**БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ**
**ИНСТИТУТ ПО БИОФИЗИКА И БИОМЕДИЦИНСКО ИНЖЕНЕРСТВО**

---

**АВТОРЕФЕРАТ**
**ЗА ПРИДОБИВАНЕ НА НАУЧНА СТЕПЕН „ДОКТОР”**
**НА ГЛ. АС. ИВЕЛИНА МИТКОВА ВАРДЕВА**

ТЕМА: **МОДЕЛИ НА ПРОЦЕСИ В МРЕЖОВА СИГУРНОСТ ЧРЕЗ ОБОБЩЕНИ МРЕЖИ**

по шифър 01.01.12 „Информатика”

**НАУЧНИ РЪКОВОДИТЕЛИ:**
**проф. дтн дмн КРАСИМИР АТАНАСОВ**
**доц. д-р СОТИР СОТИРОВ**

**РЕЦЕНЗЕНТИ:**
**1. Проф. дтн ЛЮДМИЛ ДАКОВСКИ**
**2. Доц. д-р СТОЯН ПОРЯЗОВ**

София
2012

Защитата на дисертационнния труд ще се състои на 18.04.2012 г. от 11:00 часа в заседателната зала на Институт по биофизика и биомедицинско инженерство – Българска академия на науките (ул. „Акад. Г. Бончев”, бл.105).

Дисертационният труд е обсъждан на разширен научен семинар на секция „Биоинформатика и математическо моделиране” на ИБФБМИ на 17.02.2012 г.

Рецензенти:

1. Проф. дтн Людмил Даковски
2. Доц. д-р Стоян Порязов

Автор:

Ивелина Вардева

ЗАГЛАВИЕ:

„Модели на процеси в мрежова сигурност чрез обобщени мрежи”

**ОТПЕЧАТАНО В 20 БРОЯ**

## УВОД

Динамиката на днешното общество неизбежно води до търсене на нови пътища за развитие на компютърните технологии. Компютрите достигат до обикновените хора, навлизат на работните им места, в домовете им, в бизнеса и здравеопазването, хората обменят информация, учат и работят, без да са зависими от разстоянието и времето.

Бързото навлизане на компютърните комуникации и Интернет в различни сфери поставя множество въпроси, свързани със сигурността при обмен на информация. Това е от особено голямо значение при предаване на конфиденциални данни по мрежата. Изследването и анализирането на процесите, свързани с обмена на такъв тип информация, е от изключителна важност за повишаване на сигурността при предаването й.

Европейската харта за правата на човека дава право на всяко лице да „има право на поверителност на личната информация, включваща данни относно здравното му състояние и потенциални диагнози или терапевтични процедури, както и защитата на конфиденциалността по време на изпълнението на диагностичните процедури, посещенията от специалист и медицинско хирургично лечение като цяло”.

Сериозен проблем при гарантиране на тези права е създаване на достатъчно добра информационна сигурност и стандартизация и изграждане на интегрирана система за обмен на информация между заетите в сферата на здравеопазването.

Компютърните мрежи в областта на здравеопазването трябва да осигуряват качествено здравеопазване, ефективност, медицина базирана на доказателства с цел подпомагането на вземане на медицински решения, равноправен достъп на всички граждани до медицинска информация през Интернет, възможност за избор на гражданина на здравни услуги, насърчаване на нов вид взаимоотношения между гражданите и здравните институции, както и нови форми на взаимоотношения между пациент и лекар, конфиденциалност и др.

## ЦЕЛ И ЗАДАЧИ НА ДИСЕРТАЦИОННИЯ ТРУД

**Основна цел** на разработката е да се изследват информационните процеси, протичащи в компютърните мрежи, и мрежовата сигурност чрез моделирането им с обобщени мрежи. Това ще позволи да се проследят и анализират процесите, протичащи в компютърните мрежи, възможностите за изграждане на мрежови връзки между болнични заведения, процесите за атакуване при обмен на медицинска информация, както и повишаване на сигурността в мрежата. Получените резултати са в основата на научно обосновани препоръки, свързани с реализацията на компютърните мрежи, повишаване на мрежовата сигурност и защитата на конфиденциална информация, предавана през обществената мрежа.

**Основните задачи**, които трябва да се решават за постигане на горната цел, се отнасят до:

1. Разработване на обобщеномрежови модели на процесите в глобален план за видовете атаки в компютърната мрежа;
2. Детайлизиране на моделите, описващи основните видове атаки;
3. Разработване на обобщеномрежови модели на процеса на изграждане на сигурни връзки при предаване на медицинска информация;
4. Построяване на симулационен модел, оценяващ степента на атакуваните съобщения през обществената мрежа.

Решението на тези задачи е направено чрез моделиране на протичащите процесите чрез обобщени мрежи и тестването им на базата на конкретни примери.

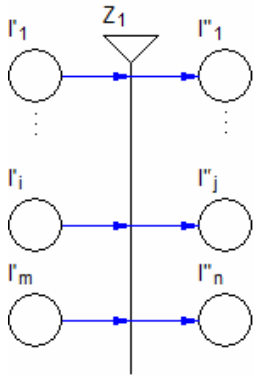
В текста с [n*] са означени статиите на автора, включени в списъка на публикациите на дисертационния труд.

Изказвам благодарност на д-р Валери Гочев за консултациите при използването на програмния пакет за ОМ.

# 1. ГЛАВА ПЪРВА – ОСНОВНИ ПОНЯТИЯ ОТ ТЕОРИЯТА НА ОБОБЩЕНИТЕ МРЕЖИ

В тази глава са дадени основни дефиниции в теорията на обобщените мрежи (ОМ).

ОМ се състои от преходи. Графично преходът в се представя като съвкупност от два елемента: ○ и | (Фиг. 1.1.).




Фиг. 1.1. Графично представяне на прехода $Z$ в ОМ

Всеки преход в ОМ има поне една входна и поне една изходна позиция. Графичното означение на позициите е кръгче (○). В позицията може да влиза не повече от една дъга и също от позицията може да излиза не повече от една дъга. Позиция, от която излиза дъга, е входна за прехода, а позиция, в която влиза дъга, е изходна за прехода.

За представяне на индексираната матрица се дефинират множествата $I$ и $R$, като $I$ е фиксирано множество от индекси, а $R$ е множеството на реалните числа. Тогава индексирана матрица с индексни множества $K$ и $L$ ($K, L \subset I$ и $K = \{k_1, k_2,\ldots, k_m\}$, $L = \{l_1, l_2,\ldots, l_n\}$), се нарича следният запис:

$$[K, L, \{ a_{k_i,l_j}\}] = \begin{array}{c|cccc} & l_1 & l_2 & \ldots & l_n \\ \hline k_1 & a_{k_1,l_1} & a_{k_1,l_2} & \ldots & a_{k_1,l_n} \\ k_2 & a_{k_2,l_1} & a_{k_2,l_2} & \ldots & a_{k_2,l_n} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ k_m & a_{k_m,l_1} & a_{k_m,l_2} & \ldots & a_{k_m,l_n} \end{array},$$

където $a_{k_i,l_j} \in R$ за $i \in [1, m]$ и $j \in [1, n]$.

## 1.1. ФОРМАЛНИ ДЕФИНИЦИИ НА ПОНЯТИЯТА “ПРЕХОД” И “ОМ”

### 1.1.1 ФОРМАЛНО ОПИСАНИЕ НА ПРЕХОД

Дадена е формална дефиниция на понятието „Преход”.

### 1.1.2 ФОРМАЛНО ОПИСАНИЕ НА ОБОБЩЕНА МРЕЖА

Дадена е формална дефиниция на понятието „ОМ”.

## 1.2. АЛГОРИТМИ ЗА ФУНКЦИОНИРАНЕ НА ПРЕХОД И ОБОБЩЕНИ МРЕЖИ

Описани са основните алгоритми за функциониране на преходите и обобщените мрежи.

## 1.3. РЕДУЦИРАНИ И РАЗШИРЕНИ ОБОБЩЕНИ МРЕЖИ

Дефинирани са понятията редуцирана и разширена обобщена мрежа. Посочени са основните видове разширения на обобщените мрежи.

## 1.4. ИЗГРАЖДАНЕ НА ОБОБЩЕНА МРЕЖА

При моделиране чрез обобщени мрежи е необходимо да се извършат редица подготвителни действия, които са описани в този параграф. Дадена е подробна методология за изграждане на обобщена мрежа, включваща: изграждане на статична структура на модела, отразяване на динамиката на моделирания процес, описание на функционирането на моделирания процес във времето, определяне на данните, които представляват интерес на моделирания процес.

## 1.5. ОПЕРАТОРЕН АСПЕКТ НА ТЕОРИЯТА НА ОБОБЩЕНИТЕ МРЕЖИ

Накратко са описани отделните оператори, които могат да се приложат над частите на обобщените мрежи. Те се разделят на шест групи: глобални, локални, йерархични, редуциращи, разширяващи и динамични.

## 1.6. ИЗВОДИ

Движението на информацията се извършва на потоци, които протичат между отделните звена в рамките на здравни структури и между самите структури. За целта се изследват и анализират различни процеси за изграждане на защита между две крайни точки, които могат да бъдат както болнични заведения, здравни структури, така и пациенти, изискващи лична здравна информация. Необходимо е да се осигури защита на личните данни и здравната информация, защита на потребителите, на интелектуалната и индустриална собственост. В този аспект обобщените мрежи са изключително подходящо средство за моделиране и симулация на процесите в здравеопазването.

