СПЕЦИАЛИЗИРАН НАУЧЕН СЪВЕТ ПО ИНФОРМАТИКА
И МАТЕМАТИЧЕСКО МОДЕЛИРАНЕ ПРИ ВАК

ВЕСЕЛИНА ГОСПОДИНОВА ЖЕЧЕВА

ИЗСЛЕДВАНИЯ НА ИНФОРМАЦИОННАТА СИГУРНОСТ НА СИСТЕМИТЕ ЗА ЕЛЕКТРОННА ТЪРГОВИЯ

АВТОРЕФЕРАТ

на дисертация за присъждане на образователната и научна степен "доктор"
по научна специалност: 01.01.12 Информатика

Научен ръководител:
ст.н.с. I ст. д.м.н. Евгений Николов

София, 2005

Дисертационният труд "Изследвания на информационната сигурност на системите за електронна търговия" съдържа 132 страници в основен текст и 77 страници в приложенията. Състои се от увод, четири глави, заключение и три приложения. В основния текст са включени 68 фигури и 1 таблица. Използвани са 164 литературни източника, от които 3 на кирилица и 161 на латиница.

СПЕЦИАЛИЗИРАН НАУЧЕН СЪВЕТ ПО ИНФОРМАТИКА
И МАТЕМАТИЧЕСКО МОДЕЛИРАНЕ ПРИ ВАК

ВЕСЕЛИНА ГОСПОДИНОВА ЖЕЧЕВА

ИЗСЛЕДВАНИЯ НА ИНФОРМАЦИОННАТА СИГУРНОСТ НА СИСТЕМИТЕ ЗА ЕЛЕКТРОННА ТЪРГОВИЯ

АВТОРЕФЕРАТ

на дисертация за присъждане на образователната и научна степен "доктор"

Научен ръководител:
ст.н.с. I ст. д.м.н. Евгений Николов

Рецензенти:

София, 2005

I. Актуалност на темата.

През последните години в областта на информационните технологии се наблюдава тенденция към развитие на отворени системи, съвместими помежду си независимо от различните платформи и производители. От друга страна информационната сигурност е ключов проблем при комуникациите и обмена на данни в мрежова среда. Това ни доведе до идеята, че би било полезно да се разработи архитектура на система за електронна търговия, базирана на компонентния подход, която удовлетворява изискванията на определена политика на сигурност по отношение транзакциите между компонентите.

1. Тенденции и развитие на Интернет и електронната търговия. Съвременното развитие на информационните технологии, съчетано с експанзията на Интернет и глобализацията на икономиката създаде нови възможности за комуникации и обмен на технологии. Интернет създаде дигиталната икономика с присъщите й характерни черти: нови връзки между икономическите субекти, търговия, маркетинг и законодателни рамки.

Независимо от честите съобщения за хакерски атаки, нанасящи съществени загуби на бизнеса, все повече и повече компании използват Интернет в дейността си и увеличаването на техния брой е неизбежно. Бизнесът, който става все по-глобален и разпределен, се нуждае от единна среда, единно пространство за работа с информацията и засега в това отношение алтернатива на Интернет няма. Глобалната мрежа неизбежно се превърна в среда, предоставяща достъп до корпоративна информация, в това число и до критични за организацията данни. Нарушението на сигурността при обработката и предаването на информацията води до щети, чиито мащаби се определят от предназначението на информацията и могат да имат фатални за организацията последствия. Като основни причини за наличието на уязвимости в съвременните системи могат да бъдат посочени:

- ✓ Отсъствието или недостатъчната ефективност на функциите на защитата в прилаганите технологии за обработка на данните и протоколите за информационен обмен;
- ✓ Наличие на грешки в програмното осигуряване;
- ✓ Нарастващата сложност в управлението на съвременните програмни системи.

2. Тенденции в областта на системите за електронна търговия. В съвременния си вид Интернет предоставя широк набор от предимно независими ресурси, чиято обработка се извършва на базата на разпределените системи. Прилагането на отворени архитектури е критично средство за успеха на даден продукт в сферата на информационните технологии. Те позволяват на производителя да снижи както времето за пускане на продукта на пазара, така и

разходите по създаването му.Тази задача е от особена важност при системите за електронна търговия, които изискват обмен на данни в реално време, сигурност при разплащанията и надеждна връзка на компанията с нейните клиенти и партньори.

Изследвани са технологиите и протоколите, които лежат в основата на функционирането на съвременните системи за електронна търговия, както и техните недостатъци от гледна точка на информационната сигурност:

- ✓ Много от прилаганите технологии и протоколи се появиха сравнително отдавна, когато информационната сигурност не беше приоритетно направление;
- ✓ През последните години се появиха нови технологии и реализирани на тяхна база програмни системи, които повишават ефективността, но намаляват сигурността при обработката и използването на данните (например Web-технологията, както и свързаните с нея технологии за разпределена обработка на базата на мобилни програми, например Java и ActiveX);
- ✓ Съвременните програмни продукти, представляващи достатъчно сложни системи, попадат на пазара с грешки и недостатъци, водещи до случайни или преднамерени нарушения на информационната сигурност.

Задачата на информационната сигурност се свежда до предотвратяване на възможни въздействия с вредителска цел, както и до минимизиране на щетите върху системата, ако неоторизирано проникване стане факт.

В дисертационния труд са анализирани особеностите при проектиране на системи за електронна търговия чрез дефиниране на основните компоненти и характеристики на търговски сайт. Разработен е формален модел на система за електронна търговия, като са разгледани различните видове политики на сигурност и са определени условия, на които трябва да отговаря системата, за да бъде спазена политиката на сигурност. Разгледани са методи за оценка на ценността на информацията в системата за електронна търговия, както и оценка на риска, като е създаден математически метод за оценка ефективността на защитата на системата. Разработена е архитектура на система за електронна търговия, базирана на трикомпонентния модел на технологията клиент/сървер. Разгледано е интегрирането на защитните механизми в архитектурата на системата, като са представени три конфигурации за интегриране на защитните механизми за контрол на достъпа в компонентите на системата. Разработен е симулационен модел за оценка на информационната сигурност на системата спрямо DoS атаки. Изследвана е зависимостта на сигурността на системата за електронна търговия от прилаганите защитни механизми, като за целта е разработен съответен програмен пакет на езика C++.

II. Цели и задачи на дисертацията.

Целта на работата е изследване на проблемите при проектиране на системи за електронна търговия, които отговарят на предварително дефинирани политики на сигурност, както и оценяване на информационната сигурност на такива системи спрямо DoS (Denial of Service) атаки. В съответствие с това са поставени следните основни **задачи**:

1. Анализ на особеностите при проектиране на системи за електронна търговия чрез дефиниране на компоненти, характеристики и изисквания към съответен сайт.
2. Разработване на формален модел на система за електронна търговия, която отговаря на определена политика на сигурност.
3. Създаване на метод за оценка ефективността на защитата на система за електронна търговия.
4. Разработване на архитектура на система за електронна търговия, която отговаря на изискванията на предварително дефинирана политика на сигурност.
5. Разработване на симулационен модел за оценка на информационната сигурност на система за електронна търговия спрямо DoS атаки.

В резултат от изпълнението на поставените задачи става възможно да се създаде архитектура на система за електронна търговия, базирана на компонентния подход, която не е свързана с конкретно приложение, платформа или операционна система. Тя ще позволи на производителите да включват и/или изключват компоненти, при което получената система ще удовлетворява изискванията на определена политика на сигурност по отношение транзакциите между компонентите. Тази архитектура ще стандартизира комуникациите и взаимодействието в 3-компонентния модел на технологията клиент/сървер, ще позволи лесно включване и/или изключване на компоненти от системата, без да се нарушава определената политика на сигурност. Изследването на влиянието на защитните механизми, респективно тяхната цена върху информационната сигурност на системата би позволило на мениджърите на организациите да определят необходимото ниво на защитата на системата съобразно нуждите и особеностите на организацията във функция от финансовите разходи.

III. Съдържание.

Дисертационният труд се състои от увод, четири глави, заключение и три приложения.

Глава 1 – Основни принципи и аспекти на развитие на електронната търговия – има описателно-обзорен и изследователски характер. Разгледани са

основните аспекти и тенденции на развитие на електронната търговия. Нейните основни елементи са илюстрирани на фиг. 1-1:

Фиг.1-1. *Елементи на електронната търговия.*

Разгледан е бизнес-моделът за електронна търговия, като са представени основните характеристики, които трябва да притежава системата за електронна търговия :

- ✓ Online магазин;
- ✓ Система за разплащания;
- ✓ Изпълнение на поръчките;
- ✓ Сервизна поддръжка и работа с клиентите;
- ✓ Маркетингови изследвания и рекламна дейност.

Разгледани са основните сектори на електронната търговия, както и техните важни характеристики:

- ✓ Потребителски електронен пазар (B2C);
- ✓ Междуфирмен електронен пазар (B2B);
- ✓ Вътрешноорганизационен (Интранет) пазар.

Специално внимание е отделено на Web банкирането и особеностите на трите основни типа системи за електронни разплащания:

- ✓ Кредитни карти;
- ✓ Електронни пари;
- ✓ Електронни чекове.

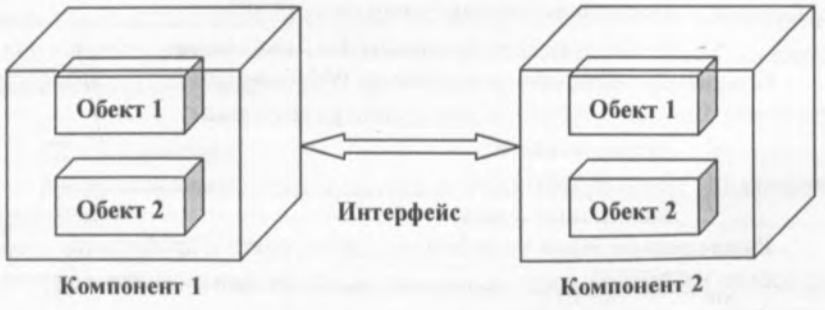
Разгледани са някои въведени стандарти, както и проблемите относно сигурността на предаваните данни при всяка от прилаганите системи за разплащания.

