УДК 004

В. Большов, магістр гр. КІ-21М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ТЕРМІНАЛІВ МЕРЕЖІ ПЛАТІЖНИХ АВТОМАТІВ

У статті розроблено програмне забезпечення, яке призначено для системи терміналів мережі платіжних автоматів. Метою розробки є дослідження та програмна реалізація системи терміналів мережі платіжних автоматів. Об'єктом дослідження є процес терміналів мережі платіжних автоматів. Предметом дослідження є методи терміналів мережі платіжних автоматів. Методи дослідження базуються на методах теорії комп'ютерних систем та мереж, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи терміналів мережі платіжних автоматів. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп'ютерна інженерія, платіжні автомати

Постановка проблеми. Сучасний світ неможливо уявити без мобільного зв'язку. Він проник в усі ніши нашого життя. Причому сучасний мобільний зв'язок виконує не тільки роль телефонного зв'язку, але є й могутнім центром телекомунікаційних засобів передачі інформації. GSM, CDMA, GPRS, EDGE, 3G, 4G, 5G – це далеко не повний перелік стандартів стільникового зв'язку та технологій передачі різного виду даних, починаючи від суто телефонної розмови і відеозв'язку й закінчуючи мобільним з'єднанням з мережею INTERNET [1-3]. Але як відомо за усе в житті приходиться платити. І тут виникає наступна задача, що потребує вирішення: як можна спростити процедуру оплати мобільного зв'язку. Звісно можна зайти до магазину й поповнити рахунок у продавця. Та на даному етапі розвитку техніки, існує й альтернативний варіант оплати витрат з мобільного зв'язку – це застосування автоматів самообслуговування. Термінал мережі платіжних автоматів (ТПМА) дозволяє повністю автоматизувати різні елементи процесів торгівлі й обслуговування залежно від розглянутої галузі, представляючи надійне й функціональне рішення, що дозволяє приймати наявні платежі [1-5]. Термінал мережі платіжних автоматів поставляється у вандалостійкому виконанні, що припускає здатність витримувати агресивні впливи з боку зовнішнього середовища зі збереженням повної працездатності [6]. Термінал мережі платіжних автоматів ідеально підходить для установки на частково охоронюваних територіях адміністративних будинків, торгових центрів і т.д.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи терміналів мережі платіжних автоматів.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи терміналів мережі платіжних автоматів.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем терміналів мережі платіжних автоматів.
- Дослідження системи терміналів мережі платіжних автоматів.
- Програмна реалізація системи терміналів мережі платіжних автоматів.

Об'єктом дослідження є процес терміналів мережі платіжних автоматів.

Предметом дослідження є методи терміналів мережі платіжних автоматів.

Методи дослідження базуються на методах теорії комп'ютерних систем та мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу.

Опис GSM/GPRS

Як було відмічено вище, для організації обміну інформацією між автоматом і віддаленим комп'ютером (сервером), використовується технологія бездротового зв'язку GPRS або GSM. Розглянемо ці технології.

Опис стандарту GSM

Стандарт GSM відноситься до другого покоління стандартів для стільникового зв'язку, заснованому на цифрових технологіях. Реалізоване в системах GSM повношвидкісне кодування мови дозволяє зробити її якість порівнянною з якістю стаціонарних телефонних мереж. Радіотелефон стандарту GSM можна умовно розділити на дві частини: абонентський модуль SIM (SIM-карта) і безпосередньо сам телефон, що містить апаратне й програмне забезпечення. SIM-карта служить підтвердженням дійсності абонента й містить у своїй пам'яті всі необхідні дані, пов'язані з повноваженнями конкретного абонента. Щоб викрадач не зміг нею скористатися, у неї вводять спеціальний ідентифікаційний номер (PIN-код). Використання SIM-карти також зручно тим, що при зміні апарата абонентові не потрібно міняти свій мобільний номер, він просто переставляє карту, і всі збережені на ній дані, включаючи записну книжку, стають доступними в новому апарату. Коли SIM-карти немає в апарату, доступ до абсолютної більшості послуг закритий, за винятком екстрених викликів (якщо дозволяє мережа). Виготовити дублікат SIM-карти дуже складно й у сукупності з функціями захисту, вона дає високий рівень захисту користувачів і мереж від несанкціонованого доступу.

Можливості GSM

У стандарті GSM уведено кілька функцій захисту. У першу чергу це шифрація радіоканалу, що виключає прослуховування третьою стороною, а також захист номера абонента (для запобігання розкриття його місцезнаходження). Крім стандартних можливостей, надаваних операторами стільникового зв'язка – місцевий, міжміська й міжнародний зв'язок, переадресація виклику й інших, телефони стандарту GSM дають своїм власникам ряд додаткових функцій: збереження мовних повідомлень, що надійшли в період, коли абонент був недоступний (голосова пошта), прийом повідомлення про факс, що прийшов (факс-пошта), визначення номера що дзвонить. Передбачено можливість передачі коротких повідомлень "із точки в точку" (пейджингу), тобто абоненти при бажанні можуть обмінюватися простими короткими (кілька десятків символів) повідомленнями (тарифи на цю послугу нижче, ніж на звичайні переговори). Функція мобільного модему/факсу поряд з повсюдним поширенням портативних комп'ютерів дає можливість доступу до Інтернету й електронної пошти через мережу GSM. Ці послуги значно збільшують привабливість використання телефонів GSM для користувачів. Так, приміром, факс-пошта може бути дуже корисна діловій людині, тому що дозволяє не пропустити інформацію про факс у будь-який час, незалежно від місцезнаходження абонента. Мобільний телефон сповістить свого власника, а той може одержати факс коли завгодно й де завгодно, тому що факс автоматично надходить у його електронну поштову скриньку.

