МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Сумський державний університет

Факультет електроніки та інформаційних технологій

Кафедра електроніки і комп'ютерної техніки

«До захисту допущено»

Завідувач кафедри ЕКТ

_____ Анатолій ОПАНАСЮК

(підпис) (Ім’я та ПРІЗВИЩЕ)

____ _____ 2024 р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня «магістр»

зі спеціальності 171 «Електроніка»

освітньо-професійної програми «Електронні системи»

на тему:

ЕЛЕКТРОННА СИСТЕМА ШИФРУВАННЯ ДАНИХ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ ЕЛЕКТРОЕНЕРГЕТИКИ.

Здобувача групи ЕС.м-31 _____ Орлова Владислава Віталійовича

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

_____ Орлов Владислав

(підпис) (Ім’я та ПРІЗВИЩЕ)

Керівник від університету,
доцент, доцент, к.т.н., Ольга БЕРЕЖНА _____

(підпис)

Керівник від підприємства, Директор
ТОВ «ЕСП «Преобразователь», Володимир АРБУЗОВ _____

(підпис)

Консультант з техніко-економічної частини,
доцент, к.е.н., доцент Олександр МАЦЕНКО _____

(підпис)

Суми – 2024

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Факультет електроніки та інформаційних технологій

Кафедра електроніки і комп'ютерної техніки

Напрям підготовки 171 «Електроніка»

Освітня програма Електронні системи

ЗАТВЕРДЖУЮ

Зав. кафедрою Опанасюк А. С.

«___»_____ 2024 р.

З А В Д А Н Н Я

на кваліфікаційну роботу магістра

Орлова Владислава Віталійовича

1.Тема роботи Електронна система шифрування даних в інфокомунікаційних мережах електроенергетики

затверджена наказом по університету «01» жовтня 2024 р. № 1003-VI.

2. Термін здачі студентом завершеної роботи 10.12.24

3. Вихідні дані до роботи: Розробити електронну система шифрування даних в інфокомунікаційних мережах електроенергетики

4. Зміст розрахунково-пояснювальної записки (перелік питань, що належить розробити) 1) Огляд літератури та поставлення задачі роботи. 2) Науково-дослідна частина. 3) Розробка електронної системи з використанням отриманих результатів дослідження. 4) Техніко-економічна частина.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) 1) Схема електрична структурна. 2) Схема алгоритму. 3) Схема електрична функціональна. 4) Схема електрична принципова.

6. Консультанти з кваліфікаційної роботи

Розділи	Консультанти	Завдання видав	Завдання прийняв
Техніко-економічна частина	Арбузов В.В.		

7 Дата видачі завдання 01.11.2024

8 Керівник від університету _____ Кулик І.А.

9 Керівник від підприємства _____ Арбузов В.В.

10 Завдання прийняв до виконання Орлов В.В.

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапів дипломного проекту	Термін виконання етапів роботи	Примітки
1	Огляд літератури та постановка завдання проектування	04.11.24 – 09.11.24	
2	Науково-дослідна частина	10.11.24 – 15.11.24	
3	Розробка алгоритму функціонування та структурної схеми електронної системи	16.11.24 – 20.11.24	
4	Розробка функціональної схеми електронної системи	21.11.24 – 24.12.24	
5	Розробка схеми електричної принципової електронної системи	25.12.24 – 02.12.24	
6	Техніко-економічна частина	03.12.24 – 05.12.24	
8	Оформлення пояснювальної записки	06.12.24 – 08.12.24	
9	Оформлення графічного матеріалу	09.12.24 – 13.12.24	
10	Представлення роботи керівнику і отримання відгуку	14.12.24	
11	Представлення роботи кафедрі для отримання рецензії	15.12.24	

Керівник кваліфікаційної роботи від університету: Бережна.О.В.

Керівник кваліфікаційної роботи від підприємства: Арбузов В.В.

Студент: Орлов В.В.

"_____"_____ 2024 р

РЕФЕРАТ

Записка: (88) сторінок, (19) рисунків, (24) таблиць, (17) джерел.

Тема роботи: «Електронна система шифрування даних в інфокомунікаційних мережах електроенергетики»

Об'єктом розробки є електронний лічильник на системі на кристалі, для збору, шифрування та відправлення метрологічних данних.

Мета роботи – розробити електронну система шифрування даних в інфокомунікаційних мережах електроенергетики

Пояснювальна записка складається з п’яти розділів, вступу, висновків та додатків, що включають технічну документацію та результати моделювання.

У першому розділі проведено огляд сучасних метрологічно атестованих автоматизованих систем збору, обробки та збереження інформації, способів, приборів збору данних (лічильників) та системи й протоколи передачц даних та зв’язку.

У другому розділі представлено результати науково-дослідної частини, що включає вивчення способу криптографічного перетворення, та способій й протоколів захищеної передани інформації

У третьому розділі розроблено алгоритм функціонування системи та структурну схему блоку шифрування даних в лічильнику.

У четвертому розділі розроблено принципову схему системи, де детально описано призначення основних блоків.

У п’ятому розділі зробили відповідні розрахунки щодовитрат для створення, перевірки та монтажурозглядаємого пристрою.

Ключові слова: АСКОЕ, АСТУЕ, АСОДУ, електронний лічильник, IP-адреси, GSM модеми, GPRS модеми, VPN, VPN-тунелі, протокол IPsec, гамування, система на кристалі, структурна схема, принципова схема

ЗМІСТ

ВСТУП 5
1. ОГЛЯД ЛІТЕРАТУРИ 6
1.1 Автоматизована система комерційного обліку електричної енергії (АСКОЕ) 6
1.2 Автоматизована система технічного обліку електроенергії (АСТУЕ) 6
1.3 Автоматизована система оперативно-диспетчерського управління (АСОДУ) 6
1.4 Алгоритми управління об'єктами АСОДУ 7
1.5 Електронний лічильник 7
1.6 Статичні публічні "білі" IP-адреси 8
1.7 GSM, GPRS модеми 10
1.8 VPN. Принцип роботи 12
1.9 VPN та IP-тунелі 15
2. НАУКОВО-ДОСЛІДНА ЧАСТИНА 21
2.1 Відомості про принцип криптографічного шифрування 21
2.2 Протокол IPsec22 22
2.3 Віртуальна приватна мережа (VPN) 25
2.4 Інкапсуляція корисного навантаження безпеки (ESP) 27
2.5 Огляд IKE 30
2.6 VPN на основі маршрутизації та VPN на основі політик 32
2.7 Налаштування брандмауера 33
3. РОЗРОБЛЕННЯ АЛГОРИТМУ РОБОТИ І СТРУКТУРНОЇ СХЕМИ СИСТЕМИ 35
3.1 Алгоритм шифрування даних 35
3.2 Режим простої заміни 37
3.3 Режим гамування 37
3.4 Режим гамування зі зворотним зв'язком 38
3.5 Режим генерації імітоприставки 39
4. **РОЗРОБКА СХЕМИ ЕЛЕКТРИЧНОЇ ПРИНЦИПОВОЇ ЛІЧИЛЬНИКА ЕЛЕКТРОЕНЕРГІЇ** 43
4.1 Система на кристалі - System-on-a-Chip 43
4.2 Системи на кристалі компанії Maxim для лічильників електроенергії і систем моніторингу 44
4.3 Огляд архітектури IC для лічильників електроенергії 45
4.4 Порівняльні характеристики IC першого-третього поколінь для лічильників електроенергії 45
4.5 Створення електричної принципові схеми лічильника 48
4.6 Огляд обладнання 49
4.7 Аналоговий інтерфейс (AFE) 51
4.8 Ядро 80515 MPU 53
4.9 Організація пам'яті 54
4.10 UART 56
4.11 Ресурси на чіпі 58
4.12 Зовнішній РК-дисплей модель CFAH1602A-AGB-JP 65
4.13 Зовнішній інтерфейс I2C (EEPROM) 69
4.14 Програмне забезпечення 71
5 ТЕХНІКО - ЕКОНОМІЧНА ЧАСТИНА 73
5.1 Розрахунок повної собівартості проектованого пристрою 73
5.2 Матеріали та комплектуючі 74
5.3 Розрахунок повної собівартості проектованого пристрою 76
5.4 Відрахування на соціальні виплати 76
5.5 Видатки на утримання та експлуатацію встаткування 78
5.6 Загальновиробничі витрати 78
5.7 Виробнича собівартість 78
5.8 Адміністративні витрати 78
5.9 Витрати на збут 79
5.10 Повна собівартість пристрою 80
5.11 Розрахунок ціни пристрою 81
5.12 Розрахунок роздрібної ціни пристрою 81
ВИСНОВКИ 83
СПИСОК ДЖЕРЕЛ 84
ДОДАТОК А 86

ВСТУП

Ефективне функціонування сучасних енергетичних систем дедалі більше залежить від інтеграції інформаційно-комунікаційних технологій, які забезпечують оперативний моніторинг, управління та обмін даними. Розбудова "розумних" мереж (Smart Grid), що поєднують традиційні енергетичні системи з цифровими технологіями, створює нові можливості для підвищення енергоефективності, надійності та стійкості енергетичної інфраструктури. Водночас зростає вразливість таких систем до кіберзагроз і несанкціонованого доступу, що обумовлює необхідність впровадження високонадійних методів захисту інформації.

Якість захисту інформації залежить як і від способу передачі, так і від методів криптографічного перетворення данних. У процесі рішення цих питань розробляють протоколи захисту та передачі даних, такі як VPN, IPSec, IKEv2, PPTP та тому подібне.

Створення складних, багаторівневих систем захисту чи шифрування інформації потребує використання відповідного апаратного забеспечення. Кількість процесів для перетворення даних зростає як і потреба в більш новітньому обладнані для виконання поставленої задачі. Таким чином з великих масивних ЕОМ людсто поступово перейшло до невеликих друкованих плат, а згодом до меньших, але значно продуманіших мікросхем. Для шифрування є можливість використовувати ПЛІС, мікроконтролери чи, наприклад, системи на кристалі (СнК).

Система на кристалі на одній мікросхемі функціональні складові цілого пристрою. Цього достатньо для прграмування СнК та використання систем у якості системи збору, обробки (шифрування) та відправки інформації. Данна робота продемонструє ідею використання СнК у електронній системі шифрування даних в інфокомунікаційних мережах електроенергетики.

1.ОГЛЯД ЛІТЕРАТУРИ

1.1 Автоматизована система комерційного обліку електричної енергії (АСКОЕ)

АСКОЕ — це метрологічно атестована автоматизована система, що об'єднує локальне обладнання збору, обробки та передачі даних про облік електроенергії. Вона складається з лічильників (з вимірювальними трансформаторами), каналів передачі даних, комунікаційного обладнання та інтелектуальних концентраторів для збору і передачі інформації.

Функції системи включають:

- автоматичний збір даних споживання/відпуску електроенергії;
- контроль параметрів якості енергії;
- багатотарифний облік та контроль лімітів енергоспоживання;
- ведення архіву даних і синхронізацію системного часу.

Основна мета АСКОЕ — забезпечення взаєморозрахунків між споживачами й енергопостачальниками, а також ефективний контроль споживання енергоресурсів на різних рівнях (будинок, район, місто).

1.2 Автоматизована система технічного обліку електроенергії (АСТУЕ)

АСТУЕ призначена для автоматизації збору й аналізу даних про технічний стан електроспоживання підприємств.

Функції системи:

- моніторинг і планування електроспоживання;
- автоматизація оперативно-диспетчерського управління;
- контроль якості енергії та стану обладнання;
- оптимізація енергоспоживання і планування ремонтів.

Мета АСТУЕ — зниження витрат на енергію, мінімізація аварійних ситуацій та підвищення ефективності управління енергетичним обладнанням.

1.3 Автоматизована система оперативно-диспетчерського управління (АСОДУ)

АСОДУ — це комплекс програмно-технічних засобів для збору, обробки та архівування інформації про технологічні процеси підприємства.

Компоненти АСОДУ:

- системи автоматизованого управління технологічними процесами (АСУТП);
- автоматизовані робочі місця (АРМ) та сервери баз даних.

Функції АСОДУ:

- оперативний контроль і моніторинг процесів;
- протоколювання подій і реагування на позаштатні ситуації;
- координація роботи обладнання відповідно до графіків та нормативів.

Сфери застосування: промислові підприємства, енергетика, нафтогазовий сектор, машинобудування, гірничодобувна і харчова промисловість.

1.4 Алгоритми управління об'єктами АСОДУ

АСОДУ реалізує управління на різних рівнях завдяки сучасним комунікаційним рішенням, включаючи локальні підсистеми автоматизації.

Етапи створення АСОДУ:

- аналіз діяльності підприємства;
- розробка проєктної документації;
- постачання обладнання й пусконалагоджувальні роботи;
- навчання персоналу й подальший супровід.

Пункти 1.1-1.3 демонструють системи управління та обліку данних про технологічні процеси чи використання електроінергії. Ці данні отримуються від верстатів, електричного обладнання, джерел живлення, чи, наприклад, електроних лічильників.

1.5 Електронний лічильник

Сучасні електронні лічильники будуються на основі програмованих мікроконтролерів, що мають вбудовану пам'ять EEPROM. Це дозволяє зберігати дані обліку навіть після вимкнення живлення та забезпечує розширену функціональність у порівнянні з традиційними механічними лічильниками.

Лічильник можна реалізувати на основі універсального програмованого мікроконтролера, який інтегрує в собі широкий спектр периферійних пристроїв і володіє здатністю виконувати різноманітні завдання. Більшість сучасних мікроконтролерів оснащені енергонезалежною пам'яттю типу EEPROM, що забезпечує збереження даних, зокрема результатів обчислень або поточного стану лічби, навіть після відключення живлення, що є критично важливим для надійності системи обліку

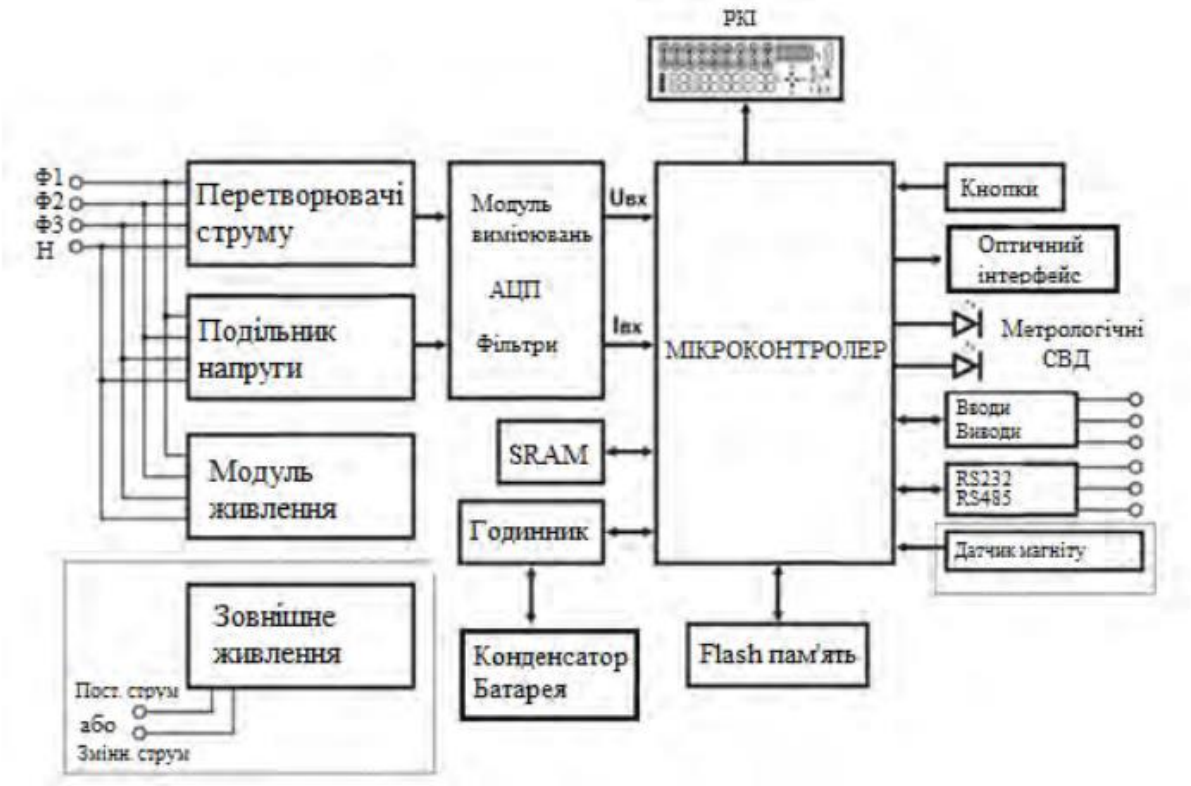


Рисунок 1.1 – Блок-схема лічильника

Одним з простих та надійних захистів електроних пристроїв є захист за допомогою реле

Релейний захист (РЗ)

РЗ забезпечує контроль стану електроенергетичної системи та автоматичне відключення несправних ділянок мережі для запобігання аваріям

шляхом впливу на комутаційне обладнання.

Отриманні дані з підприемст чи з побутових споживачів треба обробляти, зберігати та мати можливість передавати їх за відповідним запитом. Створення мережі для споживачів (як побутових так і промислових) потребується індитифікація споживачів та сховища данних (IP адреса), прилади для з’єднання абонентів (GSM і GPRS модемами) та способи створення захищених тунелів зв’явку (VPN тунелі)

1.6 Статичні публічні "білі" IP-адреси

Статичні публічні ("білі") IP-адреси є унікальними, постійно закріпленими IP-адресами, доступними в глобальній мережі Інтернет. Вони відрізняються від динамічних IP-адрес тим, що не змінюються при перезавантаженні обладнання або повторному підключенні до мережі. Основними характеристиками таких адрес є стабільність та доступність, що дозволяє використовувати їх для широкого спектра задач, зокрема веб-хостингу, налаштування серверів, VPN-з'єднань, поштових сервісів та інших мережевих рішень.

Переваги статичних публічних IP-адрес:

- Стабільність і незмінність - постійна адреса забезпечує надійний доступ до серверів та пристроїв без необхідності оновлення конфігурацій.
- Глобальний доступ - дозволяє стороннім системам і користувачам підключатися до ресурсу з будь-якої точки світу.
- Зручність для серверних рішень - використання для хостингу веб-сайтів, поштових серверів та VPN-з'єднань усуває проблеми, пов'язані з динамічними змінами адреси.
- Покращена безпека - дозволяє налаштовувати фільтрацію трафіку або обмежувати доступ до певних IP-адрес.

Недоліки статичних публічних IP-адрес:

- Вразливість до атак - постійна доступність може зробити адреси ціллю для DDoS-атак, сканування портів тощо.
- Відсутність анонімності - статичні адреси можуть полегшити відстеження активності користувача в Інтернеті.
- Додаткові витрати - провайдери часто надають статичні IP-адреси за

окрему плату.

Методи отримання статичних IP-адрес:

- Інтернет-провайдери (ISP) - ільшість провайдерів пропонують статичні IP-адреси за додатковою підпискою.
- Хостинг-провайдери - для веб-серверів, поштових серверів або інших хостингових рішень надаються статичні IP.

Застосування статичних публічних IP-адрес:

- VPN-сервери - створення стабільного з'єднання для віддаленого доступу.
- Поштові сервери – запобігання фільтрації та блокуванню через змінні адреси.
- IP-камери та IoT-пристрої - доступ до пристроїв ззовні.
- Віддалений робочий стіл - підключення до корпоративних ресурсів із глобального доступу.

Заходи захисту статичних IP-адрес:

- Брандмауери та IP-фільтрація - обмеження доступу лише до авторизованих користувачів.
- VPN-технології - захист трафіку через тунелювання з використанням шифрування.
- Двофакторна аутентифікація (2FA) - додатковий рівень захисту для сервісів, доступних через публічну IP-адресу.

Таким чином, статичні публічні IP-адреси забезпечують стабільний і надійний доступ до ресурсів в Інтернеті, проте потребують ретельного налаштування безпеки для мінімізації потенційних загроз.

1.7 GSM, GPRS модеми

GSM та GPRS модеми є пристроями для підключення до мобільних мереж, які використовують стандарти другого покоління (2G) зв'язку для передачі даних, текстових повідомлень (SMS) або голосових викликів.

GSM модеми

GSM-модеми працюють на основі стандарту GSM (Global System for Mobile Communications), що є одним із найпоширеніших у світі стандартів стільникового зв'язку. Вони забезпечують передачу даних за допомогою

традиційних методів, таких як:

- CSD (Circuit-Switched Data) - передача даних здійснюється через виділений канал, який резервується на весь час з'єднання.
- SMS - можливість відправлення та отримання коротких текстових повідомлень.

Основні обмеження GSM-модемів полягають у невисокій швидкості передачі даних, яка зазвичай становить 9.6–14.4 кбіт/с. Крім того, тарифікація здійснюється на основі часу підключення, а не обсягу переданих даних.

GPRS модеми

GPRS (General Packet Radio Service) — це технологія, що є вдосконаленням GSM і забезпечує пакетну передачу даних, що дозволяє більш ефективно використовувати мережеві ресурси. На відміну від CSD, передача даних здійснюється у вигляді окремих пакетів, що забезпечує такі переваги:

- Більша швидкість передачі даних - максимальна теоретична швидкість GPRS досягає 114 кбіт/с, хоча реальні показники зазвичай нижчі.
- Тарифікація за обсяг даних - вартість послуг визначається обсягом переданих даних, а не часом підключення, що є зручнішим для постійного доступу (Always On).
- Доступ до Інтернету та сервісів - GPRS-модеми забезпечують стабільне підключення до Інтернету, електронної пошти, а також підтримку різноманітних онлайн-сервісів.