От съществено значение при проектирането на система за електронна търговия са функционалните й характеристики: [8]:

- ✓ Съдържание и услуги в цифров вид;
- ✓ Търговски услуги;
- ✓ Управление на сделките;
- ✓ Разплащателни механизми;
- ✓ Изпълнение на поръчките;
- ✓ Сервиз и поддръжка на клиентите;
- ✓ Отчет и анализ на данните;
- ✓ Мултимедиен потребителски интерфейс;

Разгледани са някои стандарти в системите за електронна търговия, както и методите за проектиране на такива системи. Нарасналата сложност на системите за електронна търговия доведе до необходимостта от въвеждане на нива на проектирането и реализацията им, което наложи прилагането на методите на структурното и обектно-ориентираното програмиране в създаването на софтуерни "черни кутии" като функции, класове и компоненти, чиято реализация е скрита чрез съответен контрол на достъпа до данните и поведението им през интерфейс [14]. На по-ниско ниво на абстракция данните и поведението на модулите се скриват в обекти, докато на по-високо ниво тази функция се изпълнява от компонентите.

Въпреки че достъпът до обектите се контролира от техните интерфейси, възниква проблем при опит за групиране на голям брой обекти в достатъчно сложна система. Прилагането на компонентния подход предоставя добри възможности за контролиране на връзките между компонентите и съответните им услуги в система за електронна търговия. **Компонент** наричаме логически и функционално обособена част на системата, предоставяща дадена услуга на други компоненти и/или потребители. Компонентът представлява черна кутия на ниво функциониране на системата, а обектите, включени в него, са невидими за останалата част на системата, освен за самия компонент (фиг. 1-6).



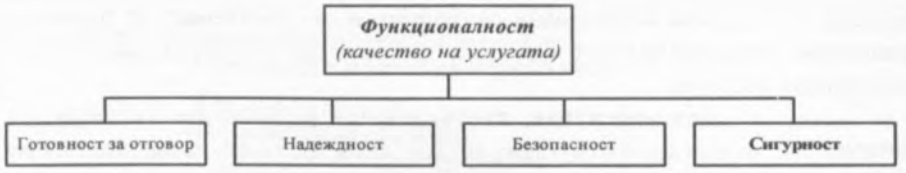
Фиг.1-6. *Взаимодействие между два компонента в системата.*

Системите за електронна търговия, които се основават на компонентния подход, са базирани на различни платформи и са собственост на различни компании, в резултат на което възникват проблеми при обмена на данни между разнородни системи:

- ✓ Компонентите, съставляващи различните системи, са хетерогенни, поради което се нуждаят от технология, чрез която да взаимодействат помежду си;
- ✓ За да бъде извикан даден компонент, извикващият модул трябва да знае точното му местоположение, типа на входните данни и интерфейса му, като тези параметри в общия случай са променливи величини;
- ✓ Сигурността на предаваните и съхраняваните данни е допълнителен проблем за приложенията, тъй като данните преминават през разнородни, в повечето случаи отворени мрежи с ниско ниво на защита на данните.

Следователно възниква необходимост от разработване на архитектура на система за електронна търговия, базирана на компонентния подход, която позволява на производителите лесно да включват и/или изключват компоненти. Освен това получената система трябва да удовлетворява изискванията на предварително дефинирана политика на сигурност при транзакциите между компонентите. За решаване на всички тези проблеми се предлага архитектура на система за електронна търговия, базирана на компоненти, при която механизмите за сигурност са интегрирани в системата. Тези услуги са предназначени за използване от други компоненти и/или потребители чрез предварително съгласуван интерфейс, като достъпът до тях се извършва чрез съответни адреси. По този начин се подобрява взаимодействието между компонентите, тъй като услугите могат да се откриват и използват динамично. Подобна архитектура не изисква непременно наличието на Интернет като среда за пренос и комуникации, тъй като представлява един подход за изграждане на приложения за електронна търговия и многообразието от платформи и услуги в Интернет разкрива най-пълно възможностите му.

Глава 2 – Модел на защита на система за електронна търговия – има описателно-обзорен и научно-изследователски характер. Дефинирано е понятието сигурност като една от присъщите характеристики на системата [16], както е представено на фиг. 2-1:



Фиг.2-1. *Характеристики на система за електронна търговия.*

Представен е формален модел на система за електронна търговия, основан на взаимодействието между обекти и субекти. ***Обект*** наричаме произволно крайно множество от думи на предварително зададен език *E*, т.е. обектът е пасивен компонент на системата, който съдържа информационни или системни ресурси. ***Субект*** наричаме активен компонент на системата, който предизвиква движение на информация между обектите или изменение в състоянието на системата. Разгледано е и множеството *R* от възможни релации на достъп в системата. Целта на защитата на системата може да се формулира по следния начин: във всеки произволно избран дискретен момент *t*, състоянието на системата $G_t \notin \Omega$, където Ω е предварително дефинирано множество от неблагоприятни състояния.

Максималното време, през което една система е изложена на риск при атака, може да се оцени по следния начин:

MT = Pr + Det + Cn, където

Pr - време, необходимо на неоторизираното лице да преодолее защитните механизми на системата (protection);

Det - време, необходимо за откриване на пробива в защитата (detection);

Cn - време за реакция и осуетяване на атаката (counteraction)

За да се минимизират стойностите на Det и Cn във всеки момент от работата на системата, трябва да се определят различните заплахи за сигурността, да се оцени оптималното отношение на сигурност и цена и да се разработи съответна политика на сигурност (ПС), след което тя се използва за определяне на конкретните защитни механизми (фиг. 2-2):

Фиг.2-2. *Роля на политиката на сигурност.*

Класифицирани са основните типове заплахи за сигурността на системите:

- ✓ Случайни заплахи;
- ✓ Умишлени заплахи (атаки):
  - Директни атаки;
  - Индиректни атаки;
  - Пасивни атаки;
  - Активни атаки.

В зависимост от типа на атакувания обект заплахите биват:

- ✓ Заплахи за секретността на информацията;
- ✓ Заплахи за цялостността на информацията.

Разгледани са основните методи за оценка на ценността на информацията в системата, като е обърнато специално внимание на модела MLS (Multi-level Security). Дефинирани са понятията информационен поток и величина на информационния поток като базови за анализа на изтичането на информация и осигуряването на нейната поверителност. Представени са основните типове ПС:

- ✓ Разграничителна ПС;
- ✓ Задължителна ПС.

Като основни представители на задължителната ПС са описани ПС на Бел – Ла Падула [4] и ПС на Биба. След приемането на ПС в системата могат да се определят и внедрят защитните механизми, реализиращи правилата, дефинирани от ПС. Така построената защита е добре проектирана, ако тя надеждно осигурява спазването на правилата, описани в ПС.

Описано е спазването на ПС в система за електронна търговия. Дефиниран е модел на система Σ, която може да бъде описана с думи от краен език E над крайна азбука A. Обект в Σ представлява крайно множество от думи от E, а състоянието му е отделен елемент от това множество. Състоянието на Σ във всеки момент може да бъде представено във вид на множество от състоянията на обектите. Тъй като броят на обектите в системата се променя динамично, разгледано е множеството от обекти на системата Σ в даден дискретен момент t, което е означено с W_t, $|W_t| < \infty$. За всеки дискретен момент t от W_t може да се отдели множество на субектите Z_t, като субект $Z \in Z_t$ представлява описание на определено преобразуване в системата Σ. За реализирането на това преобразуване са необходими определени ресурси (*домен*) и извършване на определено взаимодействие между тях, водещо до преобразуването на информацията, което се нарича *процес*. Тогава всеки субект се намира в две възможни състояния:

- ✓ *неактивирано* – субектът е под формата на описание;
- ✓ *активирано* - субектът е под формата на двойката (домен, процес).

Означено е множеството от всички релации на достъп с R, като $|R|<\infty$. Ако множеството $p \subseteq R$, то с $Z \xrightarrow{p} W$ е означен извършеният достъп на субекта Z до обекта W. Разгледан е специален вид релация на достъп, наречена *активиране*, при което процесът на активизация на субекта Z_2 от субекта Z_1 е означен с $Z_1 \xrightarrow{a} Z_2$; $Z_1, Z_2 \in Z$. Потребителите в системата са означени с $U_1, U_2, ..., U_n$, като в началния момент $t=0$ са активирани само те.

Въведен е ориентиран граф G_t, по следния начин: субектът Z и обектът W са свързани с дъга $Z \rightarrow W$, ако при активиране на субекта Z той има възможност за произволен достъп до обекта W в момента t. Разгледано е множеството $F_t(Z)=\{ W \mid Z \rightarrow^* W$ *в момента* $t \}$, където с $Z \rightarrow^* W$ е означено, че субектът Z има възможността да осъществи достъп до обекта W.

Тогава за всяко $t \in N$ в системата са определени множествата $F_t(U_i)$, $i=\{1, 2, ..., n\}$. Ще означим:

$F=F_t(U_1) \cap F_t(U_2) \cap ... \cap F_t(U_n)$ за всяко t,

$W_t=F_t(U_1) \cup F_t(U_2) \cup ... \cup F_t(U_n)$.

