**УНИВЕРСИТЕТ "ПРОФ. Д-Р АСЕН ЗЛАТАРОВ"-БУРГАС,**
**БУГАС, БЪЛГАРИЯ**

# АВТОРЕФЕРАТ

ЗА ПРИДОБИВАНЕ НА ОБРАЗОВАТЕЛНА И НАУЧНА СТЕПЕН
"ДОКТОР"

на **гл.ас. Христо Димитров Панайотов**

ТЕМА: **Обобщеномрежово моделиране**
**на използване на мобилни комуникации**
**в повишаване сигурността на информацията**

| | |
|---|---|
| Област на висшето образование: | Технически науки |
| Професионално направление: | 5.3. Комуникационна и компютърна техника |

**НАУЧНИ РЪКОВОДИТЕЛИ:**

1. чл.кор. проф. дтн дмн Красимир Т. Атанасов
2. доц.д-р Евдокия Н. Сотирова

**РЕЦЕНЗЕНТИ:**

1. проф. дтн Людмил Даковски
2. проф. д-р Магдалина Тодорова

БУРГАС, 2014

Дисертационният труд е обсъден и допуснат до защита на разширено заседание на катедра “Компютърни системи и технологии”, проведено на 20.06.2014 г. в Университет “Проф. д-р Асен Златаров” – Бургас.

Дисертационният труд съдържа 119 страници, от които 19 фигури и 1 таблица. Използвани са 123 литературни източници. Резултатите са представени в 5 публикации.

Защитата на дисертационния труд ще се състои на .....2014 г. от ..... ч. в зала ..... в Университет “Проф. д-р Асен Златаров”-Бургас на научно жури в състав:

1. доц.д-р Станислав Симеонов
2. доц.д-р Евдокия Сотирова
3. проф. дтн Людмил Даковски
4. проф. д-р Магдалина Тодорова
5. доц.д-р Таня Пенчева

Резервни членове: доц.д-р Любка Дуковска
доц.д-р Сотир Сотиров

Материалите по защитата са предоставени за заинтересуваните в кабинет 303, Органичен корпус.

Автор: Христо Димитров Панайотов
Заглавие: Обобщеномрежово моделиране на използване на мобилни комуникации в повишаване сигурността на информацията мрежи

За подкрепата изказвам благодарност на ръководителите си
чл.-кор. проф. дмн дтн Красимир Атанасов
и доц. д-р Евдокия Сотирова.

Благодаря и за подкрепата на всички колеги от катедра „Компютърни системи и технологии“ при Университет „Проф. д-р Асен Златаров“.

## Характеристика на дисертационния труд

Настоящият дисертационен труд изследва възможности за използване на мобилни комуникации в повишаване сигурността на информацията и моделирането им чрез апарата на Обобщените мрежи. Терминът „обобщена мрежа“ е въведен през 1982 г. от проф. Кр. Атанасов.

Непрекъснатото развитие на новите технологии изисква средства за защита на конфиденциалността, интегритета и достъпността на данните. Предимствата на мобилната комуникация предоставят възможност за тясното им интегриране с Интернет технологиите.

Развитието на мобилните комуникации в последното десетилетие оформя ясна тенденция за постепенната им миграция към персоналните компютри. Смартфоните, като мобилни апарати с операционна система, поставят на дневен ред същите проблеми по отношение на сигурността на информацията – неоторизиран достъп, използване, разкриване, дезинтеграция, изменение или разрушение, а също и несанкционирано подслушване на комуникациите.

Видно е, че значението на сигурността ще нараства с увеличаването както на потребителите на информационни услуги, така и на услугите, предлагани чрез публични компютърни мрежи и Интернет.

Развитието и масовизирането на GSM комуникациите биха могли да се превърнат в допълнително средство за повишаване на информационната сигурност. Както при конвенционалните информационни системи, така и при мобилните съществува един основен недостатък, а именно, че се използва един канал за предаване на конфиденциалната информация. Той може да се избегне чрез разделяне на конфиденциалната информация, предавана през стандартната инфраструктура (WAN, LAN), като едната част използва GSM комуникациите за втора независима трансмисия. Технологията е лесно осъществима, тъй като потребителите на компютризирани информационни системи, в т.ч. Интернет, разполагат с персонални мобилни апарати. Не са необходими и големи инвестиции в такава интегрирана

система откъм сървърна страна – обикновен GSM терминал, абонат на произволен мобилен оператор.

Интегрирането на мобилните комуникации в стандартни компютърни мрежи с цел повишаване на сигурността им предполага протичането на множество паралелни процеси по пренос на данни. От една страна компютърните системи с цялата сложност на работещите приложения в локална или глобална мрежа изискват оптимизация и синхронизиране на различни времеви, даннови и входно-изходни компоненти. Основна цел е повишаване на тяхната функционална ефективност. От друга страна е необходима и пълна синхронизация с модулите, осъществяващи интеграцията на мобилните допълнения към тях.

Ето защо формализирането и моделирането на процесите дава възможност да се оценят алтернативни планове. Знанието, което се получава по този начин, намалява риска и несигурността, свързани с вземането на важни решения, и увеличава надеждността, като подкрепя решението с предсказани данни. В този аспект обобщените мрежи са подходящо средство, предлагащо нов подход за моделиране и симулация на процесите, водещ до увеличаване на бързодействието, предпазване от сривове и респективно загуба на данни, както и бързи реакции при критични ситуации от страна на администратора. Досега апаратът на обобщените мрежи почти не е прилаган при моделиране на процеси от този тип.

Това обуславя и целта на настоящия дисертационен труд, за постигането на която ще бъдат разработени конкретни обобщено-мрежови модели с цел моделиране и анализиране на процесите, свързани с интегрирането на мобилните комуникации в стандартните информационни системи и с цел повишаване на сигурността и надежността им.

