

Информационная безопасность электронного города

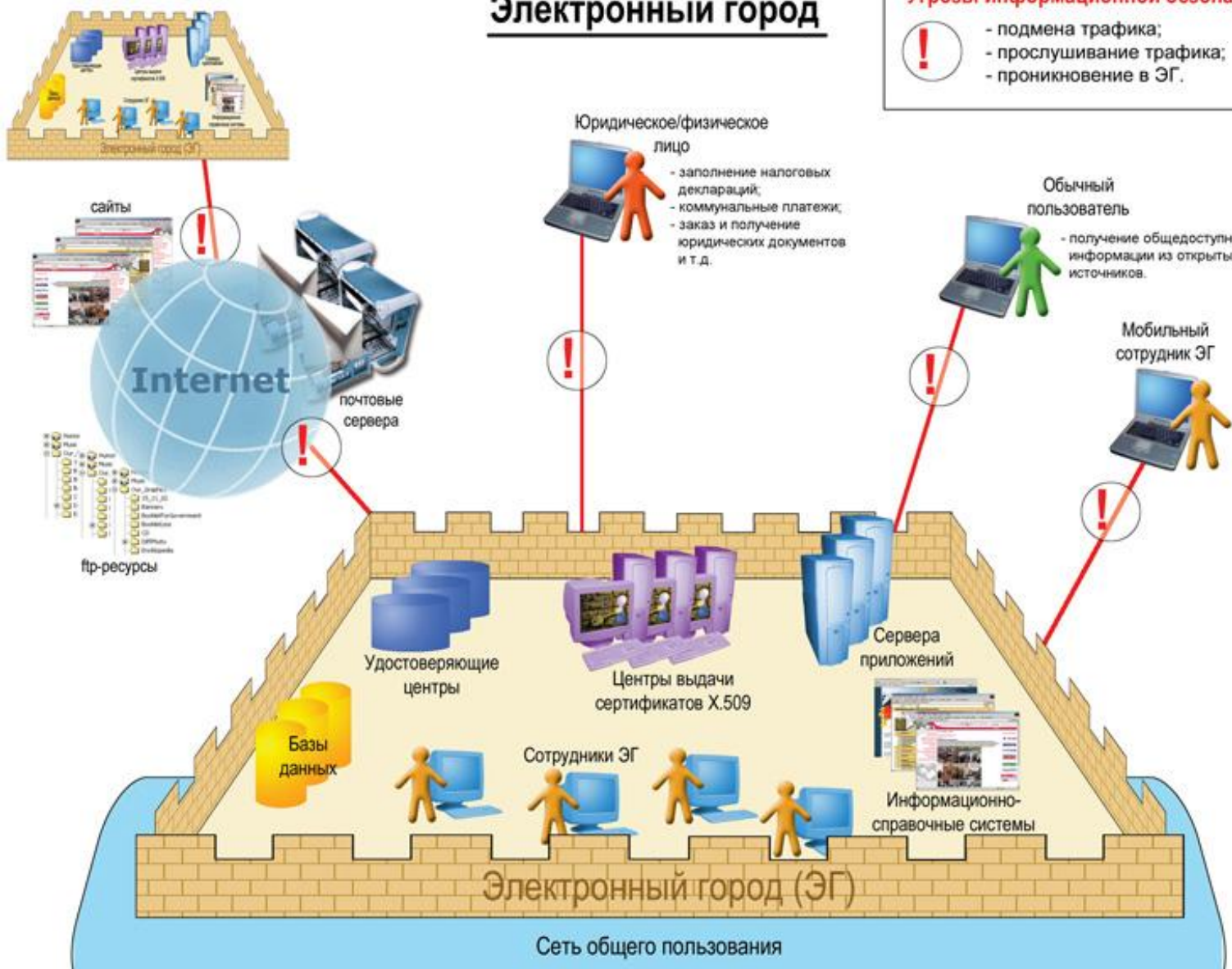
Угрозы информационной безопасности электронному городу

Электронный город

Угрозы информационной безопасности



- подмена трафика;
- прослушивание трафика;
- проникновение в ЭГ.