Таким чином, основна відмінність GPRS від традиційного GSM полягає у методі передачі даних та ефективності використання мережевих ресурсів.

CSD (Circuit-Switched Data)

CSD є застарілою технологією передачі даних у мережах GSM. Вона працює на основі виділення окремого каналу зв'язку на весь період передачі, що призводить до:

- Низької швидкості - максимум 9.6–14.4 кбіт/с.
- Високих витрат - тарифікація здійснюється за час з'єднання.

Через ці обмеження CSD поступово витісняється технологією GPRS, яка є більш гнучкою та економічно вигідною.

GPS (Global Positioning System)

GPS — це система супутникової навігації, призначена для визначення географічного положення об'єктів на основі сигналів від супутників. GPS не є

методом передачі даних, але часто використовується разом із мобільними мережами для реалізації наступних функцій:

- Визначення місцезнаходження пристроїв - передача координат через GPRS або інші канали зв'язку.
- Навігаційні сервіси - інтеграція з мобільними додатками для маршрутизації або моніторингу.

Таким чином, GPS доповнює функціональність GPRS та GSM, надаючи можливість точно визначати координати пристроїв, що здійснюють передачу даних у мобільних мережах.

Порівняння GSM та GPRS модемів

Таблиця 1.1 - Порівняння GSM та GPRS модемів

Параметр	GSM модем	GPRS модем
Метод передачі даних	Канальне з'єднання (CSD)	Пакетна передача даних
Швидкість передачі	9.6–14.4 кбіт/с	До 114 кбіт/с
Тарифікація	За час з'єднання	За обсяг переданих даних
Підключення до Інтернету	Обмежене	Постійне (Always On)

Таким чином, використання GPRS-модемів забезпечує вищу швидкість передачі даних, економічність та ефективне використання ресурсів мобільної мережі порівняно з традиційними GSM-модемами.

1.8 VPN. Принцип роботи

Функціонування віртуальної приватної мережі (VPN) базується на застосуванні технологій і протоколів тунелювання для передачі даних між кінцевими точками мережі. Основна мета протоколів тунелювання полягає у захопленні мережевих повідомлень від прикладних програм (що працюють на 7-му рівні моделі OSI) на одній стороні тунелю та їхньому відтворенні на іншій стороні. Це дозволяє забезпечити передачу даних без необхідності модифікації програмного забезпечення, оскільки віртуальні канали доступні для операційної системи як стандартні мережеві інтерфейси.

Мобільна VPN

Мобільна VPN — це різновид віртуальних приватних мереж, оптимізований для мобільних пристроїв, таких як смартфони та планшети. Її основною функцією є забезпечення захищеного доступу до приватних ресурсів або мереж через зашифрований канал, навіть у нестабільних умовах мобільних з'єднань. Мобільна VPN враховує специфічні особливості мобільних платформ, зокрема:

використання мобільних даних та мереж;

обмеження енергоспоживання (батарея);

адаптацію до мобільного інтерфейсу та умов мінливої пропускної здатності

Принцип роботи мобільної VPN

Подібно до традиційних десктопних VPN, мобільна VPN створює зашифрований канал між мобільним пристроєм та віддаленим VPN-сервером, що забезпечує конфіденційність і цілісність даних навіть при підключенні до ненадійних мереж (наприклад, публічних Wi-Fi точок доступу).

Основні етапи роботи мобільної VPN:

- Шифрування - усі дані, що передаються між мобільним пристроєм і сервером VPN, підлягають шифруванню. Це унеможливлює їх перехоплення третіми сторонами.
- Тунелювання - передані дані інкапсулюються та проходять через захищений віртуальний «тунель», що забезпечує їх захист від несанкціонованого доступу.
- Аутентифікація - підключення мобільного пристрою до VPN-сервера відбувається після успішної аутентифікації користувача або пристрою. Це гарантує, що доступ надається лише авторизованим користувачам.

Типи мобільних VPN

Мобільні VPN використовують різні протоколи тунелювання, що аналогічні протоколам стаціонарних VPN-рішень. Основні протоколи, що застосовуються для мобільних VPN, включають:

- IPsec (Internet Protocol Security) - IPsec забезпечує шифрування на мережевому рівні (рівень 3 моделі OSI) і відомий своєю високою надійністю для захисту даних на мобільних пристроях. Він гарантує конфіденційність, цілісність і аутентифікацію даних під час їхнього передавання.

- OpenVPN - це один із найбільш популярних протоколів VPN завдяки своїй гнучкості та підтримці шифрування SSL/TLS. OpenVPN часто застосовується на мобільних пристроях через спеціалізовані додатки, що дозволяють його налаштування та оптимізацію під потреби користувача.
- L2TP/IPsec (Layer 2 Tunneling Protocol з IPsec) - L2TP самостійно не забезпечує шифрування даних, тому його поєднують із IPsec для створення захищеного тунелю. Ця комбінація підходить для мобільних пристроїв, забезпечуючи високу безпеку передачі даних.
- IKEv2 (Internet Key Exchange version 2) - IKEv2 є оптимальним рішенням для мобільних пристроїв завдяки своїй швидкій реакції на перебої зв'язку. Він дозволяє автоматично відновлювати VPN-з’єднання при перемиканні між різними мережами (наприклад, Wi-Fi та мобільними даними). Завдяки стабільності та ефективності, IKEv2 є популярним вибором для мобільних платформ.

Переваги мобільної VPN

- Захист даних у публічних мережах - мобільна VPN шифрує переданий трафік, забезпечуючи захист конфіденційних даних під час підключення до публічних Wi-Fi мереж (наприклад, у кафе, аеропортах чи готелях).
- Обхід географічних обмежень - використання VPN дозволяє змінювати віртуальне місцезнаходження пристрою, що забезпечує доступ до контенту, який заблокований у певних регіонах або країнах.
- Захист від атак - мобільна VPN запобігає атакам MITM (Man-in-the-Middle) та іншим формам несанкціонованого доступу до даних, особливо при використанні публічних мереж.
- Підвищена анонімність - використання VPN приховує реальну IP-адресу мобільного пристрою, що забезпечує анонімність під час перегляду веб-ресурсів.
- Захист у роумінгу - VPN може зменшити витрати на роумінг шляхом створення тунелю через більш вигідні та безпечні канали передачі даних.

Недоліки мобільної VPN

- Підвищене споживання енергії - процес шифрування та тунелювання даних вимагає значних ресурсів пристрою, що призводить до швидшого розряджання акумулятора.

- Зниження швидкості Інтернет-з’єднання - шифрування даних та їх перенаправлення через VPN-сервер можуть спричиняти затримки, що впливають на швидкість з’єднання.
- Залежність від віддаленого сервера - географічна віддаленість VPN-сервера від користувача може збільшувати ping та зменшувати швидкість передачі даних.
- Складність налаштування - незважаючи на наявність спрощених мобільних додатків для VPN, деякі користувачі можуть зіткнутися з труднощами під час налаштування з’єднання.

1.9 VPN та IP-тунелі

VPN (Virtual Private Network) із використанням IP-тунелів дозволяє створювати захищений канал для передавання даних через Інтернет або інші незахищені мережі. Ця технологія забезпечує:

- Конфіденційність - дані шифруються для запобігання несанкціонованому доступу.
- Приватність - VPN приховує IP-адресу користувача.
- Безпеку - увесь трафік, що передається через тунель, надійно захищений від сторонніх загроз.

Принцип роботи VPN-тунелю

VPN-тунель створює захищений канал між двома точками, такими як користувач і сервер або дві корпоративні мережі. Основні етапи його роботи включають:

- Шифрування - дані шифруються на пристрої користувача перед передачею через Інтернет.
- Тунелювання - зашифровані дані інкапсулюються у стандартні IP-пакети для їхньої подальшої передачі через тунель.
- Дешифрування - на приймальній стороні дані розшифровуються для подальшої обробки

Типи VPN-тунелів відповідно протоколу тунелювання:

- Тунель на основі IPsec (IP Security) - IPsec є широко використовуваним протоколом для шифрування IP-пакетів під час передачі через тунель.

Він функціонує на мережевому рівні (рівень 3 моделі OSI) та забезпечує захист усієї мережевої інфраструктури завдяки застосуванню шифрування й методів автентифікації.

- PPTP (Point-to-Point Tunneling Protocol) - PPTP є одним із найстаріших протоколів тунелювання. Завдяки своїй простоті у налаштуванні й високій швидкості він залишається популярним, проте його рівень безпеки є недостатнім порівняно з сучасними рішеннями.
- L2TP (Layer 2 Tunneling Protocol) - L2TP дозволяє об'єднувати декілька мереж в одну, проте не забезпечує власного шифрування. Як правило, він використовується разом із IPsec, що додає необхідний рівень захисту даних.
- OpenVPN - OpenVPN є одним із найнадійніших і найбільш гнучких протоколів тунелювання. Він використовує SSL/TLS для шифрування з'єднань і характеризується високим рівнем безпеки, конфіденційності та стабільності.
- WireGuard - WireGuard є новітнім VPN-протоколом, що відрізняється високою продуктивністю та оптимізованою архітектурою. Він забезпечує швидке з'єднання, потужний рівень безпеки й ефективне використання ресурсів пристрою.

Типи VPN-тунелів відповідно к-сті споживачів:

- Site-to-Site - використовується для об'єднання двох або більше локальних мереж у єдину інфраструктуру через VPN.
- Remote Access - забезпечує можливість індивідуальним користувачам підключатися до віддаленої мережі (наприклад, до корпоративного середовища через Інтернет).

Безпека VPN-тунелів

- Шифрування - шифрування є критичним компонентом безпеки VPN, оскільки воно запобігає несанкціонованому доступу до переданих даних.
- Аутентифікація - перевірка автентичності ініціатора з'єднання виконується через паролі, сертифікати або двофакторну автентифікацію.
- Інтеграція з корпоративними системами - VPN може використовувати корпоративні сертифікати та політики безпеки для посилення захисту мережі.

Переваги використання VPN-тунелів

- Захист конфіденційних даних: VPN шифрує трафік, забезпечуючи захист інформації від несанкціонованого доступу.
- Обхід географічних обмежень: VPN дозволяє змінювати віртуальне місцезнаходження пристрою для доступу до контенту, обмеженого в певному регіоні.
- Безпечне підключення до публічних мереж: VPN забезпечує захист даних під час використання публічних Wi-Fi мереж.
- Анонімність в Інтернеті: Приховуючи реальну IP-адресу користувача, VPN сприяє збереженню анонімності в мережі.

Недоліки VPN-тунелів

- Зниження швидкості Інтернет-з'єднання - шифрування та інкапсуляція даних можуть зменшувати швидкість передавання інформації.
- Складність налаштування - коректне налаштування VPN може бути викликом для недосвідчених користувачів.
- Залежність від VPN-провайдера - використовуючи комерційні сервіси, користувачі покладаються на політики конфіденційності провайдера, який потенційно має доступ до їхніх даних.

VPN у Vodafone

Послуга «IP VPN», що надається оператором Vodafone Україна, є рішенням для побудови інтегрованої корпоративної мережі передачі даних. Ця мережа функціонує на основі технологій 2G та 3G і є повністю відокремленою від загальнодоступного Інтернету.

Основне призначення послуги полягає в організації захищеного каналу для передавання даних між віддаленими об'єктами підприємства та процесинговим центром (центральним сервером) головного офісу. Отримані дані можуть бути оброблені, проаналізовані та збережені для подальшого використання.

Особливості послуги:

- Послуга орієнтована на бізнес-клієнтів Vodafone Україна.
- Доступ до мережі може бути забезпечено як в межах України, так і в роумінгових мережах партнерів за кордоном, що підтримують сервіси передачі даних.

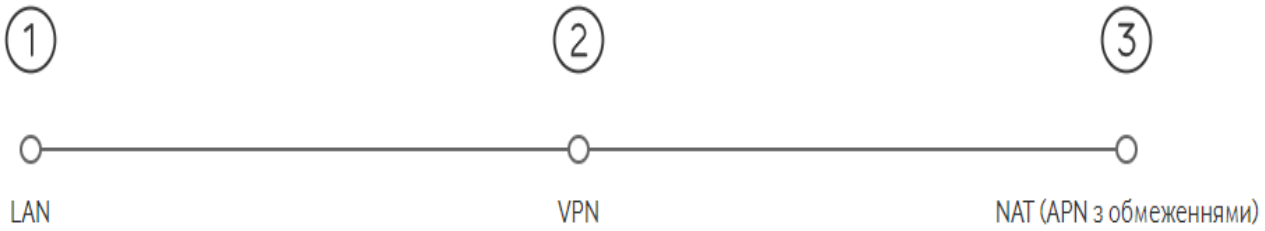


Рисунок 1.2 - Послуга з мобільного IP VPN

LAN

Закрита мобільна IP-мережа організовується на базі інфраструктури передачі даних Vodafone Україна.

Особливості:

- Статична IP-адресація: кожному пристрою призначається незмінна IP-адреса.
- Обмежений доступ: відсутня можливість підключення до глобальної мережі Інтернет.
- Обмеження на комунікацію: передача даних можлива виключно між пристроями, що мають доступ до визначеної точки доступу (APN).

VPN

VPN забезпечує підключення віддалених користувачів до корпоративної локальної мережі з можливістю ідентифікації, аутентифікації та адміністрування.

Особливості:

- Гнучка схема IP-адресації - статичне, динамічне призначення IP-адрес або на основі відповідей RADIUS-сервера абонента.
- Реалізація тунелювання - підключення може здійснюватися через GRE/IPsec або шляхом фізичного стику.

NAT (APN з обмеженнями)

Технологія NAT дозволяє обмежити або надати доступ до конкретних Інтернет-адрес у рамках послуги «Мобільний IP VPN».

Переваги:

- Спрощене налаштування - не потребує додаткових конфігурацій з боку клієнта.

- Захист від несанкціонованого трафіку - у разі збоїв клієнтського обладнання передача неконтрольованого трафіку блокується.
- Трансляція IP-адрес - усі користувачі мережі представлені в Інтернеті однією публічною IP-адресою, що оптимізує маршрутизацію та захищає мережу.

VPN у Kyivstar

Kyivstar пропонує рішення для побудови корпоративної мережі передачі даних, зокрема на основі технологій VPLS (Virtual Private LAN Service) та IP VPN (Internet Protocol Virtual Private Network):

- VPLS — це технологія, що дозволяє об'єднати географічно розподілені локальні мережі (LAN) в єдину віртуальну мережу на рівні 2 моделі OSI. Це забезпечує прозорість передачі даних і можливість централізованого управління.
- IP VPN — рішення, яке будується на основі IP-протоколу (3 рівень моделі OSI) і дозволяє безпечно передавати дані між віддаленими об'єктами корпоративної мережі. Ця технологія забезпечує шифрування трафіку, ізоляцію даних від публічного Інтернету та гнучке налаштування доступу до ресурсів.

Переваги корпоративної мережі:

- Забезпечення цілодобової технічної підтримки та швидкого відновлення зв'язку в разі виникнення несправностей, що гарантує безперервність операцій.
- Створення індивідуальних каналів зв'язку для кожної компанії з підвищеним рівнем безпеки, що забезпечує конфіденційність і захист переданої інформації.
- Мережа побудована на основі власної інфраструктури волоконно-оптичних ліній та обладнання провідних міжнародних виробників, що забезпечує надійність та високу ефективність.
- Мобільність, що досягається завдяки впровадженню технології LTE (4G), дозволяє реалізувати програми, які охоплюють широкі географічні території.
- Швидкість передачі даних варіюється від 1 Мбіт до 10 Гбіт, що дозволяє забезпечити необхідну пропускну здатність для різних корпоративних потреб.

- Впровадження технологій VPLS та IP VPN, які забезпечують гнучкість підключень через принципи "точка-точка" або "кільце".
- Мережа гарантує захищене покриття по всій території України, що забезпечує високу доступність і безпеку передачі даних.
- Всі канали зв'язку мають систему резервування на всіх етапах, що покриває як логічні, так і фізичні рівні інфраструктури оператора.

2. НАУКОВО-ДОСЛІДНА ЧАСТИНА

2.1 Відомості про принцип криптографічного шифрування

У цій роботі розглядається використання гамування як методу симетричного шифрування. Гамування полягає в накладанні спеціальної псевдовипадкової послідовності (гами шифру) на відкриті дані за визначеним алгоритмом.

Гама шифру є псевдовипадковою послідовністю, яка генерується на основі певного алгоритму для шифрування вихідних даних та розшифрування зашифрованої інформації. Оскільки псевдовипадкові послідовності утворюються алгоритмічним шляхом, вони не є абсолютно випадковими, проте володіють характеристиками, притаманними випадковим числам.

Процес шифрування реалізується через генерацію гами шифру та накладання її на вихідний текст за допомогою оборотних математичних операцій, зокрема, додавання за модулем 2. Перед шифруванням відкриті дані ділять на блоки фіксованої довжини, по 64 біти, при цьому гама шифру формується у вигляді блоків аналогічної довжини.

Ключовою умовою ефективності гамування є зміна гами шифру для кожного блоку, що підлягає шифруванню. У випадку, коли період гами перевищує довжину всього шифрованого тексту, а зловмисник не володіє жодною частиною вихідної інформації, криптоаналіз можливий лише шляхом повного перебору всіх можливих ключів. Криптографічна стійкість такого шифру визначається довжиною ключа, який задає період неповторюваної частини гами.

Завдяки можливості генерації надзвичайно довгих послідовностей за допомогою сучасних обчислювальних засобів метод гамування є одним із ключових способів забезпечення захисту інформації.

Рисунок 2.1 - Схема одноразового гамування

2.2 Протокол IPsec

IPsec є найпоширенішим механізмом забезпечення безпеки на мережевому рівні для захисту комунікацій. Це система відкритих стандартів, що забезпечує приватність передачі даних через IP-мережі. Для безпечного узгодження параметрів IPsec і ключів шифрування використовується протокол Internet Key Exchange (IKE).

Робоча група IPsec при Інженерній робочій групі Інтернету (IETF) відповідає за підтримку та публікацію стандартів IKE та IPsec. Документи, що створюються цією групою, поділяються на два типи: Запити на коментарі (RFC), які є завершеними специфікаціями, та Internet-Drafts, які є робочими документами, що можуть стати RFC. Протокол Encapsulating Security Payload (ESP) є основним механізмом безпеки в IPsec. Реалізація алгоритмів і настанови щодо використання описані для IKEv2 та IPsec. Різні розширення IKEv2 мають окремі специфікації RFC. Протоколи IKE і IPsec були розроблені в IETF майже тридцять років тому, і деякі аспекти їх розвитку, зокрема різниця між IPsec-v2 і IPsec-v3, задокументовані в документі Залежно від реалізації та налаштувань IPsec, вона може забезпечувати різні типи захисту, що

включають наступні компоненти:

- Конфіденційність - IPsec гарантує, що дані не можуть бути виявлені неавторизованими сторонами. Це досягається шляхом шифрування та дешифрування даних з використанням криптографічного алгоритму та секретного ключа, який відомий лише двом сторонам, що здійснюють обмін. Тільки особа, яка має цей секретний ключ, може розшифрувати дані. Хоча можливе використання IPsec без шифрування, такий підхід не рекомендується.
- Цілісність - IPsec забезпечує визначення змін у даних (як навмисних, так і ненавмисних) під час їх передачі. Це досягається за допомогою генерації коду автентифікації повідомлення (MAC), який є криптографічною контрольованою сумою (хешем) даних, створеною на основі узгодженого секретного ключа, відмінного від ключа шифрування. Якщо дані змінені, перевірка MAC не буде успішною.
- Конфіденційність і цілісність - обидва ці типи захисту можна об'єднати в один алгоритм автентифікованого шифрування з асоційованими даними (AEAD). Такий підхід поєднує симетричне шифрування і криптографічні контрольні суми в одному процесі, використовуючи єдиний секретний ключ замість двох окремих. Однак обидві сторони повинні використовувати однаковий секретний ключ і однакові пов'язані дані.
- Однорангова автентифікація - кожна кінцева точка IPsec підтверджує ідентичність іншої кінцевої точки, з якою вона встановлює зв'язок, гарантуючи, що мережевий трафік передається тільки авторизованій стороні.
- Захист від повторів - IPsec забезпечує захист від повторної передачі однакових даних і збереження правильного порядку передачі. Це унеможливлює для зловмисників копіювати і ретранслювати зашифровані дані з шкідливою метою. IPsec, як і UDP, не гарантує, що дані будуть доставлені в тому порядку, в якому вони були надіслані. Одержувач має механізм перевірки та відновлення порядку перед розшифруванням даних.
- Захист аналізу трафіку- у тунельному режимі IPsec особа, яка спостерігає за мережевим трафіком, не може визначити, які сторони

спілкуються, як часто відбувається зв'язок або який обсяг даних передається. Хоча можна підрахувати кількість і розмір зашифрованих пакетів, протокол ESP може вирівняти довжину пакетів і додавати фіктивні пакети, щоб заплутати час передачі.