В началния момент $t=0$, $W_0=\{U_1, U_2, ..., U_n\} \cup F$. Наричаме множеството от всички обекти W общи ресурси на системата.

Направени са следните предположения за системата:

Предположение 1. Ако субектът Z е активиран в момента t, то съществува единствен активиран субект $Z' \in G_t$, който е активирал Z. Това означава, че всеки субект може да бъде идентифициран по единствен начин. Предполага се, че всеки обект в системата има уникално име (идентификатор) и в момента $t_0=0$ са активирани само потребителите.

Предположение 2. Функционирането на системата $\sum$ може да се опише чрез последователността от достъпи на множеството на субектите до множеството на обектите във всеки момент $t \in N$.

Предположение 3. Ако $W \in F$, то достъпите от вида $U_i \xrightarrow{p_1} *W, U_j \xrightarrow{p_2} *W$, $i \neq j$ при произволни p_1 и p_2 няма да доведат до канал за изтичане на информация.

ПС в системата. ПС на системата е дефинирана по следния начин: ако субектът Z прави опит за достъп до обекта W, означен с $Z \xrightarrow{p?} W$, то при Z, $W \in W_t(U)$ достъпът $Z \xrightarrow{p} W$ е разрешен, а при $Z \in W_t(U_i)$, $W \in W_t(U_j)$, $i \neq j$, достъпът $Z \xrightarrow{p} W$ не е разрешен.

Разгледана е съвкупност от условия, на които трябва да отговаря една система, за да бъде спазена политиката на сигурност:

Условие 1. (*Идентификация и аутентификация*) Ако за произволни $t \in N$; $p \subseteq R$; Z, $W \in W_t$, $Z \xrightarrow{p?} W$, то се изчисляват функциите на принадлежност на Z и W в множествата $W_t(U_1)$, $W_t(U_2)$, ... $W_t(U_n)$, F.

Условие 2. (*Подсистема, разрешаваща достъпа*) Ако $Z \in W_t(U_i)$, $W \in W_t(U_j)$ и $Z \xrightarrow{p?} W$ в момент t, то от $i=j$ следва $Z \xrightarrow{p} W$, а от $i \neq j$ следва, че достъпът на Z до W не е разрешен.

Условие 3. (*Невъзможност за заобикаляне на ПС*) Ако субектът Z, активиран в момента t, е получил право на достъп до обекта W: за произволни $t \in N$; $p \subseteq R$; то в момента t е извършена заявка за достъп $Z \xrightarrow{p?} W$.

Теорема. Ако в система са изпълнени условията 1-3 и предположенията 1-3, то е изпълнена и политиката на сигурност.

В дисертационния труд са представени основните защитни механизми в системата, класифицирани по следния начин [12]:

- Механизми за идентификация и аутентификация;
- Механизми за контрол на достъпа;
- Механизми за разделяне в системата;
- Механизми при предаване на данни;
- Механизми за откриване на пробиви в защитата и възстановяване на щетите;

След построяване на защитата, която реализира дефинираната политика на сигурност, се налага необходимостта от оценка на защитата. Създаден е метод за оценка ефективността на защитата на система за електронна търговия. За целта са анализирани общите стратегии на неоторизирания достъп до информацията, които включват два основни взаимосвързани етапа [10]:

1. Изследване на защитата на системата;
2. Преодоляване на защитата на системата.

С цел създаване на математически метод за оценка на ефективността на защитата са въведени следните означения:

τ_{cc} - време от момента на преодоляване на защитата от атакуващите програми до момента на приключване на действията им;

τ_{di} - време за откриване и унищожаване на атакуващите програми.

Може да се счита, че защитните механизми са ефективни, ако $\tau_{di} < \tau_{cc}$, т.е. ако величината $\tau = \tau_{di} - \tau_{cc} < 0$. Тъй като величините в този израз са случайни, то изпълнението на това условие е също случайно събитие, което се оценява със съответната вероятност $P(\tau_{di} < \tau_{cc})$, която може да се използва като показател

на ефективността на защитата на системата. Времето τ_{cc} може да бъде представено като сума от времената за реализиране на всеки от двата етапа на неоторизирания достъп до системата: $\tau_{cc} = \tau_1 + \tau_2$. Предполагаме, че случайните величини τ_{di}, τ_1 и τ_2 са независими. При плътности на разпределенията $f_{di}(x)$, $f_1(x)$ и $f_2(x)$ съответно на τ_{di}, τ_1, τ_2 показателят J на ефективността на защитните механизми може да се представи във вида:

$$J = P(\tau < 0) = \int_{-\infty}^{0} f_\tau(x)dx \text{ , където}$$

$$f_\tau(x) = \int_{-\infty}^{+\infty} f_{di}(x-z) f_{cc}(-z)dz$$

Разпределенията на случайните величини τ_{di}, τ_1, τ_2 могат да се подберат въз основа на теоретични или статистически данни. Най-приемливи са разпределения от типа експоненциално, равномерно или бета-разпределение. При подходящо подбрани разпределения и техните параметри от горните зависимости могат да се получат аналитични оценки на ефективността на защитата на системата.

Глава 3 – Модел на архитектура на система за електронна търговия – има научно-изследователски и приложен характер. Разгледано е приложението на Интернет и Интранет технологиите в електронната търговия, като специално място е отделено на VPN (Virtual Private Network) като ключова технология за използването на Интернет като сигурна частна мрежа [5]. Представени са основните приложения на VPN в електронната търговия:

- Отдалечен достъп;
- Връзка между Интранет мрежи;
- Връзка между Екстранет мрежи.

Разгледани са техническите концепции и протоколите, реализиращи VPN технологията на едно от следните нива на мрежовия модел OSI:

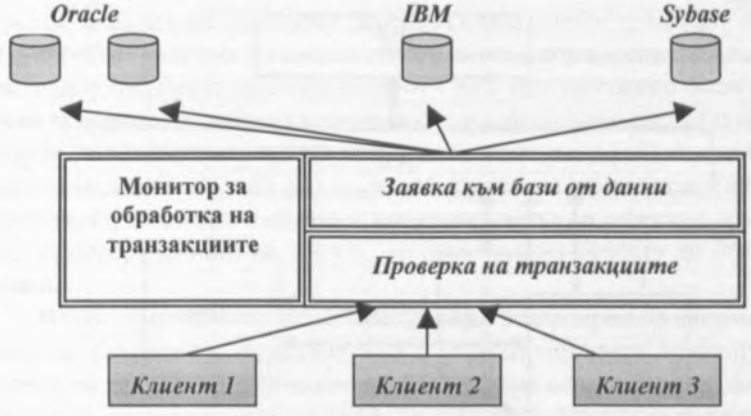
- ✓ Канално (протоколи PPTP, L2F, L2TP);
- ✓ Мрежово (протоколи IPSec, SKIP);
- ✓ Сеансово (протоколи SSL/TLS, SOCKS).

В дисертационния труд е представена обобщена структура на система за електронна търговия, базирана на компоненти. Въведени са следните понятия [2]:

- *е-услуга* - всяко взаимодействие, предоставено на потребителя чрез Интернет, което има самостоятелно обособено значение и икономическа стойност;
- *е-компонент* - модул, предоставящ една или повече е-услуги на други е-компоненти и/или потребители.

По този начин е-услугата, предоставена от даден е-компонент, представлява неговия *интерфейс*. За да предоставя е-услуги, е-компонентът обикновено трябва да комуникира с други е-компоненти. При такова взаимодействие някои е-компоненти могат да делегират изпълнението на е-услугата на други е-компоненти. По този начин един е-компонент може да изпълни ролята на доставчик на услуга (сървер) по отношение на друг, който е клиент или потребител на е-услугата.

Представена е архитектура на система за електронна търговия, базирана на 3-компонентния модел на технологията клиент-сървер (фиг. 3-12). При този модел заявките на клиентите се обслужват от монитор за обработка на транзакциите (transaction processing monitor), свързан с корпоративните сървери за обработка на заявките към базите от данни:



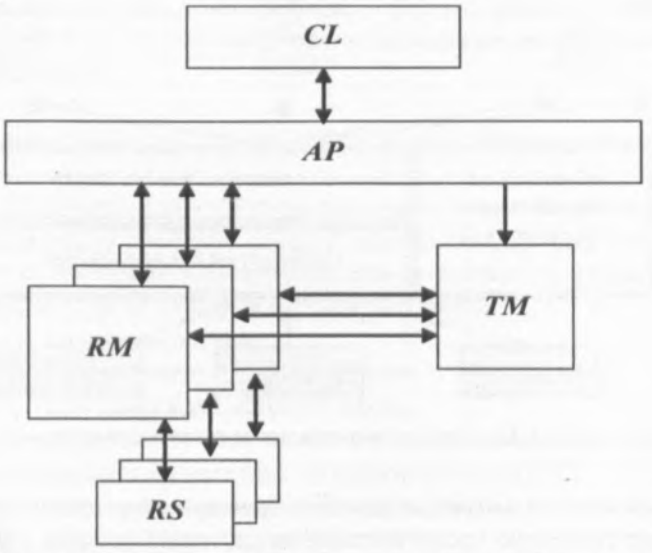
***Фиг.3-12**. Трикомпонентен модел клиент – сървер.*

Този модел позволява на различен брой приложни клиентски програми да използват съвместно предоставените от системата ресурси. При заявка за достъп от клиент, системата извършва проверка на легитимността на заявката, след което тя преминава през монитор за обработка на транзакциите, който я преобразува в съответен брой заявки до базите от данни. След изпълнение на заявките, получените данни се преобразуват във вид, удовлетворяващ първоначалната заявка и се връщат по обратния път до клиента, с което транзакцията се финализира.

