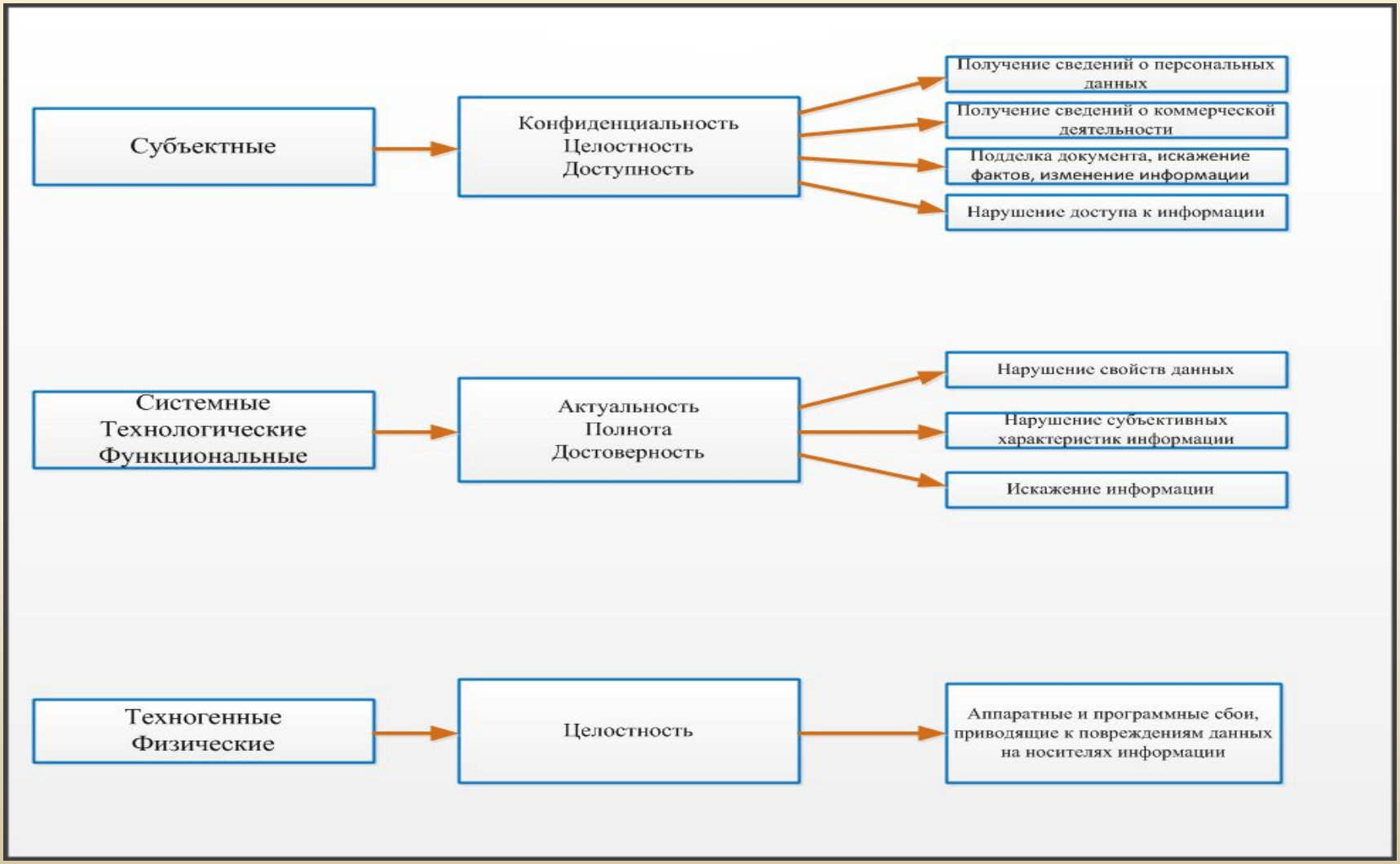
Дипломный проект на тему: «Анализ методов информационной безопасности настройки СУБД Oracle

Студента группы ИС-501
Фролова Д.С.

Встроенные методы безопасности СУБД Oracle

- Virtual Private Database (VPD) — средства разграничения доступа к данным на уровне строк (в версии 10g — и на уровне колонок) и возможность пользователю организовать работу только с виртуальной регламентированной частью данных, а не с реальной базой данных;
- Oracle Advanced Security (OAS) — широкий комплекс средств аутентификации и обеспечения сетевой безопасности, в котором осуществляется поддержка защищенных протоколов передачи данных, в том числе SSL;
- Oracle Label Security (OLS) — средства, аналогичные VPD, но с возможностью проверки уровня доступа пользователя;
- Fine Grained Audit Control (FGA) – средства подробного аудита;
- штатные средства Oracle + eToken – двухфакторная аутентификация с применением цифровых сертификатов стандарта X.509.