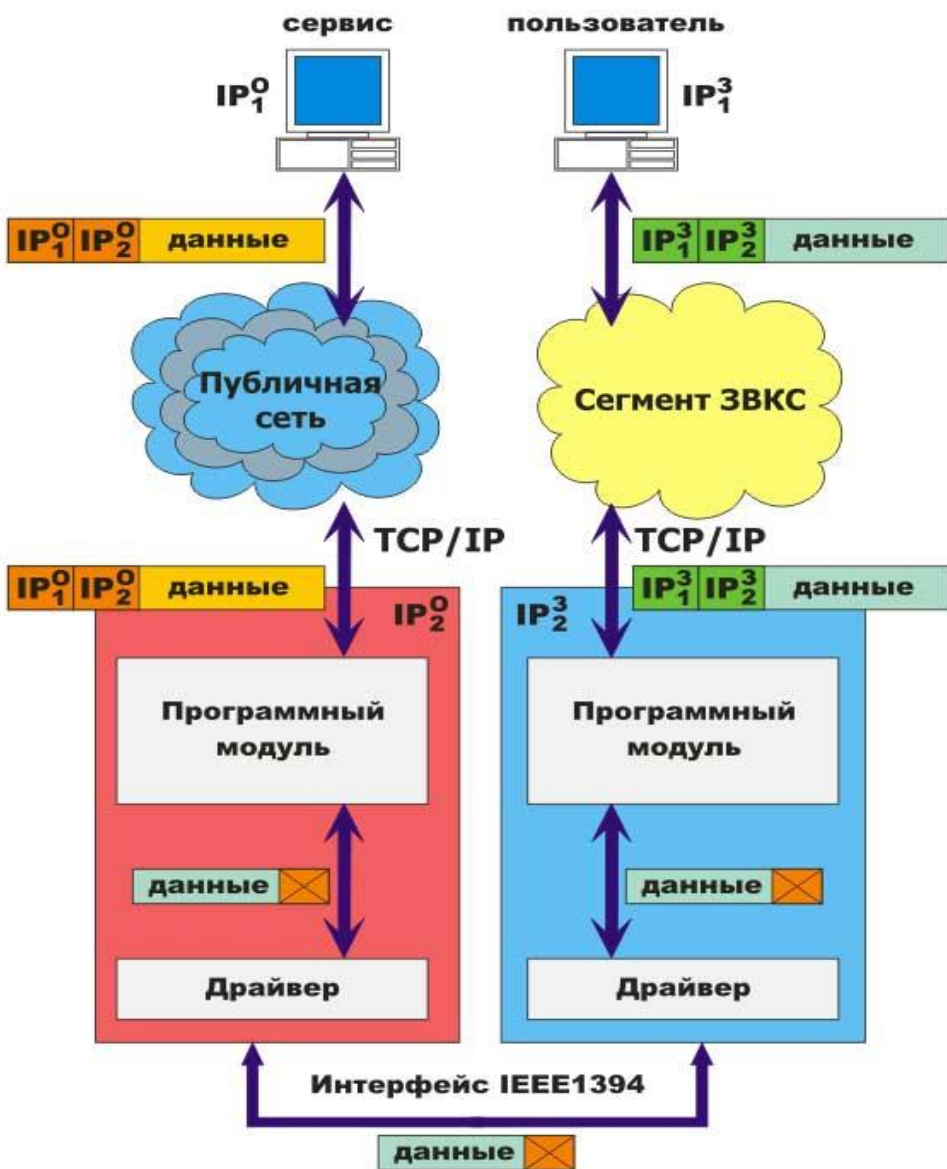


Традиционные решения не решают проблемы несанкционированного доступа из сети Интернет в электронный город

Аксиома: Точка подключения корпоративной сети к публичной сети, является частью публичной сети.

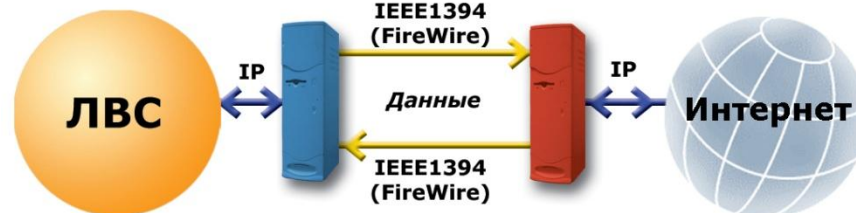
Следствие: Злоумышленник может осуществить несанкционированный доступ в точку подключения корпоративной сети к публичной сети, и, следовательно, получить доступ к корпоративной сети

Технология Shield



Взаимодействие автоматизированных систем органов государственного и местного управления с сетью Интернет без использования сетевых протоколов

Безопасный узел подключения к сети Интернет



Безопасное использование услуг/сервисов публичных сетей (E-Mail, WWW, FTP и т.д.)