# 2. ГЛАВА ВТОРА – ОСНОВНИ ПРОБЛЕМИ В МРЕЖОВАТА СИГУРНОСТ. ОБОБЩЕНОМРЕЖОВИ МОДЕЛИ В МРЕЖОВАТА СИГУРНОСТ

В тази глава са описани три обобщеномрежови модели, описващи мрежовата сигурност.

Нарастването с неподозирани темпове на Интернет се превръща в изключително мощно средство за комуникация и развитие на бизнеса. Комуникациите, които се използват в Интернет, са отворени и трудно се контролират. Този проблем поставя на преден план въпроса за сигурността на предаваните данни в обществената мрежа. Необходимостта от конфиденциалност и цялостност на транзакциите нужни на електронния бизнес трябва да се разглеждат като бизнес стратегия на всяка една фирма, имаща специфичности и собствени нужди по отношение на сигурността. Един от основните проблеми в Интернет е идентификацията на потребителите. Сигурността на информацията в обществената мрежа стои на първо място. Необходимо е да се избегне неоторизираният достъп до електронната информация във всяка фирма, особено до информация с критично значение за бизнеса. В резултат от неоторизиран достъп информацията може да бъде променена, частично подменена или подменена изцяло с друга информация, може да бъде унищожена или да бъде разпространена по време на предаването й.

## 2.1. ОСНОВНИ ПРОБЛЕМИ В МРЕЖОВАТА СИГУРНОСТ

Всяка комуникационна мрежа може да се моделира от гледна точка на надеждността като сложна система с недетерминирано поведение след отказ. Недетерминираността на поведението се определя от появата и натрупването на причини за откази в резултат на:

- Случайни неизправности;
- Шумове и други смущения;
- Грешки в процеса на създаване на системата;
- Интрузионни действия на субективни фактори.

## 2.2. ЗАПЛАХИ В ОБЩЕСТВНАТА МРЕЖА

Заплахите в обществената мрежа Интернет могат да се опишат като:

- **Загуба от цялостта на данните** – нарушителят добавя модифицира или изтрива информация;
- **Загуба на услуги** – в резултат от действията на нарушителя определена услуга не може да се изпълни (отказ на услуга, DoS);
- **Загуба на контрол** – услугите се използват от оторизирани потребители по неоторизиран начин;
- **Загуба на конфиденциалност на данните** – информацията е достъпна за неоторизирани потребители.

Всички комуникации в Интернет използват протокола TCP/IP, който позволява информацията да бъде изпратена от един до друг компютър през множество от междинни компютърни станции и различни мрежи преди да достигне до получателя. Изключително голямата гъвкавост и удобство на протокола TCP/IP води до неговото приемане в целия свят като основен протокол за комуникация в Интернет и Интранет. TCP/IP позволява информацията да преминава през междинни компютърни станции, което дава възможност на трети страни да се намесят в комуникациите по следните начини:

- **Подслушване -** информацията остава непроменена, но нейната конфиденциалност е нарушена;
- **Модифициране -** информацията по време на транспорта се променя или заменя и след това се изпраща до получателя;
- **Изфабрикуване -** информацията се предава до получател, който се представя за истинския получател;
- **Прекъсване** – прекъсване на информацията, изпращана на получателя.

В дисертационния труд са представени симулационни модели, описващи основните атаки, провеждани в компютърните мрежи, които от своя страна биват два типа – активни и пасивни. Пасивните атаки са свързани с подслушване на пакети и анализ на мрежовия трафик. Тяхната цел е да се събере информация за атакуваната цел. Събраната информация служи за анализиране на обекта и откриване на слаби страни в неговата защита. Този тип атаки са трудни за откриване и идентифициране, тъй като тяхното действие е аналогично на програмите за мониторинг на мрежата и записване на трафика. Активни са тези атаки, които са свързани с подмяна на права, унищожаване на ресурси, подмяна или изтриване на данни.

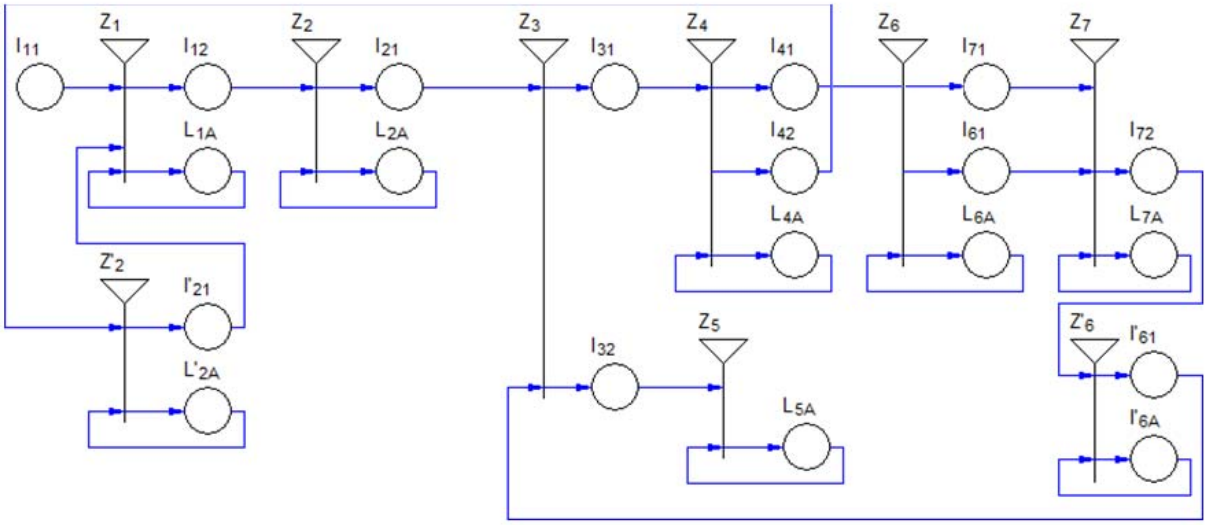
## 2.3. МОДЕЛИРАНЕ НА МРЕЖОВИ АТАКИ ЗА ПОДСЛУШВАНЕ И ПРЕКЪСВАНЕ НА КРИПТИРАНИ СЪОБЩЕНИЯ ЧРЕЗ ИЗПОЛЗВАНЕ НА ОБОБЩЕНОМРЕЖОВИ МОДЕЛ

В модела е разгледана криптографска система, използваща асиметричен ключ за криптиране и декриптиране на информацията, преминаваща през обществената мрежа.

Използван е RSA асиметричен алгоритъм, при който ключовете за кодиране ($K_E$) и декодиране ($K_D$) на информацията са различни $K_E \neq K_D$, тъй като публичният ключ на страната, която получава съобщенията, е общоизвестен. Асиметричните алгоритми се наричат още алгоритми с открит ключ, ключът за кодиране при тях може да се разпространява свободно. Така всеки може да шифрира съобщение, но само притежателя на частния ключ ще може да го дешифрира.

RSA алгоритъм е с използване на публичен ключ [53, 54], в който се описват три съставни алгоритъма: генериране на ключове, шифриране и дешифриране.

**-** Генериране на ключове – алгоритъмът за генериране на ключове взима сигурен параметър $\boldsymbol{n}$ като входящ. Използвано е $n = 1024$ като стандартен сигурен параметър. Алгоритъмът генерира две $(n/2)$ големи прости числа $\boldsymbol{p}$ и $\boldsymbol{q}$ от множество $N \leftarrow pq$. След това се избират няколко малки стойности $\boldsymbol{e}$, което е малко просто число от $\varphi(N) = (p - 1)(q - 1)$. Стойността се нарича криптирана криптографска екаспонента и обикновенно се избира като $e = 65537$.




Фиг.2.3. Обобщеномрежов модел на мрежови атаки за подслушване и прекъсване на криптирани съобщения

Обобщеномрежовият модел $A = \{Z_1, Z_2, Z'_2, Z_3, Z_4, Z_5, Z_6, Z'_6, Z_7\}$, който описва следните процеси:

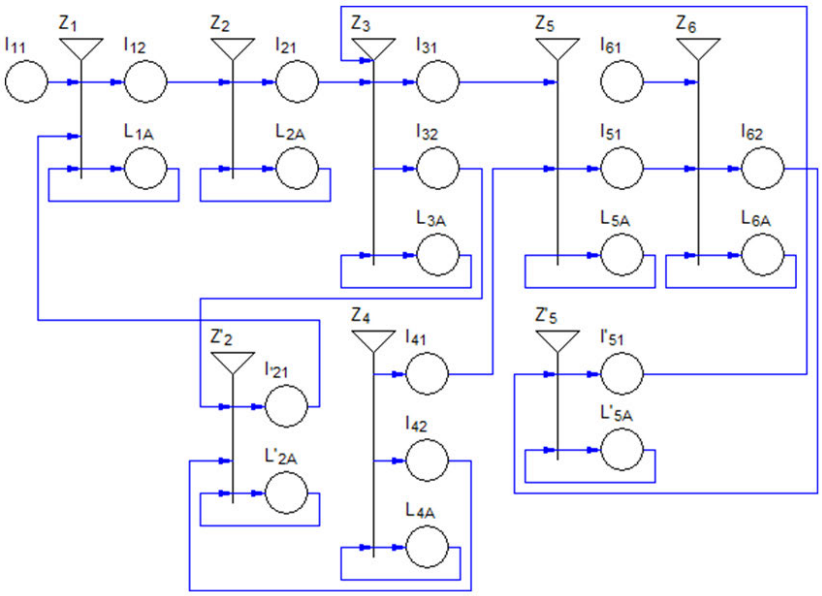
- $Z_1$ = "Задачи, извършени от източник *A*";
- $Z_2$ = "Задачи, извършени от криптографски алгоритъм за „криптиране"";
- $Z'_2$ = "Задачи, извършени от криптографски алгоритъм за „декриптиране"";
- $Z_3$ = "Извършени атаки";
- $Z_4$ = "Задачи, извършени от атака „подслушване"";
- $Z_5$ = "Задачи, извършени от атака „прекъсване"";
- $Z_6$ = "Задачи, извършени от криптографски алгоритъм за „декриптиране"";
- $Z'_6$ = "Задачи, извършени от криптографски алгоритъм за криптиране";
- $Z_7$ = "Задачи, извършени от източник *B*".