Формално този модел може да се представи чрез следните 5 типа компоненти на системата за електронна търговия (фиг. 3-13):

- ✓ приложни програми (AP);
- ✓ мениджъри на ресурси (RM), например бази от данни, файлова система, сървер за поща и др.;
- ✓ мениджъри на транзакции (TM);
- ✓ ресурси (RS);
- ✓ клиенти (CL).

Комуникация между компонентите, при която се обменят данни и се променя състоянието на един или повече обекти в системата, се нарича *транзакция.* Транзакциите могат да включват няколко операции върху обекти, както и да се изпълняват конкурентно. Една транзакция се нарича *атомарна*, ако след приключването й действието е или изцяло изпълнено, или изцяло отменено, т.е. не може да бъде разделена на части, които могат да се изпълнят поотделно. Всеки компонент съдържа един или повече субекти, т.е. активни елементи на системата, предизвикващи движение на информация между обектите или изменение в състоянието на системата, например потребител, процес или устройство.



Фиг.3-13. *Модел на архитектура на система за електронна търговия.*

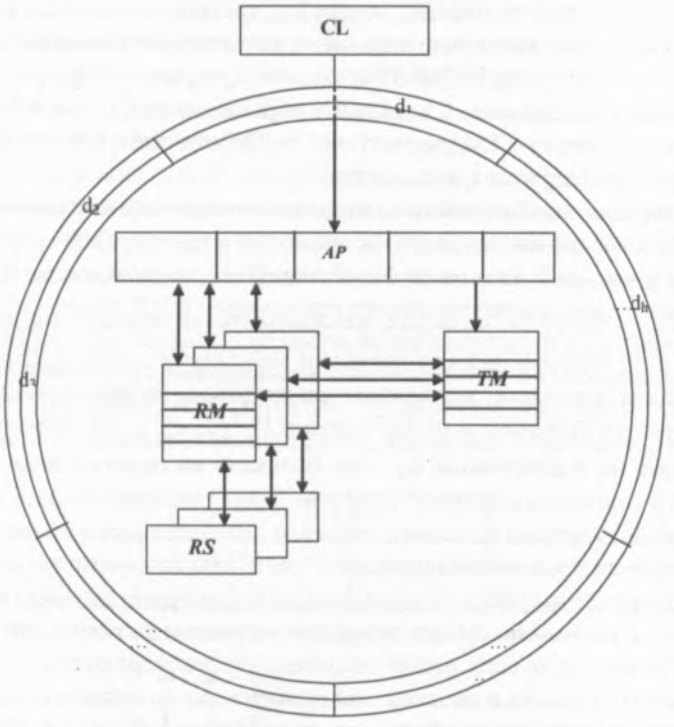
Системата функционира по следния начин (фиг. 3-13): транзакцията се инициира от клиента CL, който изпраща заявка до приложната програма AP. AP се обръща към TM за инициализиране на транзакция; TM установява

транзакцията, като връща информация на AP и установява контакт с RM (един или повече), като преобразува заявката на приложната програма AP до една или повече заявки за достъп до съответни ресурси; AP установява контакт с RM, който изпраща заявка до съответния ресурс RS, достъпът до който се управлява от него. След като тази заявка бъде изпълнена, резултатът се връща на RM, който от своя страна я препраща на AP. Приложната програма връща резултата на клиента, заявил транзакцията. Следващите обръщения на CL към AP, който от своя страна се обръща към TM (респективно от TM към RM и RM към RS) могат да продължат или прекратят транзакцията.

Разгледано е внедряването на защитните механизми в архитектурата на системата. Означаваме множеството на защитните механизми с $D=\{d_1, d_2, ..., d_g\}$, съдържащо g на брой елемента. Разделяме D на подмножества D_1 и D_2, $D = D_1 \bigcup D_2$, където D_1 съдържа механизмите за контрол на достъпа в системата, а D_2 съдържа всички останали механизми – за идентификация, аутентификация, разделяне, механизми при предаване на данни, механизми за неутрализиране на DoS атаки и др. Ще означим $D_2=\{d_1, d_2, ..., d_h\}$, където h е броят на елементите на множеството D_2. Ако оценките на ценността на обектите (ресурсите) в системата образуват наредена скала, заемаща числата от 1 до 5, като по-високият клас има по-висока степен на поверителност и с всеки субект е свързан приоритет, представляващ число от 1 до 5, като по-голямо число означава по-висок приоритет за субекта в системата, то дефинираме следната *политика на сигурност* в системата: субект има право на достъп до обект, ако неговият приоритет е по-висок или равен на оценката на ценността (нивото на поверителност) на обекта и обратно: ако приоритетът на субекта е по-нисък от нивото на поверителност на обекта, то достъпът на субекта до обекта не е разрешен.

Всеки от компонентите AP, RM и TM е реализиран по следния начин: функциите, свързани с определянето и управлението на приоритетите в системата, са логически и функционално отделени едни от други (фиг. 3-14). Защитните механизми от множеството D_2 могат схематично да се представят в кръгова структура, организирана в l на брой защитни слоеве, в която всеки механизъм от множеството D_2 заема по един или повече сектора от даден слой. На фиг. 3-14 е представен схематично случаят при $l=2$, т.е. защитните механизми са разположени в два защитни слоя, като всеки достъп до системата трябва да мине през кръга на защитата. Всеки от механизмите проверява заявката, постъпваща от даден клиент и я пропуска ако тя отговаря на изискванията, дефинирани в политиката на сигурност или я отхвърля като нелегитимна в противен случай. За простота считаме, че входът в системата става само през определен сектор и за определеност нека това е секторът d_1, съответстващ на

защитния механизъм d_1.



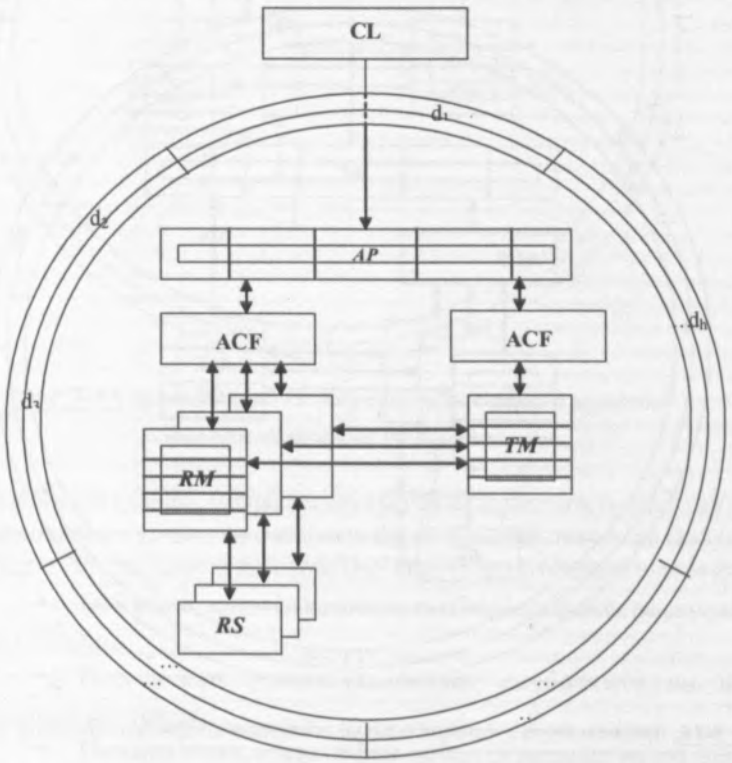
***Фиг.3-14**. Защитни механизми в архитектурата на система за електронна търговия.*

Тази архитектура функционира по следния начин: при постъпване на заявка от клиент към системата, тя преминава през входната точка на системата d_1, където заявката до системата бива приета или отхвърлена например чрез проверка на потребителско име и парола. Ако заявката е легитимна, тя се изпраща до приложната програма AP, като получава съответен приоритет, равен на приоритета на потребителя или субекта, инициирал заявката. AP се обръща към TM за инициализиране на транзакция, след което TM установява транзакцията, като връща обратна информация на AP и установява контакт с един или повече RM, като им изпраща заявка за достъп до съответните ресурси RS, достъпът до които се управлява от тях. RM изпращат заявка до съответните ресурси и след

като тя бъде изпълнена, резултатът се връща на RM. От своя страна той я изпраща на AP, която връща резултата на клиента, инициирал транзакцията.

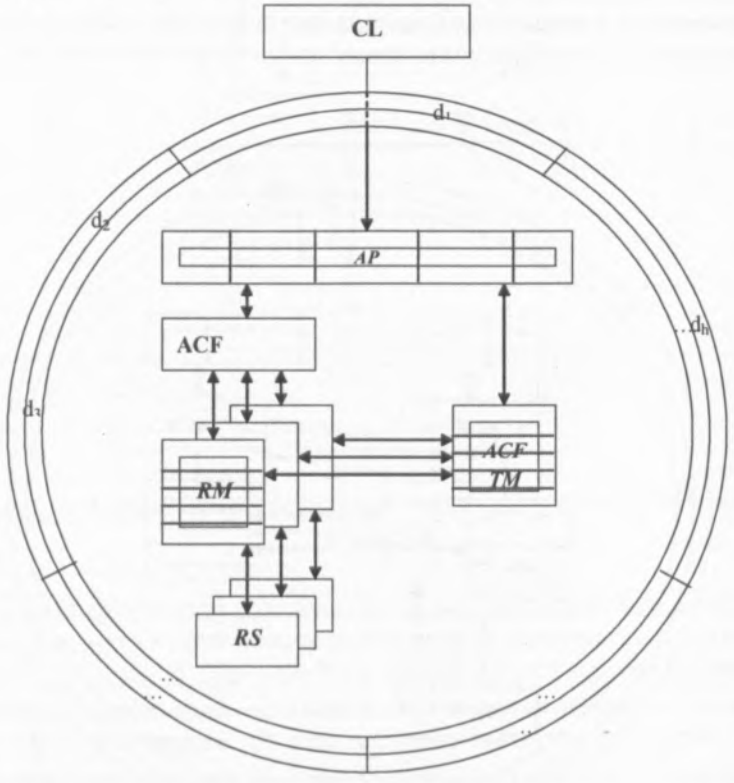
Разгледани са следните конфигурации за интегриране на защитните механизми за контрол на достъпа в компонентите на системата:

1. Архитектура с контролиращи обвивки и невградени филтри за достъп - към всеки компонент е добавена обвивка, реализираща контрола на достъпа между компонентите. Освен това между AP и TM се добавя модул, наречен филтър за контрол на достъпа (ACF), който освен контрол на достъпа на транзакциите между двата компонента извършва оценка на приоритета на заявката и ако е необходимо, повишава или понижава този приоритет. Аналогичен ACF се добавя за контрол на комуникациите между компонентите AP и RM (фиг. 3-15).