ПАК «Shield Multi Service - FW»

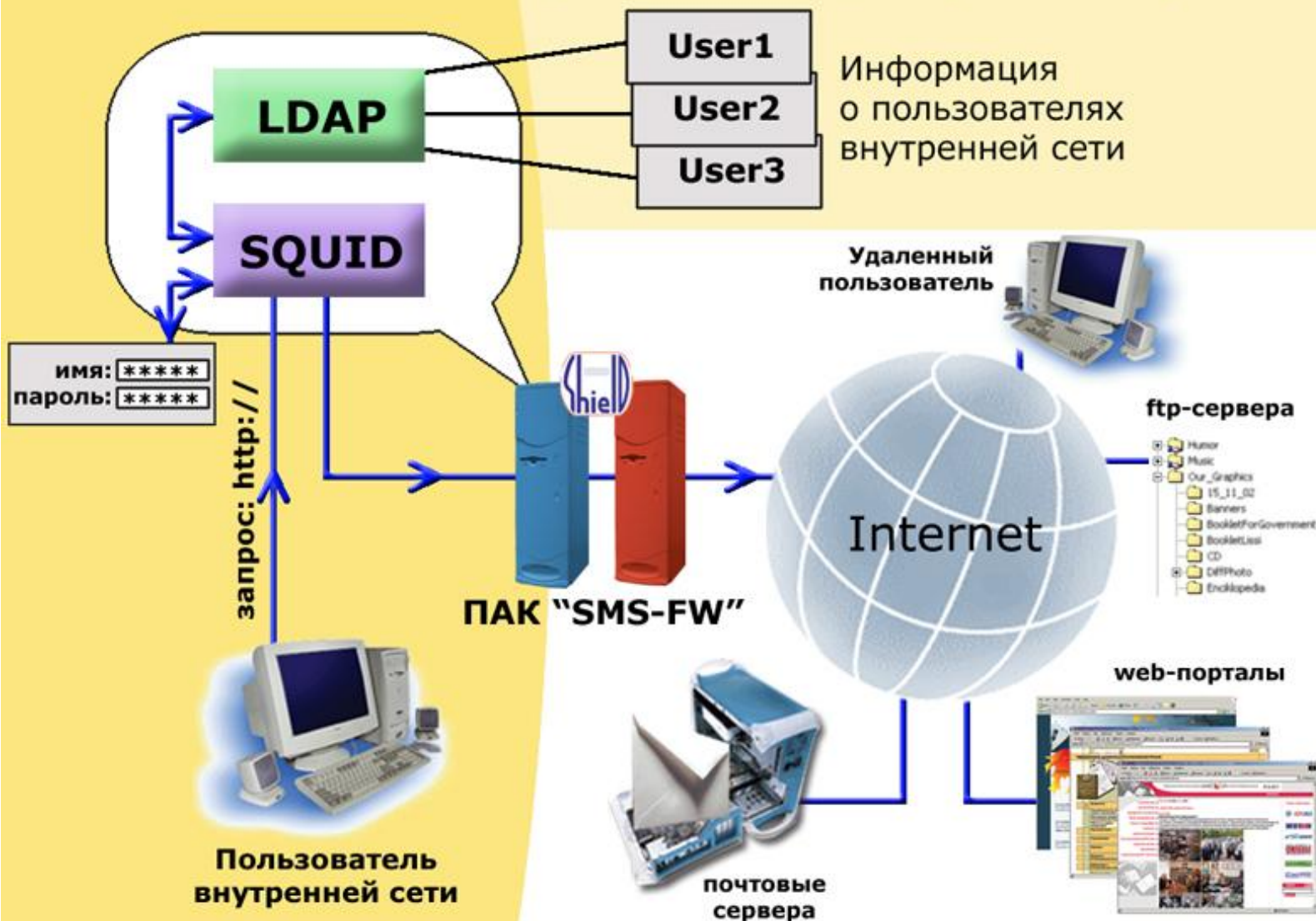


- ✓ Технология Shield
- ✓ Концепция замкнутой программной среды на базе 3L-System

ПАК «SMS-FW» обеспечивает техническую возможность исключения автоматизированных рабочих мест, серверов защищаемых сетей из состава средств международного информационного обмена при подключении к сетям общего пользования, включая сеть Internet.

