Дипломний проект

На тему: **Система захисту інформації в автоматизованих мережах обліку використання комунальних ресурсів**

Виконав: студент групи КМ-805

Саповатов Олексій Олександрович

Керівник: к.т.н., доцент

Швидкий Валерій Васильович

Мета проекту:

Проектування системи захисту інформації в автоматизованих мережах обліку використання ресурсів житлово – комунального господарства.

Основні задачі на проектування:

- захист інформації від несанкціонованого читання та модифікації;
- забезпечення необхідного рівня достовірності інформації;
- захист обладнання від негативного впливу на нього з боку абонентів.

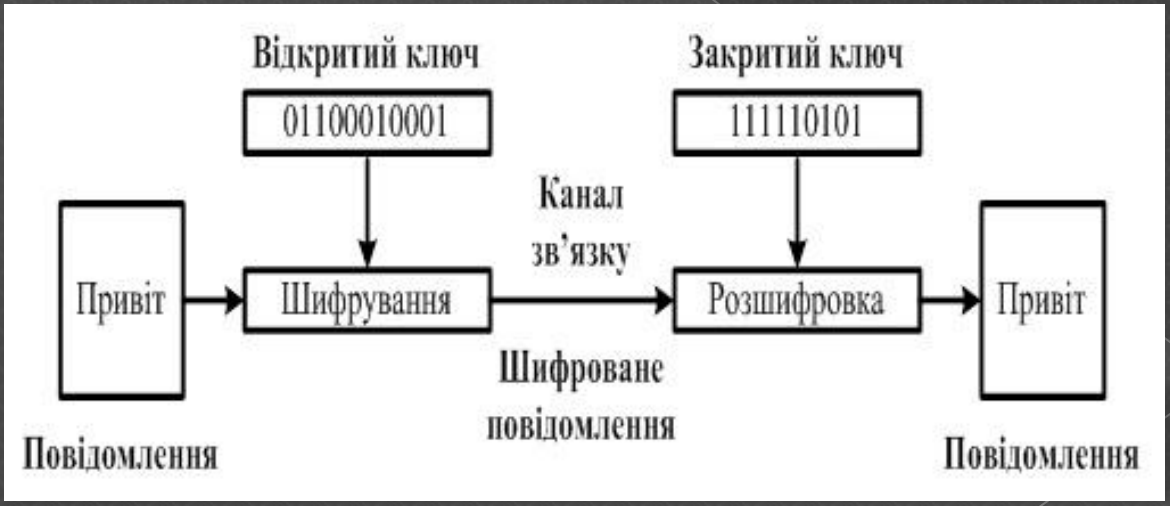
Небезпечні ситуації та явища, які можуть вплинути на роботу системи обліку:

- перехоплення абонентом інформації, що відсилається лічильником, з метою її модифікації;
- намагання абонента будь-яким способом порушити цілісність корпусу лічильника, з метою блокування механізму обліку;
- відключення будь-яких роз'ємів лічильника з метою блокування дистанційного збору даних;
- велика імовірність виникнення помилок в каналі зв' язку.

Захист інформації від читання та модифікацій

Для забезпечення захисту інформації від несанкціонованого читання та модифікацій було обрано симетричний??? алгоритм крипто захисту RSA.

Однією з головних переваг даного алгоритму над симетричними методами є те, що від допускає можливість повного перехоплення повідомлення та відкритого ключа, так як відкритий і закритий ключі не пов'язані між собою.



Приклад процедури шифрування методом RSA:

P = 7753 Q = 8269

N = P*Q = 7753 * 8269 = 64109557

M = (P-1)*(Q-1) = 7752 * 8268 = 64093536

E = 1031 – відкритий ключ

$$\frac{M}{E} = \frac{64093536}{1031} = 62166 + \cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{4+\cfrac{1}{6+\cfrac{1}{1+\frac{1}{3}}}}}}}}$$

$$\frac{P\,n-1}{Q\,n-1} = 62166 + \cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{4+\cfrac{1}{6+\frac{1}{1}}}}}}} = \frac{16598423}{267}$$

D= P_{n-1} = 16598423 – закритий ключ

Перевірка:

$$|ED|_M = |1031 * 16598423|_{64093536} = 1$$

Нехай "Абонент" відправляє "Центру" повідомлення:

S_0 = АСОВР = $1*32^0 + 21*32^1 + 18*32^2 + 3*32^3 + 20*32^4$ =

= 1 + 672+ 18432 + 98304 + 20971520 = **21088929**

Зашифроване повідомлення матиме вигляд:

$$S_{\text{ш}} = \left|S_0^E\right|_N = \left|21088929^{1031}\right|_{64109557} = 8646070$$

"Центр" після отримання $S_{\text{Ш}}$ обчислює:

$$S_2 = \left|S_{\text{ш}}^D\right|_N = \left|8646070^{16598423}\right|_{64109557} = \mathbf{21088929}$$

Рівність величин S_0 та S_2 показує, що зашифроване повідомлення розшифроване правильно.

Стійкість крипто алгоритму до дії помилок у каналі зв'язку

RSA є блоковим шифром, де все повідомлення є одним блоком даних. Кожен блок даних шифрується незалежно від попередніх і подальших блоків, унаслідок чого трек помилки дорівнює довжині одного блоку, тобто довжині повідомлення.

При імовірності помилок в каналі зв'язку 0,1 – 0,4 та довжині блоку даних $L_{бд}$ = 300біт, в кращому разі імовірність помилки в блоці даних буде дорівнювати:

$$P_б = (1 - (1 - P_0)^{L_{бд}}) = 1 - 0{,}9^{300} = 0{,}99$$

Тобто, на кожні 100 переданих блоків - 99 міститимуть помилки.

Для підвищення достовірності інформації було прийнято рішення про застосування не кодового методу, а саме – шумоподібного сигналу.

Основні відомості про шумоподібні сигнали

Широкосмуговими (складними, шумоподібним) сигналами (ШПС) називають такі сигнали, у яких добутки активної ширини спектра F на тривалість T набагато більше одиниці. Цей добуток називається базою сигналу B, для ШПС:

$$B = FT >> 1$$

Широкосмуговими сигнали іноді називають складними на відміну від простих сигналів (наприклад, прямокутні, трикутні і т.д.) з B = 1.

У системах зв'язку з ШПС ширина спектру випромінюваного сигналу F завжди набагато більше ширини спектру інформаційного повідомлення.

ШПС отримали застосування в широкосмугових системах зв'язку.

Підвищення достовірності от применения ШПС

Для достовірності інформації применен модульований по фазі ШПС. який утворюється складанням за модулем два бітів переданих даних та ПВП несучої.

При базі b=11, застосування ШПС дало наступні результати:

1) імовірність виникнення бітової помилки – 10^{-8};
2) імовірність блокової помилки – $3*10^{-6}$.

Це означає, що лише застосування ШПС знижує значення імовірності помилки (по блоках) до значення не більше 3 помилкових блоків на мільйон переданих блоків.

Імовірність безошибочного приема блока данных :

$$P(0) = q^{300} = 0,9991$$

Імовірність винекнення одинарних помилок в блоці :

$$P(1) = C^{1}_{300} * p^{1} * q^{299} = 0,000899$$

$Q = P(0) + P(1) = 0{,}9991 + 0{,}000899 = 0{,}999999$ – імовірність правильного прийому блоку, якщо він містить 0 помилок або 1 помилку.

Відповідно, імовірність помилкового прийому блоку даних з виправленням одинарних помилок рівна:

$P_c = 1 - Q = 1 - 0{,}999999 = 10^{-6}$, що більш як в 100 разів перевищує задані вимоги.

Для виправлення одинарних помилок использован стандартний БЧХ код з поліномом $G(x)=X^{16} + X^{12} + X^5 + 1$.

Код Боуза – Чоудхурі – Хоквінгема в режимі корекції помилок

,Одним из основных преимуществ БЧХ кодов является то, что синдром ошибки $S(x) = |A(x)|_{G(x)}$ где $A(x) - \text{информационный полином}, G(x) -$ кодовый полином. Не зависит от информационной части блока данных, а определяется только вектором ошибки .Это значит, что $S(x) = \sum_{j=1}^{L} \alpha_j \cdot e_j$, где α_j - примитивныйэлемент кольца вычетов, e_j - значение вектора помехи $\varepsilon(x)$ для бита «j» в блоке, L- длина блока(бит).