- Контроль доступу - кінцеві точки IPsec можуть фільтрувати трафік, забезпечуючи доступ до певних мережевих ресурсів лише для авторизованих користувачів. Вони також можуть дозволяти або блокувати певні типи трафіку, наприклад, дозволяти доступ до веб-сервера, але забороняти передачу файлів. Це здійснюється через політики IPsec, які фільтрують трафік на основі маршрутизації або політики.
- Ідеальна пряма секретність (PFS) - кінцеві точки IPsec часто генерують нові ключі сеансу (зазвичай кожну годину), після чого старі ключі видаляються з пам'яті. Це забезпечує, що навіть якщо зашифрований трафік буде перехоплений, він не може бути розшифрований, оскільки старі ключі не зберігаються. Для створення нових ключів можуть використовуватися методи обміну ключами Діффі-Хеллмана (DH), що гарантує ідеальну пряму секретність.
- Мобільність - зовнішня IP-адреса кінцевої точки може змінюватися без переривання зашифрованого з'єднання. Це дозволяє пристрою, наприклад, перемикатися з WiFi на Ethernet, зберігаючи стабільність зв'язку і безперервність передачі даних, що особливо важливо для мобільних пристроїв.

IPsec являє собою набір протоколів, що забезпечують захист комунікацій у мережах. Основним компонентом IPsec є протокол ESP (Encapsulating Security Payload), який забезпечує захист конфіденційності та цілісності даних у мережевих пакетах. Крім того, IPsec включає й інші компоненти, зокрема протокол стиснення навантаження (IP Payload Compression Protocol — IPComp) і протокол Authentication Header (AH). Для узгодження всіх необхідних параметрів та криптографічних ключів, що використовуються в IPsec, застосовується протокол обміну ключами Internet Key Exchange (IKE).

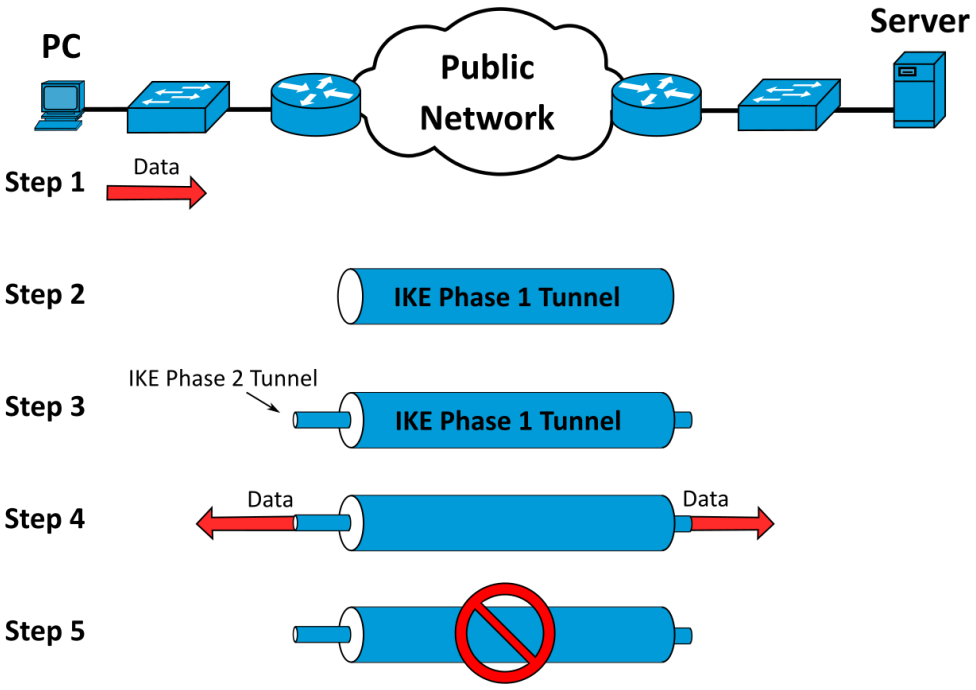


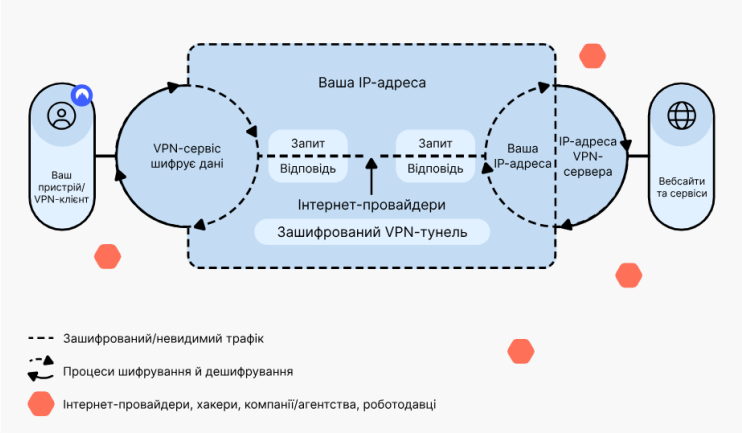
Рисунок 2.2 - Фази життєвого циклу тунелю IPSec у віртуальній приватній мережі

2.3 Віртуальна приватна мережа (VPN)

Одним із найпоширеніших застосувань IPsec є реалізація послуг віртуальної приватної мережі (VPN). VPN — це віртуальна мережа, яка будується на основі існуючих фізичних мереж і забезпечує захищену передачу даних та IP-інформації між різними мережами або вузлами однієї мережі. Завдяки можливості використання VPN поверх загальнодоступних мереж, таких як Інтернет, цей механізм забезпечує безпечну передачу конфіденційних даних через мережі загального користування. Це є більш економічно вигідним порівняно з іншими варіантами, такими як виділені приватні лінії зв'язку між організаціями або філіями.

Виділені приватні лінії часто використовуються у вигляді багатокористувацьких рішень, таких як багатопротокольна комутація з мітками (MPLS), що управляються сторонніми телекомунікаційними компаніями, і навіть у таких випадках вони також часто захищаються за допомогою IPsec VPN. VPN для віддаленого доступу пропонують гнучкі

рішення, зокрема для захисту зв'язку між віддаленими працівниками та серверами організації. Крім того, VPN можна використовувати для забезпечення безпеки всередині однієї організації, створюючи захищені канали для особливо чутливих комунікацій між учасниками тієї ж мережі або для розгортання мережі IPsec-з'єднань між всіма вузлами мережі, що гарантує відсутність незашифрованих даних.



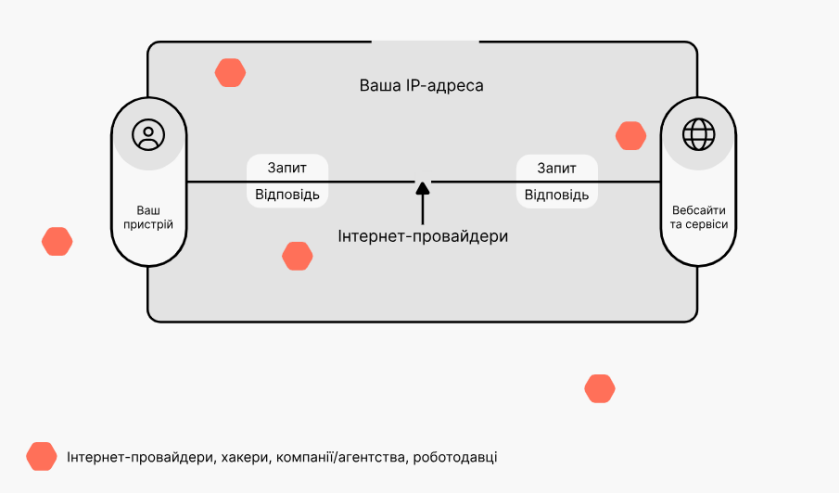


Рисунок 2.2 - ілюстрація роботи VPN

Конфіденційність

VPN використовують симетричну криптографію для шифрування та дешифрування даних у своїх каналах зв'язку. Симетрична криптографія, як правило, є більш ефективною та вимагає меншої обчислювальної потужності порівняно з асиметричною криптографією, тому вона зазвичай застосовується для шифрування більшості даних, які передаються через VPN. Серед

алгоритмів, схвалених Національним інститутом стандартів і технологій (NIST) для реалізації симетричного шифрування, виділяються Advanced Encryption Standard (AES) та Triple Data Encryption Standard (3DES). Один з рекомендованих NIST режимів для симетричних алгоритмів шифрування — це режим AES-лічильника Галуа (AES-GCM); для більш детальної інформації про інші режими симетричного шифрування, схвалені NIST.

Цілісність

Цілісність даних забезпечується за допомогою алгоритму автентифікації повідомлень, який приймає вхідні дані та секретний ключ для перевірки цілісності і генерує код автентифікації повідомлення (MAC). Ці дані та відповідний MAC передаються через мережу. Одержувач, у свою чергу, обчислює MAC на основі отриманих даних, використовуючи той самий секретний ключ, який був попередньо встановлений між відправником і отримувачем. Якщо дані або їх MAC були змінені, перевірка MAC не буде успішною, і повідомлення повинно бути відхилене.

Створення спільних секретних ключів

VPN зазвичай використовують алгоритм обміну ключами Диффі-Хеллмана (DH) для створення конфіденційного каналу зв'язку, який дозволяє обчислити спільний ключ між двома кінцевими точками, що неможливо отримати або обчислити сторонньому спостерігачеві. Обмін ключами DH може базуватися на криптографії кінцевих полів (класичний або модульний DH) або на криптографії еліптичних кривих (ECDH). Після виконання обміну ключами DH та обчислення спільного ключа кінцеві точки повинні пройти процес аутентифікації, щоб переконатися, що конфіденційний канал встановлено з очікуваною стороною, а не з потенційно недобросовісним учасником.

2.4 Інкапсуляція корисного навантаження безпеки (ESP)

ESP є основним протоколом безпеки в рамках IPsec. Його структура залишалася практично незмінною з моменту публікації другої версії в RFC 2406 у 1998 році. Поточна версія, IPsec-v3, була описана в RFC 4303 у 2005 році, і вона включає лише незначні оновлення порівняно з попередньою специфікацією IPsec-v2. Оскільки всі зміни в ESP є або зворотньо сумісними,

або стосуються нових функцій, які повинні бути узгоджені через протокол IKE перед їх впровадженням в ESP, не виникає проблем з сумісністю між різними реалізаціями IPsec, які отримують і надсилають ESP-пакети. Водночас, більшість сучасних реалізацій підтримують IPsec-v3. До функцій, доступних тільки в IPsec-v3, належать:

- Підтримка алгоритмів AEAD (Authenticated Encryption with Associated Data)
- Розширені номери послідовностей (ESN)
- Покращена підтримка політик безпеки через базу даних політик (SPD) і базу даних асоціацій безпеки (SAD)
- Підтримка пейдлінгу
- Підтримка фіктивних пакетів

Використання пейдлінгу та можливість відправки фіктивних повідомлень збільшують TFC (Traffic Flow Confidentiality), ускладнюючи підслуховування, оскільки для підслуховувача стає важче аналізувати розміри зашифрованих пакетів або їх часові характеристики. ESP забезпечує як шифрування, так і захист цілісності. Однак зовнішній заголовок не є повністю захищеним, що дає можливість маршрутизаторам, які пересилають ESP-пакети, змінювати деякі параметри, такі як Quality of Service (QoS) та час життя (TTL).

Функція шифрування в ESP може бути вимкнена через вибір алгоритму шифрування Null ESP або алгоритму AES-GMAC AEAD. AES-GMAC є варіантом AES-GCM, який забезпечує захист цілісності без використання шифрування. Таким чином, ESP може бути використаний як для шифрування та захисту цілісності, так і лише для захисту цілісності. Модернізація систем повинна включати перехід до підтримки цих алгоритмів ESP. ESP підтримує як AEAD, так і класичне шифрування з методами забезпечення цілісності.

Режим тунелю та транспортний режим

ESP має два режими: транспортний і тунельний

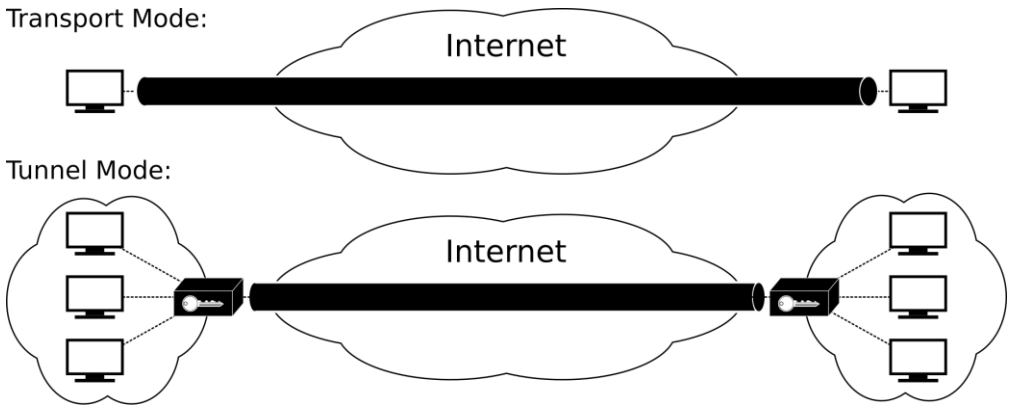


Рисунок 2.3 - VPN-міст, показаний на різних рівнях реалізації OSI

У тунельному режимі новий пакет, що містить (оригінальний) IP-пакет, передається через тунель за наступними етапами:

- Оригінальний IP-заголовок і його корисне навантаження обгортаються ESP-заголовком і трейлером.
- Виконується шифрування оригінального заголовка, корисного навантаження та трейлера ESP.
- Обчислюється значення перевірки цілісності (ICV) для заголовка ESP і зашифрованих даних, що включають як заголовок ESP, так і зашифровані дані.
- ICV додається в кінець сформованого пакета.
- На початок пакета додається новий IP-заголовок, при цьому обчислення ICV не включає новий IP-заголовок.

Новий IP-заголовок вказує на кінцеві точки тунелю ESP (наприклад, два шлюзи IPsec) як джерело та одержувача пакета і містить увесь зашифрований оригінальний пакет як його корисне навантаження. Завдяки цьому тунельний режим може застосовуватися в усіх архітектурах VPN. Тунельний режим здатен забезпечувати шифрування та захист цілісності як для даних, так і для оригінального IP-заголовка кожного пакета. Шифрування оригінального IP-заголовка та корисного навантаження гарантує їх конфіденційність; зокрема, шифрування оригінального IP-заголовка приховує деталі зв'язку, такі як фактичне джерело чи пункт призначення пакета, протокол та порти, що можуть вказувати на використовувану програму. ICV застосовується для виявлення будь-яких змін в даних, для яких воно обчислюється.

Таблиця 2.1 - Пакет тунельного режиму ESP

Новий IP заголовок	Заголовок ESP	Оригінальний IP Заголовок	Оригінальні дані IP, що містять транспорт і додаток заголовки та дані протоколу (необов'язкова підкладка TFC)	Причіп ESP(підкладка ESP, наступний заголовок)	Цілісність ESP контрольне значення - ICV (змінна)
		Зашифровано			
	Автентифікований (захист цілісності)				

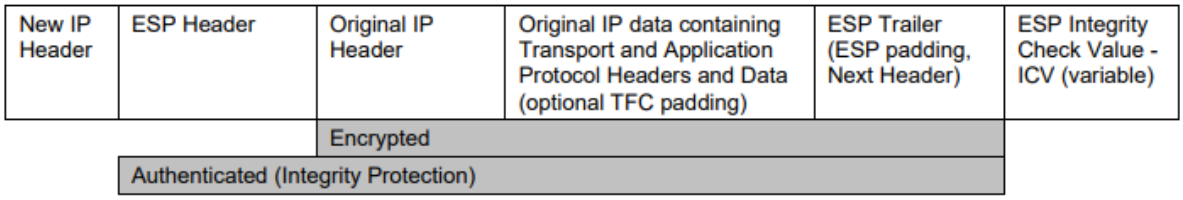


Рисунок - 2.4 Пакет тунельного режиму ESP

2.5 Огляд IKE

Протокол IKE можна вважати каналом для обміну командами, у той час як протокол IPsec слугує каналом для передачі даних, шифруючи та дешифруючи IP-пакети і перевіряючи відповідність IP-адрес джерела і призначення до узгоджених політик. Сам канал протоколу IKE також має бути зашифрованим, щоб забезпечити конфіденційність параметрів IPsec-з'єднання. Тобто спочатку встановлюється зашифроване з'єднання IKE, а потім через цей захищений канал встановлюються один або кілька IPsec-з'єднань. Протокол IKE застосовується для створення IKE Security Association (IKE SA). IPsec-з'єднання в свою чергу називається IPsec SA або Child SA. Як IKEv2 SA, так і IPsec SA ідентифікуються за допомогою номерів індексів параметрів безпеки (SPI), тоді як у IKEv1 ідентифікація SA здійснюється за допомогою інших полів, поки не будуть встановлені SPI для IPsec. Протокол IKE

використовує UDP-повідомлення на портах 500 і 4500, кожен з яких містить фіксований IKE-заголовок, за яким слідують змінні за довжиною дані IKE.

Обмін ключами в Інтернеті (IKE)

Коли два хости прагнуть встановити IPsec-з'єднання, необхідно узгодити параметри цього з'єднання, зокрема дозволені IP-адреси джерела і призначення, алгоритми шифрування для використання, а також матеріал криптографічного ключа, який буде застосовуватись для шифрування та дешифрування пакетів. Крім того, хости повинні пройти процедуру взаємної автентифікації. Усі ці дії здійснюються за допомогою протоколу обміну ключами Інтернету (IKE). У цьому розділі розглядається версія протоколу IKE 2 (IKEv2), яка описана в RFC 7296.

Зазвичай IKE функціонує як привілейований процес, тоді як IPsec, як правило, працює в ядрі операційної системи. Процес IKE відповідає за налаштування ядра для виконання IPsec, тоді як ядро безпосередньо здійснює шифрування та дешифрування пакетів. Процес IKE може також вставляти політику в ядро, що вказує на необхідність попередження процесу IKE, коли незашифрований пакет, який відповідає певним критеріям, наприклад, IP-адресам джерела і призначення, планується до передачі. Якщо однорангові вузли можуть пройти взаємну автентифікацію та узгодити інші політики, процес IKE домовляється про створення IPsec-тунелю, що покриває цей пакет. Це дозволяє створювати тунелі IPsec за вимогою.

Таблиця 2.2 - Формат пакету IKEv2

<table>
<tr><td>Байт 1</td><td>Байт 2</td><td>Байт 3</td><td colspan="2">Байт 4</td></tr>
<tr><td colspan="5">SPI ініціатора IKE SA</td></tr>
<tr><td colspan="5">SPI IKE SA відповідача</td></tr>
<tr><td>Наступне корисне навантаження</td><td>Основна версія IKE</td><td>Молодша версія IKE</td><td>Тип обміну</td><td>Прапори</td></tr>
<tr><td colspan="5">Ідентифікатор повідомлення</td></tr>
<tr><td colspan="5">Довжина всього повідомлення (заголовок IKE плюс дані)</td></tr>
<tr><td colspan="5">IKE DATA</td></tr>
</table>

2.6 VPN на основі маршрутизації та VPN на основі політик

Реалізації IPsec повинні здійснювати аналіз потоків пакетів з метою визначення, коли пакет повинен бути зашифрований, а коли може передаватися без шифрування. Одним із способів цього є використання таблиці маршрутизації. Якщо маршрут вказує на певний пристрій IPsec, реалізація IPsec обробляє пакет відповідно до правил SPD/SAD. Проте використання маршрутів може бути ненадійним. Інша підсистема може випадково або навмисно змінити маршрутизацію, що дозволяє обійти пристрій IPsec, тим самим порушуючи політику шифрування.

Ще однією проблемою політик, що ґрунтуються на маршрутизації, є те, що адміністратори часто застосовують одну політику IPsec, яка охоплює всі можливі IPv4-адреси (0.0.0.0/0) для всіх можливих IPv4-адрес (0.0.0.0/0). Після встановлення тунелю маршрутизація визначає, які пакети передавати через з'єднання IPsec. Якщо віддалений філіал розширює свою мережу, додаючи нову підмережу, наприклад, 192.0.2.0/24, для локального філіалу достатньо додати маршрут для цього діапазону IP-адрес до пристрою IPsec. Однак для спрощення такого розгортання зазвичай не додаються правила брандмауера для обмеження дозволених підмереж, що може призвести до проблем з безпекою та сумісністю. Якщо маршрути в пристроях IPsec з обох сторін не узгоджені, трафік буде шифруватися лише в одному напрямку, а в іншому передаватися незашифрованим. У найгіршому випадку шлюз IPsec може помилково переспрямувати незашифровані (і потенційно змінені) пакети до локальної мережі.

VPN, засновані на політиках, які охоплюють лише конкретні підмережі, а не всі адреси (0.0.0.0/0), є кращим рішенням і рекомендуються замість VPN, заснованих на маршрутизації, попри додаткові управлінські витрати. Залежно від реалізації, VPN на основі політик може бути складнішими для діагностики, оскільки адміністратору може бути не зовсім очевидно, де саме в IP-стеку пакет передається на обробку підсистемою IPsec. Це може призводити до неочікуваних проблем у конфігураціях типу "зірка".