Технологія GPRS

Нові можливості GPRS дозволили ввести принципово нові послуги, які раніше не були доступні. Насамперед це мобільний доступ до ресурсів Internet із задовольняючого споживача швидкістю й з дуже вигідною системою тарифікації. Приміром, за допомогою системи GPRS абонент може переглядати WEB-сторінки в Internet стільки, скільки йому необхідно, оскільки плата стягується тільки за обсяг прийнятої інформації, а не за час знаходження в мережі Internet. При введенні погодинної оплати на фіксованих телефонних лініях, тарифи на доступ в Internet з мобільного GPRS-телефону будуть ще більш конкурентоспроможні. Технологія GPRS дозволить швидко передавати й одержувати

більші обсяги даних, відеозображення, музичні файли стандарту MP3 і іншу мультимедійну інформацію. Для корпоративних користувачів система GPRS може послужити відмінним інструментом для забезпечення безпечного й швидкого доступу співробітників до корпоративних мереж підприємств, до поштових, інформаційних серверів, віддаленим базам даних. Технології GPRS може застосовуватися в системах телеметрії: пристрій може бути увесь час підключений , не займаючи при цьому окремий канал. Така послуга може бути затребувана службами охорони, банками для підключення банкоматів і в інших областях, у тому числі й промислових.

Мережі GPRS-GSM

Щоб підтримувати GPRS, мережі GSM повинні бути доповнені двома основними функціональними елементами: Serving GPRS Support Node (SGSN) – вузол, яким грає в мережі GPRS ту ж роль, що й комутатор MSC і гостьовий регістр VLR у мережі GSM: і Gateway GPRS Support Node (GGSN) – еквівалент блоку IWF (interworking unit) у мережі GSM:

- SGSN – відповідає за доступ абонентів у мережу GPRS (автентифікацію), а також моніторинг абонентів і трафика. Він служить для автентифікації встаткування й фіксує всі «дії» мобільного абонента в мережі.
- GGSN служить гейтом, тобто, з'єднує мережу GPRS і зовнішні мережі загальнодоступні або частні.

Втім, говорити про два основні елементи можна лише з деякою натяжкою, оскільки кожен контролер у мережі GSM повинен бути дообладнаний пристроєм PCU (блок керування пакетним зв'язком).

Додамо, що в мережі GSM-GPRS з'являється кілька нових інтерфейсів, кожний із префіксом «G».

- Gp – це протокол Frame Relay, однак, перехід до технології UMTC дозволить впровадити замість Frame Relay протокол ATM (Asynchronous Tr.mfer Mode) – це, до речі, викличе перехід до комутаторів ATM від сьогоднішніх комутаторів MSC.
- Gr – протокол з комутацією з'єднань типу C7.
- Gn – протокол пакетної передачі типу TCP/IP (Transmisson Control Protocol і Internet Protocol).

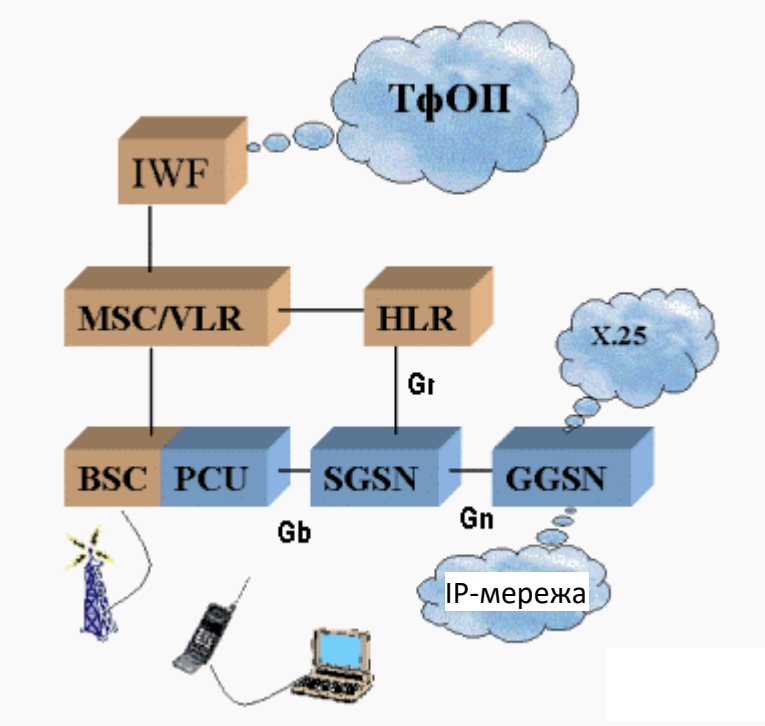

Рисунок 1 – Структура мережі GSM-GPRS

Підключення по GPRS

Набір додатків по оцінках фахівців може включати:

- e-mail;
- доступ до Internet;
- телеметрію;
- підтримка протоколу бездротових додатків (WAP);
- підтримка протоколу передачі файлів (FTP).