Угрозы информации



РД Гостехкомиссии направленный на обеспечение практического использования ГОСТ Р ИСО/МЭК 15408-2002

- Аутентификация
- Шифрование хранимых данных
- Ограничение доступа к данным
- Шифрование информации передаваемой по каналам связи
- Журнализация

Схема локальной сети рассматриваемой организации

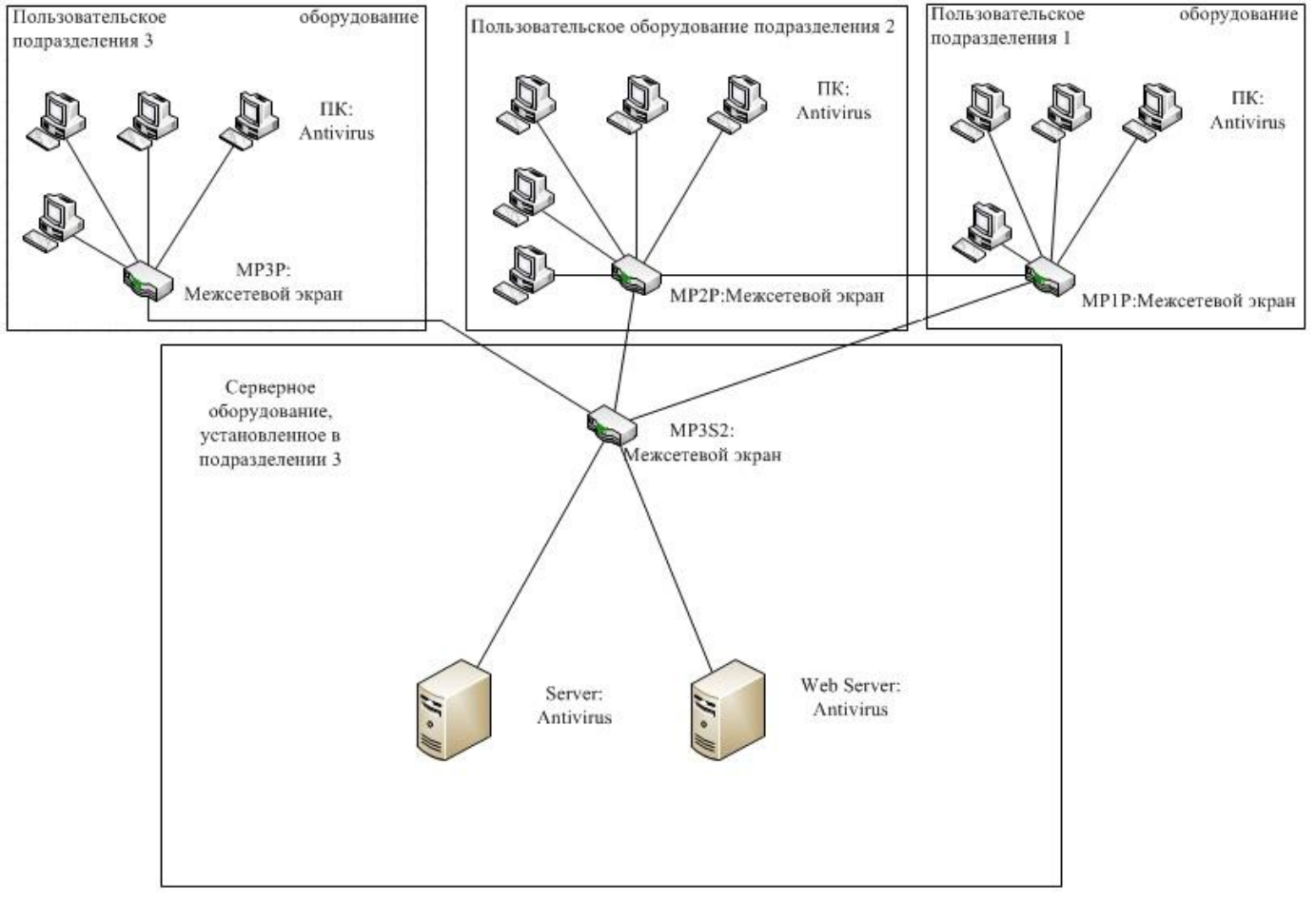
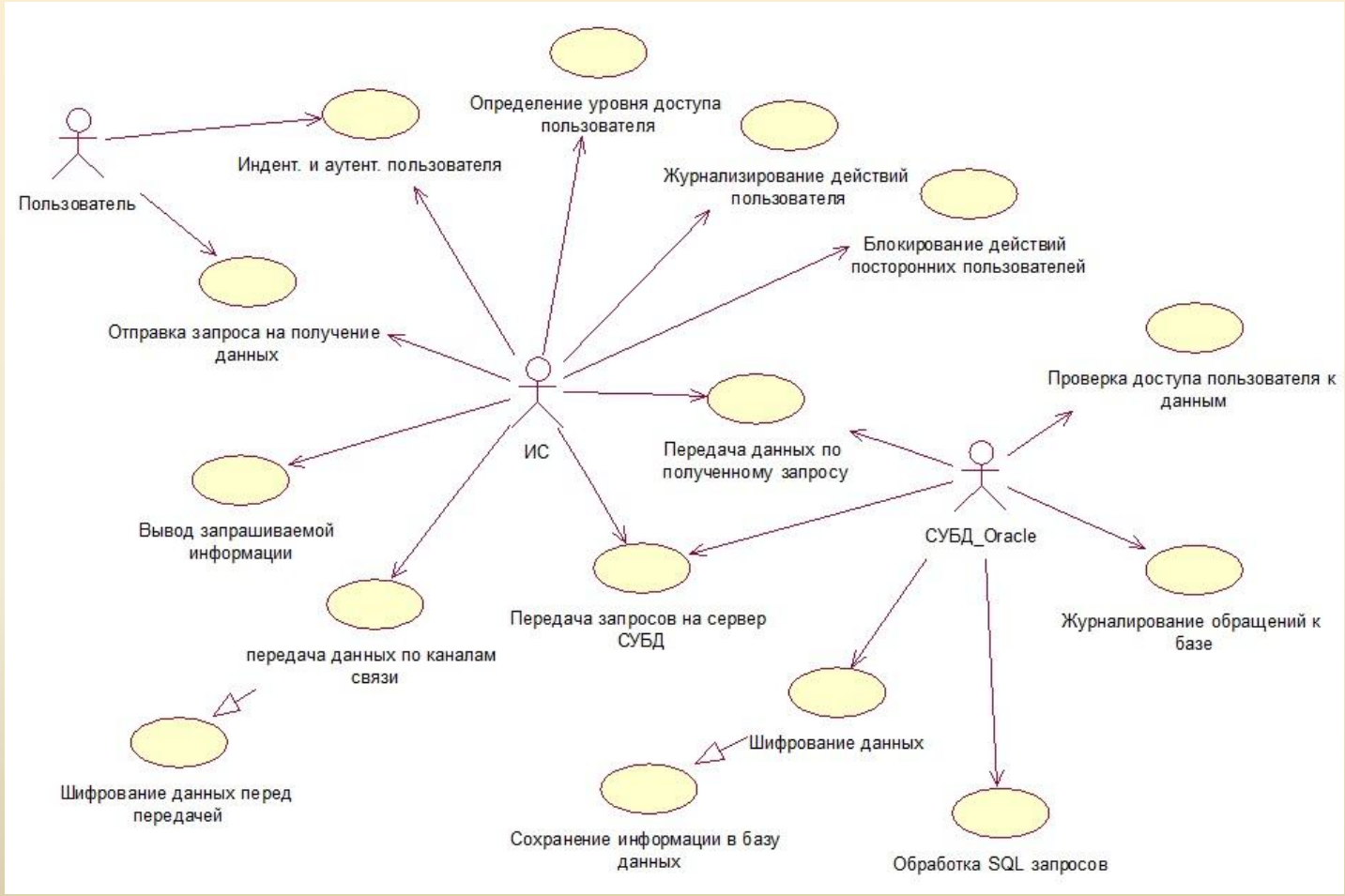
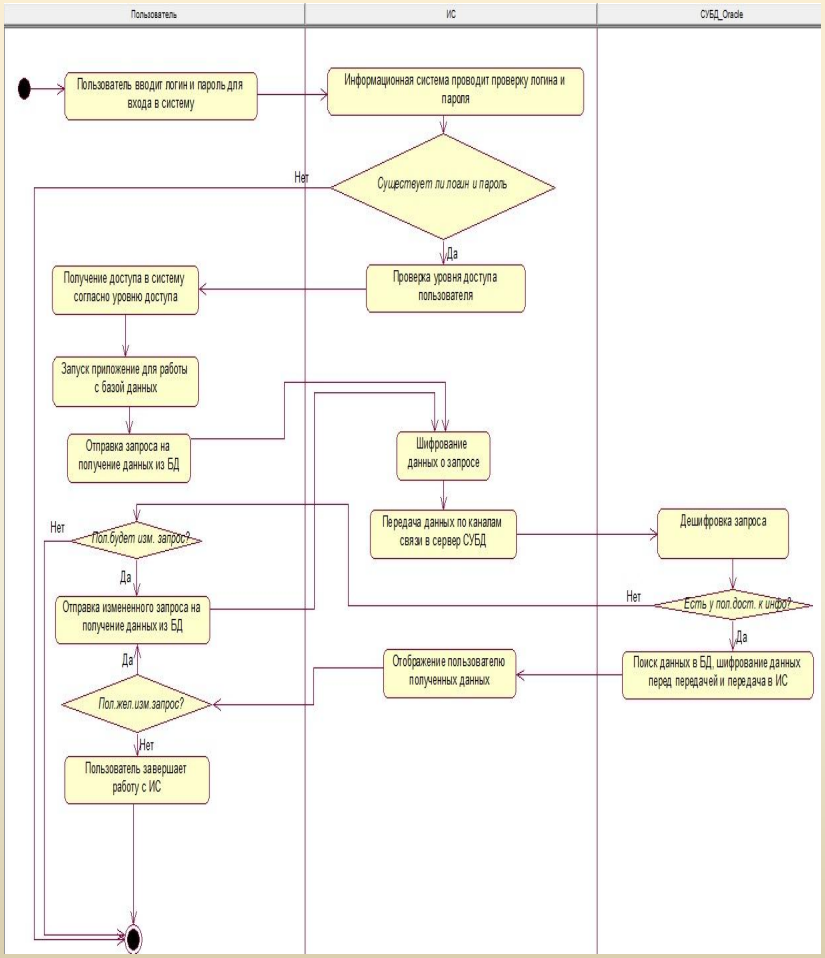
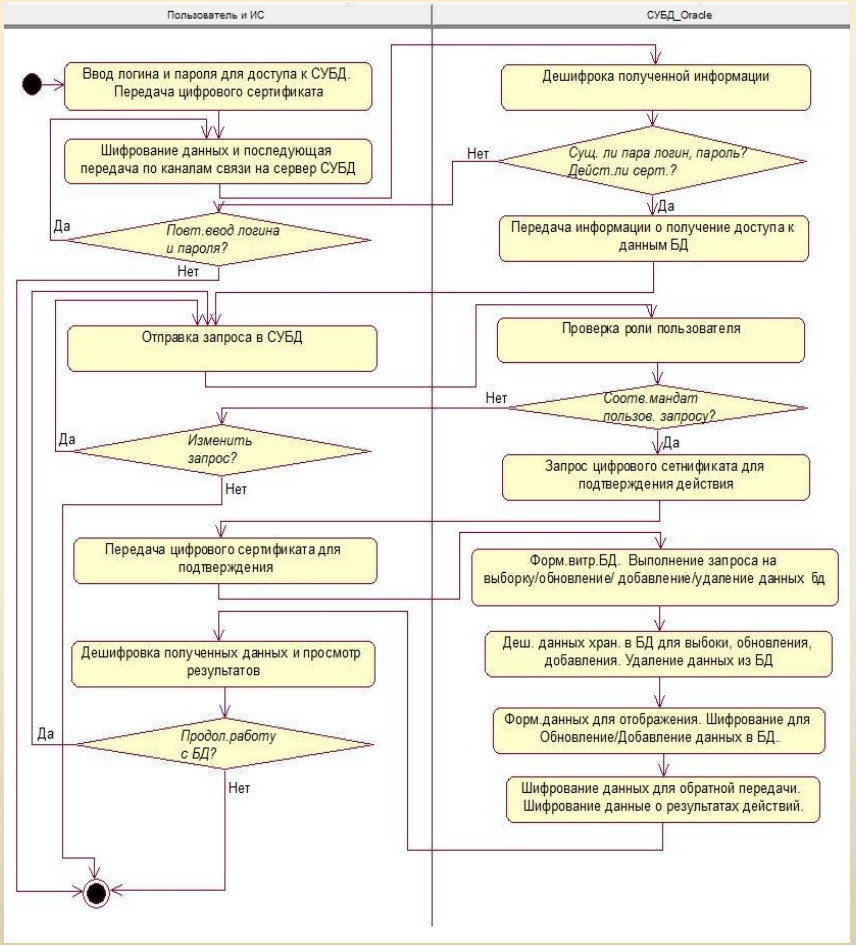