## Апробация на резултатите

Апробацията на резултатите е осъществена в рамките на представяния на доклади на няколко международни конференции и в статии в научни списания и тематични сборници.

## Съдържание на дисертационния труд

Дисертационният труд е в обем от 119 страници и се състои от увод, три глави, заключение, справка за приносите на автора, списък на публикациите по дисертационния труд, използвана литература, декларация за оригиналност на резултатите. Дисертационният труд включва 19 фигури и 1 таблица, а използваната литература към него – 123 заглавия.

## Глава първа – Въведение в мобилните комуникации и теорията на обобщените мрежи

В тази глава са дадени някои основни дефиниции, които са необходими за изложението по-нататък, и кратки бележки за мобилните комуникации и за теорията на обобщените мрежи (ОМ).

### Цел и задачи на дисертационния труд

**Целта** на настоящия дисертационен труд е конструиране на обобщеномрежови модели на процеси, свързани с интеграцията на мобилни средства в стандартни информационни системи и тяхната реализация.

За да се постигне тази цел са поставени следните задачи:

1. Разработване на обобщеномрежови модели, свързани с използването на мобилните комуникации за защита на информацията;
2. Разработване на обобщеномрежови модели на информационните потоци при стандартни информационни системи и тяхната интеграция с мобилни такива с цел повишаване на сигурността им;
3. Проектиране и реализация на технология за защита на информацията с използване на GSM комуникация;
4. Построяване на симулационен модел на работна станция (клиент), използваща мобилни устройства за защита на данните;
5. Анализ, проектиране и програмна реализация на информационна система за мобилни разплащания без ползване услугите на оператора.

## Глава втора – Обобщеномрежови модели в използване на мобилните комуникации за защита на информацията

Основната цел на изградените в Глава 2 обощеномрежови модели е да се интегрират мобилните комуникации в стандартни информационни системи с цел защита на конфиденциални данни.

## 2.1. Обобщеномрежов модел на интегриране на мобилните комуникации в електронната търговия

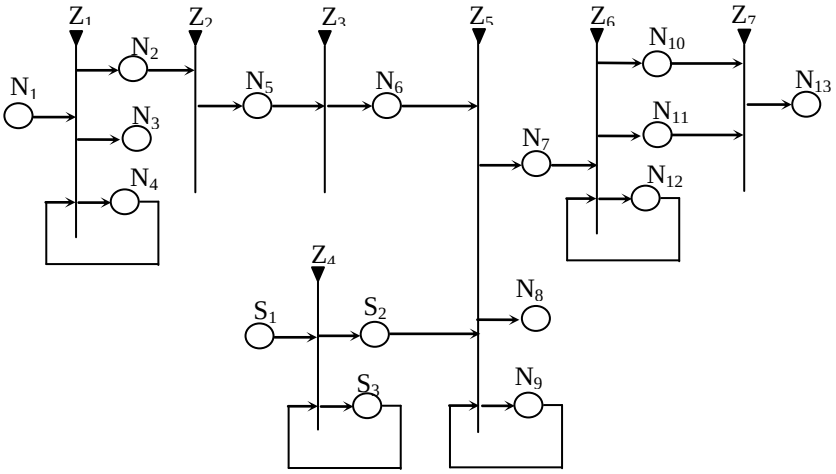
Разработеният обобщеномрежов модел е представен на Фиг. 1 и е публикуван в [1*]. Преходът $Z_6$ в ОМ модел може да се опише детайлно чрез прилагане на йерархичен оператор $H_3$ от теорията на ОМ.

ОМ съдържа следното множеството от преходи

$$A = \{Z_1, Z_2, Z_3, Z_4, Z_5, Z_6, Z_7\},$$

където преходите описват следните процеси:

- Регистриране на клиент в страницата на WEB системата за електронна търговия – преход $Z_1$;
- Попълване на заявка за услуга или за закупуване на стока – преход $Z_2$;
- Зареждане на страница със съобщение за формата и съдържанието на SMS – преход $Z_3$;
- Приемане на SMS от GSM терминал – преход $Z_4$;
- Засичане на времето за отговор на клиента – преход $Z_5$;
- Стартиране и обработка на транзакцията – преход $Z_6$;
- Извеждане на съобщение с резултата от транзакцията – преход $Z_7$.