Електронна пошта – це послуга, що забезпечує абонентів стільникової мережі (клієнтів) можливістю одержувати й відсилати повідомлення по мережі Internet без необхідності доступу до комп'ютера. Кожний, хто має адресу в Internet, зможе відіслати повідомлення будь-кому, чия електронна адреса вам відомийа. Джерелом адреси для вас може бути ISP (Internet Service Provider – провайдер) або оператор стільникової мережі, якщо він візьме на себе ці функції. У технічному плані – це комп'ютер, підключений до Internet, що буде зберігати отримані на ваше ім'я повідомлення поки ви їх не заберете (наприклад, до пам’яті телефону або вашого домашнього комп'ютера).

Доступ до Internet. Web – це розподілена інформаційна система, заснована на технології сервер-клієнт. Клієнтська програма, це ваш браузер (Internet Explorer, Netscape, Linux або який-небудь інший). Ви можете підключитися браузером до сайту, де зберігаються сторінки, що цікавлять вас, включаючи текст, графіку, а також мультимедіа (відеофрагменти, музика).

Телеметрія. Віддалений моніторинг сайтів в Internet або якого-небудь устаткування – створені нібито спеціально для GPRS, оскільки «підривний» характер передачі даних надзвичайно вдало вписується в технологію пакетного зв'язку GPRS.

WAP. Протокол Бездротових Додатків – WAP зараз рекламується як якийсь прорив, що дозволить забезпечити тотальний доступ до інтернет-ресурсам з мобільних пристроїв, насамперед телефонів. Число WAP-сумісних ресурсів в Internet зараз росте швидкими темпами, з'явилися й перші українські ресурси.

FTP. Це сервіс, призначений для копіювання файлів з одного комп'ютера на інший. Може використовуватися в торговельних й бізнес-додатках.

Стандарти GPRS-терміналів

Клас А. Термінал дозволяє одночасно здійснювати передачу мови й даних у режимі GPRS.

Клас В. Термінал підтримує й голосове з'єднання, і передачу даних у пакетному режимі (GPRS), але або режими використовуються не одночасно (під час передачі даних через GPRS абонент не може робити й приймати голосові дзвінки й навпаки).

Клас С. Термінал забезпечує тільки передачу даних у пакетному режимі. Найбільш імовірне виконання – у вигляді PCMCIA-карти, установлюваної в портативний комп'ютер.

Швидкість прийому й передачі інформації залежить від можливостей конкретної моделі мобільного термінала, а саме від кількості каналів, що підтримують прийом і передачу даних. При цьому один канал підтримує передачу інформації з максимальною швидкістю 13.4 кб/с. Повна мобільність має на увазі, що людині повсюдно стають доступні всі можливості, які він має на своєму робочому місці, такі як швидкісний доступ в Internet. GPRS (General Packet Radio Service) – технологія, що робить це реальним уже сьогодні. Суть послуги полягає в організації постійного підключення через GPRS-телефон до мережі Internet. Для роботи в мережі можливо використовувати комп'ютер (наприклад, ноутбук) або електронний органайзер (Palm Pilot, Psion, Cassiopea). При цьому абонент має можливість переглядати HTML-сторінки, перекачувати файли, працювати з електронною поштою й будь-якими іншими ресурсами Internet. Чим приваблива ця технологія:

- GPRS надає негайний доступ до послуг, без необхідності додзвонюватися до інтернет-провайдеру.
- Користувачі GPRS одержують доступ до Internet у повному обсязі, як при провідному з'єднанні.

- Можна працювати з WAP-сайтами безпосередньо з телефонного апарата GPRS.
- Оплачується тільки обсяг посланої/отриманої інформації, а не ефірний час. Дотепер у стільникових мережах для передачі або прийому даних абонентом займався цілий канал на час від установлення з'єднання до його розриву, що оплачувалося поза залежністю від його завантаження.
- В GPRS максимально можлива швидкість передачі даних становить 171,2 Кбіт/с – це більш ніж в 3 рази швидше, ніж режим роботи провідних ліній, і майже в 12 разів швидше роботи передачі даних у звичайних мережах GSM (9,6 Кбіт/с). Уже сьогодні доступна швидкість до 33 Кбіт/с.

EDGE

EDGE (Enhanced Data rates for Global Evolution) – у перекладі з англійського – це вдосконалена технологія передачі даних для глобального розвитку, що забезпечує високошвидкісну передачу великих обсягів інформації, характерну для мереж третього покоління мобільного зв'язку.

Технологія EDGE надається абонентам на базі послуги GPRS . Технологія EDGE забезпечує швидкість передачі даних, у середньому в три рази перевищуючу можливості GPRS, а також – більш ефективне використання частотних ресурсів і поліпшення покриття мережі в порівнянні зі звичайною мережею стандарту GSM. Технічні особливості EDGE дозволять абонентам більш оперативно працювати з Інтернет-ресурсами (web, wap, e-mail, ICQ) і користуватися найширшим спектром неголосових послуг, що вимагають високих швидкостей передачі даних. Виявившись у зоні дії базової станції з підтримкою EDGE, телефон абонента буде автоматично використовувати EDGE замість традиційного GPRS. Швидкість з'єднання залежить від кількості одночасних користувачів, класу телефону з підтримкою EDGE, умов радіоприйома й співвідношення сигнал/шум. Середня швидкість у мережі 80-120 Кбіт/с.

Опис програмного забезпечення

Програмне забезпечення повинне забезпечувати наступні функції:

1. Первісне налаштування.
2. Сервісне обслуговування автоматів.
3. Установка й налаштування таймера.
4. Налаштування додаткових параметрів через командний рядок.
5. Моніторинг функціонування терміналів.
6. Робочий режим.

