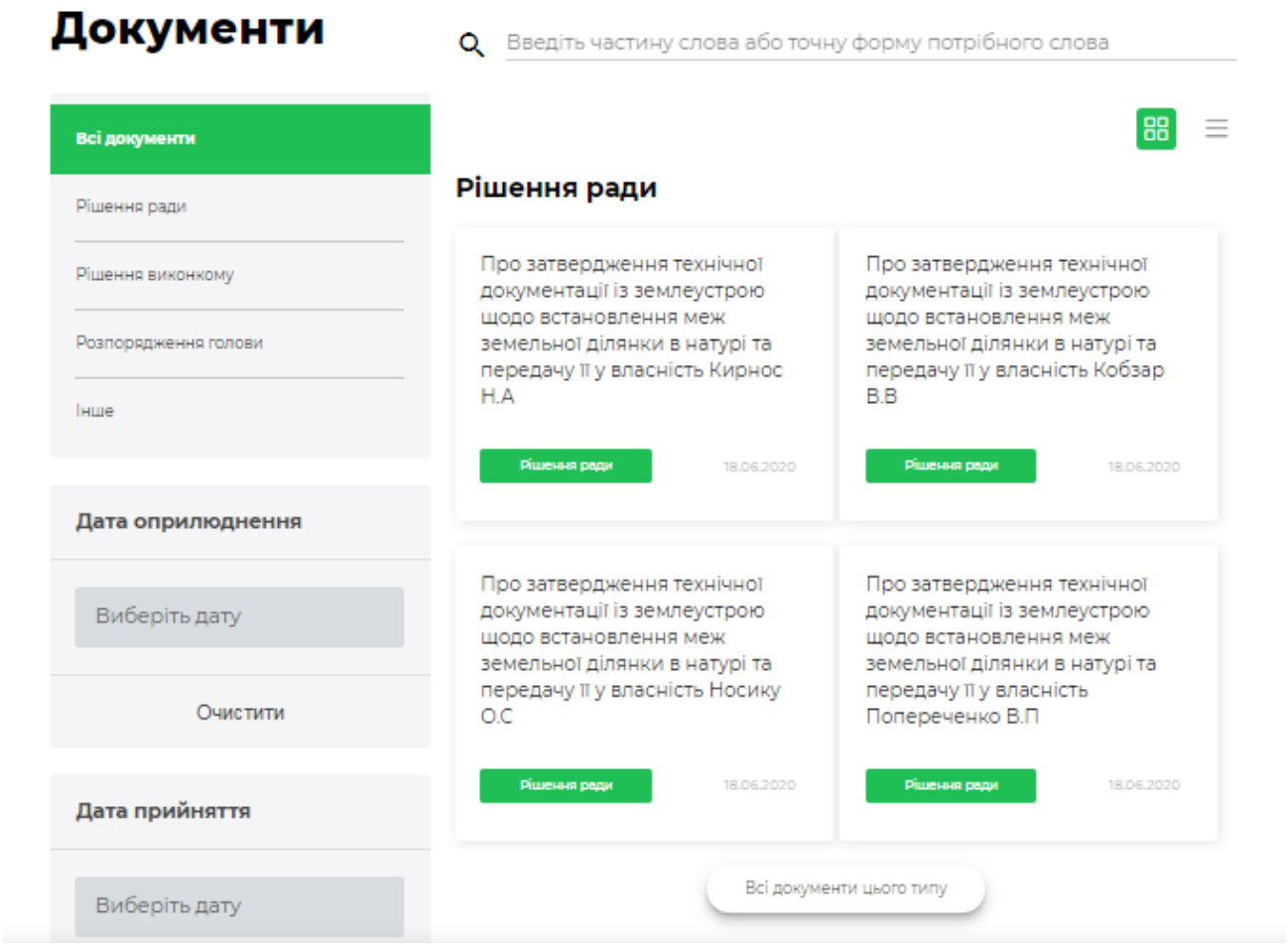

Рисунок 2.2 Скрін сайту електронних документів Софіївської ОТГ [9].