Диаграмма прецедентов проектируемой модели защиты



Диаграммы действий проектируемой модели





Диаграммы последовательности действий обработки запроса

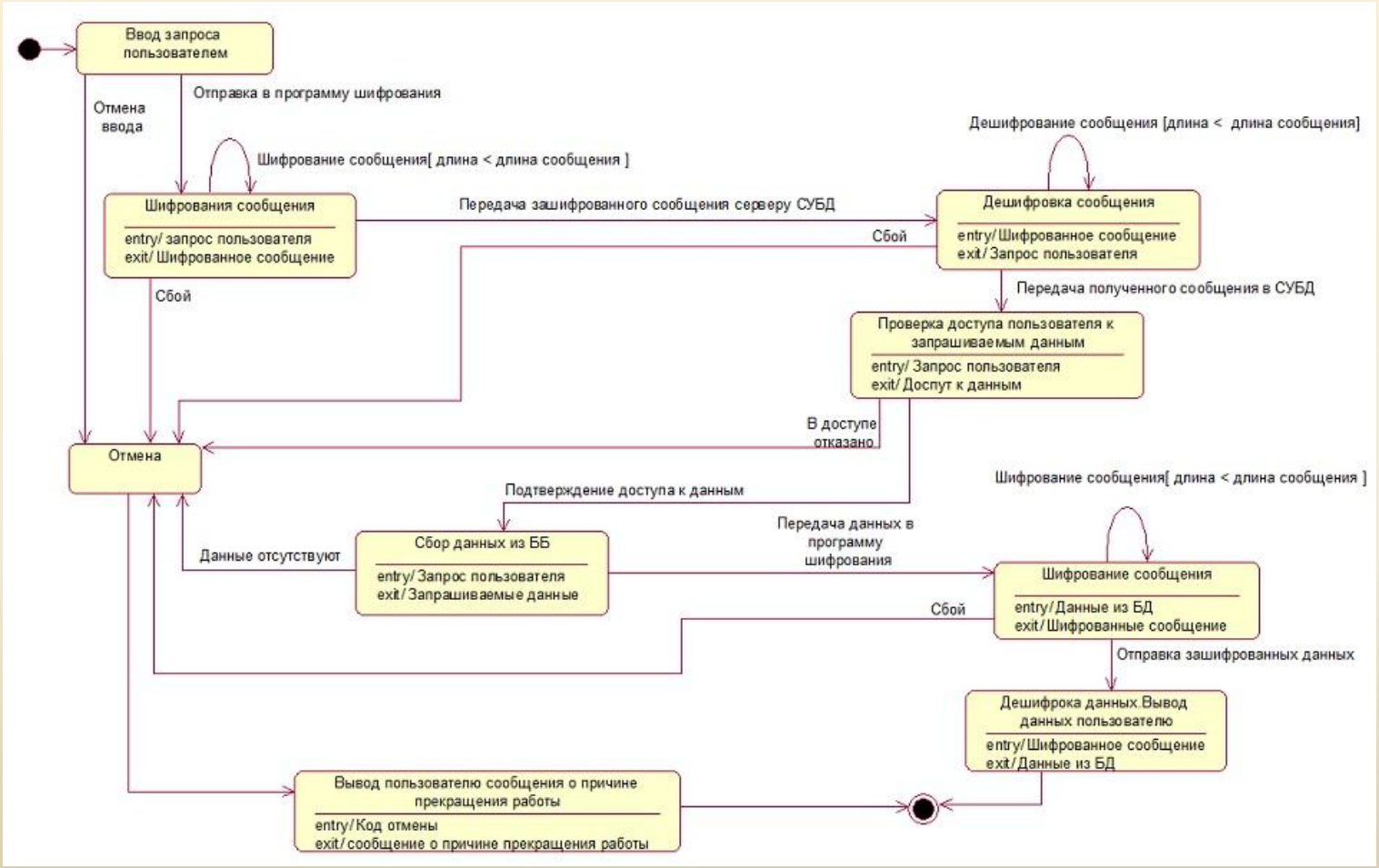
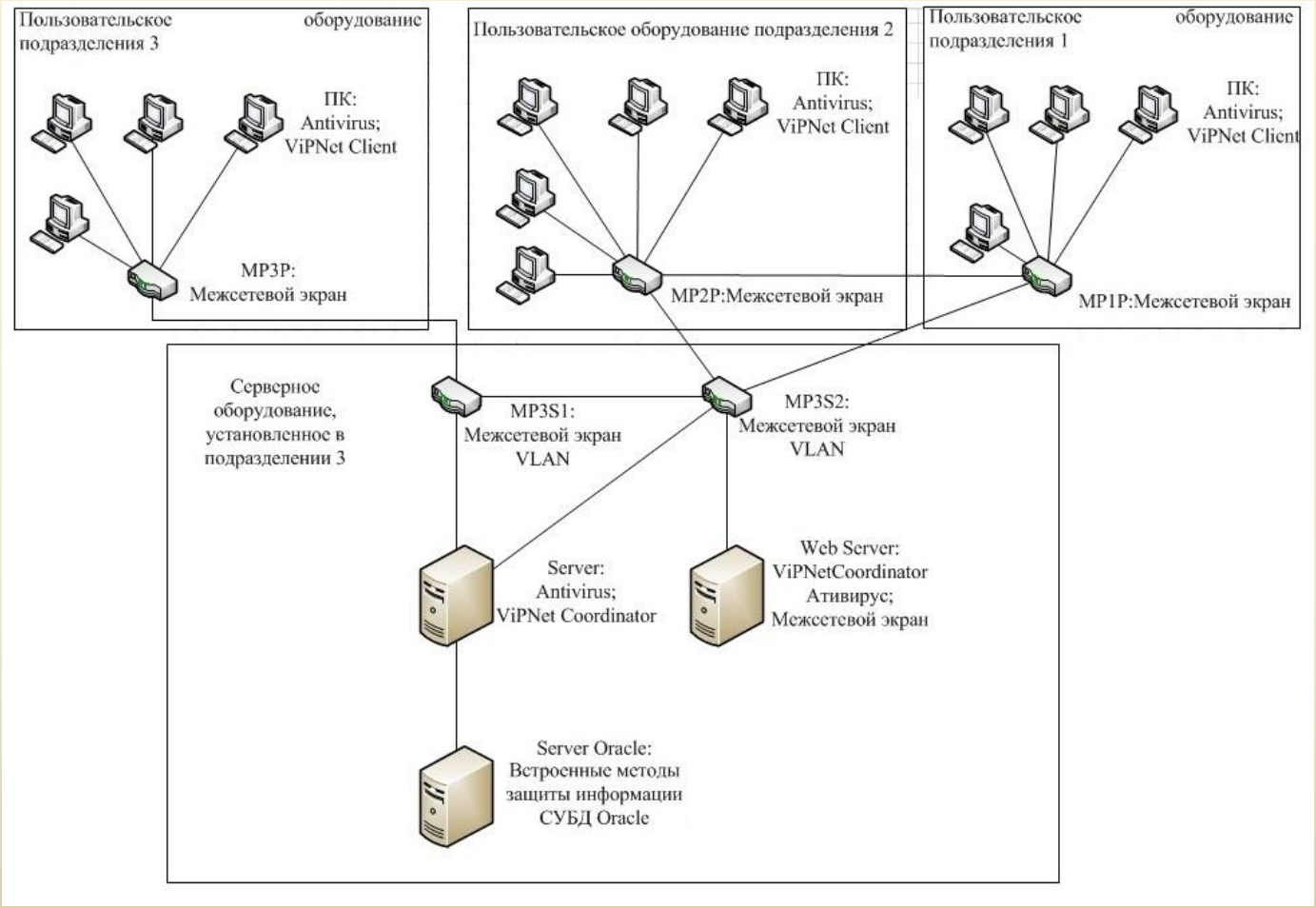
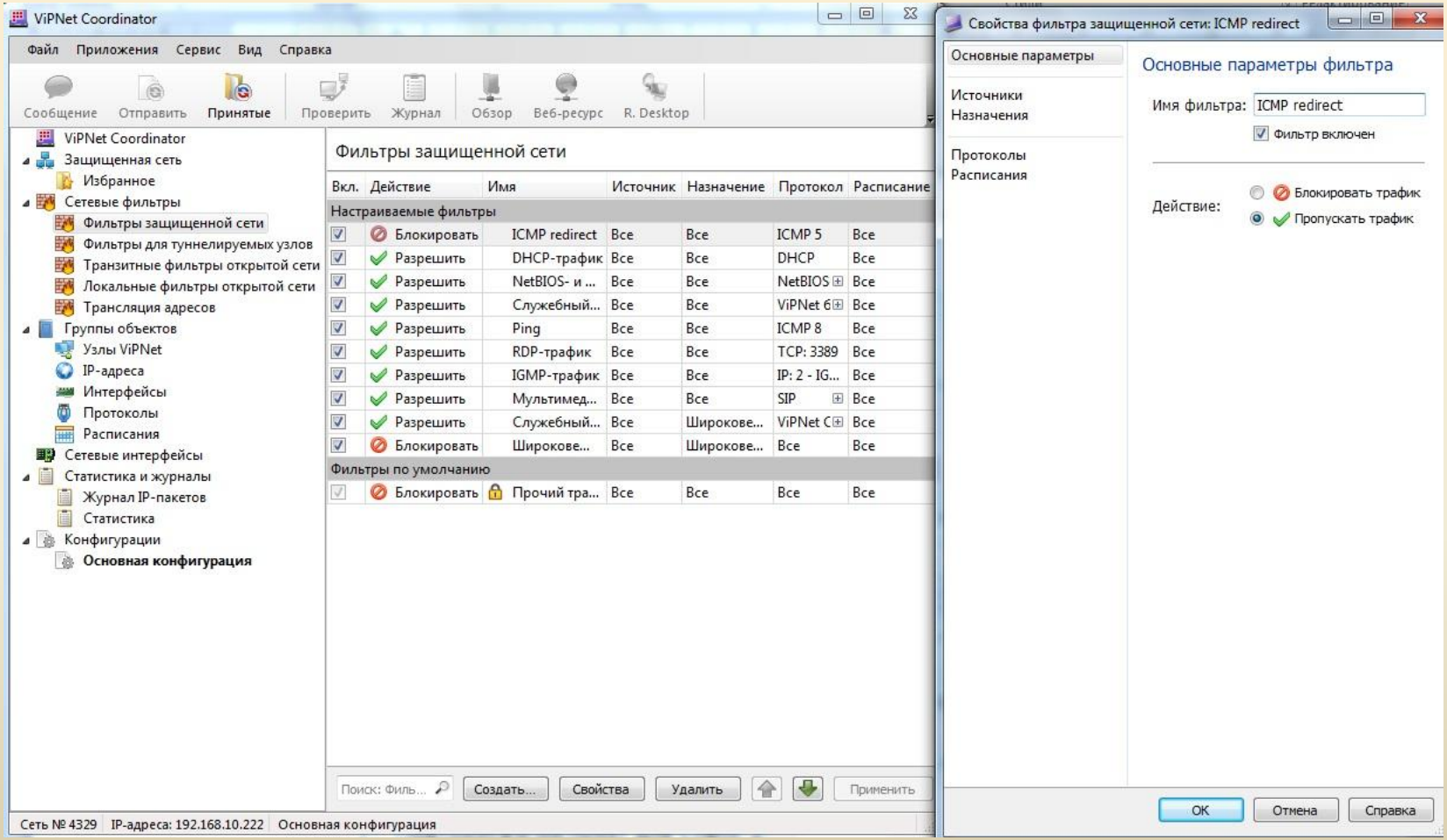