Для коректної роботи ПЗ необхідно, щоб на автоматі самообслуговування було попередньо встановлене наступне програмне забезпечення:

- Операційна система Windows 10/11.
- MS Internet Explorer версії 5 або вище.

Крім того, перед початком роботи треба переконатися, що в операційній системі автомата настроєне з'єднання з Інтернет. У якості Інтернет-з'єднання може використовуватися як канал GPRS, так і будь-який інший доступний спосіб з'єднання. Для доступу в Інтернет ПЗ використовує налаштування Internet Explorer, тому у випадку використання proxy-сервера, при підключенні автомата в локальну мережу, необхідно додати proxy у налаштування «Internet Explorer».

Розглянемо перераховані вище функції більш докладно.

1. Первісне налаштування.

При першому запуску системи вам необхідно настроїти дані для авторизації автомата в системі оплати послуг мобільних операторів. Спершу треба перейти в параметри авторизації, тобто ввести значення параметрів:

– Номер термінала – ідентифікатор термінала в системі оплати послуг оператора мобільного зв'язку (ТПМА). У модулі адміністратора системи ТПМА повинен бути зареєстрований термінал, під яким будуть проводитися платежі. Терміналу повинен бути

заданий тип Автомат ТПМА. Неприпустиме використання того самого номера термінала декількома пристроями. Для кожного автомата, реєструйте в системі новий термінал:

– Ім'я користувача – логін користувача, від імені якого будуть відбуватися платежі.

– Пароль – пароль користувача, від імені якого будуть відбуватися платежі.

– Підтвердження пароля – у дане поле необхідно повторно ввести пароль користувача для підтвердження його коректності.

У якості логіна й пароля повинні використовуватися дані персони, зареєстрованої в системі ТПМА із правами «Продавець». Припустимо використання однакових даних користувача в різних автоматах.

Після цього необхідно настроїти параметри сервісного доступу автомата, тобто ввести налаштування для входу в режим обслуговування й інкасації автомата:

- Секретний номер телефону – задається номер телефону, що дозволяє перевести автомат у сервісний режим і потрапити в панель налаштування.

- Ім'я користувача – логін користувача, що буде здійснювати сервісне обслуговування автомата.

- Пароль – пароль користувача, що буде здійснювати сервісне обслуговування автомата.

- Підтвердження пароля – у дане поле необхідно повторно ввести пароль користувача для підтвердження його коректності.

Користувач, під ім'ям якого буде здійснюватися сервісне обслуговування автомата не повинен бути зареєстрований у системі ТПМА. Тому, для логіна й пароля ви можете використовувати будь-яку комбінацію символів. Реєструвати в ТПМА даного користувача не потрібно.

Після цього етапу відбувається налаштування системи Параметри з'єднання з Інтернет і опції автомата:

- З'єднання з Інтернет – у даному полі прапором відзначте те з'єднання, через яке автомат буде здійснювати комунікацію із системою ТПМА.

- Задати рядок ініціалізації модему – дозволяє вказати нестандартний рядок ініціалізації модему для поточного обраного з'єднання.

- Включити стиск даних, переданих через Інтернет – дозволяє включити додатковий стиск даних, переданих через Інтернет з метою економії трафика.

- Включити мультиканальний режим – включення мультиканального режиму.

- Опції автомата – панель додаткових опцій автомата:

- Зупиняти автомат при помилках купюроприймача – даний прапор дозволяє припинити прийом платежів при виявленні яких-небудь проблем у роботі купюроприймача.

- Зупиняти автомат при помилках принтера – даний прапор дозволяє припинити прийом платежів при виявленні яких-небудь проблем у роботі принтера чеків. При знятому прапорі автомат буде продовжувати приймати платежі, навіть якщо в принтері закінчився папір для печаті чеків.

- Зупиняти автомат при відсутності засобів на рахунку агента – даний прапор дозволяє припинити прийом платежів на автоматі при відсутності засобів в агента.

- Зупиняти автомат при відсутності зв'язку – даний прапор дозволяє припинити прийом платежів при відсутності зв'язку з автоматом протягом зазначеного періоду часу (за замовчуванням, 15 хвилин).

- Не перезапускати програмно модем у випадку відсутності сторожового таймера – відзначте прапор, щоб відключити опцію програмного перезавантаження модему у випадку відсутності сторожового таймера.

Після цього автомат переходить у робочий режим. Якщо в автомат не завантажені файли інтерфейсу, автомат скачує їх автоматично із сервера ТПМА. Даний процес може зайняти досить тривалий час (мінут 30-40 при використанні GPRS з'єднання), при цьому на екрані буде показане повідомлення «Вибачте, автомат тимчасово не працює». У робочому

режимі в деяких випадках можлива поява наступного напису: «Вибачте, автомат тимчасово не працює» Даний напис означає, що були виявлені проблеми з купюроприймачом або принтером чеків.

2. Сервісне обслуговування автоматів.

Воно складається з наступних підрозділів:

- Перехід у режим обслуговування й інкасації.
- Сервісне меню.
- Зміна провайдеру GPRS зв'язку.
- Мультиканальний режим роботи модему.

Розглянемо їх більш докладно.

Перехід у режим обслуговування й інкасації. Для цього необхідно вибрати опцію Оплата послуг, ввести номер телефону, що задали при налаштуванні автомата й розблокувати сервісний режим за допомогою імені користувача й пароля.