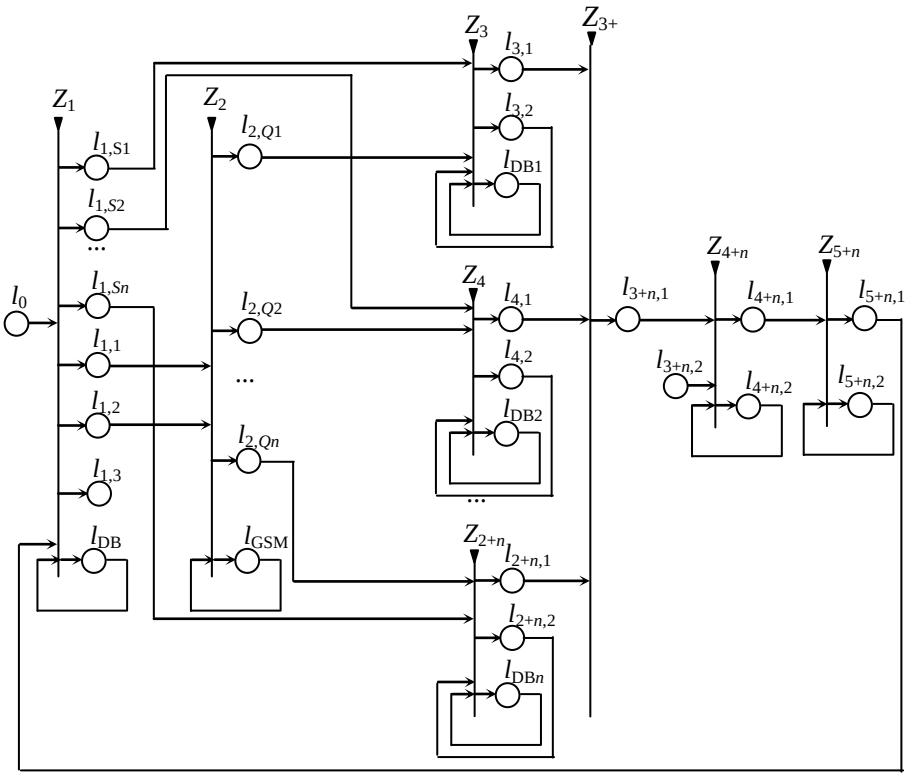

Фиг. 1. ОМ модел на електронно разплащане чрез мобилни комуникации

Обобщената мрежа съдържа следните ядра: α-ядра, представящи клиентите на WEB системата за електронна търговия, и β-ядра, свързани с GSM терминала и изпращаните от клиентите SMS.

Следва описание на модела.

## 2.2. Обобщеномрежов модел на защита на информацията в системите на здравеопазването

Конструираният в тази секция обобщеномрежов модел (Фиг. 2) описва възможност за избягване на измами в абстрактна система за здравеопазване и е публикуван в [2*].




Фиг. 2. ОМ модел за избягване на злоупотреби в здравната система

Първоналните изисквания са следните: мобилните номера на пациентите да са организирани в база данни; сървърите на регионално/национално ниво да са снабдени с GSM терминално устройство, реализиращо връзката между пациента и сървъра, съдържащ данни за пациента – телефонен номер, лични здравни данни, а при развитие на системата – и дебитна/кредитна карта за автоматизирано заплащане на медицински услуги и процедури. Контактът пациент–сървър може да се осъществява чрез безплатно позвъняване или чрез кратко текстово съобщение (SMS), съдържащо информация за приложена процедура. Опознаването от системата се извършва чрез CLIP (Calling Line Identification Presentation) на пациента и последваща обработка от софтуера.

В ОМ-модела (Фиг. 2) се съдържа следният набор от преходи:

$$A = \{Z_1, Z_2, Z_3, Z_4, \ldots, Z_{2+n}, Z_{3+n}, Z_{4+n}, Z_{5+n}\},$$

и те представляват съответно:

- $Z_1$ – Дейност на пациентите;
- $Z_2$ – Работата на GSM терминала;
  $Z_3, \ldots, Z_{2+i}$ – Дейността на база данни за услуга или процедура за достъп $i$, където $i = 1, 2, \ldots, n$, $n$ е броят на усугите;
- $Z_{3+n}$ – Криптиране на информацията;
  $Z_{4+n}$ – Работа на централната станция;
- $Z_{5+n}$ – Работа на сървъра за банкови транзакции.

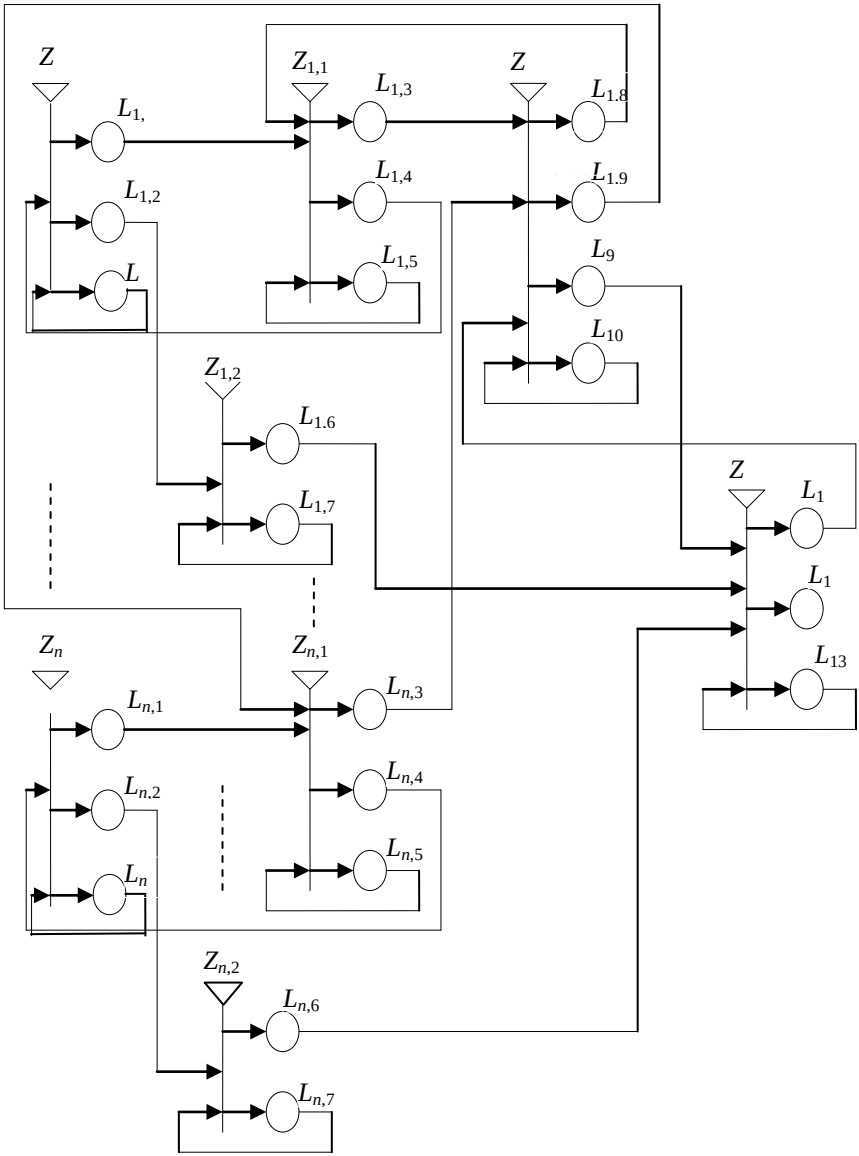
Навсякъде $i = 1, 2, \ldots, n$, където $n$ е броят на услугите и $j = 1, 2, \ldots, m$, където $m$ е броят на регистрираните пациенти.