Фиг. 3-15. *Архитектура с контролиращи обвивки и невградени филтри за достъп.*

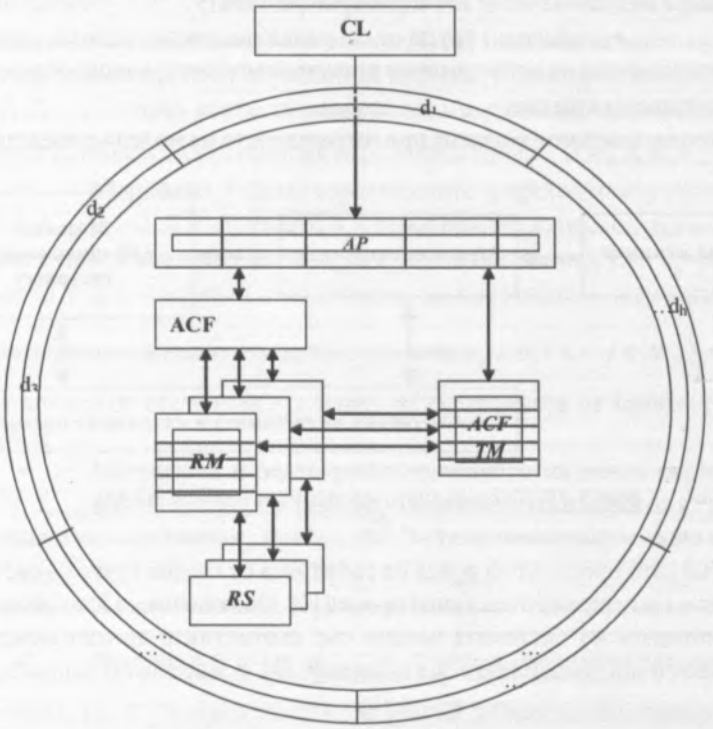
2. Архитектура с контролиращи обвивки и частично вградени филтри за достъп - ACF филтърът от предходната архитектура, който оценява приоритета на заявките между AP и TM, е включен към TM (на фиг. 3-16 е означен като ACF TM), т.е. в самия TM е добавен ACF модул, който оценява приоритета на заявката и ако е необходимо, повишава или понижава този приоритет. Освен това аналогично на предходната архитектура към всеки компонент е добавена обвивка, реализираща контрола на достъпа между компонентите. Контрол на приоритетите на заявките между AP и RM се извършва както при предходната архитектура от ACF филтър (фиг. 3-16).



Фиг. 3-16. *Архитектура с контролиращи обвивки и невградени филтри за достъп.*

3. Архитектура с контролиращи обвивки и вградени филтри за достъп - в този случай и двата ACF филтъра от първата архитектура, контролиращи

приоритета на заявките, са включени като модули съответно към компонентите TM и RM (на фиг. 3-17 означени като ACF TM и ACF RM).



Фиг. 3-17. *Архитектура с контролиращи обвивки и вградени филтри за контрол на достъпа.*

Разработен е модел, оценяващ влиянието на защитните механизми върху информационната сигурност на системата спрямо въздействието на DoS (denial of service) атаки. Разгледани са типовете DoS атаки в електронната търговия [15]:

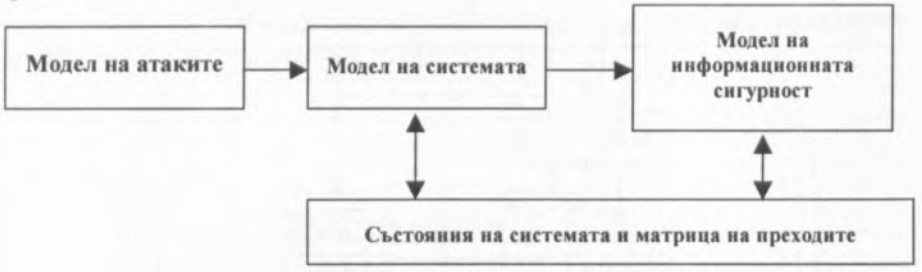
- DoS атаки, които са насочени към недостатъците на определени софтуерни системи;
- DoS атаки, които използват слабостите на някои комуникационни протоколи;
- Flooding атаки, които от своя страна се разделят на два подтипа:
  - Разпределени (distributed DoS, DDos) DoS атаки;
  - Разпределени отразяващи (distributed reflective DoS, DRDos) DoS атаки.

При дефинирането на модела са използвани следните термини,

дефинирани от [11]:

- *атака* – серия от умишлени действия, извършени от атакуващия, с цел да постигне неоторизиран резултат;
- *събитие* – група от свързани помежду си атаки, която може да бъде разграничена от останалите по атакуващи субекти, видове атаки, обекти, време и сайтове на атаките.

Прилаганата методология при изграждането на модела е представена на фиг. 3-18:



***Фиг.3-18**. Компоненти на симулационния модел.*

Тъй като процесът на поява на събитията от гледна точка на системата е случаен, то е симулиран стохастичен процес [1]. Обединението K от множеството C от компоненти на системата заедно със съответните връзки между тях и множеството на защитните механизми D, е наречено множество от конфигурациите на системата: $K=C \bigcup D$.

Разглеждаме $S=(s_1, s_2, ..., s_N)$ – множество от състояния на системата, включващо N елемента, които могат да бъдат дефинирани например по следния начин при N=5: {s_1 – системата функционира нормално, s_2 - системата работи със 75% от функциите си, s_3 - системата работи с 50% от функциите си, s_4 – системата работи с 25% от функциите си, s_5 – системата не функционира}. Означаваме $V=(v_1, v_2, ..., v_M)$ - множество от типове събития, състоящо се от M елемента, които могат да бъдат дефинирани например по следния начин при M=5: {v_1 е тип събитие, след което системата функционира нормално, v_2 е тип събитие, след което системата работи със 75% от функциите си, v_3 е тип събитие, след което системата работи с 50% от функциите си, v_4 е тип събитие, след което системата работи с 25% от функциите си, v_5 е тип събитие, след което системата не функционира}. Означаваме $Cost(D)=\sum_{i=1}^{g} cost(d_i)$ - цена на защитата на системата, представена във валутни единици и принадлежаща на множеството [1, 100], където $cost(d_i)$, $i=1, ..., g$ – цена на защитния механизъм d_i.

За описание на събитията използваме стохастичен процес, при който някои от събитията, принадлежащи на множеството V се случват в дискретните моменти от време $t=1, 2, .., T$. Всяко събитие O_t $i=1, ..., T$ е елемент на множеството V от типове събития, катоозначаваме с $k(t) \in [1, M]$ индекса, за който $O_t=v_{k(t)}$.

Разглеждаме процеса на работа на системата в дискретните моменти от време $t=1, 2, .. , T$, през които тя минава през състояния, принадлежащи на множеството S. Модел на системата е наредената тройка $\theta=(A,B,\pi)$, където:

- ✓ Матрицата A задава вероятностите за преход между състоянията: $A=\{a_{ij}\}$; $i=1, 2,...,N$; $j=1, 2,..., N$, където a_{ij} е вероятността за преход от състояние s_i в състояние s_j при условие, че събитието $v_k \in V$ е постоянно, т.е.: $a_{ij}=p(q_{t+1}=s_j \mid q_t=s_i)$, където с q_t е означено състоянието на системата в момента t. Тези вероятности удовлетворяват следните условия: $a_{ij} \geq 0, 1 \leq i, j \leq N$, $\sum_{i=1}^{N} a_{ij}=1$, т.е. системата попада от състояние s_i в някое от състоянията от множеството S с вероятност 1;
- ✓ Матрицата B задаваразпределението на всяко състояние s_j: $B=\{b_{jk}\}$;$j=1, 2,...,N$; $k=1, 2,..., M$, т.е. всяко b_{jk} е вероятността за преход в състояние s_j при случване на събитието v_k, $(k=1, ..., M)$. За тези вероятности също са в сила следните условия: $b_{jk} \geq 0, 1 \leq j \leq N, 1 \leq k \leq M$; $\sum_{k=1}^{M} b_{jk}=1$;
- ✓ Векторът $\pi=(\pi_1, \pi_2, ..., \pi_N)$ задава началното разпределение на състоянията, т.е. π_i е вероятността системата да бъде в състояние s_i, $i=1, ...,N$ в началния момент $t=1$.

Разглеждаме процеса на работа на системата като скрит Марковски процес [13] от първи ред, зададен чрез модела θ. При така дефинираните условия търсим модел $\theta_{st}=(A_{st}, B_{st}, \pi_{st})$ такъв, че вероятността $P(O \mid \theta)$ да е максимална, т.е. при какви параметри на модела θ е най-вероятно да се случи разглежданата последователност от събития. За решаването на така дефинираната задача е използван алгоритъмът на Baum-Welch (forward-backward algorithm) [3].