Як бачимо, усі документи на сайті громади гарно структуровані, об’єднані різними фільтрами. Тут можна знайти відповідне рішення Голови, розпорядження, підсумки конкретної сесії за датами тощо. Також працюють кольорові теги:

рішення ради вказані зеленим, протоколи чорним, розпорядження голови — червоним.

Для роботи журналістів та населення громади, громадських організацій та фахових активістів в Софіївській ОТГ налагоджений інформаційний доступ. Завдяки повній базі документів спеціалісти зможуть прослідкувати профільні питання — наприклад, розібратися, кому в оренду здано приміщення, або що вирішили стосовно бюджетних питань на сесії. І мова тут не лише про зручний пошук серед документів чи простий доступ до рішень. Такий підхід ще раз підкреслить відкритість Софіївській ОТГ, її прозорість та готовність до співпраці.

Зауважимо, що порушенням інформаційної безпеки можна вважати і дії, які не призводять безпосередньо до втрати або відпливу інформації, але передбачають втручання в роботу системи органів самоврядування об'єднаних територіальних громад. Загалом найбільшу загрозу безпеці інформації становлять люди, тому саме їхні навмисні чи випадкові дії потрібно передбачати, організовуючи систему захисту.

Використовуючи Інтернет та соціальні мережі огранам самоврядування ОТГ, зокрема Софіївській, не варто забувати, про те, що платою за їх користування є загальне зниження інформаційної безпеки. Кожна громада, що має справу з якими би то не було цінностями, рано чи пізно зіштовхується з зазіханням на них. В цьому випадку безпека даних є однієї з головних проблем у Internet. Усе це справедливо й у відношенні інформації.

Запровадження е-врудування та автоматизація докментообігу в ОТГ додала головного болю службам безпеки, а нові тенденції розвитку ОТГ, цілком засновані на інформаційних технологіях, збільшують проблему. Зловмисники постійно маскують так званих хробаків в інших програмах, які ми, нічого не підозрюючи, встановлюємо у своїх комп'ютерах, що призводить до загрози цілісності інформації — її викрадення, знищення чи модифікації. Такий метод єодним із найпопулярніших, адже використовує не тільки вразливості систем безпеки, але й

психологічні особливості користувача, його бажання до здійснення безкоштовного завантаження медіа-файлів (музика, відео, програмне забезпечення тощо) та простої цікавості

Причини витоку інформації в Софіївській ОТГ пов'язані, як правило, з недосконалістю керівних документів щодо збереження інформації, а також їх порушенням, у тому числі відступом від правил поводження з грифованими документами, технічними засобами, зразками продукції та носіями, що містять інформацію службового характеру. До таких факторів та порушень можна віднести:

- недостатнє знання користувачами основ захисту інформації й нерозуміння необхідності їх ретельного дотримання;
- використання неатестованих або несертифікованих технічних засобів обробки грифованої інформації, тому що це обладнання, у кращому випадку, просто може бути недоопрацьованим, а в гіршому — воно може містити закладки на фізичному або програмному рівнях;
- слабкий контроль за дотриманням правил захисту інформації з боку штатних або позаштатних служб захисту інформації та кібернетичної безпеки й інженерно-технічних підрозділів, які неналежним чином стежать за справністю обладнання або ліній;
- плинність кадрів, оскільки вони володіють інформацією з обмеженим доступом або даними службового характеру.

Усі ці фактори завдають набагато більше шкоди, ніж ціла група зловмисників. Адже своїми діями безвідповідальні особи можуть створити загрозу витоку інформації, функціонуванню системи, аж до припинення її роботи.

Захист інформації в ОТГ тією чи іншою мірою має забезпечуватися будь-якою системою обміну даними. При цьому впорядкування та консолідація інформації, впорядкування документообігу дає можливість створити більш якісну систему захисту.

На сьогодні основним і практично єдиним із запропонованих на ринку рішенням для забезпечення достовірності відправника документа є електронно-цифровий підпис (ЕЦП). Основний принцип роботи ЕЦП заснований на використанні стандартів шифрування за допомогою відкритого ключа. Голова Софіївської ОТГ Лозовий Сергій Іванович має в своєму розпорядженні електронно-цифровий підпис (ЕЦП). Слід зауважити, що ключі для шифрування і розшифрування даних різні. Є закритий ключ, який дозволяє шифрувати інформацію, він зберігається тільки у власника, а є відкритий ключ, за допомогою якого можна перевірити справжність підпису, отриманого листа, він може поширюватися публічно[9] .