При одиночной ошибке только один бит вектора ошибки равен 1, поэтому $S(x) = \alpha_j$., что и является локатором ошибки, которая исправляется..

Розміщення лінійного спектру сигналу на частотній осі

Для обеспечения электромагнитной совместимости определено положение линейного спектра на частотной оси при использовании следующих линейных сигналов:

- натуральний двійковий код;
- біімпульсний код;
- квазітроічний код;
- модульована (наприклад, по фазі) гармонійна несуча.

Найбільш оптимальним для системи обліку є застосування біімпульсного кодування.

Для забезпечення електромагнітної сумісності необхідно звести до мінімуму поза смугові електромагнітні випромінювання. Зазначена мета досягається за рахунок введення формуючого фільтра в абонентський термінал, подавляючого поза смугову компоненту як в області нижніх частот (до 3 кГц) так і в область верхніх частот (понад 9 кГц).

Захист обладнання від несанкціонованого доступу

Обладнання автоматизованої системи обліку використаних ресурсів є досить вразливим до дій абонентів, які спрямовані на порушення нормальної роботи окремих частин та всієї системи в цілому.

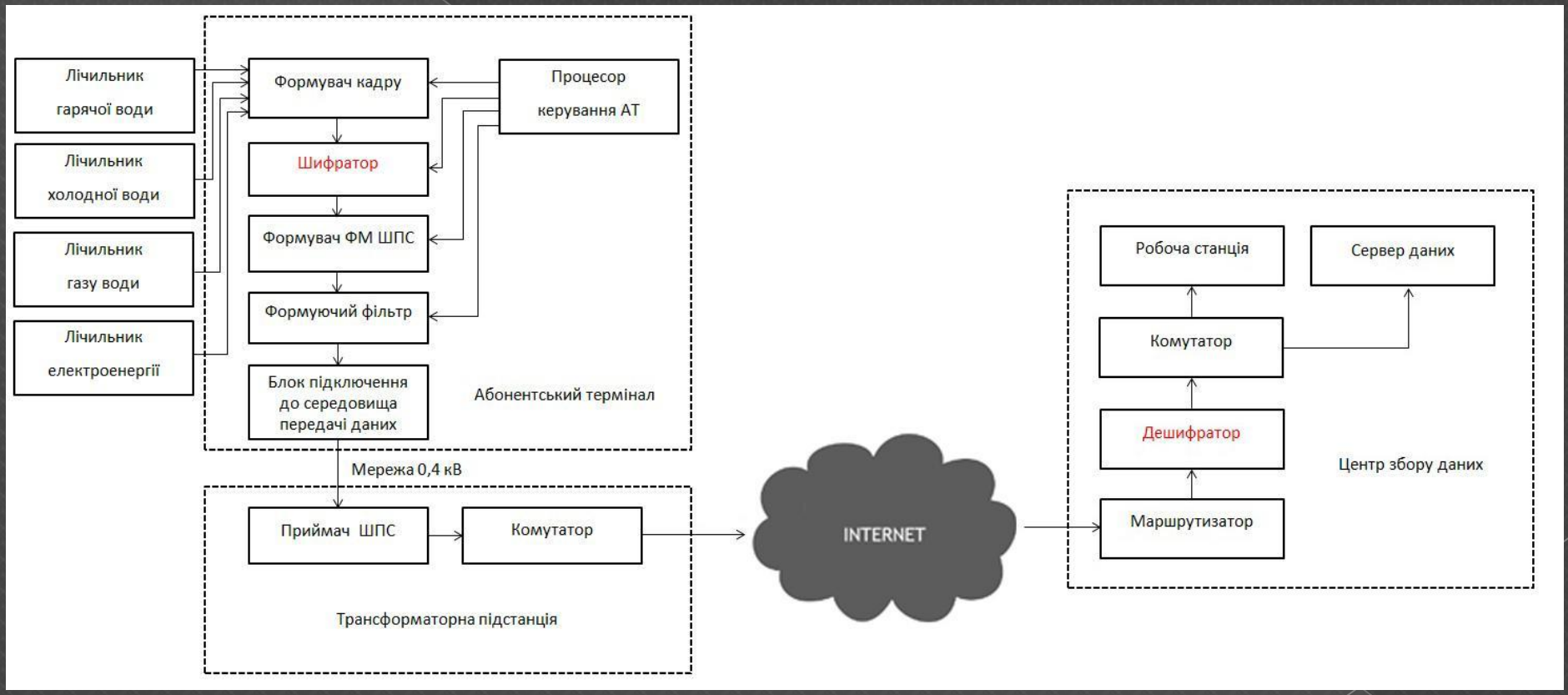
Система захисту АСОВР вирішує дві основні проблеми:

- забезпечує захист інформації від несанкціонованої модифікації;

- робить так, що будь – який вплив (контактний чи безконтактний) на обладнання відразу відслідковується.