## 2.4. МОДЕЛИРАНЕ НА МРЕЖОВИ АТАКИ ЗА МОДИФИЦИРАНЕ И ИЗФАБРИКУВАНЕ НА КРИПТИРАНИ СЪОБЩЕНИЯ ЧРЕЗ ИЗПОЛЗВАНЕ НА ОБОБЩЕНОМРЕЖОВ МОДЕЛ

В модела е разгледана структурата на атаките за модифициране и изфабрикуване на шифрирани съобщения, изпратени по обществената мрежа. Чрез използване на апарата на обобщените мрежи са моделирани процесите на атаки за модифициране и изфабрикуване на предаваните съобщения. За разглежданите криптирани съобщения е използван RSA асиметричен алгоритъм.

Разработен е обобщеномрежов модел $A = \{Z_1, Z_2, Z'_2, Z_3, Z_4, Z_5, Z'_5, Z_6\}$, който описва следните процеси:

- $Z_1$ = „Задачи, извършени от източник *A*";
- $Z_2$ = „Задачи, извършени от криптографски алгоритъм за „криптиране"";
- $Z'_2$ = „Задачи, извършени от криптографски алгоритъм за „декриптиране"";
- $Z_3$ = „Задачи, извършени от атака модифициране";
- $Z_4$ = „Задачи, извършени от атака фалшив шифрован текст „изфабрикуване"";
- $Z_5$ = „Задачи, извършени от криптографски алгоритъм за „декриптиране"";
- $Z'_5$ = „Задачи, извършени от криптографски алгоритъм за „криптиране"";
- $Z_6$ = „Задачи, извършени от източник *B*".



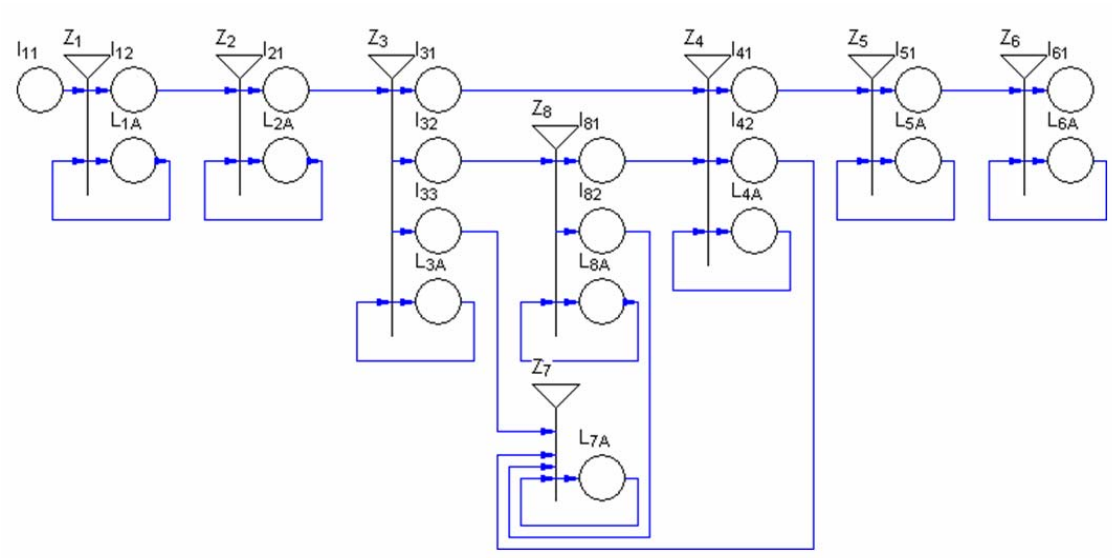

Фиг. 2.5. Обобщеномрежов модел на мрежови атаки за модифициране и изфабрикуване на криптирани съобщения

## 2.5. СКАЛА ЗА ОЦЕНЯВАНЕ СТЕПЕНТА НА АТАКУВАНИТЕ СЪОБЩЕНИЯ ПРЕДАВАНИ ПО ОБЩЕСТВЕНАТА МРЕЖА ЧРЕЗ ИЗПОЛЗВАНЕ НА ОБОБЩЕНИ МРЕЖИ

Разгледана е обобщена мрежа, оценяваща степента на атакуваните криптирани съобщения предавани през Интернет. Дефиниран е „независим наблюдател", събиращ информация за протичащите в мрежата процеси между съответните потребители, обменящи конфиденциални съобщения.

Разглежда се общата структура на криптографската система, чиито процеси се оценяват от интуиционистки размити оценки (ИРО).

Информацията, която може да бъде прочетена без специални усилия, се нарича открит или явен текст. Методът на преобразуване на открития текст по начин, по който да се скрие неговото съдържание, се нарича криптиране.




Фиг.2.6. Обобщеномрежов модел на скала за оценяване степента на атакуваните съобщения предавани по обществената мрежа

Обобщеномрежовият модел $A = \{Z_1, Z_2, Z_3, Z_4, Z_5, Z_6, Z_7, Z_8\}$ описва следните процеси:

- $Z_1$= „процеси, извършени от източника $A$ – изпращане на явен текст за криптиране”;
- $Z_2$ = „процеси, извършени от криптографски алгоритъм за криптиране”;
- $Z_3$ = „процеси, изпращане на криптирани съобщения”;
- $Z_4$ = „процеси, получаване на криптирани съобщения”;
- $Z_5$ = „процеси, извършени от криптографски алгоритми за декриптиране”;
- $Z_6$ = „процеси, извършени от източника $B$ – получен явен текст”;
- $Z_7$ = „оценки за атакувани съобщения”;
- $Z_8$ = „извършени атаки от $C$”.

## 2.6. ИЗВОДИ

Във втора глава са разгледани модели на мрежови атаки свързани с подслушване, прекъсване, промяна на информацията, както и скала за оценяване на мрежовата сигурност. Тези модели подпомагат да се определи приоритетът на различните информационни ресурси и да се гарантира възможността за анализ относно сигурността при предаване на конфиденциална информация. Ползите от разработените и изследвани модели са натрупване на история на данни за атаките на системата по време на функционирането й, както и проследяване на текущия статус на системата, което може да бъде използвано за последваща оптимизация. Поставен е акцент върху основните методи за атакуване и откриване на съответните атаки и методи за оценяването им.

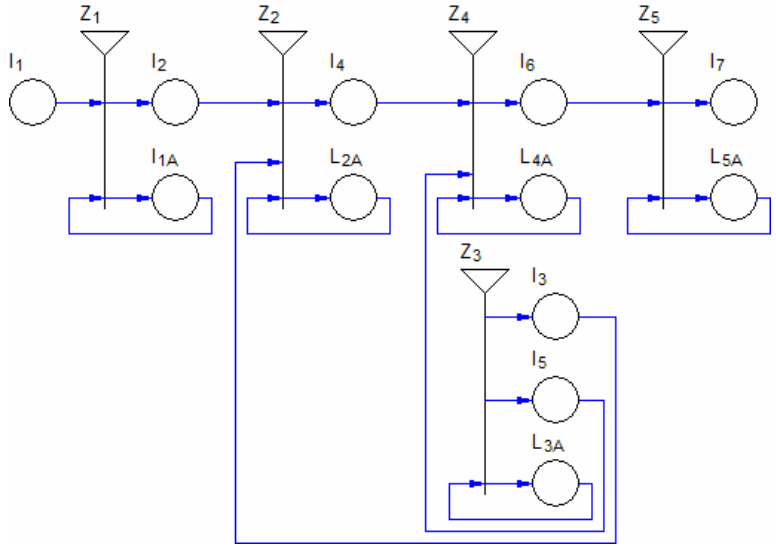
# 3. ГЛАВА ТРЕТА – ОБОБЩЕНОМРЕЖОВИ МОДЕЛИ НА ПРОЦЕСИ НА ЗАЩИТА ПРИ ОБМЕН НА ДАННИ

Сигурността на информацията е понятие, което може да се опише със следните три основни характеристики:

- *конфиденциалност*,
- *цялостност* и
- *наличност на информацията*.

## 3.1. ИЗПОЛЗВАНЕ НА ОБОБЩЕНОМРЕЖОВ МОДЕЛ НА КЛАСИЧЕСКА СТРУКТУРА НА КРИПТОГРАФСКА СИСТЕМА ЧРЕЗ ИЗПОЛЗВАНЕ НА СИМЕТРИЧЕН КЛЮЧ

Разгледана е общата структура на криптографска система, представена чрез обобщеномрежов модел. На тази база са реализирани оптимални начини за протичане на процеси за криптиране със симетричен ключ. Използвана е класическа едноключова криптографска система за защита на информацията, т.е. използван е един ключ както за криптиране, така и за декриптиране. Основно предимство на конвенционалното криптиране е бързината за криптиране и декриптиране на съобщенията, което е особено подходящо да се използва за съобщения, които няма да се изпращат.