Наприклад, якщо хост із локальною IP-адресою 10.0.2.1 і публічною IP-адресою 192.0.2.1 створює тунель IPsec до віддаленого хоста з IP 192.0.2.2 для передачі трафіку між підмережами 10.0.2.0/24 і 10.0.0.0/8, такий шлюз IPsec

може втратити доступ до своєї власної локальної мережі. Це відбувається тому, що пакет з призначенням, наприклад, 10.0.2.13, буде направлений через тунель IPsec, оскільки він відповідає діапазону політики IPsec 10.0.0.0/8. VPN на основі маршрутизації не має цієї проблеми, оскільки пакети локальної мережі не проходять через таблицю маршрутизації і знаходять цільовий хост через ARP.

Однією з поширених реалізацій IPsec є обробка пакетів після викликів гачків моніторингу мережі. Це призводить до того, що інструменти діагностики, такі як tcpdump, можуть відображати пакети як незашифровані при їх виході з хоста. Насправді ж пакети шифруються після того, як вони відображені в засобах моніторингу мережі.

2.7 Налаштування брандмауера

Однією з найбільш поширених мережевих проблем під час налаштування IPsec є блокування брандмауером на VPN-сервері або в мережі портів UDP 500 і 4500, що використовуються для IKE. Якщо IPsec-з'єднання працює для простих команд ping, але не функціонує при спробі використання IPsec-з'єднання програмою, ймовірною причиною є неправильне визначення MTU шляху. Хоча ця проблема не є безпосередньо пов'язаною з IPsec, вона часто виникає через додаткові накладні витрати, спричинені використанням заголовка ESP, що збільшує розмір кожного пакету більше за стандартні 1500 байт після додавання заголовка ESP. Унаслідок цього пакети ESP можуть фрагментуватися, і часто маршрутизатори або брандмауери з підтримкою стану помилково відкидають такі пакети.

Проблеми з максимальним розміром сегмента (MSS) можуть виникнути, коли ESP-пакет містить TCP-пакет. Для належної роботи TCP, він має можливість відправляти ICMP-пакети з повідомленням «пакет занадто великий», однак ICMP часто блокується. Деякі політики IPsec дозволяють тільки TCP-пакети і забороняють ICMP-пакети. Це може призвести до ситуації, коли адміністратор може увійти в систему через IPsec-з'єднання за допомогою SSH, але після спроби використовувати цей сеанс з'єднання зависає. Вирішенням цієї проблеми може бути зменшення розміру MTU інтерфейсу IPsec. Для TCP одним із поширених методів є встановлення

меншого розміру TCP MSS, що гарантує, що пакети не перевищать MTU шляху. Цей метод відомий як «затискання TCP MSS». Більшість реалізацій дозволяють також встановлювати фіксоване значення, яке не залежить від виявленого MTU шляху. Зазвичай використовуються фіксовані значення 1340 або навіть 1200 байт.

3. РОЗРОБЛЕННЯ АЛГОРИТМУ РОБОТИ І СТРУКТУРНОЇ СХЕМИ СИСТЕМИ

3.1 Алгоритм шифрування даних

Алгоритм шифрування даних, визначений стандартом ГОСТ 28147-89, є 64-бітовим блочним алгоритмом, що використовує 256-бітовий ключ. Вхідні дані для шифрування розбиваються на блоки довжиною 64 біти, кожен з яких ділиться на два 32-бітові субблоки, позначені як N1 та N2.

Процес обробки субблока N1 включає наступні кроки:

- Вміст субблока N1 поєднується з частиною ключа Kx за допомогою операції додавання за модулем 2^{32} (логічна операція XOR).
- Субблок N1 ділиться на 8 частин по 4 біти. Значення кожної частини замінюється відповідно до заздалегідь визначеної таблиці заміни (S-блоків).
- Отриманий результат піддається побітовому циклічному зсуву вліво на 11 біт.
- Модифікований результат субблока N1 обробляється операцією XOR із значенням субблока N2 (додавання за модулем 2).

На наступному етапі відбувається обмін субблоками: вихідне значення N1 стає новим N2 для наступного раунду, тоді як оброблене значення N1 використовується як новий N1.

Цей процес повторюється задану кількість разів (так звані раунди) — 16 або 32, залежно від режиму роботи алгоритму. Така структура забезпечує стійкість алгоритму до криптографічного аналізу за рахунок багаторазового повторення перетворень.

Ключ та таблиці заміни підлягають певним модифікаціям під час процесу шифрування. Ключ може бути згенерований або введений користувачем з довжиною 256 біт. Перед його застосуванням ключ розбивається на вісім частин по 32 біти кожна. У ході кожного циклу шифрування частини ключа, позначені як K_x, зазнають змін.

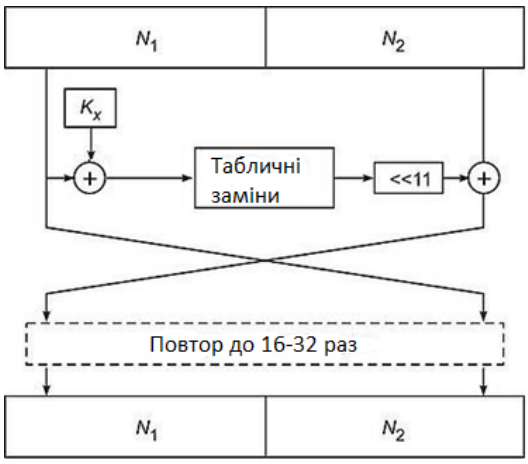


Рисунок 3.1 - Схема алгоритму ГОСТ 28147—89

Наприклад, для режиму простої заміни (докладний опис наведено на наступній сторінці) ключ змінюється таким чином:

- У раундах з 1-го по 24-й послідовність ключів виглядає як: $K_0,K_1,K_2,K_3,K_4,K_5,K_6,K_7,K_0,K_1$.
- У раундах з 25-го по 32-й послідовність ключів реверсується: $K_7,K_6,K_5,K_4,K_3,K_2,K_1,K_0$

Таблиці заміни організовані у блок підстановки, що складається з восьми S-блоків (вузлів заміни), позначених як $S_1,S_2,\ldots,S_8$ кожен з яких має розмір 64 біти. Вхідний субблок N_1 подається на блок підстановки та розбивається на вісім послідовних 4-бітових векторів. Кожен із цих векторів перетворюється у 4-бітовий вихідний вектор за допомогою відповідного вузла заміни S_i.

Вузол заміни можна представити у вигляді таблиці підстановки, яка містить 16 значень 4-бітових двійкових чисел у діапазоні від 000000000000 до 111111111111. Вхідний вектор визначає адресу рядка в таблиці, а число, що знаходиться за цією адресою, виступає вихідним вектором. Після перетворення всі 4-бітові вихідні вектори об'єднуються у 32-бітовий вихідний вектор послідовно.

Таблиця 3.1 Приклад таблиці заміни

Вхідний	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Вихідний	14	4	2	11	7	10	12	13	3	15	1	8	5	0	6	9

Якщо на вхід подається 4-бітний блок зі значенням «1010» (десяткове значення 10), то відповідно до таблиці підстановки вихідне значення буде 1 («0001»). Аналогічно, значення 3 замінюється на 11, а 1 – на 4 і так далі.
Алгоритм ГОСТ 28147-89 передбачає чотири основні режими функціонування:

1. Режим простої заміни;
2. Режим гамування;
3. Гамування зі зворотним зв'язком;
4. Генерація імітовставок.

3.2 Режим простої заміни

У цьому режимі шифрування кожного 64-бітного блоку даних виконується 32 раунди обробки. Підключі розміром 32 біти використовуються в такій послідовності:

- Раунди 1–24: $K_0,K_1,K_2,K_3,K_4,K_5,K_6,K_7,K_0,K_1$;
- Раунди 25–32: $K_7,K_6,K_5,K_4,K_3,K_2,K_1,K_0$

Блоки шифруються незалежно один від одного, і результат обробки кожного блоку визначається виключно його вмістом. Цей режим здебільшого використовується для шифрування ключів. Для шифрування інформації застосовуються інші режими, зокрема гамування та гамування зі зворотним зв'язком.

3.3 Режим гамування

У режимі гамування кожен блок відкритого тексту побітно обробляється операцією додавання за модулем 2 з гамою шифру, що має розмір 64 біти. Гама шифру є послідовністю, яка формується на основі певних операцій із регістрами N_1 та N_2.

Алгоритм роботи в режимі гамування:

1. У регістри N_1 та N_2 записується початкове значення – синхропосилка (64-бітна величина).
2. Зміст регістрів шифрується у режимі простої заміни.

3. Вміст регістра N_1 додається за модулем $2^{32}-1$ з константою $C_1=2^{24}+2^{16}+2^8+4$, а результат записується у регістр N_1.
4. Вміст регістра N_2 додається за модулем 2^{32} з константою $C_2=2^{24}+2^{16}+2^8+1$, а результат записується у регістр N_2.
5. Вміст регістрів N_1 і N_2 виводиться як 64-бітний блок гами шифру (перший блок гами).

Для продовження шифрування решти відкритого тексту процес повторюється, починаючи з кроку 2.

3.4 Режим гамування зі зворотним зв'язком

Режим гамування зі зворотним зв'язком передбачає використання результату шифрування попереднього блоку відкритого тексту для заповнення регістрів N_1 та N_2, починаючи з другого блоку. Таким чином, на відміну від звичайного режиму гамування, де для наступних блоків використовується попередня гама, у цьому випадку вхідні дані для генерації гами залежать від попереднього зашифрованого блоку тексту.

Перший блок гами у режимі зі зворотним зв'язком генерується аналогічно процедурі, що застосовується у стандартному режимі гамування

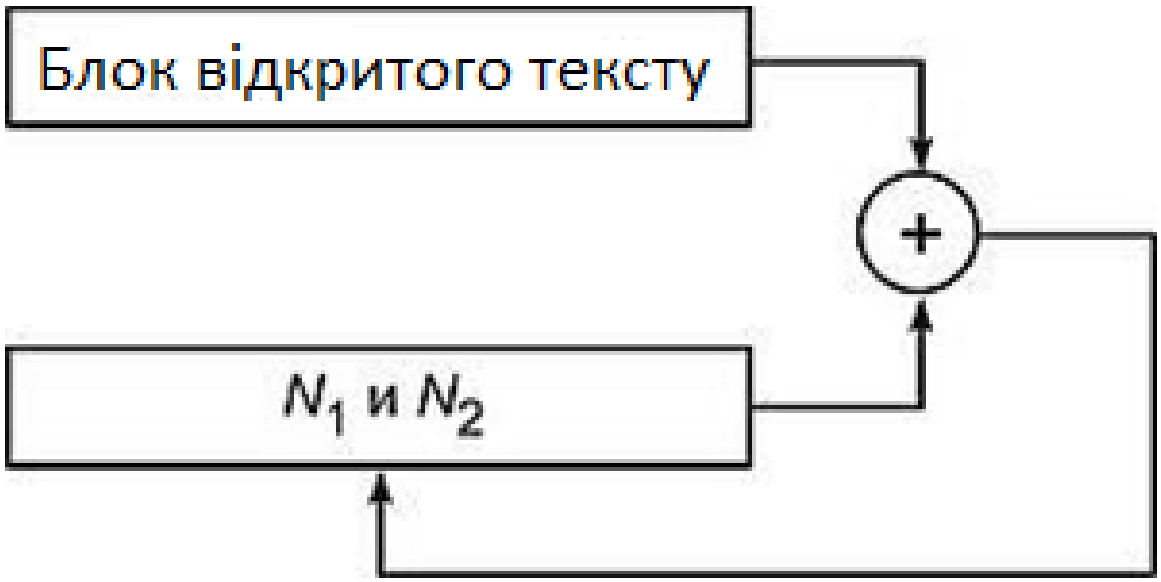


Рисунок 3.2 - Основа алгоритму гамування зі зворотним зв'язком

3.5 Режим генерації імітоприставки

Режим генерації імітоприставки передбачає обчислення криптографічної контрольної суми, яка використовується для перевірки цілісності повідомлень. Обчислення імітоприставки виконується з використанням ключа шифрування, а результатом є 64-бітовий вміст регістрів N_1 та N_2 або їх частина, що і визначається як імітоприставка.

Розмір імітоприставки обирається залежно від необхідного рівня достовірності повідомлення. Зокрема, якщо довжина імітоприставки становить n біт, ймовірність того, що зміна у повідомленні залишиться непоміченою, дорівнює 2^{-n}.

Порядок використання імітоприставки:

1. При шифруванні повідомлення обчислюється імітоприставка для відкритого тексту та надсилається разом із зашифрованими даними (шифртекстом).
2. Після розшифрування отриманого тексту обчислюється нове значення імітоприставки.
3. Порівнюються обчислене значення та отримана разом із повідомленням імітоприставка.
4. Якщо значення не збігаються, це вказує на спотворення шифртексту під час передачі або на використання неправильного ключа для розшифрування.

Схема алгоритму для генерації імітоприставки ґрунтується на режимі простої заміни.

На основі запропонованого алгоритму функціонування пристрою та відповідної структурної схеми було розроблено блок шифрування даних, який включає сукупність функціональних компонентів. Кожен із компонентів виконує специфічні функції, необхідні для реалізації процесу шифрування.

Опис функціональних блоків структурної схеми:

1. Блок введення повідомлення. Забезпечує отримання, генерацію або передачу початкового повідомлення, яке підлягає процесу шифрування
2. Блок розбиття повідомлення на 64-розрядні блоки. Виконує сегментацію вихідного повідомлення на блоки по 64 біти для подальшої обробки.

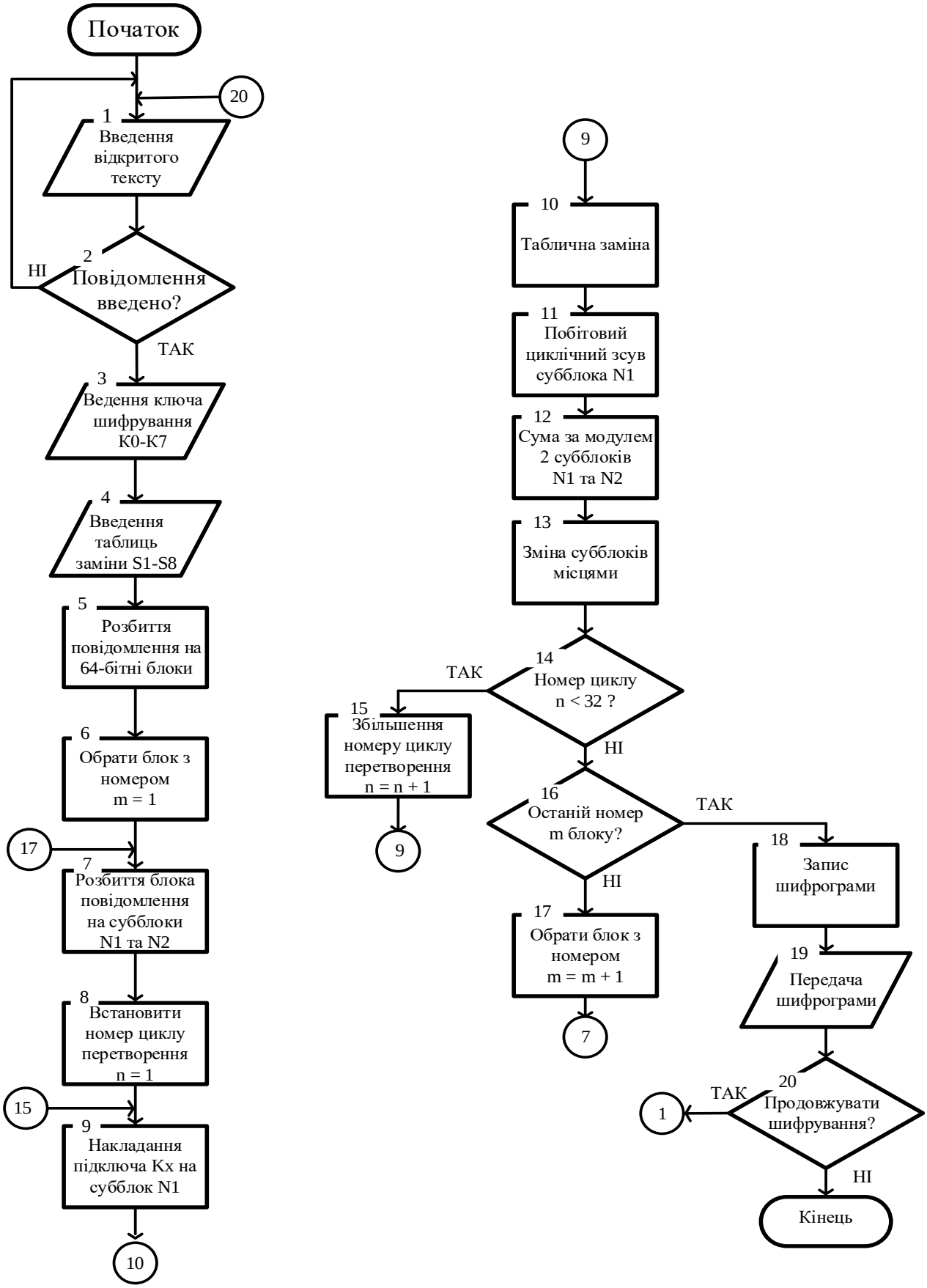


Рисунок 3.3 - Алгоритм роботи блоку шифрування даних в лічильнику

3. Блок розділення 64-розрядного блоку на 32-розрядні субблоки. Розбиває кожен 64-бітовий блок на два 32-бітові субблоки, позначені як N_1 таN_2.
4. Суматор за модулем 2^{32}. Реалізує операцію додавання за модулем 2^{32} між субблоком N_1 та частиною ключа K_x, обраного відповідно до поточного циклу шифрування.
5. Блок введення ключа шифрування. Виконує генерацію або завантаження 256-бітового ключа шифрування, який ділиться на вісім 32-бітових частин $K_0,K_1,...,K_7$, необхідних для процесу шифрування.
6. Блок введення таблиць заміни. Забезпечує створення або завантаження восьми таблиць заміни (S-блоків), позначених як $S_1,S_2,...,S_8$.
7. Блок табличної заміни 4-бітових частин проміжної шифрограми. Виконує табличну заміну кожного 4-бітового сегмента оброблюваного субблока відповідно до відповідного S-блока.
8. Регістр побітового циклічного зсуву субблока N_1. Здійснює побітовий циклічний зсув субблока N_1 вліво на 11 позицій.
9. Суматор блоків N_1 та N_2 за модулем 2. Реалізує побітове додавання за модулем 2 між субблоками N_1 та N_2.

Запропонована структурна схема забезпечує поетапну реалізацію алгоритму шифрування відповідно до стандарту ГОСТ 28147-89. Вона оптимізує виконання обчислювальних операцій на кожному етапі шифрування, що сприяє ефективній обробці даних і гарантує відповідність вимогам щодо інформаційної безпеки.

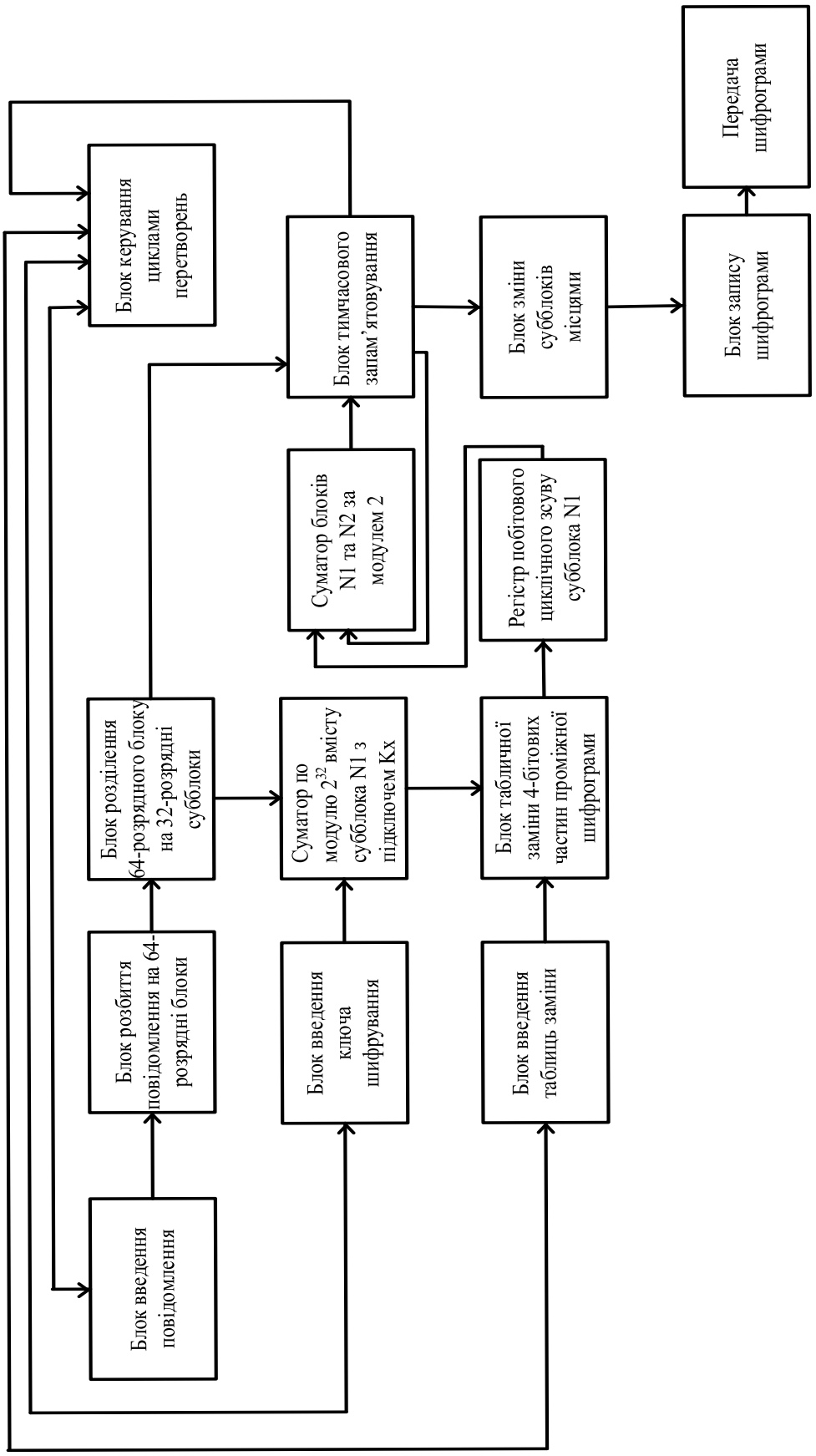


Рисунок 3.4 - Блок шифрування даних в лічильнику.