Схема локальной сети организации с ПО обеспечивающим безопасности ИС



VipNet Coordinator – шифрование информации для передачи по каналам связи



Аудит действий пользователей

```
SQL> select name,value from v$parameter
 where name like 'audit%';

NAME                           VALUE
------------------------------ ----------
audit_trail                    DB
audit_file_dest                ?/rdbms/audit
```

AUDIT_OPTION	SUCCESS	FAILURE
CREATE ANY CLUSTER	BY ACCESS	BY ACCESS
CREATE ANY INDEX	BY ACCESS	BY ACCESS
CREATE ANY INDEXTYPE	BY ACCESS	BY ACCESS
CREATE ANY LIBRARY	BY ACCESS	BY ACCESS
CREATE ANY PROCEDURE	BY ACCESS	BY ACCESS
CREATE ANY SEQUENCE	BY ACCESS	BY ACCESS
CREATE ANY TRIGGER	BY ACCESS	BY ACCESS
ALTER ANY CLUSTER	BY ACCESS	BY ACCESS
ALTER ANY INDEX	BY ACCESS	BY ACCESS
ALTER ANY INDEXTYPE	BY ACCESS	BY ACCESS
ALTER ANY LIBRARY	BY ACCESS	BY ACCESS
ALTER ANY PROCEDURE	BY ACCESS	BY ACCESS
ALTER ANY SEQUENCE	BY ACCESS	BY ACCESS
ALTER ANY TRIGGER	BY ACCESS	BY ACCESS
EXECUTE ANY INDEX	BY SESSION	BY SESSION
EXECUTE ANY LIBRARY	BY SESSION	BY SESSION
EXECUTE ANY PROCEDURE	BY SESSION	BY SESSION

```
select count(*),username,terminal,to_char
(timestamp,'DD-MON-YYYY')
  from dba_audit_session
  where returncode<>0
  group by username,terminal,to_char
(timestamp,'DD-MON-YYYY');
```

COUNT(*)	USERNAME	TERMIN	TO_CHAR(TIMESTAMP)
5	direct	pts/1	29-APR-2015

```
SQL> select count(*),username,terminal,to_char
(timestamp,'DD-MON-YYYY') as DATE,returncode
   from dba_audit_session
   group by username,terminal,to_char
(timestamp,'DD-MON-YYYY'),returncode;
```

COUNT(*)	USERNAME	TERMIN	DATE	RETURNCODE
5	direct	pts/1	29-APR-2015	1017

```
SQL> select username,terminal,to_char
(timestamp,'DD-MON-YYYY HH24:MI:SS') as DATETIME
 from dba_audit_session
 where returncode<>0
 and not exists (select 'x'
 from dba_users
 where dba_users.username=
dba_audit_session.username)
/

USERNAME   TERMIN   DATETIME
---------- -------- --------------------
PROBA      pts/3    29-APR-2015 17:31:47
```

Применение VPD

```
CREATE TABLE Client
(
 id_client NUMBER,
 Name VARCHAR2(64),
 SName VARCHAR2(64),
 Adress VARCHAR2(64),
 Schet INTEGER,
 Nomer VARCHAR2(32),
 Gorod VARCHAR2(64),
 Raspoloj VARCHAR2(32),
 CONSTRAINT " Client _PK" PRIMARY KEY ("id_client")
);
insert into Client values(1, 'Максим', 'Маничкин', 'Набережная 15, 6',
0121748596, '-', 'Тольятти', 'М');
```

```
BEGIN
DBMS_REDACT.ALTER_POLICY(
    object_schema       => 'VPD_TC',
    object_name         => 'Client',
    column_name         => 'Nomer',
    policy_name         => 'mas_client ',
    function_type       => DBMS_REDACT.REGEXP,

    regexp_pattern    => '\d+(\d{5})$',
    regexp_replace_string => '******\1',
    regexp_position     => DBMS_REDACT.RE_BEGINNING,
    regexp_occurrence   => DBMS_REDACT.RE_ALL,
    expression              => 'SYS_CONTEXT("SYS_SESSION_ROLES","
    "Client_all") = "FALSE"',
    action              => DBMS_REDACT.ADD_COLUMN
);
END;
/
SQL> select Name, SName, Adress, Schet, Nomer from Client;

Name         SName        Adress         Schet          Nomer
------------ ------------ -------------- -------------- --------------
Максим       Маничкин     **********012****596 *****
```

Применение OLS

```
create table Organizac (
 id_organ number
 Nazvanie  varchar2(10),
 Adress  varchar2(10),
 Schet integer ,
 Cont_Lico  varchar2(64),
 Nomer varchar2(15),
 Gorod char(10),
 Raspoloj char(10),
 CONSTRAINT “Organizac _PK” PRIMARY KEY (“id_organ”))
 PARTITION BY RANGE (vse_p) (
  PARTITION S VALUES LESS THAN (80000),
  PARTITION M VALUES LESS THAN (90000),
  PARTITION B VALUES LESS THAN (MAXVALUE)
 );
grant select on payments to public;
```

```
BEGIN
 SA_USER_ADMIN.SET_GROUPS (
 policy_name   => 'p_polit',
 user_name     => 'direct',
 read_groups   => 'Rasp');
 SA_USER_ADMIN.SET_GROUPS (
 policy_name   => 'p_polit',
 user_name     => 'm_polz',
 read_groups   => 'M');
SA_USER_ADMIN.SET_GROUPS (
 policy_name   => 'p_polit',
 user_name     => 'o_polz',
 read_groups   => 'O');
END;
/
```

```
SA_COMPONENTS.CREATE_GROUP (
 policy_name     => ' p_polit',
 group_num       => 10,
 short_name      => 'Rasp',
 long_name       => 'Raspolojenie');

SA_COMPONENTS.CREATE_GROUP (
 policy_name     => ' p_polit',
 group_num       => 20,
 short_name      => 'M',
 long_name       => 'Mestniy',
 parent_name     => 'Rasp');

SA_COMPONENTS.CREATE_GROUP (
 policy_name     => ' p_polit',
 group_num       => 30,
 short_name      => 'O',
 long_name       => 'Others',
 parent_name     => 'Rasp');
END;
/
```