Следва описание на модела.

## 2.3. Обобщеномрежов модел на авторизация в корпоративен сървър и мрежа с помощта на мобилни устройства

Принципът на автентификация е базиран на обмен на данни между ползвателя на ресурса посредством личния му мобилен апарат и терминала, инсталиран на сървъра на мрежата. Той може да бъде усложнен и усъвършенстван по усмотрение на администратора, добавяйки към стандартната процедура (приемане/изпращане) на допълнителни данни за проверка като PIN (Personal Identification

Number) или допълнителна парола. В основата си обменът включва позвъняване от потребителя, желаещ достъп до системния ресурс.




Фиг. 3. ОМ модел за авторизация на достъпа.

GSM терминалното устройство приема позвъняването и прекъсва връзката. Резултатът е получаването на CLIP, съдържащ телефонния номер, вкл. международния код на потребителя, дата и час на позвъняването. Сървърът проверява за наличието на такъв номер в базата и в зависимост от правата, дефинирани в досието на конкретния потребител, сървърът издава разрешение за достъп до разрешените ресурси на системата. Позвъняването е напълно безплатно за потребителя, тъй като целта е само получаванве на CLIP. Верификацията може да бъде усложнена, както беше споменато погоре, ако сигурността го изисква, тъй като апаратът може да бъде откраднат, загубен и т.н.

Обобщеномрежовият модел за авторизация на достъпа е представен на Фиг. 3.

Обобщената мрежа съдържа следното множество от преходи:

$$A = \{Z_1,\ldots, Z_n, Z_{1,1},\ldots, Z_{n,1}, Z_{1,2},\ldots, Z_{n,2}, Z_3, Z_4\},$$

където преходите представят следните процеси:

- $Z_{1,\ldots,} Z_n$ – дейностите на клиент $i$, за $i = 1, 2\ldots, n$,
- $Z_{1,1,\ldots,} Z_{n,1}$ – дейностите, свързани с GSM на клиент $i$, за $i = 1, 2\ldots, n$,
- $Z_{1,2,\ldots,} Z_{n,2}$ – дейностите, свързани с компютъра на клиент $i$, за $i = 1, 2\ldots, n$,
- $Z_3$ – дейностите, свързани с GSM терминала,
- $Z_4$ – дейностите, свързани с автентификационния сървър.

Дадено е подробно описание на модела.

## Глава трета – Реализация на програмен продукт за електронни разплащания през мобилни устройства

Програмният продукт представлява нестандартна реализация на система за електронна търговия с използване на мобилната комуникация – използване на E-pay посредством обикновено позвъняване или SMS, т.е. създаване на възможност за електронна търговия през мобилен телефон – M-pay.

M-pay носи в себе си редица преимущества като мобилност на клиента, отпадане на необходимостта от директно ползване на PC с

достъп до мрежата и т.н. М-рау е най-подходяща при закупуване на т.нар. фиксирани стоки и услуги, като ваучери за зареждане на мобилни телефони, автоматизирани паркинги, билети за културни прояви, спортни залагания и други.

## 3.1 Описание на системата за електронна търговия с използване на мобилната комуникация

Системата е разработена в три основни модула – работни станции (РС), главна станция-диспечер (ГСД) и сървър за банкови транзакции (ТС).

### 3.1.1. Работна станция

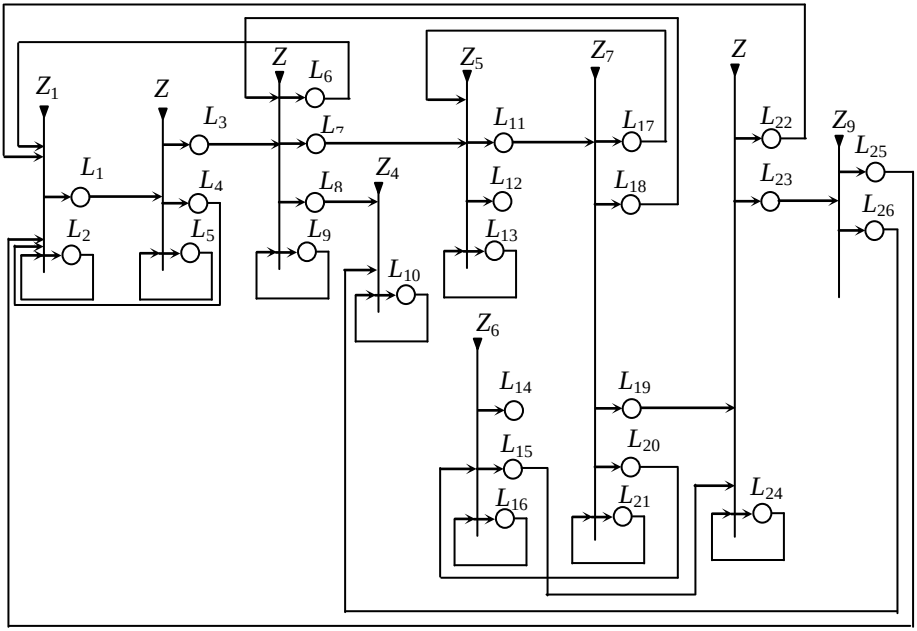
Представената реализация е публикувана в [4*]. Работната станция (РС) е основен компонент от тримодулната структура на сървъра за банкови транзакции. РС могат да бъдат локирани на различни географски места и да покриват продажба на няколко вида услуги или определен набор от стоки, предмет на Е-търговия. РС е мястото, където се изгражда базата от данни на клиентите, включваща данни за клиентите – персонални, данни за разплащателното средство, както и история на извършените плащания. Другата част включва базата на стоките и услугите – предмет на електронната търговия. Работната станция има за задача да приеме заявката на клиента от мобилен телефон, проверка на валидността на клиента и съпътстващите го изисквания (валидност на разплащателното средство), създаване и криптиране на реална банкова транзакция и нейното диспечиране в опашката за изпращане/получаване към/от главната станция-диспечер (ГСД). РС е ангажирана и с осъществяване на обратната връзка към клиента – предимно във вид на SMS. Работните станции реализират връзката си към ГСД по TCP/IP канал.