Използвана е теорема ЕМ [9] (Expectation - Maximization), която гласи:

Теорема ЕМ. Нека X и Y са случайни величини с разпределения съответно $P(X)$ и $P(Y)$ при условията на модел θ, а $P'(X)$ и $P'(Y)$ са техните разпределения при модел $\theta' \neq \theta$. Тогава ако е изпълнено неравенството

$$\sum_X P(X \mid Y) \log \frac{P'(X,Y)}{P(X,Y)} > 0 \text{, то } P'(Y) > P(Y).$$

В нашия случай разглежданият параметър на модела е случайната

величина X= f(A,B,π), където $x_{ijk} = f(A,B,\pi)$ е преходът от състояние s_i в състояние s_j при събитие v_k и $p_{ijk} = P(x_{ijk})$. На всяка итерация новият модел θ' се образува от множеството от всички $p'_{ijk} = \frac{\sum_{t=1}^{T} \alpha_t(i) a_{ij} b_j(v_k) \beta_{t+1}(j)}{K_i}$, където

$$\alpha_{t+1}(j) = \sum_{i=1}^{N} \alpha_t(i) a_{ij} b_{jk(t+1)} \; ; \beta_{t-1}(i) = \sum_{j=1}^{N} a_{ij} b_{jk(t)} \beta_t(j) \; ;$$

K_i - нормиращи константи

На всяка стъпка получаваме модел θ' такъв, че $P(O|\theta') > P(O|\theta)$. Критерий за край на алгоритъма е $P(O|\theta') = P(O|\theta)$, т.е. търсеният модел $\theta' = \theta$.

Информационната сигурност на системата е най-важната характеристика, която изследваме с настоящия модел, поради което се налага да въведем количествен измерител за това свойство на системата. Оценката на сигурността на системата спрямо DoS атаки се свежда до оценка на производителността й след атаката спрямо производителността й в нормално състояние. Оценката се базира на степента, в която всеки компонент е запазил функционалността си в новото състояние на системата след атаката.

Нека означим с $\varphi(s,k)$ степента, в която компонентът $k \in C$ е запазил функционалността си в състоянието $s \in S$, а с $w(k)$ – тегло (важност) на съответната услуга за системата. Тогава оценката на сигурността на системата може да се представи по следния начин:

$$Sec(s) = \sum_{k=1}^{c} w(k) \varphi(s,k)$$

Този подход за оценка на сигурността на системата представлява анализ по много критерии. Всяка организация може да изработи скала за оценка на услугите си – например те могат да бъдат избрани така, че $0 \le w(k) \le 1$ и $\sum_k w(k) = 1$. Аналогично оценките $\varphi(s,k)$ могат да бъдат нормирани така, че $0 \le \varphi(s,k) \le 1$. Тогава и оценката $Sec(s)$ ще бъде число от 0 до 1, като 0 показва напълно нефункциониращa, а 1 – напълно функциониращa система.

В **Глава 4** - Симулационни експерименти и анализ на резултатите - са представени резултатите от извършените експерименти върху дефинираните в точка 3.5.3 три типа архитектури на система за електронна търговия. За целта е разработен програмен пакет на езика C++, пълният код на който е представен в Приложение 1 на дисертацията. Изборът на данните за събитията е направен въз основа на:

- Аналитичен обзор на литературни източници [6], [7];
- Аналитичен обзор на web ресурси [1];
- Анализ на експерименталните резултати и съответна обратна връзка.

Данните за модела $\theta=(A, B, \pi)$ са генерирани чрез последователно обхождане на възможните стойности, тъй като получената оценка за сигурността е валидна за произволна система. Направеното позволява изследване на реална система, за която A, B и π могат да се оценят по емпиричен начин.

Начални данни на симулациите са последователността от събития $O=(O_1, O_2, \ldots O_T)$ и началният модел $\theta=(A, B, \pi)$. Следователно входни параметри на модела са: N – брой състояния на системата; M - брой събития; A - матрица с размерност $N \times N$, където $a_{ij} \in [0, 1]$; B – матрица с размерност $N \times M$, където $b_{ij} \in [0, 1]$; π - вектор от N елемента, където $\pi_i \in [0, 1]$; V – вектор от M различни елемента; T – брой моменти; O – вектор от T елемента, където $O_i \in V$, $i=1, \ldots T$. За така дефинираните параметри са разгледани следните интервали на изменение: $N \in [2, 5]$, фиксирана стойност $N=3$; $M \in [2, 8]$, фиксирана стойност $M=5$; $T \in [1, 100]$, фиксирана стойност $T=40$. За елементите на матрицата A a_{ij} и вектора π бяха разгледани стойностите от интервала [0, 1] със стъпка на изменение 0.1, като се вземе предвид, че $\sum_{j=1}^{N} a_{ij} = 1, \forall i$ и $\sum_{i=1}^{N} \pi_i = 1$, при което извършените експерименти за елементите на A са 287496, а на π - 66; аналогично за елементите на матрицата B бяха разгледани стойностите от интервала [0, 1] със стъпка на изменение 0.2, като се вземе предвид, че $\sum_{k=1}^{M} b_{jk} = 1, \forall j$, при което броят на извършените експерименти е 126. Тъй като нашата цел е да оценим сигурността на системата след приключване на събитията, то е разгледано състоянието на системата само в момента T. Тогава броят на експериментите е от порядъка на

[1] http://www.cs.unm.edu/~immsec/systemcalls.htm

3200000 при фиксираните стойности на параметрите.

Извършено е планиране на експериментите за всяка от описаните три варианта на архитектура на система за електронна търговия. С цел опростяване изчислителната сложност на алгоритъма разглежданията върху конфигурациите на системата са ограничени върху фиксирано множество C от компонентите на системата и е разгледано влиянието на множеството на защитните механизми D, респективно цената им $Cost(D)$. Чрез изменяне на множеството D от защитни механизми, т.е. модела на системата $\theta=(A, B, \pi)$ и вектора от събитията O, е определено състоянието, в което изпада системата след събитията и е изследвана зависимостта на сигурността Sec на системата от $Cost(D)$. Параметър на защитата на системата е и броят l на слоевете на защитата, като от практически съображения са разгледани стойности на $l \in [1, 4]$.

Без ограничение на общността на експериментите комбинациите за елементите на вектора O са групирани в зависимост от сериозността на събитията, т.е. от броя срещания на всеки елемент v_i на вектора V във вектора O. Дефинирани са следните параметри на симулациите: с L_i е означена степента, с която събитието v_i намалява производителността на системата, т.е. при фиксираните стойности на вектора V, $L_1=0$ (напълно функционираща система), L_2=0.25 (системата функционира със 75% от функциите си), ..., L_M=1 (нефункционираща система).

Тогава пресмятаме величината $L = \frac{\sum_{i=1}^{T} L_i}{T}$ ($L \in [0, 1]$), която е ефективна състоятелна оценка за математическото очакване на величините $L_1, L_2, \ldots, L_M$. Параметърът L е характеристика на вектора от събития O и е изследвана зависимостта на Sec от стойностите на параметъра L. Стойностите на параметъра L са закръглени с точност 0.05, поради което са разгледани 21 стойности на L. На базата на получените зависимости са направени обобщения по отношение на архитектура, брой защитни слоеве l и цена $Cost(D)$ (фиг. 4-1 – 4-36).

Планираните експерименти са обобщени и групирани както е показано в таблица 4-1 в дисертацията. Проиграването на симулациите е извършено с помощта на представения програмен пакет, а събирането на резултатите е извършено в графичен (Приложение 2, фиг. 4-1 - 4-36, в автореферата само фиг. 4-1 - 4-3 и П2-75 - П2-82) и табличен вид (Приложение 3, в автореферата само табл. П3-75 - П3-82).

Обобщение на резултатите и препоръки. За краткост разгледаните архитектури са означени съответно с А1, А2 и А3 по реда на описанието им в точка 3.5.3.

1. Сравняване на резултатите в зависимост от броя на защитните слоеве на разгледаните архитектури.

✓ **l=1**. От фиг. 4-1 – 4-3, 4-13 – 4-15, 4-25 – 4-27, фиг. П2-1 – П2-20, П2-75– П2-94, П2-149 – П2-166 и таблици П3-1 – П3-20, П3-75 – П3-94, П3-149 – П3-166 се вижда, че увеличаването на L води до намаляване на *Sec* с достигане на минимум при L=1 (архитектура А1, таблица П3-8, фиг. П2-8). Намаляването на *Sec* е най-слабо при А3, откъдето може да се направи изводът, че архитектурата А3 е препоръчителна при l=1.

✓ **l=2**. От фиг. 4-4 – 4-6, 4-16 – 4-18, 4-28 – 4-30, П2-21 – П2-40, П2-95 – П2-114, П2-167 – П2-184 и таблици П3-21 – П3-40, П3-95 – П3-144, П3-167 – П3-184 се вижда, че увеличаването на L води до намаляване на *Sec* с достигане на минимум при L=1, (архитектура А1, таблица П3-28, фиг. П2-28). В разглеждания случай архитектурата А1 показва най-ниски стойности на *Sec*, откъдето може да се направи изводът, че тя не е препоръчителна при l=2. За стойности на $L\in$[0.00, 0.50] при А2 и А3 поведението на *Sec* е сходно, откъдето може да се предположи, че двете архитектури имат сходно поведение при ниски стойности на L. При $L\in$[0.50, 1.00] намаляването на *Sec* при А3 е по-слабо, следователно А3 е препоръчителна при високи стойности на L.