Безперечно, не слід замовчувати про збої, помилки в системі чи аномальні дії робочого комп’ютера. Потрібно негайно повідомити про це відповідних осіб, адже в кожному, без винятку, підрозділі є службова особа, відповідальна за захист інформації. Решту заходів безпеки для складних систем мають забезпечувати фахівці з відповідними знаннями. Усі ми повинні завжди пам’ятати про цілісність нашої держави і дбати про її безпеку і процвітання.

Отже, захист інформації в громадах, зокрема в Софіївській ОТГ ускладнюється двома факторами: по-перше, майже всі цінності, з якими має справу громада (крім готівки і ще дечого), існують лише у виді тієї чи іншої інформації. По-друге, громада не може існувати без зв'язків із зовнішнім світом. При цьому по зовнішніх зв'язках обов'язково передається та сама інформація, що виражає собою цінності, з якими працює громада (або зведення про ці цінності і їхній рух, що іноді коштують дорожче самих цінностей).

РОЗДІЛ 3
ЗАПРОВАДЖЕННЯ АЛГОРИТМУ ШИФРУВАННЯ AES В СЕНСОРНИХ МЕРЕЖАХ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ В ОТГ

Обробка інформації в ОТГ повинна здійснюється лише на об'єкті електронно-обчислювальної техніки не нижче четвертої категорії на автоматизованих системах (далі - АС) із встановленим засобом шифрування та застосуванням комплексної системи захисту інформації (далі - КСЗІ) з підтвердженою відповідністю.

Обмін інформацією між уповноваженими органами ОТГ здійснюється у зашифрованому вигляді у форматі криптографічного повідомлення, визначеного законодавством України у сфері захисту інформації, через систему взаємодії.

Короткі відомості про алгоритм шифрування AES. Алгоритм шифрування AES представляє собою симетричний блоковий шифр, метою якого є шифрування та дешифрування даних. Під час шифрування дані перетворюються в блоки розміром 128 біт зашифровані ключем, який має довжину 128, 192 або 256 біт.

Основні принципи алгоритму: загальне число бітів ключів в раундах дорівнює довжині блока, помноженій на число раундів, плюс один; ключ шифрування перетворюється в розширений ключ; раундові ключі генеруються з розширеного ключа так: перший ключ раунду містить перші X слів, другий – наступні X слів і т. д.

Алгоритм AES – це блок даних у вигляді двовимірного масиву розміром 4x4. Всі операції проводяться над окремими байтами з масиву та над незалежними стовпцями і рядками масиву протягом кількох раундів. В кожному раунді алгоритму виконуються такі перетворення [10]:

- Операція subBytes() обробляє кожен байт масиву, проводячи нелінійну заміну байтів використовуючи таблицю замін. Така операція забезпечує нелінійність алгоритму шифрування.

- Операція ShiftRows виконує зміщення в ліво в циклі всіх рядків масиву даних, окрім нульового. Таким чином кожна колонка вихідного стану після застосування процедури ShiftRows складається з байтів з кожної колонки початкового стану.
- Операція MixColumns виконує множення кожного стовпця на многочлен $c(x) = 3x^3 + x^2 + x + 2$. Множення виконується по модулю $x^4 + 1$.
- Операція AddRoundKey додає елементи змінної RoundKey та елементи таблиці замін. Тобто і-ий стовпець даних додається до 4-байтового фрагменту розширеного ключа $W[4r + 1]$, де r – номер поточного раунду алгоритма.

Під час шифрування алгоритмом AES перше додавання ключа раунду виконується до першого виконання операції subBytes(). Кількість раундів алгоритму залежить від розміру ключа наступним чином: для 128-бітного ключа необхідно 10 раундів алгоритму, для 192-бітного ключа – 12 раундів, для 256-бітного ключа – 14 раундів. Схема функції шифрування наведена на рис. 3.1.