ОМ-моделът на функциите на РС е показан на Фиг. 4. Той съдържа девет прехода и 26 позиции. Преходите описват следните процеси:

- Дейността на клиентите – преход $Z_1$,
- Дейностите на модула за входящо повикване / SMS – преход $Z_2$,

- Дейностите на модула за проверка на потребителя – преход $Z_3$,
- LOG файл за неуспешни сделки – преход $Z_4$,
- Дейността на модул изпращането на опашката – преход $Z_5$,
- Дейността на контролния модул – преход $Z_6$,
- Дейността на опашката – преход $Z_7$,
- Дейностите на модула за анализ на резултата от сделката – преход $Z_8$,
- Тестване на модела – преход $Z_9$.

Следва подробно описание на модела.




Фиг. 4. Обобщеномрежов модел на на функциите на работна станция

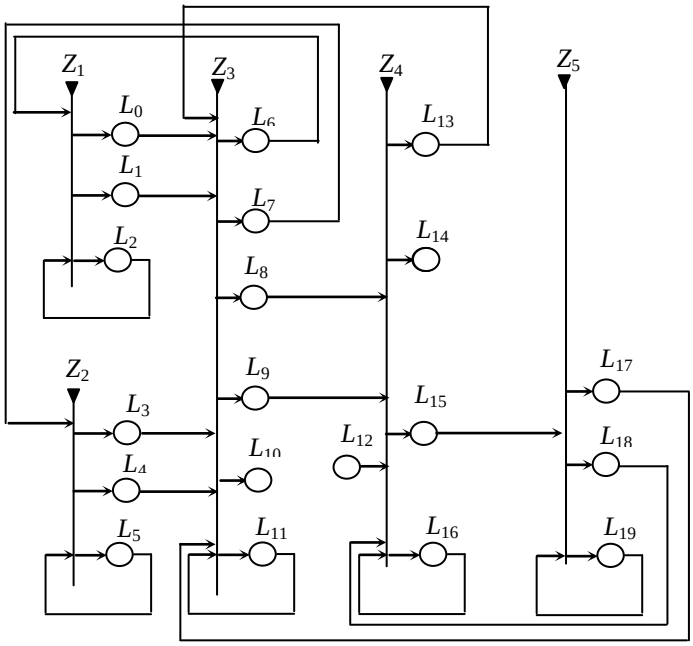
### 3.1.2. Главна станция-диспечер

Представеното по-долу описание е публикувано в [3*]. Главната станция-диспечер (ГСД) е модул, свързващ и синхронизащ стартирани транзакции от РС към Сървъра за транзакции (ТС). ГСД може да обслужва и произволни автономни уебсайтове за електронна търговия,

които да ползват ТС в качеството му на Payment Gateway (сървър за разплащания към банки), ако не разполагат със собствен такъв. ГСД и ТС физически се намират на едно и също географско място. Транзакциите, пристигнали от произволна РС, се обслужват в опашка FIFO с определено време за престой в ГСД – по-малко от това в РС и по-голямо от времеизчакването в ТС. Връзката с РС е осъществена по TCP/IP/RAW, без използване на HTTP или HTTPS протокол, със собствено 3DES криптиране в РС заявки за авторизиране на банкова транзакция. Двете страни работят с фиксирани адреси и портове, като възможността за неоторизиран достъп е сведена до минимум.

ГС приема криптирани транзакции от РС или външни уебсайтове за е-търговия. Всяка транзакция е определена с време на постъпване и IP на РС или уеб-а.

ОМ-моделът на функциите на Главна станция в трансмисия за е-търговия, базирана на мобилни комуникации, е даден на Фиг. 5.




Фиг. 5. Обобщеномрежов модел на функциите на Главна станция в трансмисия за е-търговия, базирана на мобилни комуникации

Обобщената мрежа има 5 прехода и 20 позиции.

- $Z_1$ – Функции на Работните станции (РС)
- $Z_2$ – Функции на web-приложения
- $Z_3$ – Функции на Главната станция (ГС)
- $Z_4$ – Дейности на самоконтролиращата се опашка
- $Z_5$ – Функции на Транзакционния сървър (ТС)

Следва описание на модела.

### 3.1.3. Сървър за банкови транзакции

Сърцевината на сървъра за банкови транзакции е обслужването на разплащанията клиент–банка. В зависимост от начина на комуникация с банковия сървър, сървърът за банкови транзакции може да бъде изграден по два начина – автономен и E-pay базиран.