✓ **l=3**. От фиг. 4-7 – 4-9, 4-19 – 4-21, 4-31 – 4-33, П2-41 – П2-58, П2-115 – П2-132, П2-185 – П2-198 и таблици П3-41 – П3-58, П3-115 – П3-132, П3-185 – П3-198 се вижда, че увеличаването на L води до намаляване на *Sec* с достигане на минимум при L=0.90, (архитектура А1, таблица П3-46, фиг. П2-46). В разглеждания случай архитектурата А1 показва най-ниски стойности на *Sec*, откъдето може да се направи изводът, че тя не е препоръчителна при l=3. За стойности на $L\in$[0.00, 0.50] при А2 и А3 поведението на *Sec* е сходно, откъдето може да се предположи, че двете архитектури имат сходно поведение при ниски стойности на L, като по-високи стойности на *Sec* се наблюдават при А2. При $L\in$[0.50, 1.00] намаляването на *Sec* при А2 е по-слабо, следователно А2 е препоръчителна при високи стойности на L.

✓ **l=4**. От фиг. 4-10 – 4-12, 4-22 – 4-24, 4-34 – 4-36, П2-59 – П2-74, П2-133 – П2-148, П2-199 – П2-210 и таблици П3-59 – П3-74, П3-133 – П3-148, П3-199 – П3-210 се вижда, че увеличаването на L води до намаляване на *Sec* с достигане на минимум при L=0.75, (архитектура А1, таблица П3-64, фиг. П2-64). В разглеждания случай симулационните стойности на *Sec* за $L\in$[0.00, 0.50] са следните: за А1 $Sec\in$[0.47, 1.00], за А2 $Sec\in$[0.53, 1.00] и за А3 $Sec\in$[0.60, 1.00], откъдето може да се направи изводът, че А3 е препоръчителна при ниски стойности на L. Симулационните стойности на *Sec* за $L\in$[0.50, 1.00] са: за А1 $Sec\in$[0.28, 0.80], за А2 $Sec\in$[0.48, 0.83] и за А3 $Sec\in$[0.59, 0.83], откъдето може да се направи изводът, че при четири защитни слоя А2 и А3 имат еднаква горна

граница на изменението на *Sec*, като при А3 се наблюдават по-високи стойности на *Sec*, откъдето следва, че тя е препоръчителна в този случай.

2. Сравняване на резултатите за разгледаните архитектури.
От извършените симулационни изследвания можем да обобщим следните резултати за всяка от разгледаните архитектури при всяка от разгледаните стойности на *l*:

- ✓ **Архитектура 1** – от фиг. П2-1 – П2-74, таблици П3-1 – П3-74 и фиг. 4-1 – 4-12 се вижда, че стойностите на *Sec* се увеличават с увеличаването на $l \in [1, 4]$, $Cost(D) \in [5, 86]$, $L \in [0.00, 1.00]$, като достигат максимум при $l=4$: $Sec \in [0.36, 1.00]$ при $Cost(D) \in [77, 86]$.
- ✓ **Архитектура 2** – от фиг. П2-75 – П2-148, таблици П3-75 – П3-148 и фиг. 4-13 – 4-24 се вижда, че стойностите на *Sec* се увеличават с увеличаването на $l \in [1, 4]$, $Cost(D) \in [20, 83]$, $L \in [0.00, 0.90]$, като достигат максимум при $l=4$: $Sec \in [0.55, 1.00]$ при $Cost(D) \in [75, 83]$.
- ✓ **Архитектура 3** – от фиг. П2-149 – П2-210, таблици П3-149 – П3-210 и фиг. 4-25 – 4-36 се вижда, че стойностите на *Sec* се увеличават с увеличаването на $l \in [1, 4]$, $Cost(D) \in [28, 98]$, $L \in [0.00, 0.85]$, като достигат максимум при $l=4$: $Sec \in [0.64, 1.00]$ при $Cost(D) \in [91, 98]$.

От представените резултати се вижда, че стойностите на *Sec* нарастват с нарастването на *Cost(D)*, като най-високи стойности се наблюдават при А3, $l=4$.

3. Препоръки.

1. Получените резултати за *Sec*, *Cost(D)*, *L* и *l* за трите архитектури могат да се използват при практическата реализация на система за електронна търговия за определяне на броя, размера и секционирането на буферните области в оперативната памет и в другите критични ресурси.

2. Сравнението между трите типа архитектури показва предимството по отношение на *Sec* на А3, балансираната стойност по отношение на *Sec* на А2 и критичната минимална стойност, под която стойността на *Sec* не трябва да достига.

3. Слабата чувствителност на *Sec* по отношение на броя защитни слоеве при стойности близки до максималния изследван брой показва, че не са необходими изследвания при по-голям брой защитни слоеве.

IV. Заключение.

В дисертацията са разгледани актуални въпроси, свързани с информационната сигурност и моделирането на системите за електронна търговия. Разработена е архитектура на система за електронна търговия, състояща се от 5 типа компоненти, като е предложена кръгова структура на защитата на

системата и са разгледани 3 типа архитектури, представляващи варианти на внедряването на защитните механизми в системата. На базата на разработената архитектура са извършени експериментални симулационни изследвания за влиянието на DoS атаки върху системата, както и оценка на информационната сигурност на системата след въздействието на последователност от събития. Направен е анализ на получените резултати и са дадени препоръки за избор на типа архитектура и защитни механизми при конфигуриране на конкретна система Поставените в увода проблеми са решени, в резултат на което са постигнати следните научно-приложни **приноси**:

1. Анализирани са основните характеристики и компоненти на система за електронна търговия, както и изискванията за сигурност в Интернет среда, чрез което е мотивирана необходимостта от изграждане на системи за електронна търговия, отговарящи на предварително дефинирани условия за сигурност.

2. Разработен е формален модел на система за електронна търговия, отговаряща на определена политика на сигурност. Определени са условия, на които трябва да отговаря системата, за да бъде спазена политиката на сигурност.

3. Създаден е метод за оценка ефективността на защитата на система за електронна търговия, като са изследвани стратегиите, прилагани от атакуващите програми.

4. Разработена е архитектура на система за електронна търговия на базата на компонентния подход, която отговаря на изискванията на предварително дефинирана политика на сигурност.

5. Разработен е симулационен модел за оценка на информационната сигурност на система за електронна търговия спрямо DoS атаки в зависимост от защитните механизми на системата, като за целта е съставен програмен пакет и са извършени симулационни изследвания.

Направените изследвания разкриват важността на поставените и решени проблеми, тяхната актуалност и значимост за усъвършенстване технологията за създаване на системи за електронна търговия в Интернет среда. Те могат да бъдат прилагани при проектиране на подобни системи в други предметни области, както и при разработване на конкретни приложения.

Използвана литература:

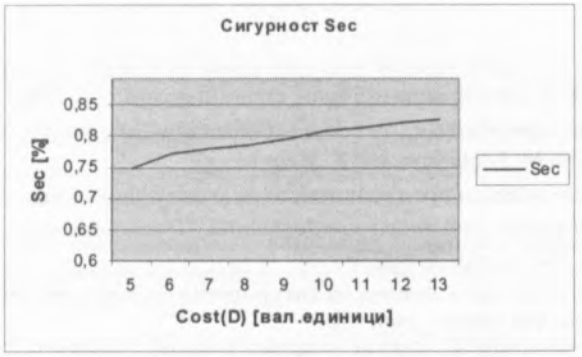
1. Обретенов А., Теория на вероятностите, *Наука и Изкуство*, София, 1974, 226-233.
2. Arbab F., Abstract Behavior Types: a foundation model for components and their composition, *Science of Computer Programming*, Vol.55, 1-3/2005, ISSN 0167-6423, 3-52.
3. Baum L.E., "An inequality and associated maximization technique in statistical estimation for probabilistic functions of a Markov process", *Inequalities*, 3, pp. 1-8, 1972.
4. Bell D, LaPadula L: Secure Computer Systems: Mathematical Foundations and Model, *MITRE ReportMTR 2547*, 1973.
5. Bollapragada V., Khalid M., Wainner S., IPSec VPN Design, *Cisco Press*, 2005, ISBN 1587051117, 256-263.
6. Forrest S., S.A. Hofmeyr, A. Somayaji, T.A. Longtaff, A Sense of Self for Unix Processes, *In Proceedings of the 1996 IEEE Symposium on Security and Privacy, IEEE Computer Society Press*, Los Alamitors, CA, pp.120-128.
7. Forrest S., S.A. Hofmeyr, A. Somayaji, Intrusion detection using sequencies of system calls, *Journal of Computer Security*, Vol. 6, 1998, pp. 151-180.
8. Gerber M.E., E-Myth Mastery: The Seven Essential Disciplines for Building a World-Class Company, *HarperCollins Publishers*, 2004, ISBN 0060723181, 315-319.
9. Dempster A.P., Laird N.M., Rubin D.B., Maximum Likelihood from Incomplete Data via the EM Algorithm, Journal of the Royal Statistical Society, Ser. B, 39: 1-38, ISSN: 09641998, 1977.
10. Heiser J.G., Understanding today's malware, *Information Security Technical Report*, Vol.9, 2/2004, ISSN 1363-4127, 47-64.
11. Howard, J. An Analysis of Security Incidents on the Internet (1989-1995), Ph.D. Dissertation, Carnegie -Mellon University, Pittsburgh. PA, 1995.
12. Northcutt S., Zeltser L., Kent K., Ritchey R., Winters S., Inside Network Perimeter Security, *Sams*, 2005, ISBN: 0672327376, 587-597.
13. Rabiner L.R., "A tutorial on Hidden Markov Models and selected applications in speech recognition", *Proc. IEEE*, 257-286, 77, 2, Feb 1989.
14. Rajsbaum S., Viso E., Object-oriented algorithm analysis and design with Java, *Science of Computer Programming*, Vol.54, 1/2005, ISSN 0167-6423, 25-47.
15. Siaterlis C., Maglaris B.S., Towards multisensor data fusion for DoS detection, *Proceedings of the 2004 ACM Symposium on Applied Computing (SAC)*, Nicosia, Cyprus, March 14-17, 2004. ACM 2004, ISBN 1-58113-812-1, 439-446.
16. Solomon M.G., Chapple M., Information Security Illuminated, *Jones & Bartlett Publishers, Inc.*, 2004, ISBN 076372677X, 226-234.