Фиг.3.1. Обобщеномрежов модел на класическа структура на криптографска система чрез използване на симетричен ключ

Разработен е обобщеномрежов модел $A = \{Z_1, Z_2, Z_3, Z_4, Z_5\}$, където преходите описват следните процеси:

- $Z_1$ = „Задачи, извършени от източник $A$”;
- $Z_2$ = „Задачи, извършени от криптографско устройство 1”;
- $Z_3$ = „Задачи, извършени от генератора на ключове”;
- $Z_4$ = „Задачи, извършени от криптографско устройство 2”;
- $Z_5$ = „Задачи, извършени от източник $B$”.

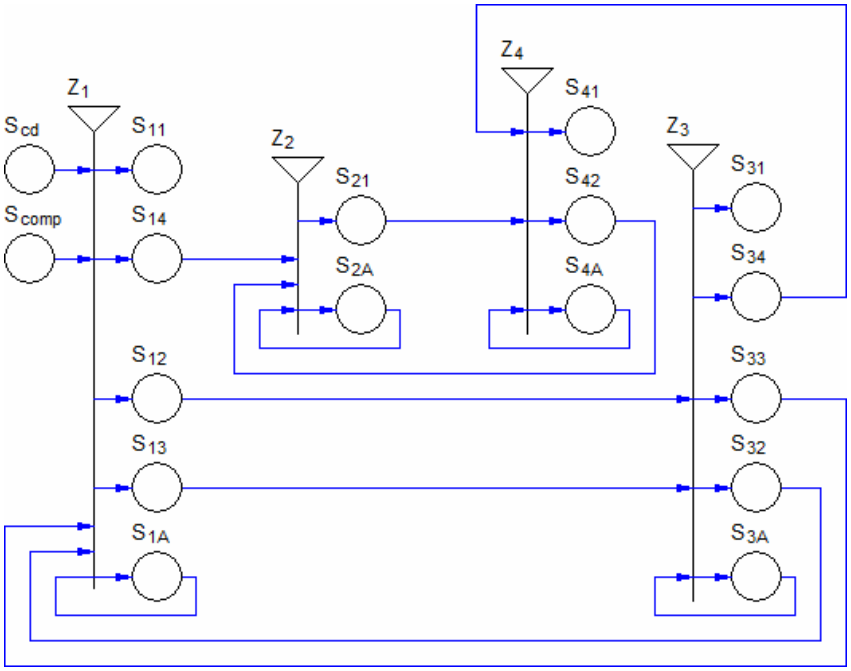
Обобщеномрежовият модел описва основната концепция от теорията на криптографията за конвенционално криптиране чрез класическа структура на криптографска система с използване на симетричен ключ. Моделът разглежда различните етапи от протичането на процесите за криптиране и декриптиране.

## 3.2. МОДЕЛИРАНЕ НА SSL ЧРЕЗ АПАРАТА НА ОБОБЩЕНИ МРЕЖИ

Разгледана е една от възможностите за защита на данни в TCP/IP-базирани мрежи чрез използването на SSL протокол. Разработен е ОМ-модел, отразяващ работата по изграждане и предаване на конфиденциална информация между клиент и сървър по криптиран тунел.

Отдалеченият хост (клиент) отправя заявка до сървъра за осъществяване на криптирана връзка, като изпраща сертификата си. Ако клиентският сертификат е достоверен, сървърът връща своя сертификат за договаряне на ключовете и криптиране на сесията.

Всяка криптирана сесия има живот, който приключва след като сървърът изпрати своето поредно съобщение до клиента, че е получил неговите поредни данни и не са постъпили нови данни от клиента за сървъра.




Фиг. 3.2. Моделиране на SSL чрез апарата на обобщени мрежи

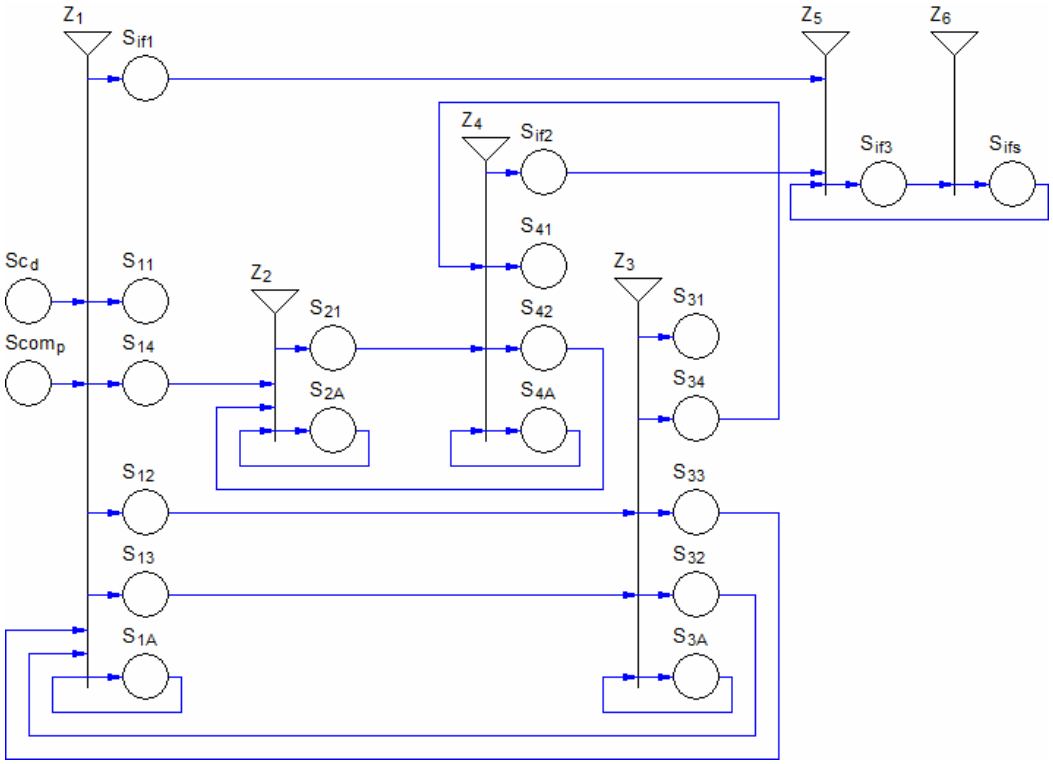
Разработен е обобщеномрежов модел $A = \{Z_1, Z_2, Z_3, Z_4\}$, където преходите описват следните процеси:

- $Z_1$ = „Изпращане на информация от клиента“;
- $Z_2$ = „Изпращане на информация от клиента по криптиран канал“;
- $Z_3$ = „Изпращане на информация от сървъра“;
- $Z_4$ = „Изпращане на информация от сървъра по криптиран канал“.

Разработения модел описва работата на SSL протокола. Той може да се използва самостоятелно или като допълнителен модул към други ОМ модели представящи работата на системи, в които се предават конфиденциални данни. Модела може да послужи за изследване, анализиране и оптимизиране на протичащите процеси при обмен на конфиденциална информация в Интернет или Интранет мрежи.

## 3.3. ОБОБЩЕНОМРЕЖОВИ МОДЕЛ НА SSL С ИНТУИЦИОНИСТКИ РАЗМИТИ ОЦЕНКИ

Предложеният модел описва процеса на обмен на конфиденциална информация.




Фиг. 3.3. Обобщеномрежов модел на SSL с интуиционистки размити оценки

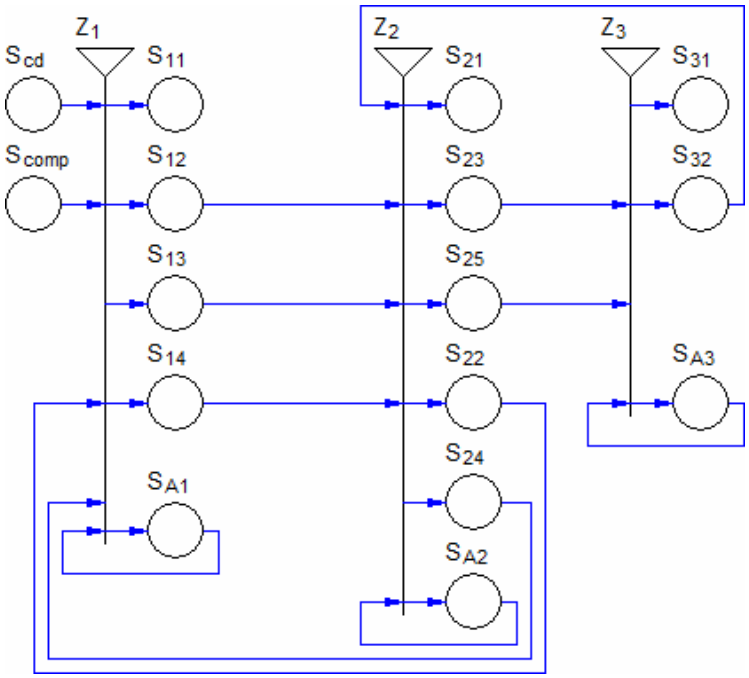
Разработен е обобщен мрежови модел $A = \{Z_1, Z_2, Z_3, Z_4, Z_5, Z_6\}$, където преходите описват следните процеси:

- $Z_1$ = „Изпращане на информация от клиента”;
- $Z_2$ = „Изпращане на информация от клиента по криптиран канал”;
- $Z_3$ = „Изпращане на информация от сървъра”;
- $Z_4$ = „Изпращане на информация от сървъра по криптиран канал”;
- $Z_5$ = „Събиране на информация от предаващата и приемащата част”;
- $Z_6$ = „Изчисляване на интуиционистки размитата оценка”.