Първият начин и значително по-сигурен по отношение преноса на данни е чрез директна връзка с банковия сървър – софтуерен POST (Point of Sale Terminal) през наета или Dial Up връзка с банката или по TCP/IP протокол.

При втория начин като средство за комуникация между Сървър за банкови транзакции и Банка би могло да бъде използван функциониращ вече сайт за електронна търговия или просто специализиран Payment Gateway (PG), който може да е локиран на произволно географско място. Изискванията са единствено създаване на сметка на търговеца (Merchant Account) и софтуер, отговарящ на изискванията на PG. Тук нараства рискът за потребителските данни и най-вече данните за разплащане – дебитна/кредитна карта, срок на валидност, тип и др., което го прави по-малко препоръчителен.

И при двата варианта механизмът на извършване на паричната транзакция е един и същ – ТС изпраща искане (authorization request), съдържащо данните на платеца-клиент (номер на кредитна/дебитна карта, валидност, вид на валутата и др.) и сумата по плащането, както и данните за сметката на търговеца (merchant account), по която ще бъдат преведени средствата. Банковият сървър връща отговор (authorization response), съдържащ резултата от транзакцията – неоторизирана, реферирана или успешна.

## 3.2 Реализация на системата за електронна търговия с използване на мобилната комуникация

И трите модула на системата са с потребителски интерфейс – текстов и графичен. Осигурена е детайлна система за пълен мониторинг на всяка транзакция в движение, както и лог файлове за цялостната работа на всеки модул. Това е необходимо във всички системи, работещи в реално време, и най-вече поради това, че системата обслужва плащания на клиенти практически от целия свят. Разработена е система за сигурност при различни критични ситуации – хардуерен срив в някой от модулите, осъществени банкови транзакции, непредадени към клиента, и др.

В РС особено значение има нормалното функциониране на GSM терминалите, като при всеки проблем (хардуер, софтуер или мобилен оператор) системата се изключва автоматично. РС може да генерира по всяко време отчети различните дейности – клиенти, продажби и т.н. Администрирането на функционалността на РС е автоматизирано в достатъчна степен, за да минимизира необходимостта от квалифициран достъп на администратор. В основното меню са застъпени най-необходимите дейности като:

**Обслужване на дейности, свързани с SMS.** Оттук се прави преглед на получени SMS от клиенти на системата или такива, които биха желали да се регистрират в нея; изпращане на SMS до клиенти с проблеми, текущо възникнали при закупуване на услуга; детайлизиран отчет на всички изпратени и получени SMS, както и изпращане на рекламни или предупредителни съобщения до група или всички потребители (bulk SMS); отчети за въведени и неизпратени по различни причини съобщения. При стартиране на РС автоматизирано се визуализират получените през времето на престой съобщения, на които предстои да се отговори.

**Меню за обслужване на информацията, свързана с платежните средства**. В този раздел се дефинират настройките за връзка с различни банки, които са част от автономния Payment Gateway – настройки на терминална конфигурация за конкретната банка, детайли на

търговеца (сметки, автентификационни параметри и др.), параметри на приеманите за обслужване платежни средства – дебитни и кредитни карти, кодове за проверка и валидизиране на карти от различни издатели. Системата автоматично следи за валидност на картите на клиентите, като генерира отчети за изтекли такива, подканвайки с SMS клиентите да ги актуализират. Тук се дефинират и платежните средства на клиентите на системата, които се криптират и са достъпни само за авторизиран администратор.

**Данни за мобилните устройства на клиентите**. Те се получават автоматично от системата при регистрация от уебсайта или се въвеждат ръчно. Включват CLIP (Caller Line Identification Presentation) за идентификация на клиента, език за общуване, включително набор от стандартни SMS при различни ситуации, които да известяват за резултата от стартирана транзакция, статус на клиента – активен или не. Всеки CLIP клиент е обвързан с платежно средство, което се използва за разплащането и т.н. Подменюто дава възможност за отчети за брой извършени транзакции по клиенти – успешни или не, ритмичност на използване на системата от всеки клиент и др.

**Меню на администратора.** В него се дефинират администраторите на РС и нивата им на достъп до конфиденциалните данни, сервизни функции по почистване на базата, *backup* на същата, автоматизиран export/import на данни за клиенти и услуги – например при продажба на ваучери за предплатени мобилни услуги данните се получават от оператор и се импортират автоматично. Подменюто за обслужване на параметрите на администратора включва телефони за известяване при проблеми, дефиниране на интервали, в които клиентът може да повтори заявка за транзакция, цени на услуги, които работната станция продава, както и валутата за разплащане. Тук се дефинират и IP адреси и портове за връзка с ГСД, която се намира в различно географско място.

Структурно разработеният софтуер за обслужване на РС се състои от няколко модула, работещи във фонов режим, и множество обслужващи. Фоновите модули се стартират със стартирането на РС и извършват основните дейности в режим на реално време:

**Модул за следене на постъпващи SMS.** Стартирането и работата му са свързани с проверка на GSM терминала/терминалите за получени и непрегледани прозвънявания или SMS, след което той влиза в режим на подслушване на COM/USB, в зависимост от типа на терминала/портовете. Получените позвънявания или SMS се поставят в опашка, задава им се начално време на постъпване. Този фонов модул се обслужва от няколко допълнителни, чието предназначение е първоначален анализ на коректността на SMS или позвъняването, както и на изпращането на уведомителен SMS при приключване на транзакцията. Всички мобилни комуникации, вкл. SMS, въведени от администратора, се обслужват отново от този модул. Сорс код на модула е показан в *Приложение 1*.