Публикации във връзка с дисертацията

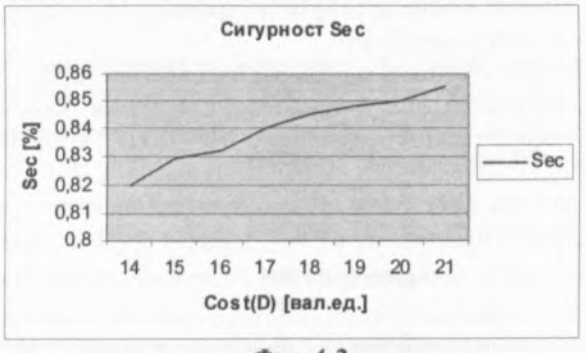
1. Stoyanova V., Risk in remote controlling of computers and networks, *INFSEC - 21st century: Global Convergence, Swedish - Bulgarian Conference*, 18-24 Sep 1999, pp.159-174. (with M. Nickolova and K. Rogalska).
2. Стоянова В., Някои аспекти пред развитието на междуфирмената електронна търговия, *Втора българо-египетска конференция "Икономиките в преход"*, Свищов, 29.05-02.06.2000 г., стр. 222-227.
3. Жечева В., Формален модел и оценка на сигурността на софтуерните системи, *Годишник на БСУ*, том VII, 2002 г., 192-196.
4. Жечева В., Модел на архитектура и защитни механизми на система за електронна търговия, *Годишник на БСУ*, том IX, 2003 г., 101-108.
5. Jecheva V., Investigation of E-commerce System Exposed to DoS Attacks, *Доклади на БАН*, Том 56, No 12, 2003 г., стр. 29-34.
6. Jecheva V., A Hidden Markov Model and Simulation Experiments for E-commerce System Exposed to DoS Attacks, *30th International Conference "Information and Communication Technologies and Programming ICT&P 2005"*, Sofia (под печат).

Цитирания

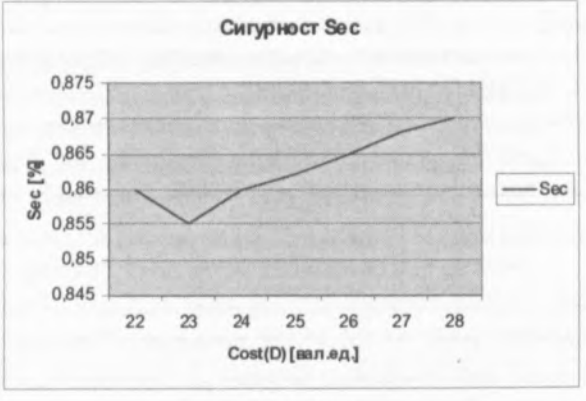
1. Димов С., *Електронно трансфериране на научен материал по учебната дисциплина "Финансов инженеринг"*, Сп. "АЛТЕРНАТИВИ", бр. 2/2000, стр. 43-44 - цитиране на [2].
2. Димитрова С., *"Защита на данните при преминаване през отворени мрежи"*, сп. "БАНКИ ИНВЕСТИЦИИ ПАРИ", бр.8-9/2001 г., стр. 64-67 - цитиране на [1].
3. Димов С., *Алтернативата "Американски счетоводни принципи – международни счетоводни стандарти" при отчитане на финансовите деривативи*, Сп. "Български счетоводител", бр. 7/2002, стр. 10-15 - цитиране на [3].



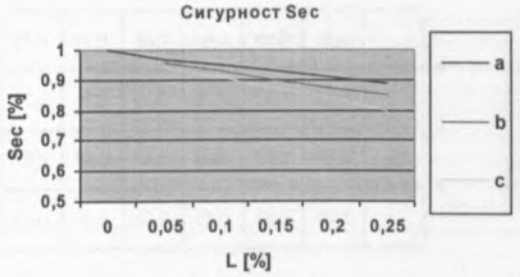
Фиг. 4-1



Фиг. 4-2



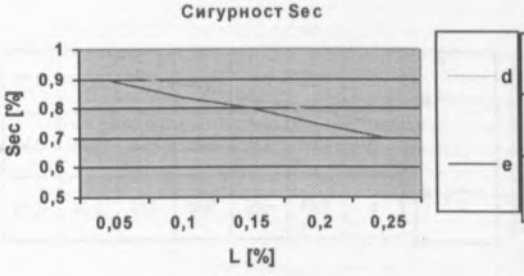
Фиг. 4-3



Фиг. П2-75

	0,00	0,05	0,10	0,15	0,20	0,25
a	1,00	0,97	0,95	0,93	0,91	0,89
b		0,96	0,93	0,90	0,87	0,85
c		0,94	0,91	0,87	0,84	0,80

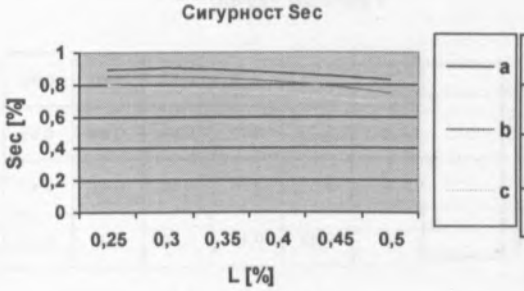
Таблица П3-75



Фиг. П2-76

	0,05	0,10	0,15	0,20	0,25
d	0,92	0,88	0,83	0,79	0,74
e	0,89	0,84	0,80	0,75	0,70

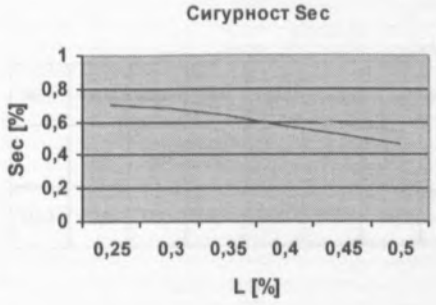
Таблица П3-76



Фиг. П2-77

	0,25	0,30	0,35	0,40	0,45	0,50
a	0,89	0,90	0,89	0,87	0,85	0,83
b	0,85	0,85	0,84	0,82	0,79	0,75
c	0,80	0,78	0,76	0,74	0,71	0,68

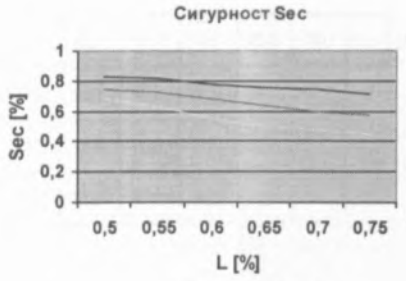
Таблица П3-77



Фиг. П2-78

	0,25	0,30	0,35	0,40	0,45	0,50
d	0,74	0,73	0,68	0,63	0,58	0,54
e	0,70	0,68	0,64	0,57	0,52	0,47

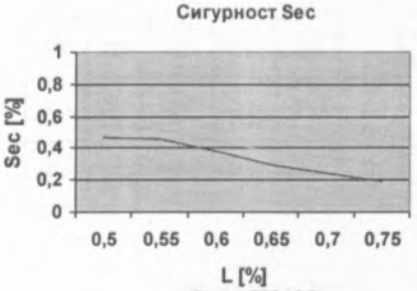
Таблица П3-78



Фиг. П2-79

	0,50	0,55	0,60	0,65	0,70	0,75
a	0,83	0,82	0,78	0,76	0,74	0,71
b	0,75	0,72	0,68	0,64	0,60	0,57
c	0,68	0,63	0,55	0,50	0,48	0,45

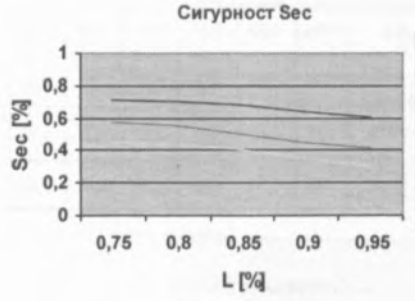
Таблица П3-79



Фиг. П2-80

	0,50	0,55	0,60	0,65	0,70	0,75
d	0,54	0,52	0,45	0,38	0,34	0,30
e	0,47	0,46	0,38	0,30	0,24	0,19

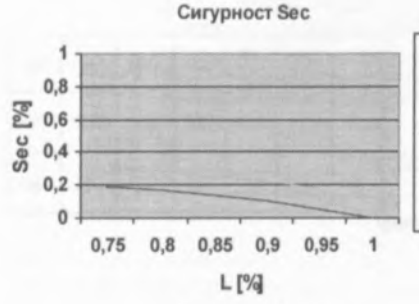
Таблица П3-80



Фиг. П2-81

	0,75	0,80	0,85	0,90	0,95
a	0,71	0,70	0,68	0,64	0,61
b	0,57	0,55	0,50	0,45	0,42
c	0,45	0,44	0,40	0,35	0,30

Таблица П3-81



Фиг. П2-82

	0,75	0,80	0,85	0,90	0,95	1,00
d	0,30	0,29	0,25	0,22	0,18	
e	0,19	0,18	0,14	0,11	0,05	0,00

Таблица П3-82