4. РОЗРОБКА СХЕМИ ЕЛЕКТРИЧНОЇ ПРИНЦИПОВОЇ ЛІЧИЛЬНИКА ЕЛЕКТРОЕНЕРГІЇ

4.1 Система на кристалі - System-on-a-Chip

Система на кристалі (СнК), однокристальна система (англ. System-on-a-Chip, SoC) електронна схема, що виконує функції цілого пристрою (наприклад, лічильника електроенергії) і розміщена на одній інтегральній схемі.

Залежно від призначення вона може оперувати як цифровими сигналами, так і аналоговими, аналого-цифровими, а також частотами радіодіапазону. Як правило, застосовуються в портативних і вбудованих системах.

Типова SoC містить:

- один або кілька мікроконтролерів, мікропроцесорів або ядер цифрової обробки сигналів (DSP). SoC, що містить кілька процесорів, називають многопроцессорной системою на кристалі (MPSoC);
- банк пам'яті, що складається з модулів ПЗУ, ОЗУ, ППЗУ або флеш;
- джерела опорної частоти, наприклад, кварцові резонатори і схеми ФАПЧ (фазового автопідстроювання частоти);
- таймери, лічильники, ланцюги затримки після включення;
- блоки, які реалізують стандартні інтерфейси для підключення зовнішніх пристроїв: USB, FireWire, Ethernet, USART, SPI;
- блоки цифро-аналогових та аналого-цифрових перетворювачів;
- регулятори напруги і стабілізатори живлення.

У програмовані SOC часто входять також блоки програмованих логічних матриць - ПЛМ, а в програмовані аналого-цифрові SOC - ще і програмовані аналогові блоки.

Блоки можуть бути з'єднані за допомогою шини власної розробки або стандартної конструкції, наприклад, AMBA [1] в чіпах компанії ARM. Якщо в складі чіпа є контролер прямого доступу до пам'яті (ПДП), то з його допомогою можна заносити дані з великою швидкістю з зовнішніх пристроїв безпосередньо в пам'ять чіпа.

Для функціонування системи програмне забезпечення не менш важливо, ніж апаратне. Розробка, як правило, ведеться паралельно. Апаратна частина

збирається зі стандартних налагоджених блоків, для складання програмної частини використовуються готові налаштування відповідних блоків, що реалізують необхідні процедури і функції, які в англомовній літературі часто називаються драйверами. Застосовуються засоби автоматизації розробки CAD та інтегровані програмні оболонки.

Для того, щоб упевнитися в правильній роботі створеної комбінації блоків, драйвери і програму завантажують в емулятор апаратної частини (мікросхему з програмованими ланцюгами, FPGA). Також потрібно задати розташування блоків і розробити міжблочні зв'язку.Перед здачею в виробництво апаратна частина тестується на коректність з використанням мов Verilog і VHDL, а для більш складних схем - SystemVerilog, SystemC, e і OpenVera. До 70% загальних зусиль на розробку витрачається саме на цьому етапі.

Системи на кристалі споживають менше енергії, коштують дешевше і працюють надійніше, ніж набори мікросхем з тією ж функціональністю. Менша кількість корпусів спрощує монтаж. Проте, проектування і налагодження однієї великої і складної системи на кристалі виявляється дорожчим процесом, ніж серії з маленьких.

4.2 Системи на кристалі компанії Maxim для лічильників електроенергії і систем моніторингу

З метою скорочення часу виведення нових виробів на ринок і зниження їх вартості, виробники лічильників електроенергії постійно підвищують вимоги до рівня інтеграції IC. Інноваційна архітектура систем на кристалі компанії Maxim для лічильників електроенергії і систем моніторингу забезпечує кращі в класі метрологічні і точності характеристики при мінімальній вартості. Спочатку ці мікросхеми випускалися компанією Teridian, яка була заснована в 1972 р під ім'ям Silicon Systems. У 1996 році вона увійшла до складу корпорації TDK і була відома як TDK Semiconductor Corp. У 2005 р компанія знову здобула самостійність і отримала нове ім'я - Teridian Semiconductor Corp. У травні 2010 р компанія була придбана компанією Maxim Integrated Products, Inc.

4.3 Огляд архітектури ІС для лічильників електроенергії

Мікросхеми Maxim для застосування в інтелектуальних лічильниках електроенергії, такі як «Система-на-кристалі» (SoC - system-on-chip), що містить в собі всі функціональні блоки, необхідні для побудови лічильника: аналогову частину, два процесорних ядра, датчик температури, годинник реального часу, драйвер РКІ, два UART'а , апаратний сторожовий таймер і т.д. Схематично архітектура системи-на-кристалі зображена на рис. 4.1.

Рисунок 4.1 - Архітектура системи-на-кристалі Maxim для лічильників електроенергії

4.4 Порівняльні характеристики ІС першого-третього поколінь для лічильників електроенергії

Аналогова частина складається з вхідного мультиплексора, здійснює комутацію вхідних сигналів, і одного 22-розрядного дельта-сигма АЦП, який здійснює дискретизацію вхідних сигналів. Дане архітектурне рішення запатентовано компанією Teridian під назвою "Single Converter TechnologyTM" і відрізняється від конкуруючих рішень із застосуванням декількох паралельних АЦП для оцифровки вхідних сигналів. Кількість комутованих мультиплексором сигналів залежить від застосування ІС в 1-фазному або 3-фазному лічильнику (від 3 до 7).

Далі вибірки АЦП в цифровому вигляді обробляються спеціалізованим 32-розрядних цифровим сигнальним процесором (так званим "Compute Engine" або CE), який робить всі обчислення метрологічних параметрів - напруги,

струму, активної і реактивної енергії, частоти відповідно до програми в флеш-пам'яті . Другим обчислювальним вузлом є стандартний мікроконтролер 8051-архітектури (один такт на інструкцію) з супутньою периферією, необхідної для побудови інтелектуального лічильника електроенергії (годинник реального часу, драйвер РКІ, лінії введення-виведення, два UART'а, флеш-пам'ять, датчик температури, схеми управління батареєю і ін.). Крім метрологічної інформації Compute Engine генерує службові переривання, а також може передавати інформацію про пропажу або «просідання» вхідних напруг.

Дана архітектура є досить універсальною і дозволяє з мінімальними витратами здійснювати адаптацію відповідно до вимог споживача. Причому метрологічна частина може бути переконфігурувати в разі, якщо у замовника виникають специфічні вимоги (наприклад, розрахунок гармонійних складових струму, напруги або енергії).

Перевагами даної архітектури є:

- мінімальна вартість системи завдяки використанню системи-на-кристалі (мінімізовані як перелік додаткових зовнішніх компонентів, так і займана площа друкованої плати).
- мінімальні вартість розробки і час виходу на ринок (повністю програмована платформа, багатий набір периферії).
- мінімальний ризик розробки (програмовані метрологічні алгоритми, широкий динамічний діапазон, різні опції розміру вбудованої флеш-пам'яті програм від 8 кбайт до 256кбайт).
- кращі в класі метрологічні і точності характеристики (залежність від температури і навантаження, програмовані механізми компенсації нелінійності датчиків).

На рис. 4.2 представлено сімейство мікросхем для лічильників електроенергії, що включає в себе як уже випускаються продукти, так і розробляються компанією в даний час.

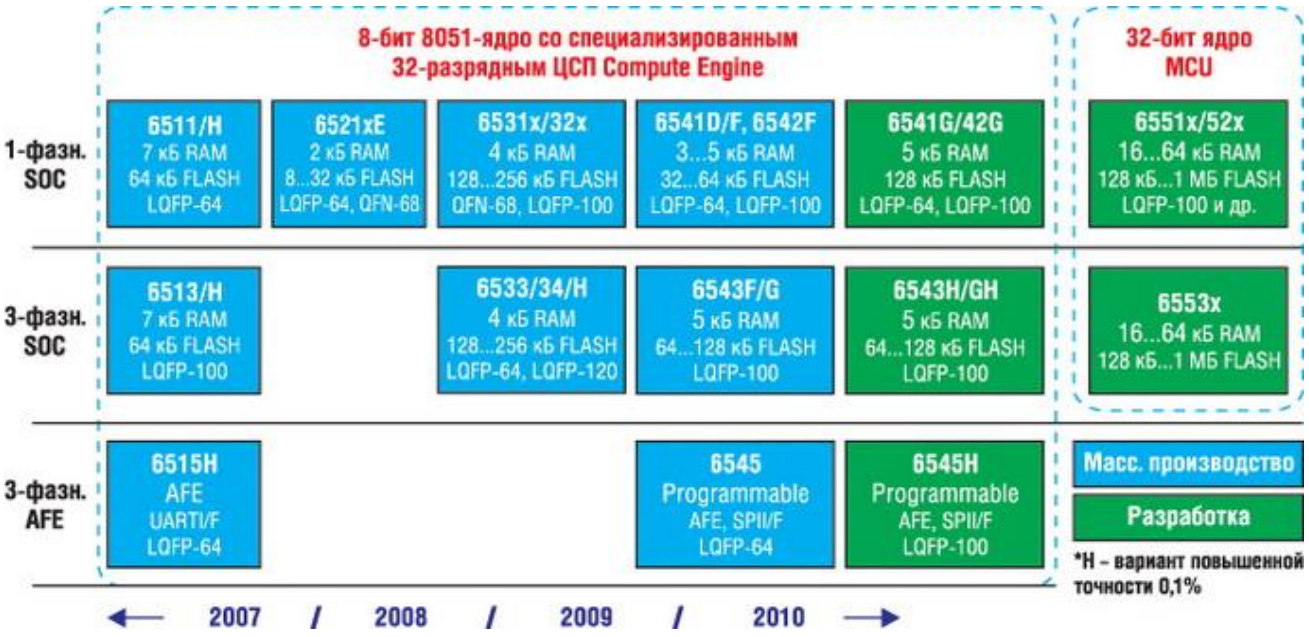


Рисунок 4.2 - IC для лічильників електроенергії компанії Maxim

Їх поділяють на покоління, всередині кожного з яких IC мають подібну структуру, відрізняючись незначними параметрами функціональних блоків. Розглянемо IC кожного покоління окремо.

1-е покоління

71M6511 / H, 71M6513 / H. Дані IC, виробництво яких почалося ще в 2005 р, є базові системи-на-кристалі для побудови інтелектуального лічильника середнього рівня (71M6511 / H - однофазного, 71M6513 / H - трифазного).

2-е покоління

71M6521BE / DE / FE. IC 2-го покоління призначені для побудови однофазних інтелектуальних лічильників економ-класу. Пропонується кілька опцій цієї IC з різним обсягом флеш-пам'яті починаючи з 8 кбайт (71M6521BE, без RTC), 16 кбайт (71M6521DE) і закінчуючи 32 кбайт (71M6521FE)

3-е покоління

71M6531D / F, 71M6532D / F (для однофазних додатків) і 71M6533 / H, 71M6534 / H (для трифазних додатків).IC 3-го покоління є подальший розвиток в сторону доповнення функціональності лічильників за рахунок збільшеного обсягу флеш-пам'яті (128 ... 256 кбайт), можливості використання PKI з великою кількістю сегментів (див. Табл. 1) або управління великим

числом периферійних пристроїв

Фукціональні особливості мікросхем 4-го покоління

В даний час ІС 4-го покоління 71M654x вже запущені в масове виробництво. Ці ІС призначені для побудови бюджетних інтелектуальних лічильників електроенергії, так і лічильників середнього і високого рівня. При розробці цих ІС був врахований значний досвід і побажання споживачів, накопичені в ході реалізації проектів на базі ІС перших трьох поколінь. В ІС 4-го покоління реалізована революційна технологія, що дозволяє побудувати лічильник електроенергії із застосуванням шунтів замість традиційно використовуваних трансформаторів струму або котушок Роговского.

Зразки мікросхем 4-го покоління, а також демонстраційні плати для оцінки параметрів рішення та прискорення циклу розробки доступні для замовлення. Вже розпочато роботу по розробці ІС 5-го покоління, призначених для високоінтелектуальних лічильників електроенергії найвищого рівня і з підтримкою різних інтерфейсів передачі даних із зовнішніми пристроями збору (DLMS, SFSK, TCP / IP та ін.).

З метою прискорення розробки та оцінки технічних рішень, пропонованих компанією, випускаються демонстраційні плати, що представляють собою практично готовий лічильник електроенергії, який можна використовувати як основу для побудови власної розробки.

Системи-на-кристалі компанії Maxim є основою для побудови інтелектуальних лічильників електроенергії різного рівня, починаючи з бюджетного побутового лічильника електроенергії і закінчуючи промисловим лічильником високого класу точності (0,2%). Однокристальні рішення з широким набором периферії, повністю цифровою і реконфігурованою метрологічної частиною, забезпечує мінімальний час реалізації проекту при низькій вартості пристрою. Завдяки нововведенням, ІС 4-го покоління надають більше функціональних можливостей при розробці лічильників електроенергії, а також, при одночасному зниженні вартості рішення.

4.5 Створення електричної принципової схеми лічильника

На основі схеми електричної структурної побудована схема електрична функціональна, максимальну гнучкість якої забезпечують порти UART, I2C

порти, компаратор контролю падіння напруги живлення, 5-вольтовий підвищує джерело живлення РК, 22 двонаправлених паралельних портів введення-виведення і програмована «в-системі» FLASH, яка може оновлюватися новими даними або прикладними кодами.

Можливість заміни на FLASH ROM дає значні переваги в вартості мікросхеми. Мікросхема забезпечує підвищену точність вимірювань 0,1% так і стандартну 0,5% для багатофункціональних побутових і комерційних лічильників, що вимагають підвищеного кількість портів вводу-выода і функціонального РКІ індикатора.

Повний внутрісхемний емулятор і засоби для розробника, в комплекті з бібліотекою програм і керівництва з розробки дозволяють прискорити і спростити процедуру конструювання лічильника електроенергії.

У мікросхемах 71M6513 інтегровані всі основні функціональні блоки, необхідні для цифрового вимірювача споживаної електроенергії.

Схема електрична функціональна електронного лічильника наведена на рисунку 4.3.

4.6 Огляд обладнання

Однокристальний багатофазний лічильник 71M6513 інтегрує всі основні функціональні блоки, необхідні для реалізації твердотільного лічильника електроенергії. Мікросхема включає аналоговий інтерфейс (AFE), 8051-сумісний мікропроцесор (MPU), що виконує одну інструкцію за такт (80515), незалежний 32-розрядний механізм цифрових обчислень (CE), джерело опорної напруги, датчик температури, драйвери РК-дисплеїв, оперативну пам'ять, флеш-пам'ять, годинник реального часу (RTC) та різноманітні контакти для введення/виведення. Пристрій підтримує різні технології датчиків струму, зокрема трансформатори струму (CT), резистивні шунти та котушки Роговського.

Мікросхема 71M6513 містить кілька периферійних функцій вводу/виводу, що покращують функціональність пристрою та зменшують кількість компонентів у більшості застосувань лічильника. До периферійних пристроїв вводу/виводу відносяться два UART, цифровий вхід/вихід, входи компаратора, драйвери РК-дисплеїв, інтерфейс I2C та оптичний/ІЧ-інтерфейс.

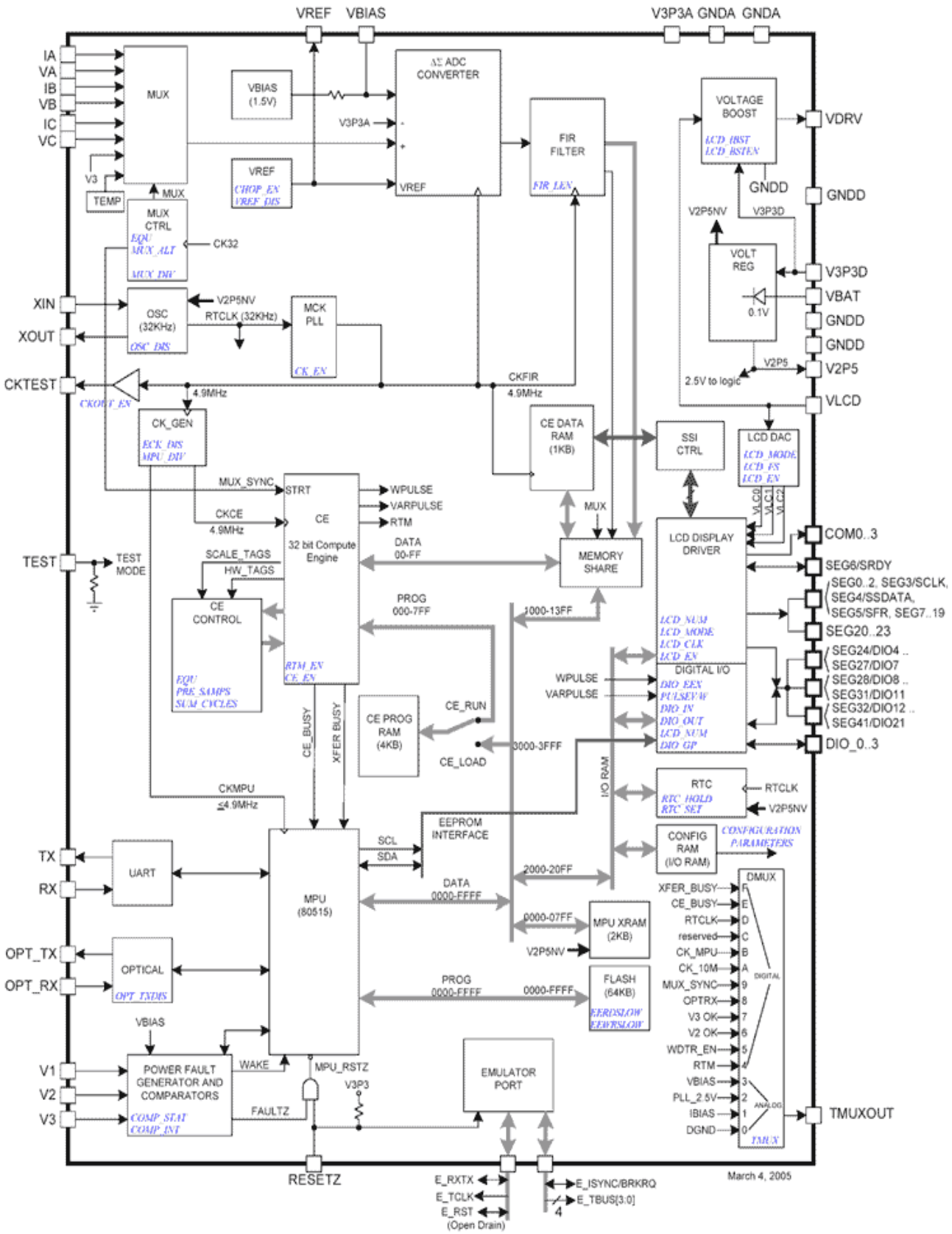


Рисунок 4.3 – Схема електрична функціональна електронного лічильника

Один із двох внутрішніх UART (UART1) адаптований для підтримки інфрачервоного світлодіода, має внутрішній вихід приводу та сенсорний вхід, але також може функціонувати як стандартний UART.

4.7 Аналоговий інтерфейс (AFE)

Аналоговий інтерфейс (AFE) мікросхеми 71M6513 для вимірювання потужності складається з вхідного мультиплексора, дельта-сигма аналого-цифрового перетворювача з опорною напругою, за яким слідує фільтр FIR.

Мультиплексор

Вхідний мультиплексор підтримує вісім вхідних сигналів, які подаються на контакти IA, VA, IB, VB, IC, VC та V3, а також вихід внутрішнього датчика температури. Мультиплексор може працювати в двох режимах:

- Під час нормального циклу вибираються сигнали з шести контактів IA, VA, IB, VB, IC та VC.
- Під час альтернативного циклу вибираються сигнали температури (TEMP) та додатковий вхід монітора, V3, а також інші джерела сигналу, зазначені в таблиці 1.

Альтернативні цикли мультиплексора зазвичай виконуються рідко (близько кожної секунди). Водночас VA, VB і VC не замінюються в альтернативних циклах мультиплексора.