**Диспечиращ модул**. Той се явява водещ за системата по отношение на опознаване на повикванията/SMS от страна на клиента. GSM терминалът, обслужващ конкретна услуга, получава повикването на база CLIP. Следва проверка в базата за регистриран потребител с такъв CLIP. При липса на такъв, системата може да отговори с SMS с покана за регистрация. При другата опция – клиентът съществува, се преминава към следващата проверка – коректни данни на регистриран потребител. Модулът обслужва цялостната комуникация с ГСД – изпращане на транзакция и приемане на отговор за отработена такава, както и пълното обслужване на FIFO опашката. *Приложение 2* съдържа код на диспечиращия модул – най-важния за РС.

**Контролен модул**. Следи за изтичане на времевия лимит. При изтичането му без отговор от ГС, тригерът се променя, а транзакцията се премахва от опашката и поставя в „кошчето“. Следва уведомителен SMS към клиента за неуспешна транзакция поради проблеми в системата и покана за нов опит.

**Структура на данните в РС.** Основните данни, необходими за нормално функциониране на системата, са в работната станция, тъй като ГСД и ТС са предимно транспортни модули.

- **Номенклатури** – съдържат основно данни за клиента (CLIP, име, платежно средство, език за комуникация и др.); банкова информация (име на банка, терминална конфигурация, типове карти); услуги предлагани от конкретната РС – например

ваучерни кодове за зареждане на сметка; формализирани текстове за SMS на различни езици.

- **Файлове с данни.** Основният обем данни в системата, съдържащ: Отработени транзакции за период с резултат успешни/неуспешни и причина; хронология на изпратени SMS за резултат от транзакции и получени позвънявания или SMS от клиенти на системата; стартирани транзакции в развитие, както и такива очакващи резултат
- **Тригери –** файлове, съдържащи данни за състоянието на всяка стартирана транзакция.
- **LOG – файлове.** В тях се съхранява пълно досие на всяка транзакция от РС към останалите модули на системата по време, място (IP на инициращата РС) и криптиран/ декриптиран стринг към ТС. В аварийни логове се съдържа информация за непредадени към конкретен модул данни при срив на някой от тях.

Времевата синхронизация е особено важна за правилното функциониране на системата. РС могат да се намират на различни географски места, в различни часови пояси, докато ГСД и ТС са на хиляди километри от тях. Синхронизирането е каскадно в следния смисъл: времето на живот на стартирана транзакция в опашката на РС е по-голямо от това в ГСД, което от своя страна е по-голямо от това в ТС. Когато няма отговор в рамките на определеното време (delay time) за конкретна транзакция в РС, то тя се изтрива от опашката и клиентът получава известие чрез SMS. Ако липсва такава времева каскада, е много вероятно една транзакция, забавена в ТС, но обслужена от банката, да бъде вече изтрита в РС или ГСД. Така клиентът ще бъде ощетен и необслужен. Ето защо трите модула работят в еднакво часово време с каскадиране на времето за забавяне.

Софтуерът на другите два модула – ГСД и ТС, е значително по-опростен с оглед на тяхното предназначение.

**Главната станция-диспечер** приема заявки от РС или други уеб-базирани приложения, генерира опашка и ги предава към ТС. Два програмни модула обслужват цялата трансмисия. Те работят във фонов режим, като първият от тях е предназначен за комуникация с

работните станции (*Приложение 3*). ГСД получава форматиран низ със заявка за авторизация от РС, като заглавната му част съдържа идентификационни данни за изпращача – IP адрес на РС, време на постъпване на заявката в ГСД и данни (CLIP) на клиента. Следва криптиран низ със заявката към конкретната банка или външен Payment Gateway. Другият резидентен модул е ангажиран с трансмисията към сървъра за транзакции. Той изпраща заявките към него и изчаква отговор, който е отново криптиран. При срив на ТС и липса на отговор транзакцията с изтекло време за отговор се канцелира и се формира съответен отговор към РС. В ГСД отново е предвиден потребителски интерфейс, основно за мониторинг и параметризация.

**Сървър за банкови транзакции.** Както в ГСД, така и тук работят два модула – един за връзка с ГСД и втори, осъществяващ връзка с банков сървър или външен Payment Gateway. Освен работа в TCP/IP, в ТС има разработен софтуер за емулация на обикновен POST (Point Of Sale Terminal). POST обикновено се ползва като резервен вариант при срив на интернет.

В софтуера на системата са реализирани онлайн протоколи за банкови транзакции към различни банки, работещи с най-популярните средства за разплащане – VISA, MASTER CARD, DINERS CLUB и др. В зависимост от параметрите на заявката от РС-ГСД, сървърът за банкови транзакции адресира конкретната транзакция към изискваната банка.

Външните PG имат изисквания към клиентите си, което изисква разработка на отделен модул за конкретен PG. Това обикновено са модули на Java, Perl, C, HTML и други програмни езици според спецификацията на PG. В системата има разработени такъв тип модули към популярни PG.

Допълнителен мониторинг в ТС е разработен за VBV протокол, чийто сорс код е показан в *Приложение 4*. Модулът е реализиран на Visual Basic с използване на VBV плъгин e24VbVPlugin.dll. Предназначението му е да улесни администратора при възникнали проблеми с банки, използващи този протокол за връзка.

Във всички модули е заложена система за лог на всяка транзакция. Особено важно това е в ТС, поради недоразумения, които могат да

възникнат между клиент, търговец и банка при евентуален срив в някое звено. В *Приложение 6* е показана извадка от лог файл на ТС, която съдържа успешна транзакция към банка, работеща с VBV протокол.