Применение OLS

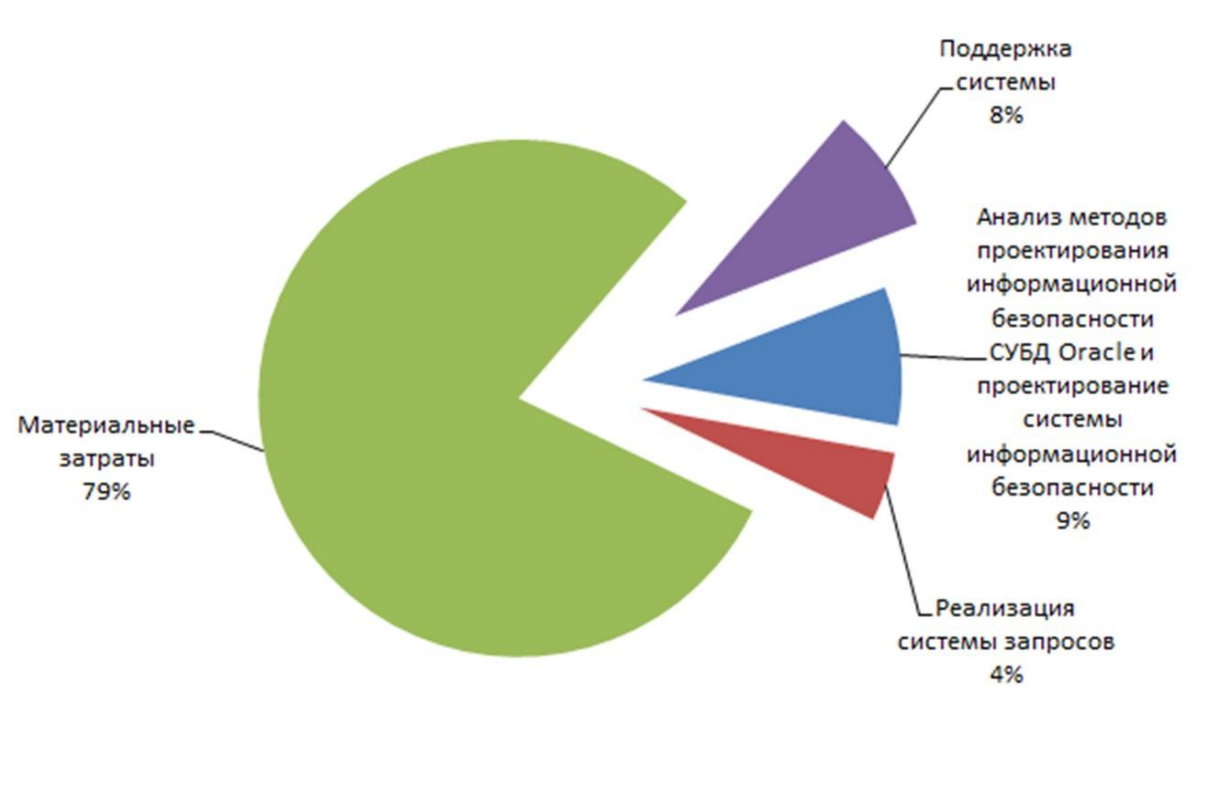
```
insert into Organizac values(1, 'ОАО Ростелеком', 'Самарская 68', 06548593321,
'Туманова Н.С', '123456', 'Тольятти',  'М');
insert into Organizac values(2, 'ЗАО Электрощит', 'Жигули 6', 03987527123,
'Медведев В.А', '123456', 'Самара',  'О');
insert into Organizac values(3, 'Детский сад №75', 'Гидротехническая 25',
02149321484, 'Степанова А.Ю', '123456', 'Тольятти',  'М');
insert into Organizac values(4, 'Детский сад №22', 'Кутузова 73', 03187594424,
'Парядина В.А', '123456', 'Жигулевск',  'О');
```

```
$ sqlplus direct /qw
SQL> select id_org, Nazvanie, Gorod from Organizac;
 id_org Nazvanie                          Gorod
-------- ---------------------------------- ----------
       1 ОАО Ростелеком                     Тольятти
       2 ЗАО Электрощит                     Самара
       3 Детский сад №75                    Тольятти
       4 Детский сад №22                    Жигулевск

$ sqlplus m_polz /qw
SQL> select id_org, Nazvanie, Gorod from Organizac;
 id_org Nazvanie                          Gorod
-------- ---------------------------------- ----------
       1 ОАО Ростелеком                     Тольятти
       3 Детский сад №75                    Тольятти

$ sqlplus o_polz /qw
SQL> select id_org, Nazvanie, Gorod from Organizac;
 id_org Nazvanie                          Gorod
-------- ---------------------------------- ----------
       2 ЗАО Электрощит                     Самара
       4 Детский сад №22                    Жигулевск
```

Экономические показатели реализации ДП



Стоимость анализа методов проектирования информационной безопасности СУБД Oracle и проектирования системы информационной безопасности – 20800р.

Стоимость реализации системы запросов – 10400р.

Стоимость поддержки системы – 19000р.

Общая стоимость материальных затрат – 190000р.

Спасибо за внимание.

Доклад окончен.