Таблиця 4.1 - Входи, вибрані в регулярних і альтернативних циклах мультиплексора

Мультиплексорний стан регулярної послідовності мультиплексора:						Стан мультиплексора альтернативної послідовності мультиплексора:					
0	1	2	3	4	5	0	1	2	3	4	5
IA	VA	IB	VB	IC	VC	ТЕМП	VA	V3	VB	IC	VC

У типовому використанні входи IA, IB та IC підключаються до трансформаторів струму, що визначають струм на кожній фазі лінійної напруги. Вхідні сигнали VA, VB та VC зазвичай підключаються до датчиків напруги через резисторні дільники. Керування мультиплексором здійснюється через схему керування, яка регулює налаштування мультиплексора.

Функціонування цієї схеми контролюється регістрами оперативної пам'яті введення/виведення, що визначають кількість проб за цикл. Вона може опитувати 2, 3, 4 або 6 станів мультиплексора за один цикл.

V3

V3 є додатковим аналоговим входом монітора, який можна використовувати для вимірювання аналогових величин, таких як струм нейтралі. Цей вхід вибирається під час виконання альтернативного циклу мультиплексора. Нульовим посиланням для входу V3 є VBIAS. Сигнал V3 також подається до блоку компаратора, де порівнюється з VBIAS. Переривання компаратора повинні бути відключені, коли вхід V3 використовується для аналогових вимірювань

Функціональний опис AFE

AFE функціонує як система збору даних, що керується MPU. Основні сигнали (IA, VA, IB, VB, IC, VC) зчитуються, і отримані показники АЦП зберігаються в оперативній пам'яті RAM CE, до яких має доступ як CE, так і MPU, якщо це необхідно. Альтернативні цикли мультиплексора ініціюються MPU рідше для доступу до повільних сигналів, таких як температура та V3.

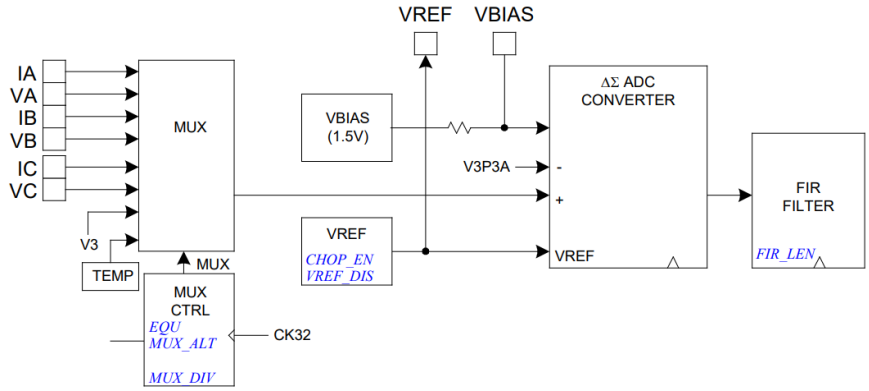


Рисунок 4.4 - Блок-схема AFE

Обчислювальний механізм (CE)

Обчислювальний механізм (CE) являє собою спеціалізований 32-розрядний процесор архітектури RISC, що виконує точні обчислення, необхідні для високоточного вимірювання енергії. Основні функції та процеси, що здійснюються CE, включають:

- Множення кожної вибірки струму на відповідну вибірку напруги для

отримання енергетичного значення на одну вибірку, за умови постійного часу вибірки.

- Компенсацію затримки, яка не залежить від частоти, на всіх шести каналах, що дозволяє врахувати затримки між вибірками, спричинені мультиплексуванням.
- Використання фазозрушителя на 90° для обчислень реактивної потужності (VAR).
- Генерацію імпульсів.
- Моніторинг частоти вхідного сигналу, що дає інформацію про фазу та частоту.
- Виявлення амплітудних коливань вхідного сигналу для визначення можливих провисань.
- Масштабування оброблених зразків з урахуванням температури мікросхеми (температурна компенсація) та коефіцієнтів калібрування для забезпечення точності вимірювань.

Таблиця 4.2 - Розташування DRAM CE для результатів АЦП

Адреса	Ім’я	Zero Reference	Опис
0x00	IA	V3P3	Струм фази A
0x01	VA	V3P3	Напруга фази A
0x02	IB	V3P3	Струм фази B
0x03	VB	V3P3	Напруга фази B
0x04	IC	V3P3	Струм фази C
0x05	VC	V3P3	Напруга фази C
0x06	ТЕМП	VBIAS	Температура
0x07	V3	VBIAS	Монітор V3

4.8 Ядро 80515 MPU

Мікросхема 71M6513/6513H містить процесор 80515 MPU (8-розрядний, сумісний з 8051), який виконує більшість інструкцій за один такт.

Використання тактової частоти 5 МГц забезпечує пропускну здатність обробки до 5 MIPS. Архітектура 80515 дозволяє усунути надмірні стани шини та реалізує паралельне виконання фаз вибірки та обробки. Як правило, машинний цикл синхронізовано з вибіркою з пам’яті, що дозволяє виконувати більшість 1-байтових інструкцій за один цикл. Це сприяє 8-кратному підвищенню продуктивності (з точки зору MIPS) порівняно з процесором Intel 8051, що працює на тій же тактовій частоті. Тактову частоту процесора можна налаштувати в залежності від вимог програми за допомогою регістра RAM вводу/виводу MPU_DIV [2:0]. Для спрощення циклу проєктування доступна стандартна бібліотека програмного інтерфейсу на основі ANSI C для 80515, що включає функції для вимірювань та розрахунків на основі результатів, наданих внутрішнім 32-розрядним обчислювальним механізмом (CE).

4.9 Організація пам'яті

Ядро 80515 MPU використовує гарвардську архітектуру з окремими просторами для коду та даних. Структура пам’яті в 80515 подібна до стандарту 8051. Пам’ять розділена на три основні області: програмну пам’ять (флеш-пам’ять), зовнішню пам’ять даних (XRAM), яка фізично складається з XRAM, CE DRAM, CE PRAM і I/O RAM, а також внутрішню пам'ять даних (Internal RAM).

Внутрішня та зовнішня пам'ять даних

І внутрішня, і зовнішня пам’ять даних фізично розташовані на мікросхемі 71M6513. Зовнішня пам'ять даних є зовнішньою лише для ядра 80515 MPU, яке використовує її як доповнення до внутрішньої пам’яті.

Пам'ять програми

Процесор 80515 може адресувати до 64 Кбайт програмної пам'яті в межах адресного простору від 0x0000 до 0xFFFF. Пам'ять програм зчитується в процесі отримання інструкцій MPU або виконання операції MOVC. Після скидання MPU починає виконання програми з початкового адресного простору 0x0000. У нижній частині програмної пам'яті містяться вектори скидання та переривань, при цьому вектори переривань мають інтервал у 8 байтів, починаючи з адреси 0x0003.

Таблиця 4.3 - Карта пам'яті

0xFFFF	Флеш-пам'ять
0x0000	
Програмна пам'ять	

0xFFFF	
0x4000	
0x3FFF	CE PRAM
0x3000	
0x2FFF	
0x2100	
0x20FF	I/O RAM
0x2000	
0x1FFF	
0x1400	
0x13FF	CE DRAM
0x1000	
0x0FFF	
0x0800	
0x07FF	XRAM
0x0000	
Зовнішня пам'ять даних	

0xFF	SFRs, RAM, reg. banks
0x00	
Внутрішня пам'ять даних	

Зовнішня пам'ять даних

Процесор 80515 здатен адресувати до 64 Кбайт зовнішньої пам'яті даних у межах адресного простору від 0x0000 до 0xFFFF. Однак фізична пам'ять є доступною лише в деяких діапазонах адрес, зазначених на малюнку 3. Доступ до зовнішньої пам'яті відбувається під час виконання інструкцій MOVX @Ri, A або MOVX @DPTR, A, коли MPU записує дані в пам'ять.

Внутрішня пам'ять даних

Внутрішня пам'ять даних надає 256 байт пам'яті, адресованої в діапазоні від 0x00 до 0xFF. Адресація внутрішньої пам'яті даних здійснюється за допомогою 1 байта, що дозволяє доступ як через пряму, так і через непряму адресацію. Верхні 128 байт цієї пам'яті займають регістри спеціальних функцій (SFR), доступ до яких можливий лише через пряму адресацію. Нижні 128 байт містять робочі регістри та пам'ять з бітовою адресацією. Перші 32

байти формують чотири банки по вісім регістрів (R0-R7), де вибір активного банку здійснюється за допомогою двох бітів стану пам'яті програми (PSW). Наступні 16 байт представляють блок пам'яті з бітовою адресацією в діапазоні адрес 0x00-0x7F. Всі байти в межах нижніх 128 байт доступні як через пряму, так і через непряму адресацію.

Таблиця 4.4 - Карта внутрішньої пам'яті даних

Адреса	Пряма адресація	Непряма адресація
0xFF	Регістри спеціальних функцій (SFR)	ОЗУ
0x80		
0x7F	Байтово-адресована область	
0x30		
0x2F	Бітово-адресована область	
0x20		
0x1F	Комірки регістра R0…R7	
0x00		

4.10 UART

Мікросхема 71M6513 містить UART (UART0), який може бути налаштований для взаємодії з різними модулями AMR, а також другий UART (UART1), що підключається до оптичного порту.

UART є спеціалізованим 2-провідним послідовним інтерфейсом, здатним здійснювати обмін даними з зовнішнім хост-процесором зі швидкістю до 38 400 біт/с при тактовій частоті MPU, рівній 1,2288 МГц.
Мікросхема 71M6513 має кілька регістрів, що забезпечують керування і буферизацію послідовних даних для UART. Один із цих регістрів спеціальних функцій (SFR) виконує роль буфера як для передавання, так і для прийому даних. Обидва UART можуть одночасно передавати і отримувати інформацію.

Таблиц 4.5 - Генерація швидкості передачі даних

	Використання таймера 1	Використання внутрішнього генератора швидкості передачі даних
Послідовний інтерфейс 0	$2^{smod} * f_{CKMPU}/ (384 * (256-TH1))$	$2^{smod} * f_{CKMPU}/(64 * (2^{10}-S0REL))$
Послідовний інтерфейс 1	N/A	$f_{CKMPU}/(32 * (2^{10}-S1REL))$

Таблиця 4.6 - Режими UART

	UART 0	UART 1
Режим 0	N/A	Стартовий біт, 8 біт даних, парність, стоп-біт, змінна швидкість передачі (внутрішній генератор швидкості передачі)
Режим 1	Початковий біт, 8 біт даних, стоп-біт, змінна швидкість передачі (внутрішня передача даних). генератор швидкості або таймер 1)	Початковий біт, 8 біт даних, стоп-біт, змінна швидкість передачі даних (генератор внутрішньої швидкості передачі даних
Режим 2	Стартовий біт, 8 біт даних, парність, стоп-біт, фіксована швидкість передачі даних 1/32 або 1/64 від $f_{ЦКМПУ}$	N/A
Режим 3	Стартовий біт, 8 біт даних, парність, стоп-біт, змінна швидкість передачі (внутр генератор швидкості або таймер 1)	N/A

Регістр WDCON визначає, чи використовуватиметься для передачі таймер 1 або внутрішній генератор швидкості передачі даних. Усі передачі

через UART налаштовуються для підтримки парності, паритету, а також для використання двох або одного стоп-біта, а також параметрів XON/XOFF для регулювання змінної швидкості передачі даних у діапазоні від 300 до 38400 біт/с.

Переривання

Мікросхема 80515 підтримує 11 джерел переривань, які організовані в чотири рівні пріоритету. Кожне джерело переривання має відповідний прапор запиту, розміщений у спеціальних функціональних регістрах (TCON, IPKOH, iSCON). Переривання, що активується відповідним прапором, може бути окремо ввімкнене або вимкнене за допомогою бітів дозволу в регістрах SFRIEN0, IEN1 і IEN2. Зовнішні переривання відносяться до тих, що надходять від компонентів, розташованих поза ядром 80515, тобто сигнали, що постають із інших частин мікросхеми 71M6513/6513H, таких як інтерфейси CE, DIO, RTC, EEPROM або компаратори.

4.11 Ресурси на чіпі

Порти DIO

Мікросхема 71M6513/6513H містить до 22 контактів для цифрового вводу/виводу загального призначення. 18 з цих контактів мають подвійну функцію і можуть бути налаштовані для використання як драйвери для LCD. Після скидання або включення живлення всі контакти DIO спочатку працюють як входи, поки їх не налаштують для необхідного напрямку. Напрямок роботи виводів контролюється за допомогою регістрів DIO та DIO_DIR (SFR), а також п’яти бітів у регістрі введення/виведення LCD_NUM (0x2020[4:0]).

Флеш-пам'ять

Мікросхема 71M6513 містить 64 КБ вбудованої флеш-пам'яті, що використовується для зберігання програмного коду MPU. Зазвичай вона також включає зображення програмного коду CE, коефіцієнтів CE, RAM MPU та RAM вводу/виводу. Під час увімкнення, перед активуванням CE, MPU має скопіювати ці зображення у відповідні області пам'яті.

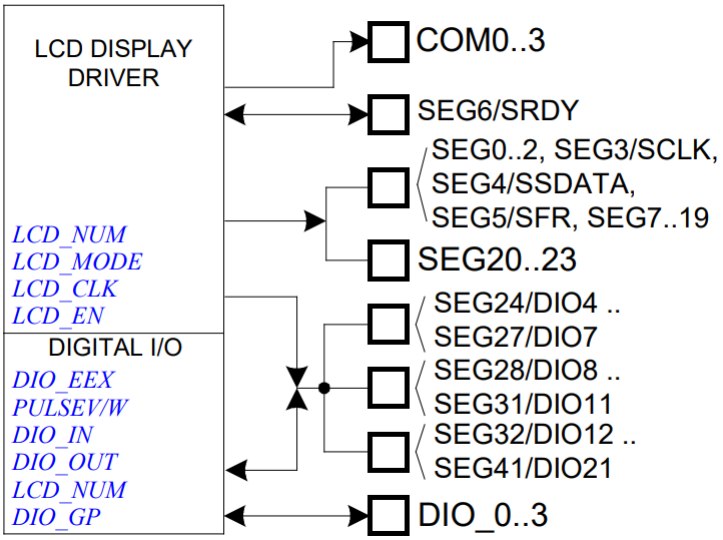


Рисунок 4.5 - Блок-схема портів DIO

Фізична пам'ять

Таблиця 4.7 - Карта пам'яті даних MPU

Адреса	Пам'ять	Тип пам'яті	Типове використання	Стани очікування	Розмір пам'яті
0000-FFFF	Флеш-пам'ять	Енергонезалежний	Програмні та енергонезалежні дані	0	64кБ
0000-07FF	Статична RAM	Батарейний буфер	ОЗП даних MPU	0	2 кБ
1000-13FF	Статична RAM	Енергозалежний	дані CE	5	1 кБ
2000-20FF	Статична RAM	Енергозалежний	I/O RAM	0	256 кБ
3000-3FFF	Статична RAM	Енергозалежний	Програмний код CE	5	4 кБ

MPU RAM

Мікросхема 71M6513 містить 2 КБ статичної оперативної пам'яті на кристалі (XRAM), яка підтримується акумулятором, а також 256 байт внутрішньої пам'яті даних у ядрі MPU. Зазначені 2 КБ статичної пам'яті використовуються для зберігання даних під час виконання звичайних операцій MPU.

CE DRAM / CE PRAM

CE DRAM — це пам'ять даних CE, що служить основним засобом передачі даних між MPU та CE. MPU може як зчитувати, так і записувати в CE DRAM.

CE PRAM — це програмна пам'ять CE, яка повинна бути завантажена програмним кодом CE перед початком його роботи. MPU не має доступу до CE PRAM під час роботи CE.

Осцилятор

Генератор мікросхеми 71M6513 керує стандартним кристалом годинника з частотою 32,768 кГц. Цей генератор розроблений спеціально для роботи з кварцовими кристалами і сумісний із їх високим імпедансом та обмеженою потужністю. Він має дуже низьку потужність розсіювання, що дозволяє максимально подовжити термін служби акумуляторів, підключених до контакту VBAT.

Годинник реального часу (RTC)

RTC працює безпосередньо від кварцевого генератора. У разі відсутності джерела живлення 3,3 В, RTC отримує енергію від зовнішньої батареї, підключеної до контакту VBAT. RTC складається з ланцюга лічильників, що вимірюють секунди, хвилини, години, день тижня, день місяця, місяць і рік. Він здатний обробляти високосні роки, причому кожен лічильник має свій вихідний регістр.

Драйвери LCD

Мікросхема 71M6513 містить 24 спеціалізовані драйвери для РК-сегментів, а також 18 багатоцільових контактів, які можуть бути налаштовані як додаткові драйвери для РК-сегментів. Мікросхема здатна керувати РК-дисплеєм з роздільною здатністю від 96 до 168 пікселів із робочим циклом 25%. З дисплеєм, що має сім сегментів на цифру, можна реалізувати відображення від 13 до 24 цифр.

Схема підвищення напруги для РК-дисплея

Схема підвищення напруги дозволяє генерувати 5 В з джерела живлення 3,3 В для живлення малопотужних пристроїв, таких як РК-дисплеї. При активації за допомогою регістра RAM вводу/виводу LCD_BSTEN (0x2020[7]), схема підсилення забезпечує необхідну напругу на вихідному контакті VDRV.

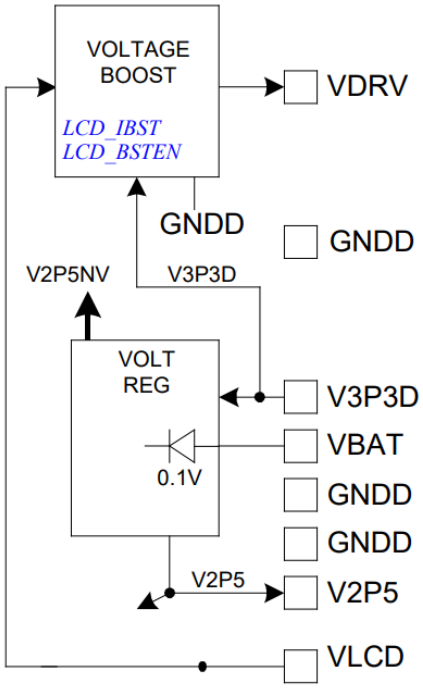


Рисунок 4.6 Схема підвищення напруги РК-дисплея

UART (UART0) і оптичний порт (UART1)

Мікросхема 71M6513/6513H оснащена інтерфейсом для реалізації інфрачервоного порту або оптичного порту. Вивід OPT_TX використовується для безпосереднього керування зовнішнім світлодіодом для передачі даних через оптичний канал (низькоактивний). Вивід OPT_RX, також низькоактивний, відповідає за прийом сигналів від зовнішнього фотодетектора, який використовується як приймач для оптичного зв'язку. Ці два виводи підключені до спеціального порту UART. Вивід OPT_TX може бути тристандартним для мультиплексування іншого контакту вводу-виводу на вихід OPT_TX. Керування виходом OPT_TX здійснюється за допомогою біта регістра RAM вводу/виводу OPT_TXDIS (0x2008 [5]).

Механізми апаратного скидання

Існує кілька умов, які можуть спричинити апаратне скидання мікросхеми 71M6513/6513H:

- Низька напруга на контакті RESETZ
- Низька напруга на виводі E_RST
- Напруга на контакті V1 нижче порогу скидання (VBIAS)
- Виявлення несправності кристала за допомогою монітора частоти кристала
- Апаратний сторожовий таймер

Внутрішні годинники та дільники годинників

Усі внутрішні годинники базуються на частоті кристала годинника (CK32 = 32,768 Гц), що застосовується до контактів XIN і XOUT. ФАПЧ (фазово-амплітудна частотна модуляція) збільшує цю частоту до 4,9152 МГц. Ця частота використовується для АЦП, FIR-фільтра (CKFIR), тестового виходу синхронізації (CKTEST), CE DRAM і тактового генератора. Тактовий генератор забезпечує два тактових сигнали: один для MPU (CKMPU) та інший для CE (CKCE). Тактова частота MPU визначається за допомогою регістра RAM вводу/виводу MPU_DIV (0x2004[2:0]) і може бути виражена як CE*2-MPU_DIV Гц, де MPU_DIV змінюється в межах від 0 до 7 (MPU_DIV дорівнює 0 після увімкнення). Це дає змогу змінювати тактову частоту MPU в діапазоні від 4,9152 МГц до 38,4 кГц.

Інтерфейс I2C (EEPROM)

Мікросхема 71M6513/6513H має спеціальний 2-контактний послідовний інтерфейс, який реалізує драйвер I2C для зв'язку із зовнішніми пристроями EEPROM. Інтерфейс може бути мультиплексований на контакти DIO4 (SCK) і DIO5 (SDA), що встановлюється через регістр RAM вводу/виводу. MPU взаємодіє з інтерфейсом через два регістри SFR: EEDATA (0x9E) і EECTRL (0x9F). Тактова частота послідовної передачі та прийому становить 78 кГц, а сигнал SCL утримується у високому стані до наступної передачі. Однак керувати EEPROM можна і безпосередньо через контакти DIO4 і DIO5, хоча це не рекомендується, оскільки таке підключення може знизити ефективність MPU при обробці переривань.