Безопасный авторизованный доступ к информационным ресурсам сети Интернет из защищенной корпоративной сети

Безопасный авторизованный доступ в Интернет



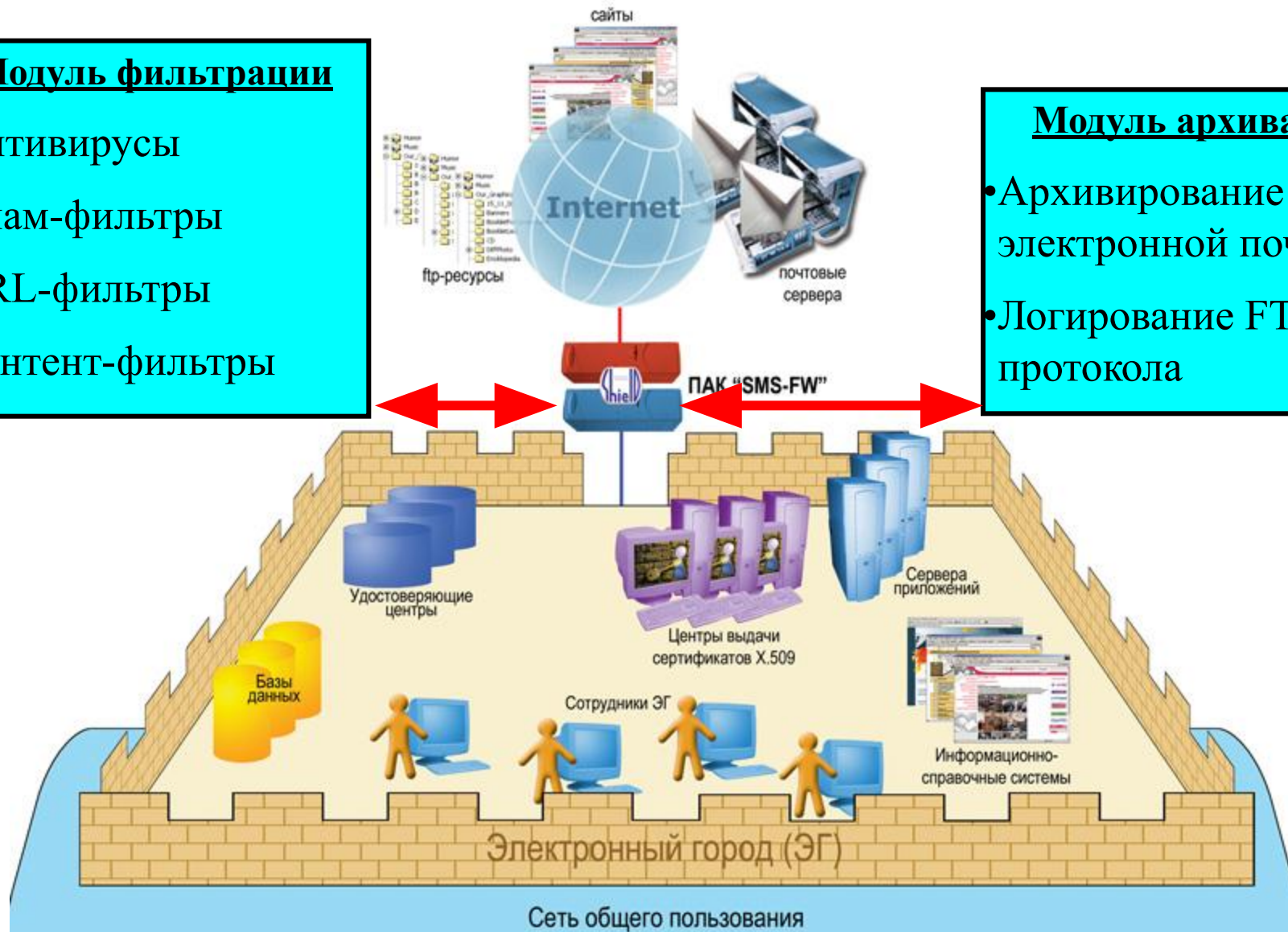
Безопасный доступ из электронного города к информационным ресурсам сети Интернет