## 3.4. ОБОБЩЕНОМРЕЖОВ МОДЕЛ ЗА СЪЗДАВАНЕ НА VIRTUAL PRIVATE NETWORK ЧРЕЗ ИЗПОЛЗВАНЕ НА POINT-TO-POINT PROTOCOL ВЪРХУ SECURE SHELL

Тук се разглежда изграждане на VPN тунел между мобилен клиент и сървър, отразяващ изграждането на криптиран тунел за отдалечена комуникация между мобилен потребител и частна мрежа.

VPN мрежите се използват за осигуряване на отдалечен достъп до мобилни служители, осигуряване на екстранет мрежа с достъп до нейни служители и клиенти или за осигуряване на връзка между два офиса в различни местоположения.




Фиг. 3.4. ОМ модел за създаване на Virtual Private Network чрез използване на Point-to-Point Protocol върху Secure Shell

Разработен е обобщеномрежов модел A = {Z1, Z2, Z3}, където преходите описват следните процеси:

- $Z_1$ = „Задачи, извършени от клиента”;
- $Z_2$ = „Задачи, извършени от доставчика на интернет”;
- $Z_3$ = „Задачи, извършени от сървъра”.

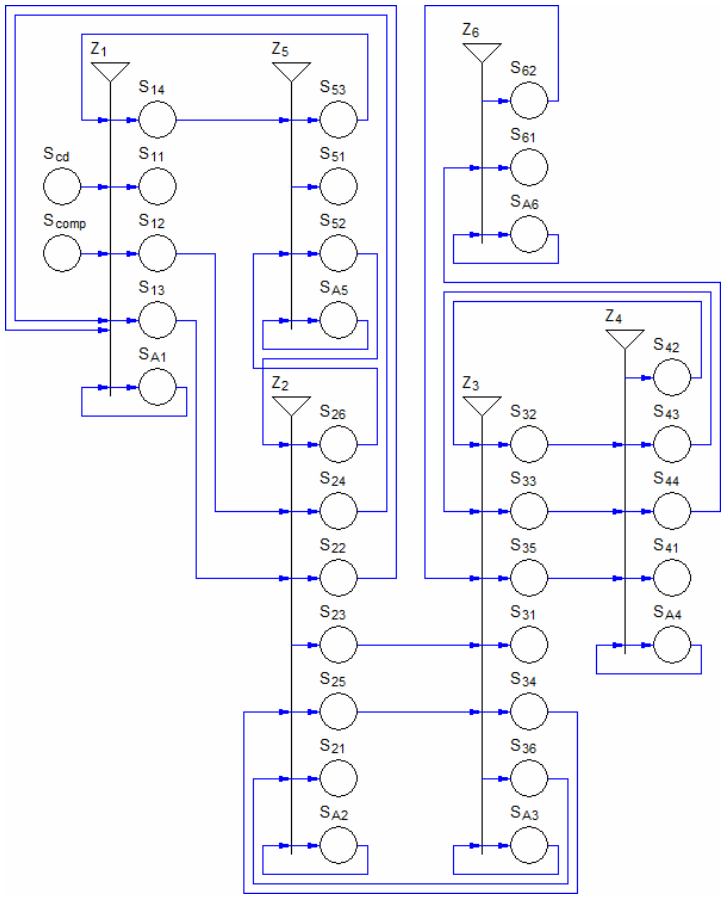
## 3.5. ОБОБЩЕНОМРЕЖОВ МОДЕЛ НА СЪЗДАВАНЕ НА VIRTUAL PRIVATE NETWORK ЧРЕЗ ИЗПОЛЗВАНЕ НА POINT-TO-POINT PROTOCOL ВЪРХУ SCURE SHELL2 ЗА ИЗГРАЖДАНЕ НА БЕЗПАРОЛНА VPN ВРЪЗКА

Изграждането на виртуален тунел представлява логическа връзка между две крайни точки, в които се поддържа автентикация и криптиране на данните от едната до другата точка.

При VPN се изгражда тунел през Интернет и данните се изпращат по обществената мрежа по начин, който пресъздава връзка от тип „от точка до точка” PPP. Това се постига чрез капсулиране на данните. По този начин се създава логическа независима мрежа от местоположението на крайните точки, в които се поддържа автентикация. Данните се криптират – остават частни, и това е от изключително значение, за да могат да бъдат защитени. В противен случай всеки може да ги прихване по време на преминаването през обществената Интернет мрежа между предаващата и приемащата крайна точка на тунела.

VPN позволява да се създаде логическа мрежа, която е независима от местоположението на служителите или клиентите, дава възможност за установяване на директна физическа връзка.

Разработеният ОМ модел е създаден в допълнение на предходния.




Фиг.3.5. ОМ модел на създаване на Virtual Private Network чрез използване на Point-to-Point Potocol върху Scure Shell2 за изграждане на безпаролна VPN връзка

Разработен е обобщеномрежов модел A = {Z1, Z2, Z3, Z4, Z5, Z6}, където преходите описват следните процеси:

- $Z_1$ = „Задачи, извършени от клиента”;
- $Z_2$ = „Задачи, извършени от ISP”;
- $Z_3$ = „Задачи, извършени от LAN сървър”;
- $Z_4$ = „Задачи, извършени от VPN сървър”;
- $Z_5$ = „Криптирана връзка от клиента”;
- $Z_6$ = „Криптирана връзка от сървъра”.

## 3.6. ИЗВОДИ

В главата са разработени пет обобщеномрежови модела. Първият от тях разглежда основната концепция от теорията на криптографията за конвенционално криптиране чрез класическа структура на криптографска система с използване на симетричен ключ. Той разглежда различните етапи от протичането на процеса и позволява неговата симулация и поведението му в бъдеще.

Вторият модел разглежда работата на SSL протокола. Той може да се използва самостоятелно или като допълнителен модул към други ОМ модели, представящи работата на системи, в които се предават конфиденциални данни.

В третия модел е описана работата на мрежа, работеща със SSL, в допълнение от [8*] с изчисляване на интуиционистки размити оценки. Моделът може да бъде използван като средство за изследване и анализиране на протичащите процеси, както и на тяхното поведение.

Следващият модел разглежда създаването на виртуална частна мрежа (VPN), изградена на базата на протоколи PPP и SSH. Моделът може да бъде използван като средство за изследване на процеси, както и за прогнозиране на тяхното поведение в бъдеще.

Последният модел към главата е разгледана VPN технологията, която предлага изграждане на сигурна „безпаролна връзка", като разширява традиционното обслужване, предоставяйки нови услуги.

# 4. ГЛАВА ЧЕТВЪРТА – ЗАЩИТА НА Е-ДАННИ НА ПАЦИЕНТИ

В тази глава са разгледани модели, илюстриращи различни аспекти на конфиденциалност на медицински данни предавани и използвани при съвременните медицински системи.

Според чл. 5, ал. 1 от ЗЗЛД в дела „чувствителни" лични данни са посочени личните данни, които се отнасят до здравето.

Европейската харта за правата на човека, т. 6, гласи „Право на тайна и конфиденциалност: Всяко лице има право на поверителност на личната информация, включваща данни относно здравното му състояние и потенциални диагнози или терапевтични процедури, както и защитата на конфиденциалността по време на изпълнението на диагностичните процедури, посещенията от специалист и медицинско хирургично лечение като цяло".

Относно създаването на интегрирана система за електронен обмен на данни в здравеопазването са приети:

- Стандартизация и информационна сигурност [103];
- Изграждане на интегрирана система за обмен на информация между заетите в сферата на здравеопазването (здравни, лечебни, учебни, научни, финансови и административни звена);
- Информираност и обучение чрез предоставяне на уеб-базирани услуги;
- Прилагане на добри практики и оперативна съвместимост.

## 4.1. ЕЛЕКТРОННО ЗДРАВЕОПАЗВАНЕ В БЪЛГАРИЯ

Една от основните цели на електронното здравеопазване е да се повиши качеството и обема на предлаганите услуги в здравеопазването, обмен на електронни данни между отделни болнични звена, като при това се запазят или намалят разходите за съответните услуги.

Главните **направления** при електронното здравеопазване са:

1. **Системи и услуги, предназначени за сектора по здравеопазване** – за доставяне на по-добри и по-ефективни здравни услуги, създаване на благоприятни условия за развитие на медицинската научноизследователска дейност, осигуряване на ефективно управление и разпространение на медицински знания;
2. **Възможности за потребителите на здравни услуги – пациенти и здрави граждани** – по-добро здравно образование, превенция, информация за здравното състояние, възможност за активно участие на пациентите във вземането на решения относно тяхното здраве;
3. **Съдействие на професионалистите в сферата на здравеопазването** – бърз и лесен достъп до информация, диагностика и извършване на сложни интервенции от разстояние, както и достъп до специализирани ресурси за образование и обучение;
4. **Съдействие на здравните власти и здравните ръководители –** достъп и разпространение на най-добри практики за обработка на данните, свързани с управлението, планирането, организирането и разпределението на здравните ресурси.
5. **Ускорено внедряване на ИКТ след извършване на обстоен анализ на работните процеси в здравеопазването.**

Националната стратегия за внедряване на електронно здравеопазване в България включва:

1. Стандартизация и информационна сигурност;
2. Внедряване на електронни здравни карти;
3. Създаване на пълно електронно медицинско досие на пациента;
4. Изграждане на комплексни болнични информационни системи;
5. Изграждане на интегрирана информационна система за обмен на информация между здравните звена;
6. Изграждане и развитие на телемедицински проекти.