Сервісне меню. Містить такі дані як:

- Версія інтерфейсу.
- Кількість купюр у купюроприймачі й суму.
- Статус купюроприймача.
- Статус принтера.
- Статус з'єднання.
- Статус сторожового таймера.
- Статус платежів.

За допомогою кнопок у вікні сервісного меню можна виконувати також наступні дії:

- Змінити номер термінала, логін і пароль ТПМА.
- Змінити параметри входу в сервісний режим.
- Змінити параметри Інтернет і опції автомата.
- Налаштування інтерфейсу.
- Налаштування e-mail оповіщень.
- Налаштування Multi SIM підключення.
- Видалити файл конфігурації й запустити знову програму.
- Переглянути лог.
- Запустити відновлення.
- Видалити файл конфігурації й запустити знову програму.
- Вийти й запустити знову програму.
- Настроїти параметри безпеки при роботі з додатком.

Крім цього, дозволяє виконувати й контролювати наступні дії:

- Проведення інкасації.
- Налаштування параметрів принтера.
- Рівень сигналу GSM мережі.
- Налаштування одержання балансу.
- Налаштування оповіщень.
- Налаштування параметрів сторожового таймера.
- Налаштування інтерфейсу.
- Режим підтримки двох SIM-карт.
- Безпека.
- Режим блокування системних комбінацій клавіатури.

Зміна провайдеру GPRS зв'язку. Призначено для введення параметрів передачі даних по мережі GSM, операторів, які не прописані в автоматі ТПМА.

Мультиканальний режим роботи модему. Даний режим дозволяє здійснювати одночасно наступні дії:

- передача даних по Інтернет;
- відправлення SMS;
- одержання рівня сигналу й інших даних про стан GSM мережі;

- відправлення USSD запитів балансу SIM карти.

Таким чином, використання даного режиму дозволяє, не розриваючи модемне з'єднання з Інтернет, одержувати безупинно дані про баланс SIM карти, коливання рівня сигналу й дані про стан GSM мережі. Підключення мультиканального режиму відбувається в кілька етапів:

- Установка драйвера для мультиканального режиму.
- Установка стандартного драйвера модему.
- Створення модемного з'єднання.
- Налаштування ПЗ автомата.

3. Установка й налаштування таймера.

Таймер дозволяє здійснювати дві основні функції:

- Перезавантаження модему, при відсутності відгуку від модему протягом деякого часу. Даний режим роботи включений за замовчуванням.
- Перезавантаження комп'ютера при відсутності сигналу від комп'ютера протягом 30 мінут.

Таким чином, за допомогою плати відслідковується «зависання» комп'ютера або модему й коректуються дані проблеми шляхом перезавантаження модему або комп'ютера. Період в 30 мінут для перезавантаження комп'ютера обраний з метою виключення ситуацій помилкового спрацьовування: при відновленні даних із сервера й т.п.

4. Налаштування додаткових параметрів через командний рядок.

За допомогою командного рядка ви можете вказати параметри, відмінні від параметрів за замовчуванням для принтера й купюроприймача. Вони підрозділяються на:

- Параметри принтера й купюроприймача.
- Додаткові параметри.

5. Моніторинг функціонування терміналів.

Для зручності відстеження роботи ваших автоматів самообслуговування, у системі ТПМА передбачена можливість віддаленого моніторингу в реальному часі. Дана функціональність доступна користувачам із правами головного менеджера, і містить у собі:

- Моніторинг через Інтернет.
- Моніторинг за допомогою мобільного телефону.

6. Робочий режим.

Його робота полягає у виконанні трьох основних функцій:

- Прийом платежів. Інтерфейс для прийому платежів розроблений таким чином, щоб максимально спростити процес звернення клієнта до автомату і зробити прийом платежів за допомогою автомата інтуїтивно зрозумілим без додаткових інструкцій.
- Відновлення ПЗ. Після виходу нової версії ПЗ, автомат автоматично завантажує відновлення, не припиняючи роботу. Також автоматично відбувається відновлення зовнішнього вигляду інтерфейсу автомата: додавання можливості оплати послуг нових провайдерів і т.п.
- Режим автоматичного включення автомата. Призначений для того, щоб настроїти автоматичне включення автомата після збоїв електрики в мережі.

Розробка структурної схеми

Створене програмне забезпечення призначене для забезпечення користувачів послугою поповнення рахунку мобільного телефону. Воно універсальне, може бути використана терміналах фірми «Об'єднана система швидких платежів» серії: ОСМП-2; ОСМП-МІНІ; ОСМП-ВУЛИЦЯ; ОСМП 2 з лайт-боксом; ОСМП 2 з двома моніторами. На рисунку 2 показана структурна схема програмного забезпечення, розглянемо її з верху долілиць.

Рисунок 2 – Структурна схема програмної частини

Коли на термінал надходить запит обслуговування, невідомо користувач є адміністратором чи ні. Для проходження автентифікації крім магнітного ключа адміністраторові необхідно знати системний 9 значний номер телефону перекладу термінала в інтерфейс адміністратора.

Коли магнітний ключ приєднаний до термінала, й користувач ввів системний номер телефону, на екрані з'являється форма автентифікації, що запитує ім'я користувача й пароль, при правильному введенні даних користувачеві привласнюється статус адміністратора й автомат переходить у режим налаштування, у противному випадку користувачеві дається ще дві спроби після відбування, яких відбувається включення тривоги, передача сигналу на базовий ПК і повне блокування термінала.