Модуль фильтрации

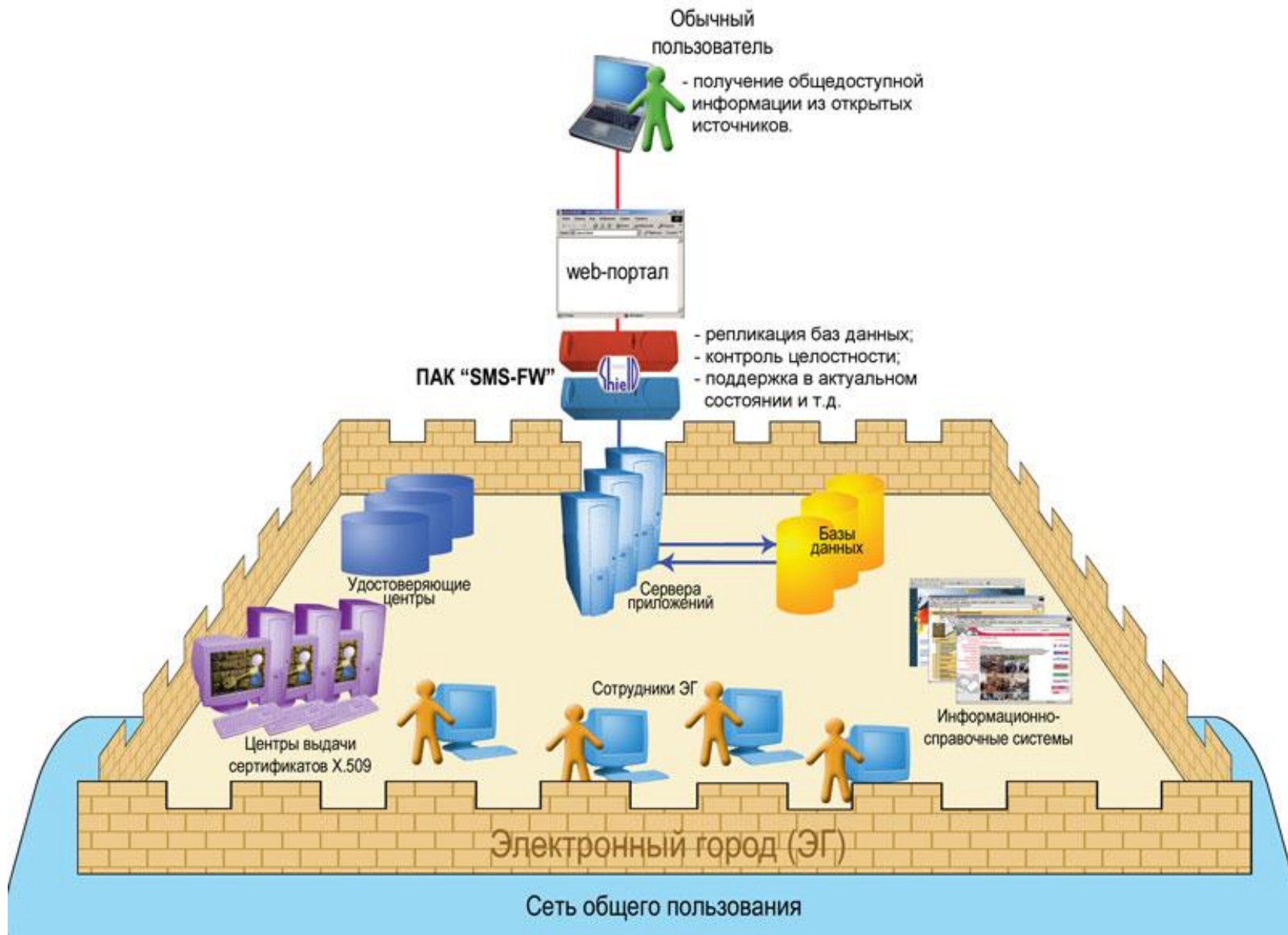
- Антивирусы
- Спам-фильтры
- URL-фильтры
- Контент-фильтры

Модуль архивации

- Архивирование электронной почты
- Логиrowание FTP протокола



Безопасное предоставление информационных услуг жителям и гостям электронного города