Алгоритм AES дуже ефективний та стійкий проти таких видів криптоаналітичних атак: диференціальний криптоаналіз; лінійний криптоаналіз; криптоаналіз на основі пов’язаних ключів.

Для повного перебирання ключів трьох варіантів алгоритму AES необхідно виконати $2^{127}, 2^{191}, 2^{255}$ операцій відповідно, що і зумовило використання цього алгоритму в сучасному програмному забезпеченні [11]. Наприклад, алгоритм AES зараз часто використовується в багатьох віртуальних приватних мережах (VPN), розробленими компаніями Checkpoint, Cisco і Symantec.

Іншими напрямами використання алгоритму AES є безпека мережевих пристроїв (безпека телефонних розмов, безпека мереж Wi-Fi, безпека камер відеоспостереження), безпека управління технологічними процесами систем (SCADA), шифрування файлів під час їх стиснення в різних програмах. В

бездротових сенсорних мережах Bluetooth та Wi-Fi алгоритм шифрування AES використовується для двосторонньої автентифікації пристроїв.

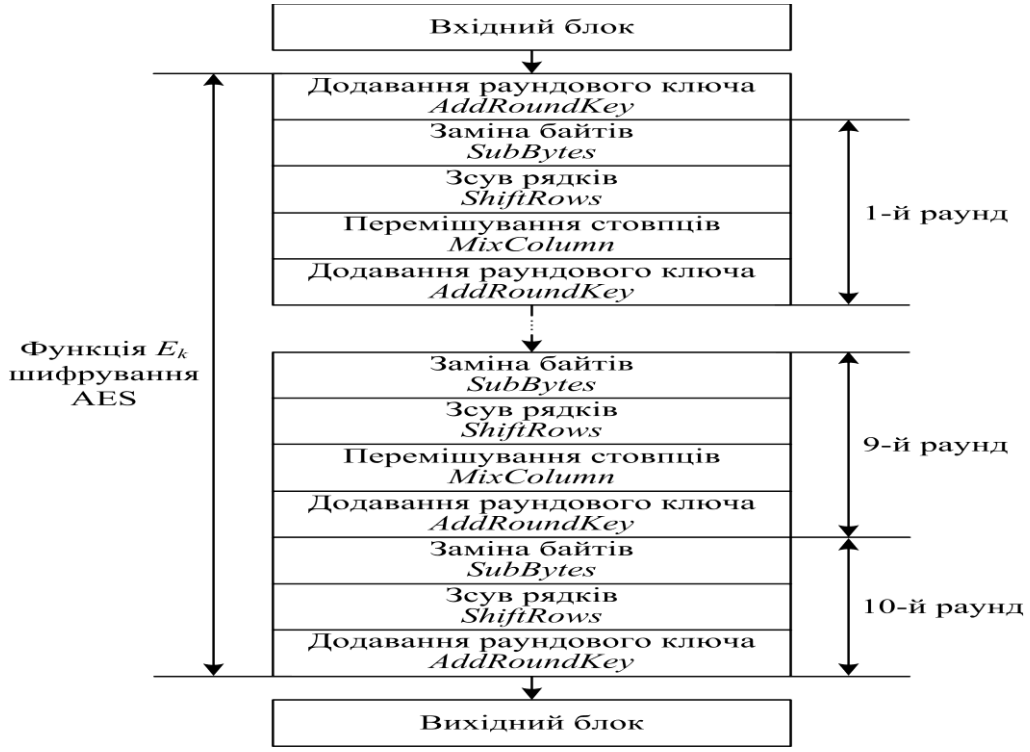

Рис.3.1. Схема функції шифрування алгоритму AES

Доцільність використання алгоритму шифрування AES в сенсорних мережах для захисту інформації в ОТГ. З точки зору економії ресурсів алгоритм шифрування AES є найефективнішим, що робить його найкращим алгоритмом шифрування для бездротових сенсорних мереж. Важливим також є збереження цілісності даних таким чином, щоб інформація, яка передається між вузлами бездротової сенсорної мережі, використовуваної в ОТГ, не піддавалась модифікації або підміні.