Използването на информационни и комуникационни технологии в здравния сектор е свързано с необходимостта от гарантиране защитата на авторските и сродни права върху здравни разработки, защита на личните данни и здравната информация както нейното съхранение и обмен по електронен път на регистри, здравни досиета и други лични данни.

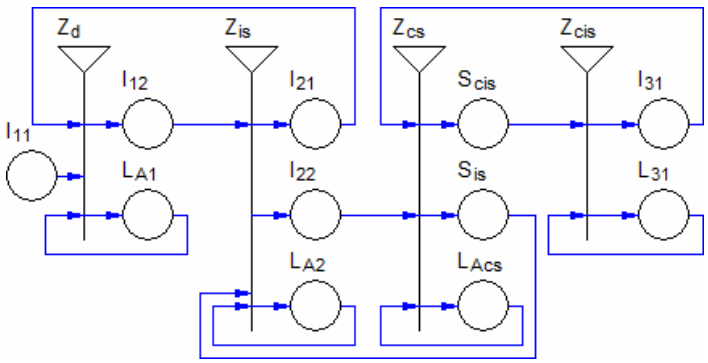
## 4.2. ОБОБЩЕНОМРЕЖОВИ МОДЕЛ ЗА ЗАЩИТА НА Е-ДАННИ НА ПАЦИЕНТИ ПРЕДАВАНИ МЕЖДУ ИНФОРМАЦИОННИ БОЛНИЧНИ СИСТЕМИ В ОБЩЕСТВЕНАТА МРЕЖА

В представения модел се описва процесът на протичане на информация за пациентите между различни болнични заведения (БЗ) по криптиран тунел през обществената мрежа. Моделът е базиран на ОМ [2*], който в тази статия е подобрен и е насочен към целите на конкретното изследване.

Разгледаният ОМ модел предоставя възможност за обслужване на един и същи пациент в различни болнични системи (БС). Също така разглежда процеса на постъпване на пациент, който не е регистриран в съответното БЗ, изпращане на лекарско запитване до текущата информационна БС (ИБС). Тя от своя страна проверява регистрацията на пациента дали е в текущата ИБС или изпраща запитване до ИБС, в която той е регистриран, за да получи достъп до неговото електронно досие. Този процес протича по криптиран канал с цел сигурност/защита на личните данни на пациента.

Тук са описани два ОМ модела. Първият от тях разглежда връзките между две БЗ, а във втория е използвано разширение на преход $Z_{cs}$, описващ предаването на лични данни за пациентите по сигурен канал.

**Първи ОМ модел**



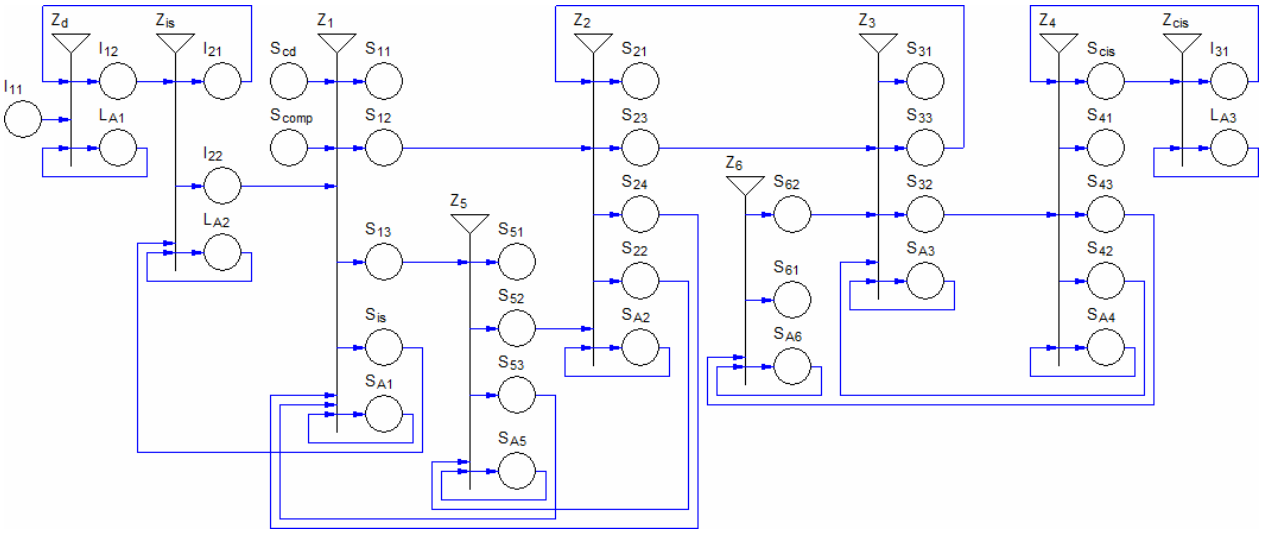

Фиг. 4.1. $OM_1$ за защита на е-данни на пациенти предавани между информационни болнични системи в обществената мрежа

Множеството от преходи на тази ОМ е $A = \{Z_d, Z_{is}, Z_{cs}, Z_{cis}\}$, където преходите описват следните процеси:

- $Z_d$ = „Дейности извършени от здравен специалист”;
- $Z_{is}$ = „Задачи извършени от ИБС1”;
- $Z_{cs}$ = „Задачи извършени от Криптираща система”;
- $Z_{cis}$ = „Задачи извършени от ИБС2”.

**Втори ОМ модел**

Оператор $H_3$ замества фиксиран преход на дадена ОМ с нов ОМ, имаща същите входни и изходни позиции. Ако $Z$ е фиксиран преход на дадена ОМ $E$, а $E'$ е новата ОМ, за която $pr_1Z=Q_E^i$ и $pr_2Z= Q_E^0$, то операторът има вида $H_3(E, Z, E') = E''$. Сега върху $OM_1$ прилагаме оператор $H_3$, който замества преход $Z_{cs}$ в ОМ [4*] в резултат получаваме $OM_2$ от Фиг. 4.2.




Фиг. 4.2. $OM_2$ за защита на е-данни на пациенти предавани между информационни болнични системи в обществената мрежа

ОМ мрежата $A= \{Z_1, Z_2, Z_3, Z_4, Z_5, Z_6\}$ се описва с множество от преходи, които описват следните процеси:

- $Z_1$ = „задачи, извършени от клиента”;
- $Z_2$ = „задачи, извършени от интернет доставчик”;
- $Z_3$ = „задачи, извършени от LAN сървър”;
- $Z_4$ = „задачи, извършени от VPN сървър”;
- $Z_5$ = „криптирана връзка от клиента”;
- $Z_6$ = „криптирана връзка от сървъра”.

## 4.3. ИЗВОДИ

Разработеният модел подпомага за създаването и внедряването на специфични за здравеопазването софтуерни и хардуерни продукти, които да бъдат съобразени с интернационалните стандарти за обмен и защита на медицинските данни.

Моделът представя разработването и въвеждането на изисквания за съвместимост на информационните системи в здравеопазването посредством:

- Осигуряване на сигурност за информационните системи в здравеопазването и за защита на личните данни.

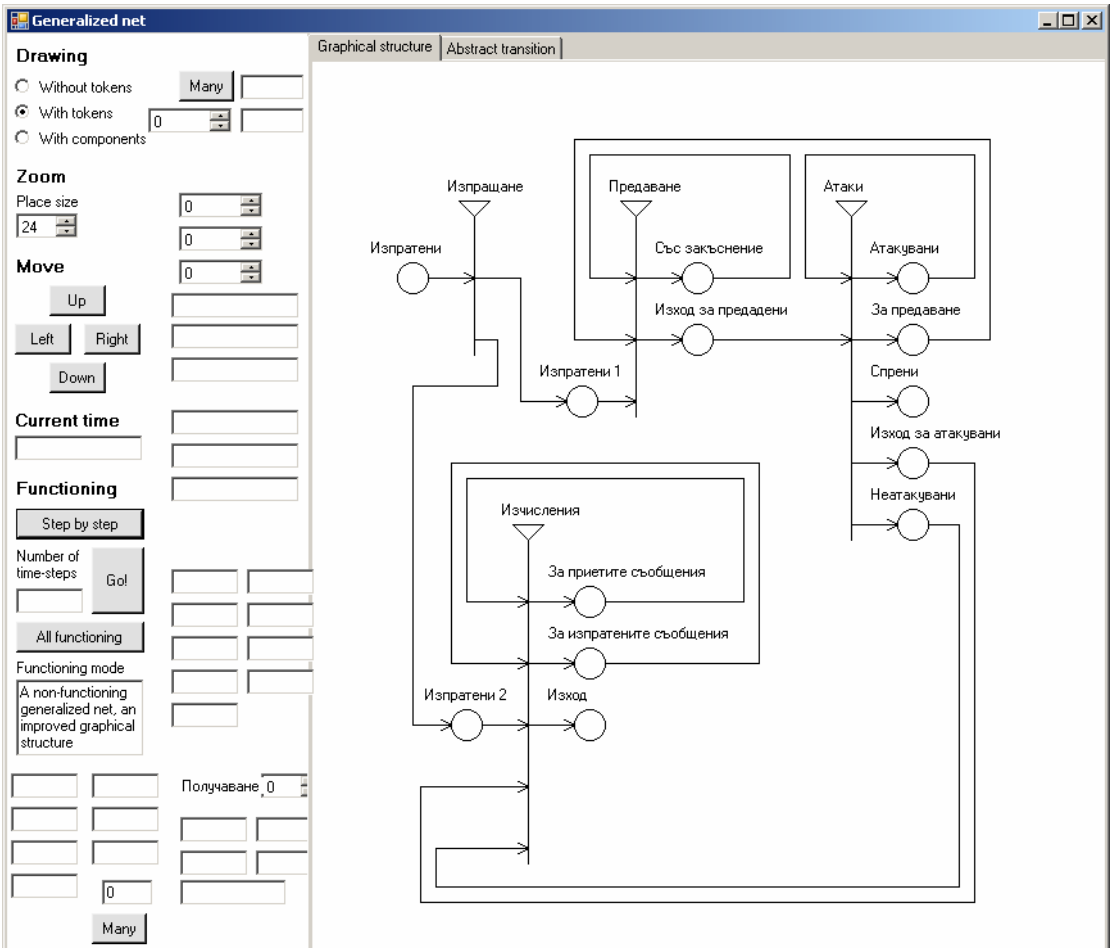
- Внедряване на софтуерни приложения за комплексно обработване на информацията, в това число: електронни направления, електронни рецепти, лабораторни данни и други изследвания.