Адміністратор повністю управляє комп'ютером, він може управляти всіма налаштуваннями й опціями термінала: статус з'єднання; встановлення рядка ініціалізації модему; встановлення архівації та кодування даних; кількість купюр у купюроприймачі й суму; статус купюроприймача; статус принтера; статус сторожового таймера; статус платежів; налаштування інтерфейсу; налаштування e-mail оповіщень; налаштування Multi SIM підключення; видалення файлу конфігурації й перезапуск терміналу.

Також за допомогою кнопок у вікні сервісного меню можна управляти наступними опціями: зупиняти авт. при помилках купюроприймача; зупиняти автомат при помилках принтера; зупиняти автомат при відсутності засобів на рахунку користувача; зупиняти автомат при відсутності зв'язку; змінювати номер термінала, логін і пароль; змінити параметри входу в сервісний режим; переглядати лог. файл.

Також адміністратор може зробити інкасацію коштів. Виконання даної операції здійснюється через комп'ютерний відсік шляхом зняття грошової касети із кріплення купюроприймача, попередньо запустивши процес інкасації в програмному забезпеченні термінала.

Якщо системний номер адміністратора не був введений, термінал переходить в інтерфейс користувача, перемикається на режим обслуговування клієнтів, і користувач,

натискаючи на сенсорній панелі кнопки, вибирає необхідні розділи, після чого відбувається видача чека з поповненням рахунку мобільного телефону.

На рисунку 3 можна побачити складові частини термінала, а саме: TFT 17" вандалостійкий сенсорний монітор; Вандалостійкий корпус; IBM PC сумісний комп'ютер; Пристрій для печатки бланків; Пристрій для прийому грошей.

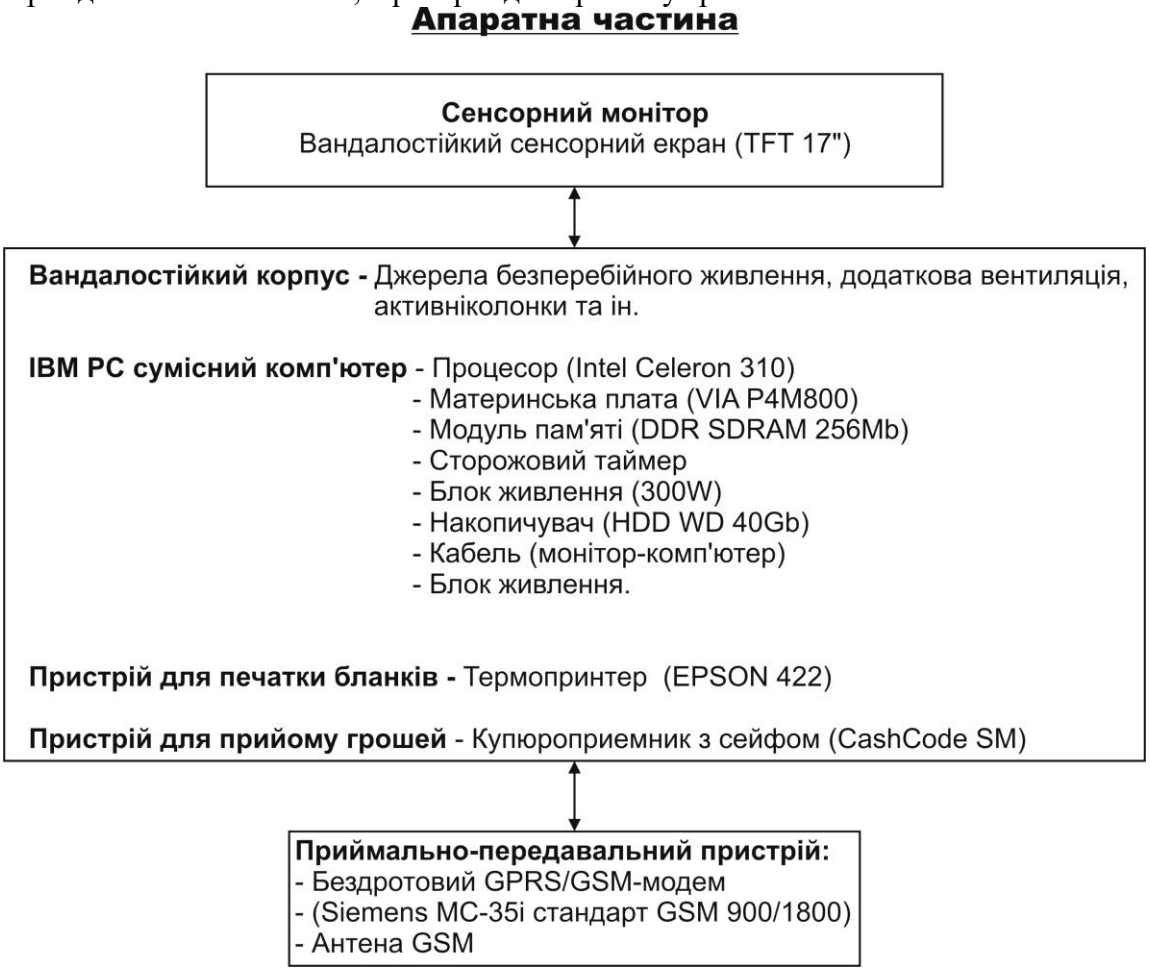

Рисунок 3 – Структурна схема апаратної частини

Розглянемо докладніше основні елементи терміналу. Серце термінала комп'ютерний відсік, що знаходиться у вандалостійкому корпусі. Являє собою комп'ютерну частину термінала й вузол об'єднання всіх пристроїв у єдину систему. Включає у свій состав IBM PC сумісний комп'ютер, розташований у верхній частині термінала (рисунок 4), що складається з наступних складових елементів**:**

– Процесор (Intel Celeron 310);
– Материнська плата (VIA P4M800);
– Модуль пам'яті (DDR SDRAM 256Mb);
– Сторожовий таймер;
– Блок живлення (300W);
– Накопичувач (HDD WD 40Gb);
– Кабель (монітор-комп'ютер)
– Блок живлення.