З кожним днем в світі зростає обсяг інформації, що передається, ускладняється будова та структура сенсорних мереж, розширюються кількість користувачів, що мають доступ до сенсорних мереж. Тому і виникає необхідність використання надійних алгоритмів шифрування даних з метою конфіденційності та цілісності інформації в ОТГ.

Популярність алгоритму шифрування AES зумовлено його перевагами та особливостями, що характеризуються продуктивністю, стійкістю та ефективністю реалізації, зокрема на рівні шифрування даних в бездротових сенсорних мережах.

До основних переваг алгоритму шифрування AES відносять [10]: відносно висока пропускна здатність, ключі для шифрів відносно короткі, можливість використання алгоритму як основу для побудови різних криптографічних, висока швидкість шифрування, висока стійкість шифрування, мінімальні вимоги до обчислювальних ресурсів. Вибір мови програмування. Розробка та реалізація алгоритмічно-програмного забезпечення криптографічного захисту інформації в сенсорних мережах для захисту інформації в ОТГ відповідно до алгоритму блокового шифрування даних AES та мови програмування C# проводилась за алгоритмом шифрування зображеним на рис.3.2 в додатку А.

Для програмної реалізації шифрування даних алгоритмом AES в сенсорних мережах було обрано мову C#, адже вона має такі особливості: об'єктно-орієнтована мова програмування з безпечною системою типізації, підтримує поліморфізм, перевантаження операторів, вказівники на функції-члени класів виключає деякі моделі, що зарекомендували себе як проблематичні при розробці програмних систем, висока ефективність виконавчого коду [12].

Програма для шифрування даних алгоритмом AES. Результат роботи програми для шифрування даних алгоритмом шифрування AES представлено на рис. 3.3. Програмний код наведено у додатку Б.

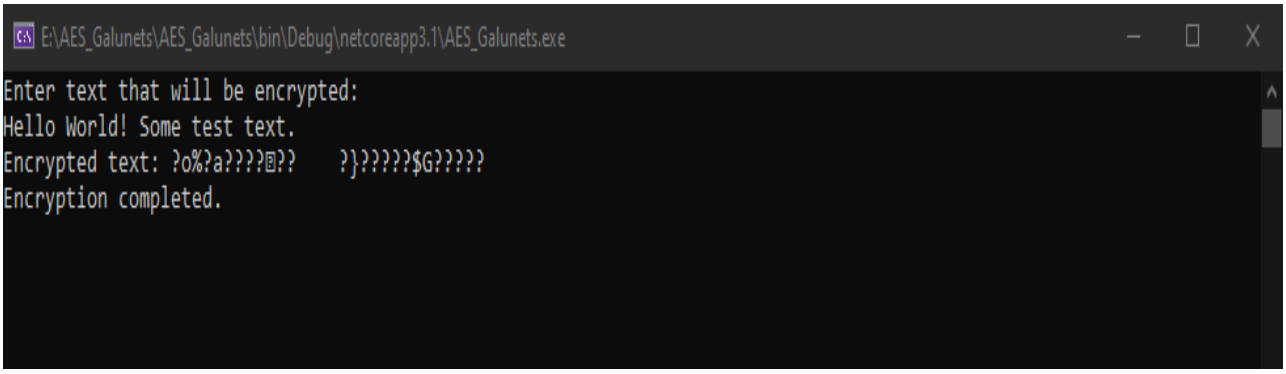

Рис.3.3. Результати роботи програми для шифрування даних

ВИСНОВКИ

У науковій роботі на підставі проведених теоретичних та емпіричних досліджень розроблено наукові засади і практичні рекомендації щодо запровадження алгоритму шифрування AES в сенсорних мережах для захисту інформації в ОТГ. За результатами дослідження зроблено висновки і пропозиції, які відображають вирішення задач відповідно до поставленої мети:

1. Встановлено, що захист інформації — це сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією. Базовими принципами інформаційної безпеки є забезпечення цілісності інформації, її конфіденційності і водночас доступності для всіх авторизованих користувачів. Залежно від можливих порушень у роботі системи та загроз несанкціонованого доступу до інформації численні види захисту можна об'єднати у такі групи: моральноетичні, правові, адміністративні (організаційні), технічні (фізичні), програмні. Зазначено, що такий поділ є досить умовним.