Основната част на софтуера е базиран на платформа CACHE – пострелационна база данни, естествен наследник на MUMPS (Massachusetts General Hospital Utility Multi-Programming System) на InterSystems Corporation™. CACHE има редица технологически преимущества като единната архитектура на данните и пълната подръжка на обектно-ориентирани технологии. СУБД двигателят (DB engine) разполага със сървър за многомерни данни, т.е. данните се съхраняват така, както най-често се налага да бъдат използвани. Той позволява да бъдат премахнати редица ограничения, налагани от класическите релационни бази, съхраняващи данните в двумерни таблици, което при сложни структури усложнява и забавя изпълнението на сложни транзакции и често води до създаване и съхраняване на излишна междинна информация. От друга страна CACHE е ориентирана за обработка на транзакции в системи с огромни бази от порядъка на стотици гигабайти и даже терабайти с достъп едновременно от множество ползватели. Този транзакционен модел позволява на CACHE да оптимизира данните на ниво съхраняване, да подържа обектов модел и сложни типове данни, постигайки висока производителност.

Системата за мобилни плащания е адаптивна, тъй като може да бъде добавяна без допълнителна доработка директно към вече работещ E-pay сървър. Модулната и структура и в частност модулът, реализиращ връзката Клиент-ТС с помощта на GSM терминалите, дава възможност за изграждане на глобална M-pay мрежа – базирани на различни места ТС сървъри, предлагащи различни видове услуги с централизиран сървър за банкови плащания (Payment Gateway). По този начин системата може лесно да бъде интернационализирана – предлагане на локални услуги с централизирано банково обслужване. Естествено, това е реализируемо при масово използване на кредитни карти при разплащането. Така потребители от различни географски места биха могли да ползват M-pay за покупка на стоки и услуги без

да се интересуват от детайлите на самото плащане. Голямо преимущество на тази система е изключително ниската й себестойност, което я прави лесно приложима в различни области. Освен това съществува пълна дискретност при комуникацията с клиента, като сигурността може да бъде повишена чрез допълнителна обратна връзка, код за проверка на идентичността, разширяване на обсега на операторска намеса, осигуряване на сигурността при аварийни ситуации и т.н. Всички тези предимства са гаранция за добри перспективи за бъдещото й използване като модерен и достъпен за все повече хора начин при ползването на масови услуги.

## Заключение

В дисертационния труд са конструирани 5 обобщеномрежови модели на процеси, свързани с интеграцията на мобилни средства в стандартни информационни системи и тяхната реализация, което води до повишване на защитата на информацията.

Конструираните модели предоставят възможност:

1. Да се анализират информационните потоци при обмен на конфиденциални данни;
2. Да се симулират процесите с цел подобряване на начина на тяхното протичане;
3. Да се направи оценка на възможностите за подобряване на някои от параметрите на информационните потоци;
4. Да се анализират и управляват в реално време протичащите процеси;

## Справка за приносите на автора

1. Разработени са три обобщеномрежови модела, интегриращи мобилните комуникации в глобализирани или широкообхватни информационни системи с цел защита на конфиденциални данни, предотвратяване на кражбите на лични данни и злоупотребите:

- Обобщеномрежов модел на интегриране на мобилните комуникации в електронната търговия [1*];
- Обобщеномрежов модел на защита на информацията в системите на здравеопазването [2*];
- Обобщеномрежов модел на авторизация в корпоративен сървър и мрежа с помощта на мобилни устройства [5*].

2. Проектирана е система за електронна търговия с използване на мобилна комуникация, осигуряваща защита на информацията, тъй като конфиденциалната информация се предава не по един, а по два канала – интернет среда (стандартна или мобилна) и ползване на GSM услуга – SMS или удостоверително позвъняване до корпоративен или уеб сървър. При проектирането са конструирани два обобщеномрежови модела:

- Обобщеномрежов модел на функциите на работна станция [4*];
- Обобщеномрежов модел на функциите на Главна станция в трансмисия за е-търговия, базирана на мобилни комуникации [3*];

3. Реализирана е система за електронна търговия с използване на мобилна комуникация на пострелационна база данни CACHE, ориентирана към обработка на транзакции в системи с големи бази.

## Списък на публикациите

1*. Sotirova, E., H. Panayotov, Modeling of e-trade with Mobile Communications by the Apparatus of Generalized Net, Fifth International Workshop on Generalized Nets, 10 November 2004, Sofia, Bulgaria, 41-48.

2*. Panayotov, H., Generalized net model of the process of avoiding healthcare fraud, Developments in Fuzzy Sets, Intuitionistic Fuzzy Sets, Generalized Nets and Related Topics. Foundations and Applications Warsaw, Poland, 2011, 185-192.

3*. Панайотов, Хр., Обобщеномрежов модел на функциите на главна станция в трансмисия за е-търговия, базирана на мобилни комуникации, Годишник на секция "Информатика" към СУБ, Том 6, 2013, 62–67.

4*. Panayotov, H., A generalized net model of transaction workflow in GSM based station for e-commerce, Issues in IFS and GNs, Vol. 10, 2013, 152-162.

5*. Обобщеномрежов модел на авторизация в корпоративен сървър и мрежа с помощта на мобилни устройства, Годишник на секция "Информатика" към СУБ, 2014 (под печат)

## Приложения

**Приложение 1**

Представен е код на модул за работа с GSM терминалите в Работна станция /DV01SAA/ Cache Direct

**Приложение 2**

Представен е код на основен модул за диспечиране на FIFO опашка на транзакции в Работна станция /DV01SMA/ Cache Direct

**Приложение 3**

Представен е Диспечиращ модул в Главна станция–диспечер от страна на Работна станция /DV01SCA/ Cache Direct

**Приложение 4**

Представен е VB модул за авторизация и мониторинг на транзакции към банка с VBV /Verified By Visa/ Gateway с използване на стандартна библиотека e24VbVPlugin.dll

**Приложение 5**

Представен е PERL код /HOP.PL/за авторизация на транзакции към външен Payment Gateway

**Приложение 6**

Представен е LOG файл на транзакции в ТС