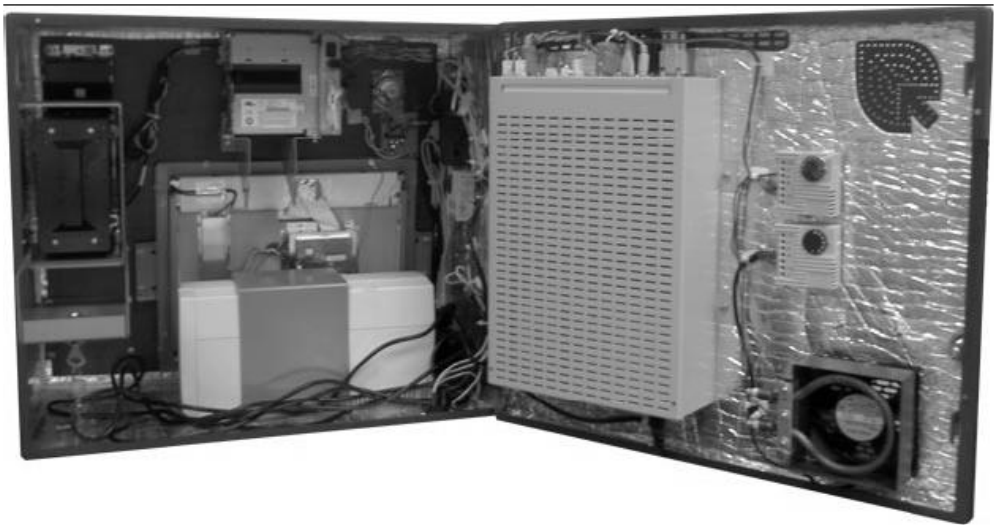

Рисунок 4 – Комп'ютерний відсік

Як видно з основних характеристик комп'ютерного відсіку комп'ютер повністю сполучимий з настільним ПК, у ньому встановлена операційна система Windows 10/11 (залежно від конфігурації складових елементів) з відповідними перевагами й недоліками. Всі вузли термінала (сенсорний монітор, принтер, GPRS/GSM модем, і т.д.) підключаються через стандартні роз'ми ПК. Основна відмінність від настільного ПК є форма корпуса, який поміщено у вандалостійкий корпус (рисунок 4).

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів терміналів мережі платіжних автоматів. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем терміналів мережі платіжних автоматів; Досліджена система терміналів мережі платіжних автоматів; На основі отриманих результатів досліджень створена програмна реалізація системи терміналів мережі платіжних автоматів; Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Kovalenko Oleksandr Qualitative risk analysis of software development / Oleksandr Kovalenko, Jamil Al-Azzeh, Oleksii Smirnov, Anna Kovalenko, Serhii Smirnov // Asian Journal of Information Technology. – Volume 17 Issue 3. – Medwell Journals. – 2018. – P. 218-230. ISSN: 1682-3915. URL: http://medwelljournals.com/abstract/?doi=ajit.2018.218.230 Doi: ajit.2018.218.230
2. Kovalenko Oleksandr, The mathematical model of the testing technology for DOM XSS vulnerabilities / O. Kovalenko, O. Smirnov, A.Kovalenko, S. Smirnov, V. Vialkova // Scientific & practical cyber security journal (SPCSJ) Volume 2 Issue 1, P. 22-28. Georgia. Tbilisi. Scientific Cyber Security Association (SCSA), 2018 ISSN: 2587-4667. URL: https://journal.scsa.ge/wp-content/uploads/2018/12/04-3-o.kovalenko-a.kovalenko-o.smirnov-s.smirnov-v.vialkova.pdf
3. Коваленко А.В. Технология тестирования DOM XSS уязвимости / А.В. Коваленко, А.С. Коваленко, А.А. Смирнов, С.А. Смирнов // Scientific & practical cyber security journal (SPCSJ) Volume 1. Issue 1. P. 38-45 Georgia. Tbilisi. Scientific Cyber Security Association (SCSA), 2017 ISSN: 2587-4667. URL: https://journal.scsa.ge/wp-content/uploads/2018/12/8-dom-xss-testing-technology-vulnerabilities.pdf
4. Коваленко А.В. Методы качественного анализа и количественной оценки рисков разработки программного обеспечения / А.В. Коваленко, А.А. Смирнов // Информационные технологии в управлении, образовании, науке и промышленности: монография / Под редакцией профессора В.С. Пономаренко. – Х.: Видавець Рожко С.Г., 2016. – 566 с.
5. Коваленко А.В. Разработка метода управления рисками разработки программного обеспечения / А.В. Коваленко, А.А. Смирнов // Інформаційні технології: проблеми та перспективи: монографія / За загальною редакцією В.С. Пономаренка. – Х.: Видавець Рожко С.Г., 2017. – 447 с.
6. Коваленко А.В. Комплекс математических моделей технологии тестирования web-