2. Smart-технологій можна визначити як сукупність різноманітних технологічних інструментів і ресурсів, які використовуються для забезпечення процесу комунікації та створення, поширення, збереження та управління інформацією. Наразі Smart-технології включають апаратні засоби (комп'ютери, сервери, тощо) та програмне забезпечення (операційні системи, мережеві протоколи, пошукові системи, тощо). Розглянуто інформаційну модель «розумного міста» у контексті складові – технології, яка є підґрунтям вибору засобів забезпечення безпеки адекватно до складової: криптографічного захисту інформації в сенсорних мережах інтернету речей.

3. В процесі аналізу стану інфраструктури інформатизації Софіївської ОТГ, було встановлено, що в громаді громадяни у віці понад 15 років користуються Інтернетом через персональні комп’ютери та мобільні телефони. Користувачі мобільних телефонів саме завдяки впроваджуваній в Україні технології передачі

даних 3G є активними абонентами Інтернету. Мобільні оператори покривають більшість території громади, в центрі громади запущено 4G. В громаді активно використовується сайт громади та соціальні мережі у сфері інформування та взаємодії між мешканцями та органами місцевого самоврядування В громаді працюють декілька приватних підприємців у сфері продажу та обслуговування ПК та оргтехніки. Було здійснено SWOT-аналізу інформатизації Софіївської ОТГ.

4. Розроблено алгоритмічно-програмне забезпечення криптографічного захисту інформації в сенсорних мережах відповідно до алгоритму блокового шифрування даних AES та мови програмування C#, що забезпечує захищений обмін інформацією за профілями конфіденційності та цілісності в Софіївській ОТГ. Обґрунтовано доцільність використання алгоритму шифрування AES в сенсорних мережах для захисту інформації в ОТГ. Зокрема, з точки зору економії ресурсів алгоритм шифрування AES є найефективнішим, що робить його найкращим алгоритмом шифрування для бездротових сенсорних мереж.

Список використаної літератури

1. Definition internet of things (IoT) [Електронний ресурс]. URL: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT (дата звернення: 13.01.2020)

2. Дудикевич В.Б. Елементи безпеки Інтернету речей / В.Б. Дудикевич, Г.В. Микитин, М.О. Галунець // Матеріали VI-ої Міжнародної науково-технічної Internet конференції "Сучасні методи, інформаційне, програмне та технічне забезпечення систем управління організаційно-технічними та технологічними комплексами" . – Київ: НУХТ, листопад 2019 р. – С.117-118 – Режим доступу:https://drive.google.com/file/d/1x8T9WLyke0v6jdvGmspVjSlGC0gyAsJe/view (дата звернення: 13.01.2020)

3. Виявлення та розслідування злочинів, що вичиняються у сфері інформаційних технологій: Наук.-практ.посіб./ За заг.ред.проф. Я.Ю.Кондратьєва. – К., 2004.

4. Кунанець Н. Досвід реалізації проектів класу «розумне місто» на основі інформаційних і телекомунікаційних технологій / Н. Кунанець, В. Пасічник, Г. Химич // Вісник ЛДУ БЖД. – 2016. – № 14. – С. 17–37.

5. Антоненко В. М. Сучасні інформаційні системи і технології. Навчальний посібник / В. М. Антоненко, Ю. В. Ратушна. – К.: КСУМГІ. – 2015. – 131 с.

6. Друкер П. Практика менеджмента / П. Друкер. – М. : Вильямс, 2007. – 400 с.

7. Creating the smart cities of the future : smart cities development gather pace around the world : [Електронний ресурс]. URL : https://www.pwc.com/us/en/industries/capital-projectsinfrastructure/library/future-smart-cities.html (дата звернення: 14.01.2020)

8. Інтернет речей: що це та як його використовують розумні міста. [Електронний ресурс] – URL: https://www.kyivsmartcity.com/news/internet-rechej-rozumni-mista/ (дата звернення: 14.01.2020)

9. Офіційний сайт Софіївської об’єднаної територіальної громади, Новобузького району, Миколаївської області https://sfotg.gov.ua/

10. Довідка щодо стандарту розширеного шифрування (AES). [Електронний ресурс] – URL: https://uk.wizcase.com/blog/ (дата звернення: 25.01.2020)

11. AES-шифрування. [Електронний ресурс] – URL: https://memory.net.ua/blog/aes-shifruvannja.html (дата звернення: 23.01.2020)

12. Лабор В. В. Си Шарп: Создание приложений для Windows // В. В. Лабор. Мн.: Харвест, 2003. - 384 с.