- Изграждане на комплексни и интегрирани помежду си, както и с външни приложения болнични информационни системи.

# 5. ТЕСТВАНЕ НА МОДЕЛ НА ИЗЧИСЛЯВАНЕ НА ОЦЕНКИ ЗА АТАКУВАНЕ НА СЪОБЩЕНИЯ ЧРЕЗ ОБОБЩЕНИ МРЕЖИ И ИНТУИЦИОНИСТКИ РАЗМИТИ ВЯРНОСТНИ СТОЙНОСТИ

Всяка комуникационна мрежа може да се моделира от гледна точка на надеждността като сложна система с недетерминирано поведение след отказ. Недетерминираността на поведението се определя от появата и натрупването на причини за откази в резултат на случайни неизправности, шумове и други смущения, грешки в процеса на създаване на системата, интрузионни действия на субективни фактори.

В резултат от неоторизиран достъп информацията може да бъде променена, частично подменена или подменена изцяло с друга информация, може да бъде унищожена или да бъде разпространена по време на предаването ѝ. Комуникациите, които се използват в Интернет, са отворени и трудно се контролират. Този проблем поставя на преден план въпроса за сигурността на предаваните данни в обществената мрежа.




Фиг. 5.1. Интерфейс на софтуер за тестване на ОМ

Анализът на системата се извършва, като обобщената мрежа се натовари, като се настрои симулатора така, че през определен период от време в мрежата да постъпва ново ядро. След определен брой итерации (колкото повече, толкова по-точна ще бъде оценката) се правят изчисления за оценка на атакуваните съобщения.

**Резулати от симулации**

С цел верификация, характеристики на ядра, преминаващи през две позиции, са сравнени с резултати, получени аналитично чрез използване на марковски процеси. Симулациите са извършени с използване на разработен от д-р Валери Гочев софтуер [99]. Следват резултатите от симулациите и получените аналитично стойности при зададените входни данни.

В първата таблица са зададени стойности за описани в изложението параметри.

Таблица 1

| Входни данни | |
|---|---|
| Дял на незабавно предадените съобщения, $p$ | 50% |
| Средно време за предаване на съобщение при наличие на закъснение, $a$ [ms] | 5 |
| Дял на прихванатите съобщения, $q$ | 40% |
| Средно време, необходимо за атака, $b$ [ms] | 80 |
| Дял на спрените съобщения, $r$ | 20% |
| Времева стъпка [ms] | 0.3 |

Навсякъде в тази точка при работата със софтуер резултатите са получени на базата на $10^4$ симулирани съобщения, постъпващи средно през 80ms съгласно поасоново разпределение. Следващите резултати показват получени интуиционистки размити стойности при вариране на параметъра $c$, указващ пределно закъснение.

За да можем да анализираме работоспособността на тествания модел, подаваме 16384 ($2^{14}$) броя съобщения.

Таблица 6

| **Разпределение на степента на вярност, невярност и неопределеност по отношение на броя на изпратените съобщения при пределно закъснение 7,5 ms** | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Брой съобщения | 16 | 32 | 64 | 128 | 256 | 512 | 1024 | 2048 | 4096 | 8192 | 16384 |
| Степен на вярност | 0,3125 | 0,29881 | 0,29992 | 0,30858 | 0,30447 | 0,30162 | 0,29922 | 0,3015 | 0,30079 | 0,29958 | 0,30055 |
| Степен на невярност | 0,44583 | 0,46052 | 0,46593 | 0,45029 | 0,44823 | 0,45004 | 0,45485 | 0,45379 | 0,4535 | 0,45384 | 0,45488 |
| Степен на неопределеност | 0,24167 | 0,24067 | 0,23415 | 0,24113 | 0,2473 | 0,24834 | 0,24593 | 0,24471 | 0,24571 | 0,24658 | 0,24457 |

От направената симулация за изпратени съобщения се вижда, че:

- степените на вярност, невярност и неопределеност са относително постоянни във времето, което показва стабилност на модела;

- с увеличаване на броя на изпратените съобщения измененията на степените на вярност, невярност и неопределеност намаляват като в края на интервала измененията са минимални;

- поради това, че голямата част от изпратените съобщение имат времезакъснение, т.е. се определят като неправилно приети, което увеличава степента на невярност и тя е най-голяма;

- степента на неопределеност е също с голяма стойност, тъй като при поасоновото разпределение на времезакъсненията съществена част от съобщенията попадат в средата на интервала от 0 до 7,5ms, т.е. трудно е да се определи дали те са атакувани или не;

- степента на вярност е ниска, поради това, че на входа на мрежата се подават с времезакъснения по-големи от 0, което е предпоставка за малкия брой съобщения предадени без закъснение.


Фиг. 5.7. Разпределение на степента на вярност, невярност и неопределеност по отношение на броя на изпратените съобщения при пределно закъснение 7,5 ms

Таблица 8

| **Разпределение на степента на вярност, невярност и неопределеност по отношение на броя на приетите съобщения при пределно закъснение 7,5 ms** | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Брой съобщения | 16 | 32 | 64 | 128 | 256 | 512 | 1024 | 2048 | 4096 | 8192 | 16384 |
| Степен на вярност | 0,33784 | 0,3209 | 0,32098 | 0,33167 | 0,32907 | 0,32735 | 0,32509 | 0,3277 | 0,32736 | 0,32548 | 0,32634 |
| Степен на невярност | 0,4009 | 0,42071 | 0,42836 | 0,40931 | 0,40373 | 0,40325 | 0,40924 | 0,40651 | 0,40609 | 0,40675 | 0,40766 |
| Степен на неопределеност | 0,26126 | 0,25839 | 0,25066 | 0,25902 | 0,2672 | 0,2694 | 0,26567 | 0,26579 | 0,26655 | 0,26777 | 0,266 |

От направената симулация за приети съобщения се вижда, че:

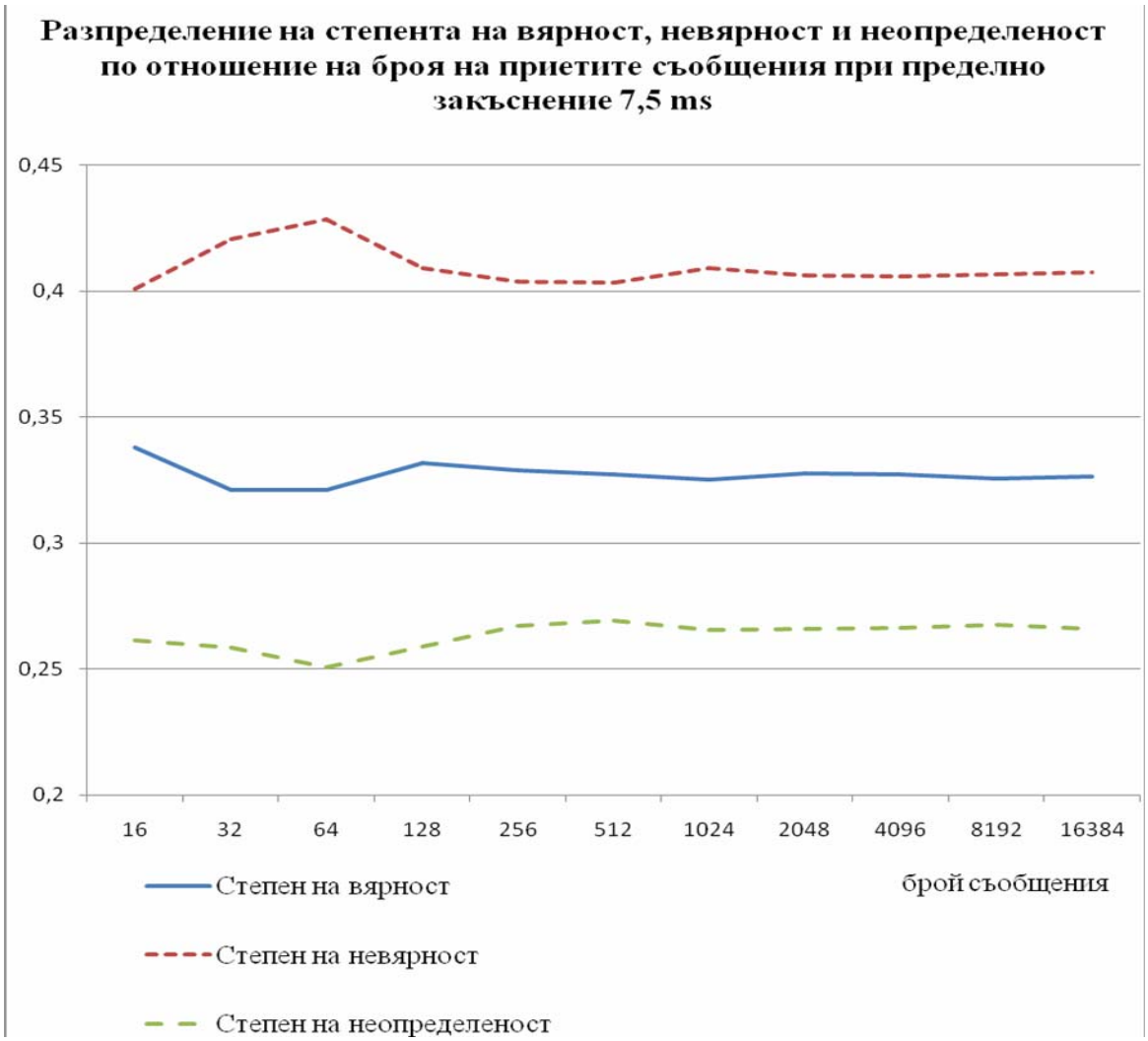
- степените на вярност, невярност и неопределеност са относително постоянни във времето, което показва стабилност на модела;