приложений / А.В. Коваленко, А.А. Смирнов // Інформаційні технології: сучасний стан та перспективи: монографія / За загальною редакцією В.С. Пономаренка. – Х.: ТОВ «ДІСА ПЛЮС», 2018. – 461 с.
7. Коваленко А.В. Задачи распознавания ситуаций в erp системах / А.В. Коваленко, А.А. Смирнов, А.С. Коваленко // Збірник наукових праць "Системи обробки інформації". – Випуск 4(120). – Х.: ХУПС – 2014. – С. 161-164.
8. Коваленко А.В. Методы качественного анализа и количественной оценки рисков разработки программного обеспечения / А.В. Коваленко, А.А. Смирнов // Збірник наукових праць "Системи обробки інформації". – Випуск 5(142). – Х.: ХУПС – 2016. – С. 153-157.
9. Коваленко А.В. Проблемы анализа и оценки рисков информационной деятельности / А.В. Коваленко, А.А. Смирнов, Н.Н. Якименко, А.П. Доренский // Збірник наукових праць "Системи обробки інформації". – Випуск 3(140). – Х.: ХУПС – 2016. – С. 40-42.
10. Коваленко А.В. Метод качественного анализа рисков разработки программного обеспечения / А.В. Коваленко, А.А. Смирнов, Н.Н. Якименко, А.П. Доренский // Наука і техніка Повітряних Сил Збройних Сил України. – Випуск 2(23). – Харків: ХУПС. – 2016. – С. 150-158.
11. Коваленко А.В. Метод количественной оценки рисков разработки программного обеспечения / А.В. Коваленко, А.А. Смирнов, Н.Н. Якименко, А.П. Доренский // Збірник наукових праць Харківського університету Повітряних Сил. Випуск 2 (47). – Харків: ХУПС. – 2016. – С. 128-133.
12. Коваленко А.В. Использование псевдобулевых методов бивалентного программирования для управления рисками разработки программного обеспечения / А.В. Коваленко, А.А. Смирнов // Системи управління, навігації та зв'язку. – Випуск 1 (37). – Полтава: ПолтНТУ. – 2016. – С. 98-103.
13. Коваленко А.В. Проблемы анализа и оценки рисков информационной деятельности / А.В. Коваленко, А.А. Смирнов // Збірник наукових праць II міжнародної науково-практичної конференції «Актуальні питання забезпечення кібернетичної безпеки та захисту інформації». м. Київ. 24-27 лютого 2016 р. – Київ: Європейський університет. – 2016. – С. 138-139.
14. Коваленко А.В. Анализ и оценка рисков разработки программного обеспечения / А.В. Коваленко, А.А. Смирнов // Збірник тез «Securitea informationala 2015-2016». Conferenta internationala (editia a XII-a). Chisinau. Moldova. 3 martie 2016. – Chisinau: ADSEM. – 2016. – P. 96-102.
15. Коваленко А.В. Исследование источников и причин риска разработки программного обеспечения, этапов и работ, при выполнении которых возникает риск / А.В. Коваленко, А.А. Смирнов // Збірник тез VII всеукраїнської науково-практичної конференції "Інформатика та системні науки (ІСН-2016)". м. Полтава. 10-12 березня 2016 р. – Полтава.: ПУЕТ – 2016. – С. 264-266.
16. Коваленко А.В. Оценка показателя чистой приведенной стоимости для количественной оценки рисков проекта разработки программного обеспечения / А.В. Коваленко, А.А. Смирнов // Збірник тез науково-практичної конференції "Проблеми кібербезпеки інформаційно-телекомунікаційних систем". м. Київ. 10-11 березня 2016 р. – Київ: КНУ ім. Тараса Шевченко – 2016. – С. 81-82.
17. Коваленко А.В. Методика структурной идентификации рисков разработки программного обеспечения / А.В. Коваленко, А.А. Смирнов // Збірник тез Міжнародної науково-практичної конференції «Інформаційна безпека та комп'ютерні технології» (IS&CT). м. Кіровоград. 24-25 березня 2016 р. – Кіровоград: КНТУ. – 2016. – С. 71-72.
18. Коваленко А.В. Методы качественного анализа рисков разработки программного обеспечения / А.В. Коваленко, А.А. Смирнов // Збірник тез першої міжнародної науково-практичної конференції «Проблеми науково-технічного та правового забезпечення кібербезпеки у сучасному світі» (ПНПЗК-2016). м. Харків. 30 березня – 1 квітня 2016 р. – Харків: НТУ «ХПІ». – 2016. – С. 6-7.
19. Коваленко А.В. Структурная идентификация рисков разработки программного обеспечения / А.В. Коваленко, А.А. Смирнов // Збірник тез XVIII міжнародного науково-практичного семінару «Комбінаторні конфігурації та їх застосування». м. Кіровоград. 15-16 квітня 2016 р. – Кіровоград: КНТУ. – 2016. – С. 175-182.
20. Коваленко А.В. Исследование разработанной методики структурной идентификации рисков разработки программного обеспечения / А.В. Коваленко, А.А. Смирнов // Збірник тез VIII міжнародної науково-практичної конференції "Проблеми і перспективи розвитку IT-індустрії". м. Харків. 28-29 квітня 2016 р. – Харків: ХНЕУ. – 2016. – С. 49.