ДОДАТКИ

Додаток А

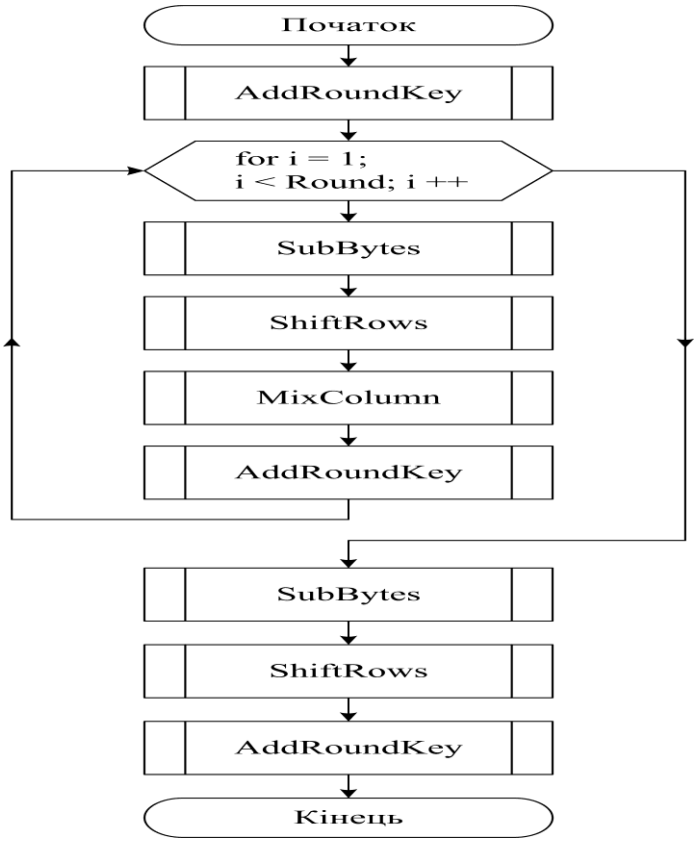

Рис.3.2. Блок-схема програмного забезпечення відповідно до алгоритму AES

Додаток Б

Програмний код програми криптографічного захисту даних відповідно до алгоритму блокового шифрування даних AES та мови програмування C#

```
using System;
using System.IO;
using System.Security.Cryptography;
class ManagedAesSample
{
   public static void Main()
   {
      Console.WriteLine("Enter text that will be encrypted:");
      string data = Console.ReadLine();
      EncryptAesManaged(data);
      Console.WriteLine("Encryption completed.");
      Console.ReadLine();
   }
   static void EncryptAesManaged(string raw)
   {
      try
      {
         using (AesManaged aes = new AesManaged())
         {
            byte[] encrypted = Encrypt(raw, aes.Key, aes.IV);
            Console.WriteLine($"Encrypted                                    text:
{System.Text.Encoding.UTF8.GetString(encrypted)}");
         }
      }
```

```
        catch (Exception exp)
        {
            Console.WriteLine(exp.Message);
        }
        Console.ReadKey();
    }
    static byte[] Encrypt(string plainText, byte[] Key, byte[] IV)
    {
        byte[] encrypted;
        using (AesManaged aes = new AesManaged())
        {
            ICryptoTransform encryptor = aes.CreateEncryptor(Key, IV);
            using (MemoryStream ms = new MemoryStream())
            {
                using (CryptoStream cs = new CryptoStream(ms, encryptor,
CryptoStreamMode.Write))
                {
                    using (StreamWriter sw = new StreamWriter(cs))
                        sw.Write(plainText);
                    encrypted = ms.ToArray();
                }
            }
        }

        return encrypted;
    }
}
```