Акумулятор

Контакт VBAT забезпечує вхід для зовнішньої батареї, що

використовується для підтримки роботи кварцевого генератора, RTC, WD_OVF-біта та XRAM за відсутності основного джерела живлення. Якщо акумулятор не підключено, контакт VBAT має бути з'єднаний з V3P3.

Внутрішня напруга (VBIAS, VBAT, V2P5)

Для мікросхеми 71M6513 необхідні дві напруги живлення: V3P3A для аналогової частини та V3P3D для цифрової. Обидві напруги можуть бути об'єднані зовні чіпа. Внутрішня напруга V2P5 генерується регулятором з джерела живлення 3,3 В. Напруга VBAT необхідна для роботи кварцевого генератора, RTC і XRAM у разі вилучення живлення з V3P3D (режим батареї). Зазвичай VBAT живиться від зовнішнього акумулятора і забезпечує живлення для кварцевого генератора, RTC, XRAM та WD_OVF-біта. Внутрішня напруга VBIAS (1,5 В) генерується для використання в компараторах V1, V2 і V3.

Таблиця 4.8 - Виводи живлення/заземлення

Ім'я	Pin #	«Type»	опис
GNDA	76,91	«P»	Аналогове заземлення:
GNDD	1, 40, 75	«P»	Цифрове заземлення:
V3P3A	77	«P»	Аналогове джерело живлення
V3P3D	9	«P»	Цифровий блок живлення
VBAT	72	«P»	Резервне живлення від акумулятора
V2P5	73	«P»	Вихід регулятора 2,5 В
VLCD	96	«O»	Блок живлення LCD
NC	32,33,36, 42,43,44, 47,55,90,95	-	Немає підключення

Таблиця 4.9 - Аналогові контакти

Ім'я	«Pin #»	«Type»	Опис
IA IB IC	84 83 82	I	Входи вимірюваного струму
VA VB VC	80 79 78	I	Входи вимірюваної напруги
V1 V2 V3	88 87 86	I	Входи компаратора порівнюється з VBIAS.

Таблтця 4.10 - Продовження табл.4.9

VBIAS	81	O	Опорна напруга, для виявлення несправності живлення.
VREF	85	I/O	Еталонна напруга для АЦП
XIN, XOUT	92 94	I	Кристалічні входи: через ці контакти слід підключити кристал у стилі 32 кГц.
VDRV	7	O	Вихід підвищення напруги.

Табл.4.11 Цифрові піни

Ім'я	Pin №	«Type»	Опис
DIO_3, DIO_2, DIO_1, DIO_0	21,20,19,18	I/O	Цифрові входи/виходи від 0 до 3
COM3, COM2, COM1, COM0	25,24,23,22	O	Загальні виходи РК-дисплея: ці 4 контакти забезпечують вибір сигналів для РК-дисплея.
SEG0…SEG2, SEG8…SEG23	Див. разпіновка	O	Виділений сегментний вихід LCD
SEG24/DIO4… SEG41/DIO21	Див. разпіновка	I/O	Багатофункціональні контакти (драйвер LCD SEG або DIO)
SEG7/MUX_SYNC	37	O	Багатофункціональний РК-сегментний вихід/ MUX_SYNC виводиться для синхронного послідовного інтерфейсу
SEG6/SRDY	35	I/O	Багатофункціональні контакти, сегментні виходи LCD/вхід SRDY для синхронного послідовного інтерфейсу
SEG5/SFR	11	O	Багатофункціональний контактний, РК-сегментний вихід/ вихід SFR для SSI.

Таблтця 4.12 - Продовження табл.4.11

SEG4/SDATA	10	O	Багатофункціональний контактний, РК-сегментний вихід/ вихід SDATA для SSI.
SEG3/SCLK	6	O	Багатофункціональний контактний, РК-сегментний вихід/ вихід SCLK для SSI.
RESETZ	74	I	Цей вивід використовується для скидання мікросхеми у відомий стан.
RX	71	I	Вхід UART
TX	5	O	Вихід UART
OPT_RX	89	I	Оптичний вхід
OPT_TX	3	O	Оптичний вихід
CKTEST	8	O	Тактовий вихід PLL.
TMUXOUT	4	O	Тестовий цифровий вихід мультиплексора
E_RXTX	2	I/O	Емулятор серійних даних
E_TBUS[3] E_TBUS[2] E_TBUS[1] E_TBUS[0]	12,13,14,15	O	Шина трасування емулятора
E_ISYNC/BRKRQ	29	I/O	Емулятор «handshake»
E_TCLK	100	O	Емулятор годинника
E_RST	97	I/O	Скидання емулятора
TECT	93	I	Для внутрішнього застосування Терідіан

4.12 Зовнішній РК-дисплей модель CFAH1602A-AGB-JP

Модуль рідкокристалічного дисплея інтегровано в контролер LSI, який містить два 8-розрядних регістри: регістр інструкцій (IR) та регістр даних (DR). Регістри IR зберігають коди інструкцій, такі як очищення дисплея та зсув курсору, а також адресну інформацію для відображення даних в пам'яті DDRAM та генератора символів (CGRAM). Запис в IR можливий тільки з боку MPU. Регістри DR тимчасово зберігають дані, що передаються для запису або зчитування з DDRAM або CGRAM. Коли адреса запису передається в IR, дані зберігаються в DR і зчитуються з DDRAM або CGRAM. Вибір між цими двома регистрами здійснюється за допомогою сигналу вибору регістра (RS).

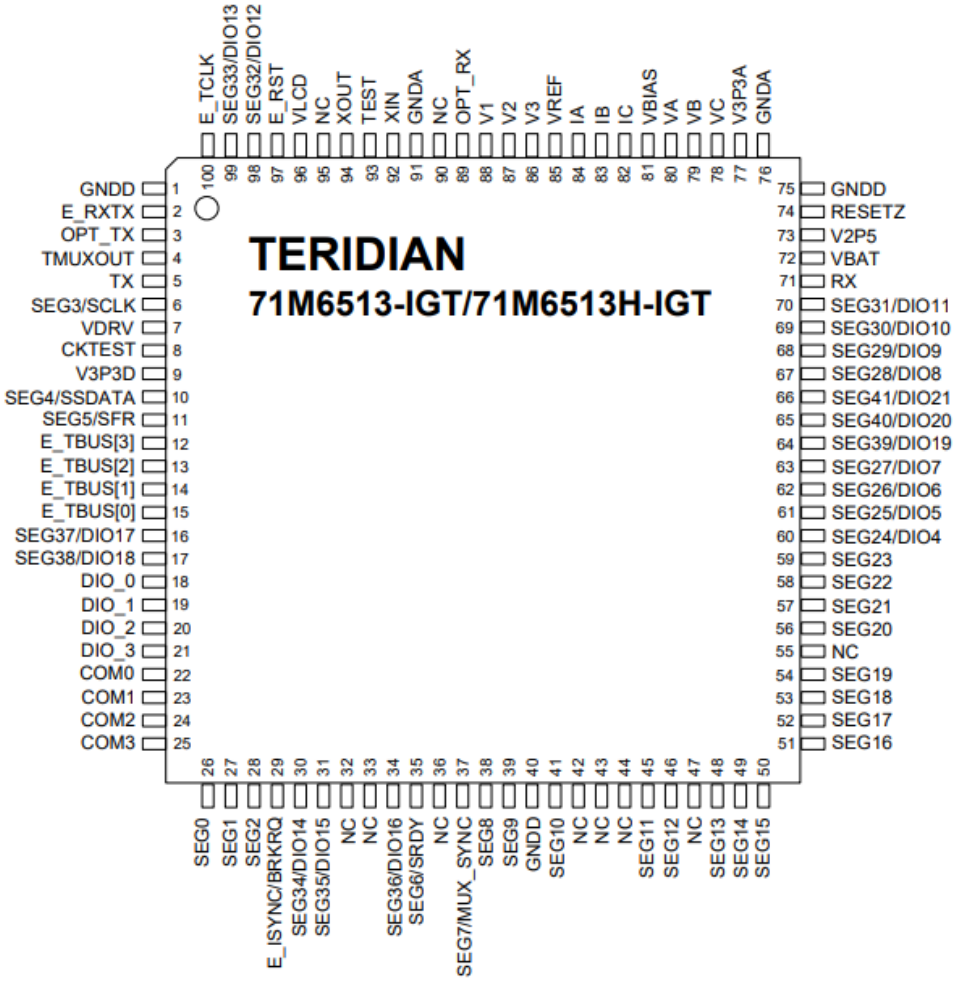


Рисунок 4.7 – Розпіновка

Таблиця 4.13 - Електричні характеристики

Елемент	Символ	Умова	MIN	TYP	MAX	Одиниця виміру
Напруга живлення для логіки	V_{DD}-V_{SS}	-	4.5	-	5.5	V
Напруга живлення для РК-дисплея	V_{DD}-V_0	Ta=0 °C Ta=25 °C Ta=50 °C	- - 3.6	- 3.8 -	4.2 - -	V V V
Вхідна висока напруга.	V_{IH}	-	2.2	-	V_{DD}	V
Вхідна низька напруга	V_{IL}	-	-	-	0.6	V
Вихідна висока напруга	V_{OH}	-	2.4	-	-	V
Вихідна низька напруга.	V_{OL}	-	-	-	0.4	V
Струм живлення	I_{DD}	V_{DD}=5V	-	1.2	-	mA

Таблиця 4.14 - Оптичні характеристики

Елемент	Символ	Умова	MIN	TYP	MAX	Одиниця виміру
Кут огляду	(V)θ	CR ≥ 2	10	-	105	градуси.
	(H) φ	CR ≥ 2	-30	-	30	градуси.
Коефіцієнт контрастності	CR	-	-	3	-	-
Час відгуку	T rise	-	-	150	200	мс
	T fall	-	-	150	200	мс

Прапор зайнятості (BF)

Коли прапор зайнятості має значення 1, контролер LSI перебуває в внутрішньому режимі роботи, і наступна інструкція не буде прийнята. Якщо значення сигналів RS=0 і R/W=1, прапор зайнятості виводиться на лінію DB7. Нову інструкцію можна записати лише після того, як буде підтверджено, що прапор зайнятості дорівнює 0.

Таблиця 4.15 - Піни

Pin #	символ	Рівень	Опис
1	B_{SS}	0V	Земля
2	B_{DD}	5.0V	Напруга живлення для логіки
3	VO	(Змінна)	Робоча напруга для LCD
4	RS	H/L	H: ДАНІ, L: код інструкції
5	R/W	H/L	H: Читання (MPU (модуль) L: Запис (MPU (модуль)
6	E	H,H/L	Сигнал включення мікросхеми
7	DB0	H/L	Біт даних 0
8	DB1	H/L	Біт даних 1
9	DB2	H/L	Біт даних 2
10	DB3	H/L	Біт даних 3
11	DB4	H/L	Біт даних 4
12	DB5	H/L	Біт даних 5

Таблтця 4.16 - Продовження табл.4.15

13	DB6	H/L	Біт даних 6
14	DB7	H/L	Біт даних 7
15	A/V_{EE}	-	LED +
16	K	-	LED -

Лічильник адрес (AC)

Лічильник адрес (AC) відповідає за призначення адрес як для DDRAM, так і для CGRAM.

RAM для відображення даних (DDRAM)

DDRAM призначена для зберігання даних, що відображаються на дисплеї, у вигляді 8-бітових кодів символів. Її ємність складає 80 байтів або 80 символів. Нижче наведено відповідність між адресами DDRAM і розташуваннями на рідкокристалічному дисплеї.

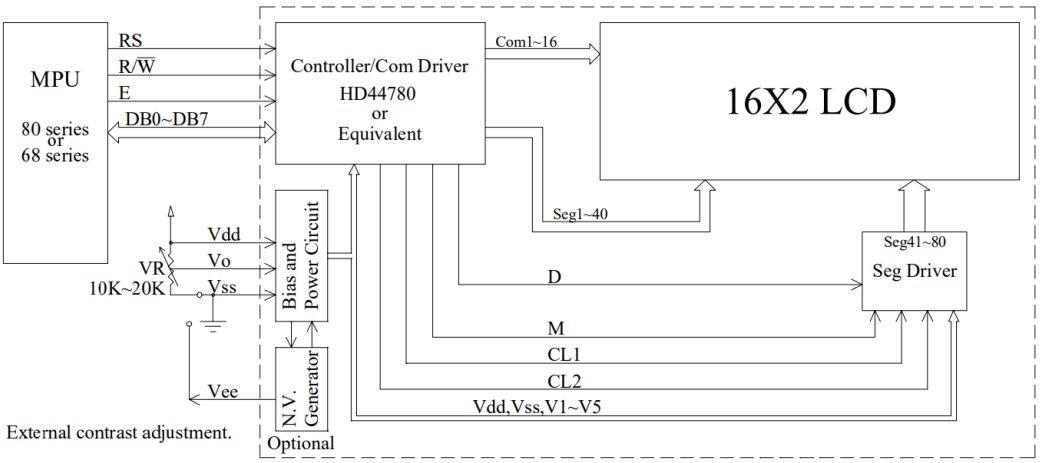


Рисунок 8 - Функціональна блок-схема LCD

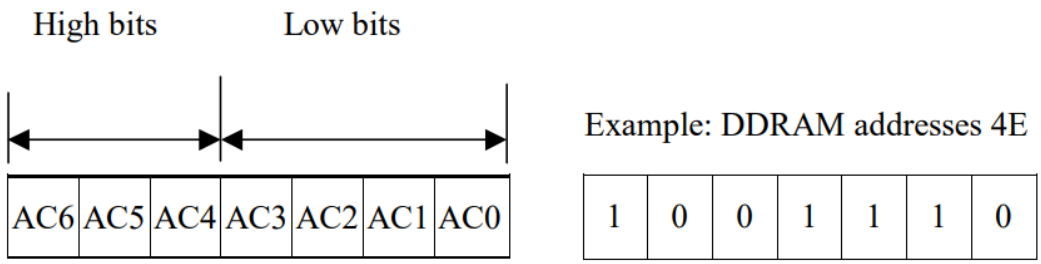


Рисунок 4.9 - Розподіл бітів

Таблиця 4.17 - Позиція відображення адреси DDRAM

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
40	41	42	43	44	45	46	47	48	49	4A	4B	4C	4D	4E	4F

Генератор символів ПЗУ (CGROM)

CGROM відповідає за генерацію шаблонів символів, що складаються з 5-8 або 5-10 крапок, використовуючи 8-бітові коди символів.

4.13 Зовнішній інтерфейс I2C (EEPROM)

Модулі AT24C32/64 надають 32768/65536 біт послідовної електрично стираної та програмованої постійної пам'яті (EEPROM), організованої у вигляді 4096/8192 слів по 8 біт кожне. Завдяки каскадному підключенню, до 8 пристроїв можуть спільно використовувати одну 2-провідну шину. Цей пристрій оптимізований для застосувань з низьким споживанням енергії та низькою напругою, що робить його ідеальним для промислових і комерційних умов. AT24C32/64 доступний у компактних корпусах: 8-контактному JEDEC PDIP, 8-контактному JEDEC SOIC, 8-контактному EIAJ SOIC та 8-контактному TSSOP (для AT24C64). Доступ до пристрою здійснюється через 2-провідний послідовний інтерфейс, і він доступний у версіях з напругою 2,7 В (від 2,7 В до 5,5 В) та 1,8 В (від 1,8 В до 5,5 В).

Таблиця 4.18 - Конфігурації пінів

Назва PIN	Функція
A0 - A2	Вхідні адреси
SDA	Послідовні дані
SCL	Послідовний вхід годинника
WP	Write Protect

Таблиця 4.19 - Характеристики DC

Символ	Парамет	Тестовий стан		Min	Typ	Max	Одиниці
$V_{CC1/4}$	Напруга живлення	-		1,8/2,5/ 2,7/4,5	-	5,5	V
$I_{CC1/2}$	Струм живлення	VCC = 5.0V	Read/Write на 100 kHz	-	0,4/ 2,0	1,0/3,0	мА
$I_{SB1/3}$	Струм очікування	$V_{CC1/3}$ – min V_{CC} = 5.5V	V_{IN} = V_{CC} or V_{SS}	-	-	0,1/0,5/ 0,5 2,0	µA
I_{SB4}	Струм очікування	V_{CC} = 4,5 – 5,5V	V_{IN} = V_{CC} or V_{SS}	-	20	35	µA
I_{LI}	Вхідний контакт поточний		VIN = VCC or VSS		0,10	3,0	µA
I_{LO}	Вихідний контакт поточний		VOUT = VCC or VS		0,05	3,0	µA
V_{IL}	Низький рівень входу			-0,6		V_{CC} x 0.3	V
V_{IH}	Високий рівень входу			V_{CC} x 0.7		V_{CC} + 0.5	V
$V_{OL2/1}$	Низький вихідний рівень	V_{CC} = 3,0/1,8	I_{OL} = 2,1/0,15 mA				V

4.14 Програмне забезпечення

Компанія Texas Instruments випустила модульну та масштабовану налагоджувальну платформу Smart Meter Board 3.0 (SMB 3.0), що забезпечує підтримку розробки однофазних і трифазних інтелектуальних лічильників електроенергії, сумісних із вимогами технології SmartGrid щодо комунікаційних протоколів. Ця інноваційна платформа об'єднує в собі ключові компоненти з широкого асортименту вбудовуваних, аналогових та комунікаційних рішень SmartGrid від Texas Instruments, що дає можливість продемонструвати функціональні можливості інтелектуальних приладів для обліку споживаної електроенергії.

Налагоджувальна платформа підтримує різноманітні дротові та бездротові комунікаційні протоколи, включаючи передачу даних через лінії електропередач (PLC), протокол бездротового зв'язку ближнього радіусу дії (NFC), Wi-Fi, бездротову передачу даних в субгігагерцовому діапазоні та 2.4 ГГц ZigBee Smart Energy Pro.

Також компанія анонсувала систему-на-кристалі Smart Meter SoC, яка сумісна з цією платформою та може підключатися до неї для тестування можливостей та розширення функціональності.

Основні характеристики налагоджувальної платформи SMB 3.0:

- Модульність та масштабованість для розробки інтелектуальних лічильників електроенергії для систем автоматичного обліку;
- Відкритість платформи, що дозволяє розробникам адаптувати свої проекти для подальшого налагодження та/або диференціації, з підтримкою процесорів від ARM Cortex-M до Cortex-A8, що дозволяє вибрати оптимальний процесор для конкретного проекту лічильника;
- Підтримка малопотужних радіочастотних інтерфейсів, що забезпечує можливість підключення лічильників до мережі HAN (Home Area Network) для зв'язку ближнього радіусу дії, а також підтримка передачі даних через лінії електропередач (Power Line Communication);
- Можливість NFC-комунікації, що відкриває можливість для застосування функцій попередньої оплати за електропостачання;
- Підтримка протоколу Wi-Fi, що дає змогу під'єднувати лічильники до мережі HAN та забезпечує зручний зв'язок через ПК, смартфони чи

планшети без додаткових витрат;

- Простота програмної інтеграції завдяки підтримці програмних бібліотек smartgrid для комунікаційних протоколів та метрологічних функцій.

5 ТЕХНІКО - ЕКОНОМІЧНА ЧАСТИНА

5.1 Розрахунок повної собівартості проектованого пристрою

Собівартість продукції, що виготовляється підприємством, визначається як сукупність витрат, понесених на виробництво та реалізацію продукції, виражених у грошовій формі. До витрат, пов’язаних безпосередньо з виробничим процесом, належить виробнича собівартість, яка в поєднанні з витратами на збут формує повну собівартість продукції. Процес визначення собівартості конкретного виробу за статтями витрат отримав назву калькуляції. Такий розрахунок здійснюється відповідно до нормативного документа «Типове положення із планування, обліку й калькулювання собівартості продукції (робіт, послуг) у промисловості».

У виробничому процесі будь-якого виробу використовуються різноманітні матеріали, комплектуючі, обладнання та інструменти, а також виконується значна кількість технологічних операцій. Для забезпечення точного обліку фактичних витрат на виробництво та формування обґрунтованої собівартості продукції важливою є класифікація цих витрат. Калькуляція собівартості конкретного виду продукції базується на систематизації витрат за калькуляційними статтями.

У плануванні та обліку собівартості продукції застосовується типове групування витрат за статтями калькуляції:

- основна заробітна плата;
- додаткова заробітна плата;
- відрахування на соціальні потреби;
- матеріали та комплектуючі;
- витрати на утримання та експлуатацію обладнання;
- виробничі витрати;
- адміністративні витрати;
- позавиробничі витрати (комерційні витрати).

Систематизація витрат за зазначеними статтями дозволяє визначити рівень собівартості продукції, що, своєю чергою, впливає на її ринкову ціну. Такий підхід надає можливість ідентифікувати джерела витрат та їх призначення.
Для складання калькуляції собівартості проектованого пристрою основою слугують статті витрат, пов’язані із закупівлею комплектуючих елементів. Окрім того, необхідно враховувати вартість напівфабрикатів, які використовуються у процесі виготовлення друкованих плат.

5.2 Матеріали та комплектуючі

Матеріали та комплектуючі визначаються на основі інформаційних джерел, таких як каталоги, прайс-листи, веб-сайти виробників і постачальників, а також з урахуванням даних про матеріали, сировину, комплектуючі та технологічні операції, розрахованих на одну одиницю продукції.

Дані за цією статтею витрат наведені у таблиці 7.1.