- с увеличаване на броя на приетите съобщения измененията на степените на вярност, невярност и неопределеност намаляват като в края на интервала измененията са минимални;

- поради това, че голямата част от приетите съобщение имат времезакъснение т.е. се определят като неправилно приети, което увеличава степента на невярност и тя е най-голяма;

- степента на неопределеност са също с голяма стойност, тъй като при поасоновото разпределение на времезакъсненията съществена част от съобщенията попадат в средата на интервала от 0 до 7,5ms  т.е трудно е да се определи дали те са атакувани или не;

- степента на вярност е ниска поради това, че на входа на мрежата се подават с времезакъснения по-големи от 0, което е предпоставка за малкия брой предадени без закъснение.




Фиг. 5.8. Разпределение на степента на вярност, невярност и неопределеност  по отношение на броя на приетите съобщения при пределно закъснение 7,5 ms

Разработеният модел може да бъде свързан със създаване и внедряване на специфични софтуерни и хардуерни продукти, съобразени с интернационалните стандарти

за обмен и защита на данни. Използваното поасоново разпределение обуславя конструиране на псевдослучайна величина, отразяваща вероятността описваните събития да се случват за определен интервал от време при съответна фиксирана интензивност на постъпване на съобщения. Разгледаният модел може да подпомогне и изследването на процеси на атакуване на кодирани съобщения, обменяни в различни мрежи. Той разглежда етапи от протичането на телекомуникационни процеси, както и особености в тяхната симулация.

## 6. ОСНОВНИ РЕЗУЛТАТИ И ИЗВОДИ

В дисертационния труд са изследвани, моделирани и анализирани основни проблеми в мрежовата сигурност, защитата при обмен на данни, създаването и внедряването на специфични за здравеопазването софтуерни и хардуерни продукти. Конструиран е модел за скала на оценяване на степента на атакуваните съобщения, предавани през обществената мрежа.

Разработени са обобщеномрежови модели на:

- мрежови атаки за подслушване и прекъсване на криптирани съобщения;
- мрежови атаки за модифициране и изфабрикуване на криптирани съобщения;
- скала за оценяване степента на атакуваните съобщения предавани по обществената мрежа;
- класическа структура на криптографска система чрез използване на симетричен ключ;
- secure socket layer;
- secure socket layer с интуиционистки размити оценки;
- виртуална частна мрежа чрез използване на point-to-point protocol върху secure shell;
- виртуална частна мрежа чрез използване на point-to-point protocol върху secure shell2 за изграждане на безпаролна vpn връзка;
- - защита на е-данни на пациенти предавани между информационни болнични системи в обществената мрежа.

Конструираните модели осигуряват възможност:

1) Да се симулират моделираните процеси с цел да се определи приоритетът на използване на различните информационни ресурси и да се гарантира възможността за анализ относно сигурността при предаване на конфиденциална информация (глава 3). Това дава възможност за изследване на поведението им в бъдеще.

2) Да се оптимизира начина на обмен на конфиденциалната информация по предварително зададени критерии за протичането на процеса;

3) Управление на отделни параметри при обмен на информация в здравеопазването;

4) Анализиране на информация относно атаките на системата по време на функционирането й, както и проследяване на текущия й статус, което може да бъде използвано за анализ и последваща оптимизация;

5) Качествена характеристика при обмен на конфиденциална информация с изчисляване на интуиционистки размити оценки.

*Бъдещи намерения за развитие:*

- *Разработените в дисертационния труд модели представят част от процесите, свързани с обмен на конфиденциална информация. Те могат да послужат като основа за изграждане на нови такива и свързването им в по-глобални модели. От друга страна предстои детайлизиране на някои компоненти;*

- *За изградените модели могат да се конструират различни разширения, по-специално чрез мрежите от високо ниво и обектно-ориентираните мрежи,*

*които могат да отразят аспектите на функционалния, информационния и ресурсен изглед;*

- *Към представените обобщеномрежови модели могат да се добавят интуиционистки размити оценки;*
- *Събираните за по-дълъг период от време данни от работата на моделите може да послужи за количествен и качествен анализ на моделираните системи, на база на което да се оптимизират някои от параметрите им.*
- *Моделите могат да се използват за обучение на специалисти по мрежова сигурност, както и по разработване и експлоатация.*
- *Модели [3*, 5*, 8*] са разработени въз основа на изградени системи на съответните видове сигурни връзки, тествани върху конкретни работни станции.*

## 7. СПРАВКА ЗА ПРИНОСИТЕ В ДИСЕРТАЦИОННИЯ ТРУД

Приносите в дисертационния труд имат научен и научно-приложен характер и могат да се формулират по следния начин.

1. Разработени са обобщеномрежови модели на:
   - мрежови атаки за подслушване и прекъсване на криптирани съобщения;
   - мрежови атаки за модифициране и изфабрикуване на криптирани съобщения;
   - скала за оценяване степента на атакуваните съобщения предавани по обществената мрежа;
   - криптографска система с използване на симетричен ключ;
   - затворен съединителен слой (secure socket layer) и на вариант с интуиционистки размити оценки;
   - виртуална частна мрежа (virtual private network) от типа point-to-point върху secure shell и вариант за secure shell2 за изграждане на безпаролна VPN връзка;
   - защита на е-данни на болнични пациенти.

2. Проведено е тестване на обобщеномрежов модел на скала за оценяване степента на атакуваните съобщения, предавани по обществената мрежа, получените резултати от който имат научно-приложен характер.

СПИСЪК НА ПУБЛИКАЦИИТЕ ПО ДИСЕРТАЦИОННИЯ ТРУД


[*1] Atanassov, K., I. Vardeva, Generalized net model for protection of patients' personal e-data, transmitted between healthcare information systems over the Internet. *Comptes rendus de l'Academie Bulgare des Sciences*, Vol. 65, No. 3, 2012 (in press).

[*2] Atanassov, K., I. Vardeva, Generalized net model with intuitionistic fuzzy scale for evaluating the degree of attacked messages sent over the public network. *Development in Fuzzy Sets, Intuitionistic Fuzzy Sets, Generalized Nets and Related Topics. Vol. II: Aplications*, SRI – Polish Academy of Science, Warsaw, 2010, 1–12.

[*3] Vardeva, I., Generalized net model for creating virtual private network using point-to-point protocol over secure shell2 for building passwordless VPN connection. *Development in Fuzzy Sets, Intuitionistic Fuzzy Sets, Generalized Nets and Related Topics. Vol. II: Aplications*, SRI – Polish Academy of Science, Warsaw, 2010, 293–302.

[*4] Vardeva, I., Modeling net attacks for modifying and counterfeit encrypted messages by using generalized nets model. *Issues in Intuitionistic Fuzzy Sets and Generalized Nets*, Vol. 7, 2008, 83–92.

[*5] Vardeva, I., Generalized net model of the creation of virtual private network by using point-to-point protocol over secure shell. *Issues in Intuitionistic Fuzzy Sets and Generalized Nets*, Vol. 6, 2008, 69–75.

[*6] Vardeva, I., Modeling net attacks for listening and break-down encrypted messages by using generalized nets model. *Proceedings of the Ninth Int. Workshop on Generalized Nets*, Sofia, 4 July 2008, Vol. 1, 20–27.

[*7] Vardeva, I., S. Sotirov. Generalized Net model of SSL with intuitionistic fuzzy estimations, *Notes on Intuitionistic Fuzzy Sets*, Vol. 13, No. 2, 2007, 48–53.

[*8] Vardeva,. I, SSL modeling by the apparatus of generalized net, *Proceedings of the Sixth Int. Workshop on Generalized Nets*, Sofia, 17 Dec. 2005, 29–33.

[*9] Вардева, И., Използване на обобщеномрежови модел на класическа структура на криптографска система чрез използване на симетричен ключ, *Годишник на секция „Информатика", Съюз на учените в България*, Том 1, 2008, 112–116.