Застосування у складі АСОВР сучасних лічильників до мінімуму скорочує небезпеку, яку можуть нанести абоненти обладнанню системи, маючи при цьому на меті заощадити будь – яким нечесним шляхом.

Структурна схема автоматизованої системи обліку використання ресурсів



Охорона праці та безпека в надзвичайних ситуаціях

Пристрої захисного вимкнення

Принцип роботи

Через пристрій проходить два провідники - нуль і фаза. В ідеалі струми, що проходять по обох провідниках, однакові. Якщо виникає різниця - це означає, що в якомусь із провідників є витік струму. Струм витоку виникає у випадках порушення ізоляції або подібним. При цьому в котушці диференційного реле виникає диференційний струм, спрацьовує штовхач та струм відключається. Повторне включення ПЗВ можливе тільки людиною.

Струмом витоку називають будь-який струм, який йде "на сторону" оминаючи штатних споживачів. Це відбувається при поганій ізоляції кабелю та / або при випадкових дотиках до оголених провідників, а в деяких випадках при спробах несанкціонованого використання електроенергії, тобто в обхід лічильника.

Час спрацьовування ПЗВ

Визначена затримка спрацьовування характеризується терміном - граничний час невимикання . Протягом цього нормованого відрізку часу ПЗВ не повинен спрацьовувати навіть при великому диференційному струмі. При короткочасному імпульсі диференційного струму енергія імпульсу недостатня для заряду конденсатора до рівня граничної напруги перекидного органа, а отже, не відбудеться спрацьовування вимикаючого реле і вимикання ПЗВ.

Метою затримки спрацьовування є усунення помилкових вимикань, що були і дотепер часто є аргументом проти використання ПЗВ.

Тип ПЗВ	Час вимкнення, с, при			
	$I_\Delta = I_{\Delta n}$	$I_\Delta = 2I_{\Delta n}$	$I_\Delta = 5I_{\Delta n}$	I_Δ = 500 mA
Для загального використання без затримки	<0,3	<0,15	<0,04	<0,04
З мінімальною затримкою 10 мс	0,01÷0,3	0,01÷0,15	0,01÷0,04	0,01÷0,04
Селективне з мінімальною затримкою 40 мс	0,13÷0,5	0,06÷0,2	0,05÷0,15	0,04÷0,15

Надзвичайні ситуації в ЖКГ

Економічна частина

Витрати на нову розробку:

Витрати	Грн.
Основна заробітна плата розробників	5600
Основна заробітна плата робітників	13100
Додаткова заробітна плата	1870
Нарахування на заробітну плату	7466
Амортизація	93
Витрати на комплектуючі	275000
Витрати на електроенергію	18
Інші витрати	37400
Всього	**340547**

Експлуатаційні витрати :

Витрати	Грн./рік
Заробітна плата обслуговуючого персоналу	3000
Додаткова заробітна плата	300
Нарахування на заробітну плату	2000
Амортизаційні відрахування	6250
Інші витрати	577
Всього	**12127**

Проведені розрахунки показали, що впровадження даної системи є економічно ефективним, так як шляхом модифікацій було значно зменшено експлуатаційні витрати на використання системи в порівнянні з її аналогами.

Висновки

В результаті проектування системи захисту даних було вирішено такі основні проблеми:

- захист інформації від несанкціонованого доступу до неї абонентів, зацікавлених у передачі неправдивих даних;

- забезпечення необхідного рівня достовірності інформації при передачі до центру збору даних;

- захист обладнання, його зовнішніх та внутрішніх частин, від негативного впливу абонентів.

Дипломний проект виконано в повній відповідності з технічним завданням.

Дякую за увагу!