Таблиця 5.1 – Розрахунок витрат на комплектуючі

№ п/п	Найменуванння	Кількість, од.	Ціна за одиницю, грн.	Сума, грн.
1	2	3	4	5
МІКРОСХЕМИ				
1	AT24C64	1	71,00	71,00
2	CFAH1602A-AGB-JP	1	125,00	125,00
3	71M6513	1	125,00	125,00
КОНДЕНСАТОРИ				
4	SMD 0805 X7R-50В-1000 пФ	2	0,54	1,08
5	SMD 0805 X7R-50В-0,1 мкФ	3	0,4	1,2

Таблиця 5.2 – Продовження таблиці 5.1

6	SMD 0805 NPO-50В-22 пФ	2	0,38	0,76
7	SMD 0805 NPO-50В-33 пФ	1	0,38	0,38
8	SMD 0805 X7R -50В-0,22 мкФ	1	1,00	1,00
РЕЗИСТОРИ				
9	MFR 9,1 Ом	1	8,00	8,00
10	MFR 200 Ом	1	9,00	9,00
11	MFR 3,3 kОм	2	8,00	16,00
12	VR 3266P 10кОм	1	13,50	13,50
Кварцовий генератор				
13	ECS-.327-9-34QS-TR	1	54,50	54,50
Кнопка				
14	КН-11В	1	8,00	8,00
Роз’єми				
15	DB-9	3	13	39
Разом, К				473,42

Загальна вартість усіх комплектуючих складає 473,42 грн. Розрахунок витрат за матеріали наведений у таблиці 5.3.

З урахуванням транспортно-заготівельних витрат (kт-з = 5 ÷ 15%) вартість комплектуючих та матеріалів становитиме:

$$КМ = (К + М) \cdot (100 + k_{т\text{-}з}) / 100. \quad (5.1)$$

$$КМ = (473,42 + 256,48) \cdot (100 + 10) / 100 = 802,428 \text{ грн.}$$

Витрати на основну заробітну плату:

$$Зо = \sum_{i=1}^{n} Тг_i \cdot Нч_i \ . \quad (5.2)$$

Таблиця 5.3 – Розрахунок витрат за матеріали

Матеріал	Одиниця вимірювання	Норма витрат	Ціна за од, грн.	Ціна, грн.
1	2	3	4	5
Провід монтажний	м	0,5	2,56	1,28
Стеклотекстолит	$м^2$	0,2	60	12
Каніфоль	кг	0,1	1008	100,8
Флюс	кг	0,02	840	16,8
Припой	кг	0,1	320	32
Лак	кг	0,03	120	3,6
Речовина для корпусу	кг	0,3	300	90
Разом, М				256,48

де $Тг_i$ – годинна тарифна ставка окремого спеціаліста (інженера-електронника, лаборанта тощо), який задіяний у виробництві пристрою (установки), грн/год;

$Нч_i$ – витрачений час робітником на виробництво та налагодження пристрою (установки), год, $Нч_i$ = 2 год.;

n – кількість працівників, задіяних у виробництві пристрою (установки), n = 1.

Годинна тарифна ставка розраховується, виходячи із величини місячного окладу спеціаліста:

$$Тг_i = \frac{Тм_i}{Вф_i \cdot 8} . \quad (5.3)$$

де $Тм_i$ – місячний оклад (ставка) спеціаліста, грн;

$Вф_i$ – фактично відпрацьований час за розрахунковий період (місяць), днів (змін);

8 – кількість відпрацьованих годин за зміну.

$$Тг_i = \frac{Тм_i}{Вф_i \cdot 8} = \frac{15000}{22 \cdot 8} = 88{,}23 \text{ грн.}$$

$$З_о = \sum_{i=1}^{1} 88{,}23 \cdot 2 = 1 \cdot 88{,}23 \cdot 4 = 352{,}92 \text{ грн}$$

5.3 Витрати на додаткову заробітну плату

Додаткова заробітна плата (10 – 30% від $З_о$):

$$Зд = Зо \cdot \frac{Кд}{100}. \qquad (5.4)$$

де $К_д$ – відсоток додаткової заробітної плати, $К_д$ = 10%.

$З_д$ = 352,92* (10% / 100%) = 35,292 (грн.).

5.4 Відрахування на соціальні виплати

Відрахування на соціальні виплати містять відрахування від сукупної основної та додаткової заробітної плати відповідно до встановлених тарифів. Ці утримання включають:

- обов’язкові внески до державної пенсійної системи;
- страхові внески у разі нещасних випадків;
- обов’язкові внески до державного соціального страхування від безробіття;
- витрати, що пов’язані з тимчасовою втратою працездатності;
- витрати, що пов’язані з народженням дитини та похованням.

Нарахування на заробітну плату – єдиний соціальний внесок у розмірі 22%.

$$В_{св} = (З_о + З_д) * 22/100. \qquad (5.5)$$

$В_{св} = (352,92 + 35,292) * 22/100 = 85,4$ (грн.).

5.5 Видатки на утримання та експлуатацію встаткування

Витрати на утримання та експлуатацію встаткування (ВУЕ) перебувають на балансі підприємства міста і розраховуються за такою формулою:

ВУЕ = основна заробітна плата * відсоток ВУЕ (приймають відсоток ВУЕ рівним 120 ÷ 150%).

ВУЕ = 352,92 * 1,2 = 423,5 грн.

5.6 Загальновиробничі витрати

Загальновиробничі витрати містять у собі різноманітні витрати, пов'язані з керуванням підрозділом. Це охоплює витрати на управлінські заходи в межах підрозділу, витрати на відрядження співробітників, а також амортизаційні відрахування вид вартості основних фондів загальноцехового призначення та інші подібні витрати.

Загальновиробничі витрати ($В_{зв}$) визначаються у розмірі 130-250% від основної заробітної плати.

$$В_{зв} = З_{о} * \% В_{зв} = 352,92 * 1,3 = 457,96 \text{ (грн.).} \quad (5.6)$$

5.7 Виробнича собівартість

Виробнича собівартість розраховується за формулою:

$$В_{с} = З_{о} + З_{д} + В_{св} + КМ + ВУЕ + В_{зв} =$$
$$= 352,92 + 35,29 + 85,4 + 802,43 + 423,5 + 457,96 = 2157,5 \text{ (грн.).} \quad (5.7)$$

5.8 Адміністративні витрати

Адміністративні витрати можуть охоплювати широкий спектр

складових, серед яких:

- витрати, пов’язані з управлінням підприємством, включаючи планування, координацію та контроль за виробничими й організаційними процесами;
- витрати на організацію службових відряджень адміністративного персоналу;
- витрати, спрямовані на утримання пожежної безпеки та сторожової охорони об’єктів підприємства;
- витрати на організацію навчання й перепідготовки персоналу з метою підтримання їхньої кваліфікації;
- витрати, що забезпечують транспортування працівників до місця роботи та назад;
- витрати на сплату відсотків за фінансовими й комерційними кредитами;
- витрати, пов’язані з використанням орендованих або лізингованих матеріальних ресурсів;
- витрати на оплату послуг комерційних банків та інших фінансово-кредитних установ;
- податки та інші обов’язкові відрахування.

Ці витрати є ключовими для забезпечення ефективного функціонування підприємства та підтримання стабільності його операційної діяльності.

Адміністративні витрати ($В_а$) визначаються у розмірі 140 - 200% від основної заробітної плати.

$$В_а = З_о * \% В_а = 352,92 * 1,4 = 494,09 \text{ (грн.)}. \quad (5.8)$$

5.9 Витрати на збут

Витрати на збут (Вз) включають різноманітні компоненти, зокрема витрати на рекламу та заходи з передреалізаційної підготовки пристрою. Орієнтовно їхній обсяг становить 5-10% від виробничої собівартості продукції. Цей показник є важливим фактором забезпечення ринкової активності та успішного впровадження пристрою на ринок.

Витрати на рекламу охоплюють ресурси, що використовуються для організації рекламних кампаній, створення промоційних матеріалів,

проведення рекламних заходів та інших дій, спрямованих на просування продукції серед цільової аудиторії.

Передреалізаційна підготовка пристрою передбачає витрати на тестування, сертифікацію, розробку технічної документації, ліцензування та виконання інших необхідних процедур, які забезпечують відповідність пристрою стандартам і вимогам для введення в експлуатацію.

Зазначені витрати є критично важливими для формування позитивного іміджу продукту, підвищення обізнаності споживачів і стимулювання попиту на ринку.

$$B_з = B_с * (5 - 10)\% = 2157,5 * 0,05 = 107,88 \text{ (грн.)}. \quad (5.9)$$

Калькуляцію собівартості виробу зведено в таблицю 5.4.

Таблиця 5.4 – Калькуляція собівартості пристрою

№	Найменування статей калькуляції	Значення, грн.
1.	Основна заробітна плата	352,92
2.	Додаткова заробітна плата	35,29
3.	Відрахування на соціальні виплати	85,4
4.	Видатки на утримання та експлуатацію встаткування	423,5
5.	Загальновиробничі витрати	457,96
6.	Матеріали та комплектуючі	802,428
Виробнича собівартість		2157,5
7.	Адміністративні витрати	494,1
8.	Витрати на збут	107,9
Повна собівартість пристрою		4917

5.10 Повна собівартість пристрою

Повна собівартість пристрою (С) розраховується за формулою:

$$C = B_с + B_а + B_з. \quad (5.10)$$

С = 2157,5 + 494,09 + 107, 9 = 2759,5 (грн.).

5.11 Розрахунок ціни пристрою

Розрахунок оптової ціни пристрою

В ринковій економіці застосовують різні методи ціноутворення: собівартість плюс прибуток, забезпечення фіксованого обсягу прибутку, залежно від рівня попиту.

Розрахунок оптової ціни пристрою проведемо за схемою «собівартість плюс прибуток»:

$$Ц_{опт} = С + П, \qquad (5.11)$$

де С – собівартість пристрою;

П – величина прибутку.

Прибуток визначається виходячи з нормативу рентабельності виробництва продукції:

$$R = (П / С) * 100\%, \qquad (5.12)$$

де R - рентабельність продукції (продукту), що приймається у розмірі до 35%.

R = 10%.

Тоді оптова ціна:

$$Ц_{опт} = С + (R * С / 100) = 4917 + 0,1 * 4917 = 5408,7 \text{ (грн.)}. \qquad (5.13)$$

5.12 Розрахунок роздрібної ціни пристрою

Визначимо роздрібну ціну розробленого пристрою:

$$Ц_{розн} = Ц_{опт} * 1,2 = 5408,7 * 1,2 = 6490,44 \text{ (грн.)}, \qquad (5.14)$$

де 20% ПДВ.

Методика визначення ціни, описана вище, має як переваги, так і недоліки. До її позитивних аспектів належать простота у застосуванні та комплексна логічна структура, яка забезпечує відшкодування витрат на виробництво та гарантує прибутковість у процесі створення і реалізації пристрою.

Однак, дана методика має обмеження, зокрема недостатню увагу до ринкових чинників ціноутворення, таких як рівень попиту. Це може спричинити невідповідність встановленої ціни реальним умовам ринку. Особливо суттєвим недоліком є відсутність врахування конкуренції, рентабельності продукції з точки зору державного регулювання та інших зовнішніх ринкових впливів. Таким чином, застосування цієї методики є доцільним лише за специфічних обставин, зокрема у разі монопольного становища, обмеженої рентабельності, виконання одноразових замовлень або виробництва унікальної продукції.

Для встановлення ціни, яка відповідала б сучасним ринковим умовам, необхідно доповнити дану методику результатами маркетингових досліджень, що враховують вплив конкурентного середовища, попиту та інших ринкових чинників.

ВИСНОВКИ

Створення данної роботи призвело до розробки прототипу електронного 3-фазного лічильника електроінергії на основі системи на кристалі. Данний прилад дозволяє якісний збір інформації, щодо вимірюваних величин ліній енергоживлення, вільний та постійний мониторинг данних, можливість програмування цього лічильника на виміри під конкретні задачі, без спеціаліста з глибокими знаннями в машинному програмуванні. Однією з головних переваг таких систем – це можливість використання простого програмного забеспечення, для корекції чи повної зміни пріоритетів для вимірювання чи обробки данних.

Додатково розглянуто способи захисту зібраних данних. На основі одного з методів криптографічного перетворення створений алгоритм роботи шифрування.

Під наведені потреби створенна принципова схема електронного лічильника електроінергії на основі системи на кристалі.

Також розглянуто способи захищенної передачі данних, створення безпечних тунелей та протоколів зв’язку. На основі цих данних створенна ідея щодо передачі інформації через мобільних операторів на VPN тунелі.

Список джерел

1. https://www.analog.com/en/resources/app-notes/2022/07/16/11/04/71m6513-neutral-current-measurement.html / 71M6513 Neutral Current Measurement
2. https://www.analog.com/media/en/technical-documentation/app-notes/71m6513-standards-compliance-test-report.pdf / 71M6513 Standards Compliance Test Report
3. https://www.analog.com/media/en/technical-documentation/data-sheets/71m6513-71m6513h.pdf / 71M6513/71M6513H 3-Phase Energy Meter IC
4. https://www.analog.com/en/products/71m6513.html / Documentation 71M6513
5. https://www.analog.com/en/resources/app-notes/71m6513-standards-compliance-test-report.html / 71M6513 Standards Compliance Test Report
6. https://www.jotrin.com/technology/details/system-on-chip-measures-and-monitors-ac-power-outlets-?srsltid=AfmBOopX_3rre2vNXyE7yrchgo4zfcUzlzrWU7srZ3RlQ-73VazmVKJE / System On Chip measures and monitors AC power outlets.
7. https://kyivstar.ua/business/products/vpn / Створення корпоративної мережі передачі даних (VPLS, IP VPN)
8. https://business.vodafone.ua/produkty/internet/mobilniy-ip-vpn / Мобільний IP VPN
9. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-77r1.pdf#page=53&zoom=100,93,96 / NIST Special Publication 800-77 Revision.Guide to IPsec VPNs
10. https://ww1.microchip.com/downloads/en/DeviceDoc/doc0336.pdf / 2-Wire Serial EEPROM. AT24C32 AT24C64
11. https://www.kosmodrom.ua/ru/rezistor-podstroechnyy/3266p-10k.html
12. «175 Zettabytes By 2025» 2018 https://www.forbes.com/sites/tomcoughlin/2018/11/27/175-zettabytes-by-2025/?sh=4b329d3b5459
13. Ю. С. Грищук: МІКРОКОНТРОЛЕРИ: АРХІТЕКТУРА, ПРОГРАМУВАННЯ ТА ЗАСТОСУВАННЯ В ЕЛЕКТРОМЕХАНІЦІ

Харків НТУ «ХПІ» 2019 https://repository.kpi.kharkov.ua/server/api/core/bitstreams/fd62cd97-3ae1-4bf7-b213-2f37c6f4e72c/content
14. Статті про криптографію https://esu.com.ua/article-1576
15. Захист інформації в телекомунікаційних системах https://tks.nau.edu.ua/wp-content/uploads/2016/05/Zahyst-informatsiyi-v-telekomunikatsijnyh-systemah.pdf
16. Введение в криптографию / под ред. Ященко. — Litres, 2017
17. Технологія блокчейн як інструмент побудови розподіленої системи довіри в системах моніторингу громадського транспорту\ студ. Мазуркевич О.А., студ. Орлов В.В., асп. Сердюк В.В. Керівник: доц. Бережна О.В директор Арбузов В.В., \Фізика, електроніка, електротехніка (ФЕЕ-2022). Матеріали та програма науково-технічної конференції. – Суми: СумДу, 2023. – С.82

ДОДАТОК А

Технологія блокчейн як інструмент побудови розподіленої системи довіри в системах моніторингу громадського транспорту

Бережна О.В.[1], *доц.*; Арбузов В.В.[2], *директор*;
Мазуркевич О.А.[1], *студент гр. ТК-01*;
Орлов В.В.[1], *студент гр. ЕС-91*
[1]Сумський державний університет, м. Суми, Україна
[2]ТОВ Енергосервісне підприємство «Преобразователь», м. Суми

Стрімкий розвиток Інтернету речей надає нові можливості для задоволення таких важливих суспільних потреб, як підвищення ефективності роботи систем моніторингу громадського транспорту.

Сучасні системи моніторингу, як правило, є централізованими автоматизованими системами трекінгу з єдиним сервером бази даних, де обмін інформацією між GPS датчиками транспортних засобів та сервером здійснюється за допомогою супутникових та GPRS мереж.

Власник централізованої системи моніторингу, як правило державний орган (Регулятор), не може гарантувати повноту бази даних або відсутність несанкціонованого втручання до її роботи на користь будь-кого. В свою чергу власник транспортних засобів (Оператор послуг) не може гарантувати їх рух із увімкненими GPS датчиками, а пасажир (Споживач послуг) не має достовірної інформації про наявність транспорту на встановлених Регулятором маршрутах. Між учасниками такої ієрархічної централізованої бізнес-моделі є низький рівень довіри до результатів трекінгу, а сама модель досягла максимуму своєї ефективності та потребує для подальшого свого розвитку підвищення рівня контролю, взаємодії та довіри між всіма учасниками.

Дослідження показали, що підвищення ефективності у наданні транспортних послуг пов'язане з залученням Споживача до моніторингу переміщення транспорту, що потребує міграції від ієрархічної централізованої бізнес-моделі до децентралізованої моделі із встановленням пірингових горизонтальних спорадичних бізнес-відносин з високим рівнем довіри між суб'єктами моделі без посередників. Така реорганізація потребує створення пірингової децентралізованої системи з децентралізованою базою даних, розподіленою між суб'єктами взаємовідносин. З цією метою у кожному транспортному засобі необхідно забезпечити підключення до корпоративної пірингової мережі GPS датчиків, транспондерів та смартфонів пасажирів з можливістю реєстрації в них транзакцій,

пов'язаних з наданням транспортних послуг шляхом запису інформаційного блоку щодо всіх параметрів здійсненої транзакції.

В інформаційних блоках міститься інформація з міткою часу про такі транзакції, як наявність транспорту на маршруті, факт вимкнення GPS датчику або транспондеру, реєстрація пасажирів, реакція Регулятора та Оператору послуг на зафіксовані порушення. При несанкціонованому вимкненні транспондерів факт находження транспорту на маршруті оцінюється завдяки наявності зафіксованих транзакцій в смартфонах пасажирів про їх геолокацію, завдяки підключенню смартфонів до GPS та 4G/5G мереж.

Інструментом підвищення довіри між суб'єктами, що здійснюють транзакції за допомогою мережі Інтернет, доцільно використовувати технології блокчейн. Використання цієї технології дозволяє у кожному пристрої для кожного інформаційного блоку обчислювати за криптографічними алгоритмами значення відповідної хеш-функції, яка враховує хеш-значення попередніх інформаційних блоків. Ця особливість унеможливлює зміни історії та змісту інформаційних блоків про виконані транзакцій заднім числом непомітно для всіх інших учасників. Копії ланцюжків таких блоків зберігаються на різних смартфонах, транспондерах та серверах Регулятору або Оператору послуг незалежно друг від друга шляхом створення реплікованої розподіленої бази даних децентралізованої системи моніторингу.

Застосування технології блокчейн усуває потребу у наявності будь-яких традиційних в економіці посередників довіри до результатів моніторингу (суди, комісії), оскільки усуває саму необхідність довіри та замінює її доказами. Таким чином завдяки технології блокчейн стає можливим використання нової бізнес-моделі організації трекінгу на основі впровадження розподіленої системи довіри в рамках якої невідомі один одному учасники, можуть вступати в безпосередні, рівні довірливі стосунки на засадах добровільного приєднання до цієї системи без звернення до будь-якої центральної організації.

Використання технології «блокчейн» як інструменту побудови розподіленої системи довіри між Споживачем, Регулятором та Оператором послуг в системах моніторингу громадського транспорту дозволяє підвищити якість та прозорість надання транспортних послуг, зменшити транзакційні витрати Регулятора за рахунок міграції від ієрархічних зв'язків до горизонтальних без участі посередників, підвищення доходів у Оператора послуг та державних бюджетів.

Поз. обозн.	Найменування	Кіл.	Примітка
	Конденсатори		
C1/C2	SMD 0805 NPO-50В-22 пФ	2	
C3/C5/C8	SMD 0805 X7R-50В-0,1 мкФ	3	
C4	SMD 0805 X7R -50В-0,22 мкФ	1	
C6/C7	SMD 0805 X7R-50В-1000 пФ	2	
C9	SMD 0805 NPO-50В-33 пФ	1	
	Мікросхеми		
DD1	71M6513	1	
DD2	CFAH1602A-AGB-JP	1	
DD3	AT24C64	1	
	Резистори		
R1	MFR 200 Ом	1	
R2	MFR 9,1 Ом	1	
R3	VR 3266P 10кОм	1	
R4	MFR 3,3 кОм	2	
	Резонатори		
ZQ1	ECS-.327-9-34QS-TR	1	
	Кнопка		
SB1		1	
	Роз'єми		
X1-3	DB-9	3	

					ЕлІТ 8.171.00.10. 479 ПЕ
Зм.	Арк	№ докум.	Підпис	Дата	
Розроб.		Орлов В.В.			Перелік елементів
Перевір.		Бережна О.В.			
Т.Контр					
Н. Контр.		Гапич В.М.			
Затверд.		Опанасюк А.С.			

Літ.	Аркуш	Аркушів
	1	1

СумДУ, гр. ЕС.м-31