Создание защищенной виртуальной корпоративной сети электронного города

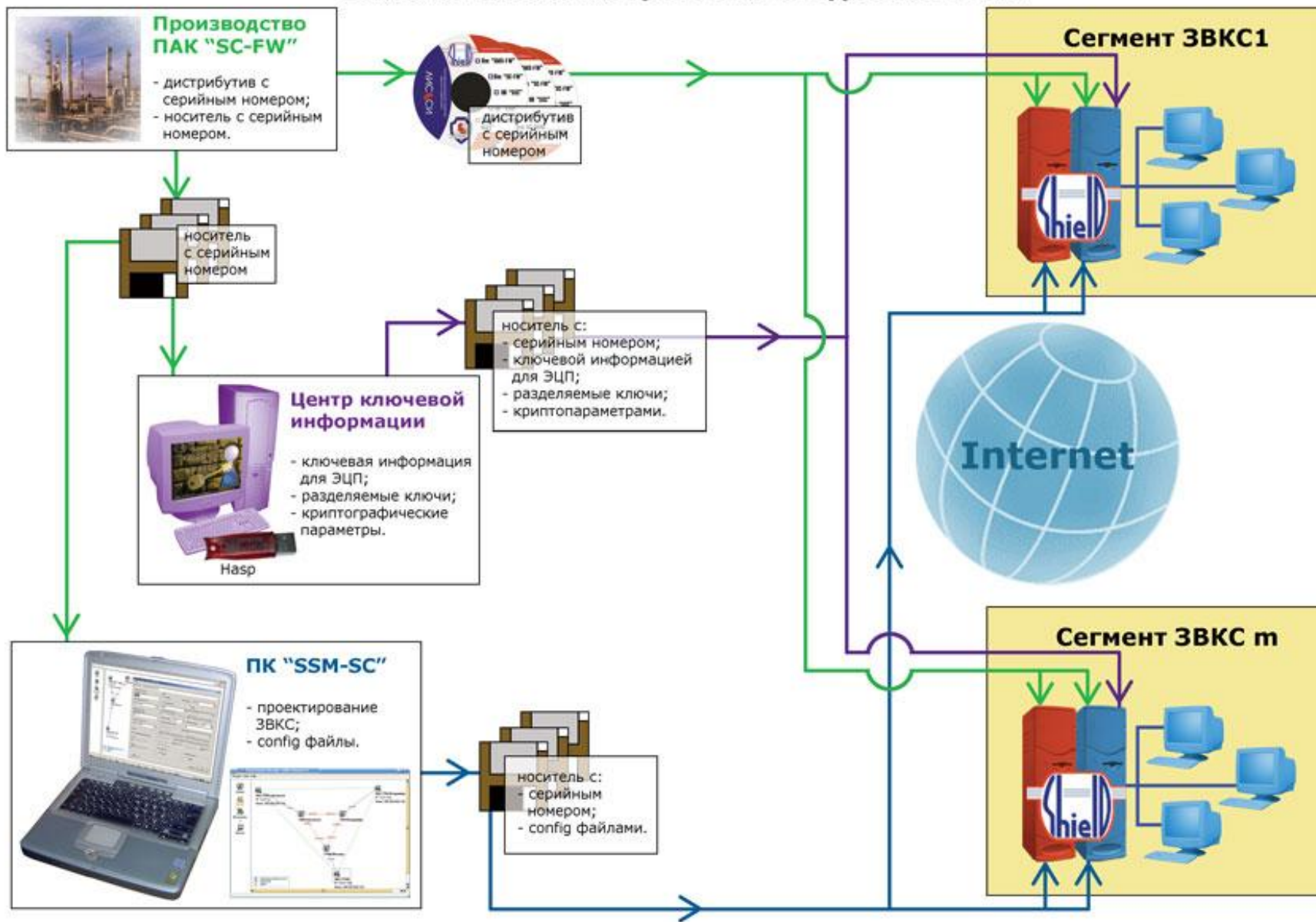
ПАК «Shield Channel - FW»



- ✓ Технология Shield
- ✓ Концепция замкнутой программной среды на базе 3L-System

ПАК «SC-FW» обеспечивает техническую возможность исключения автоматизированных рабочих мест, серверов защищаемых сетей из состава средств международного информационного обмена при подключении к сетям общего пользования, включая сеть Internet.

Технологическая цепочка создания ЗВКС



Организация криптоканала

Контроль целостности ПО по ГОСТ Р34.11-94

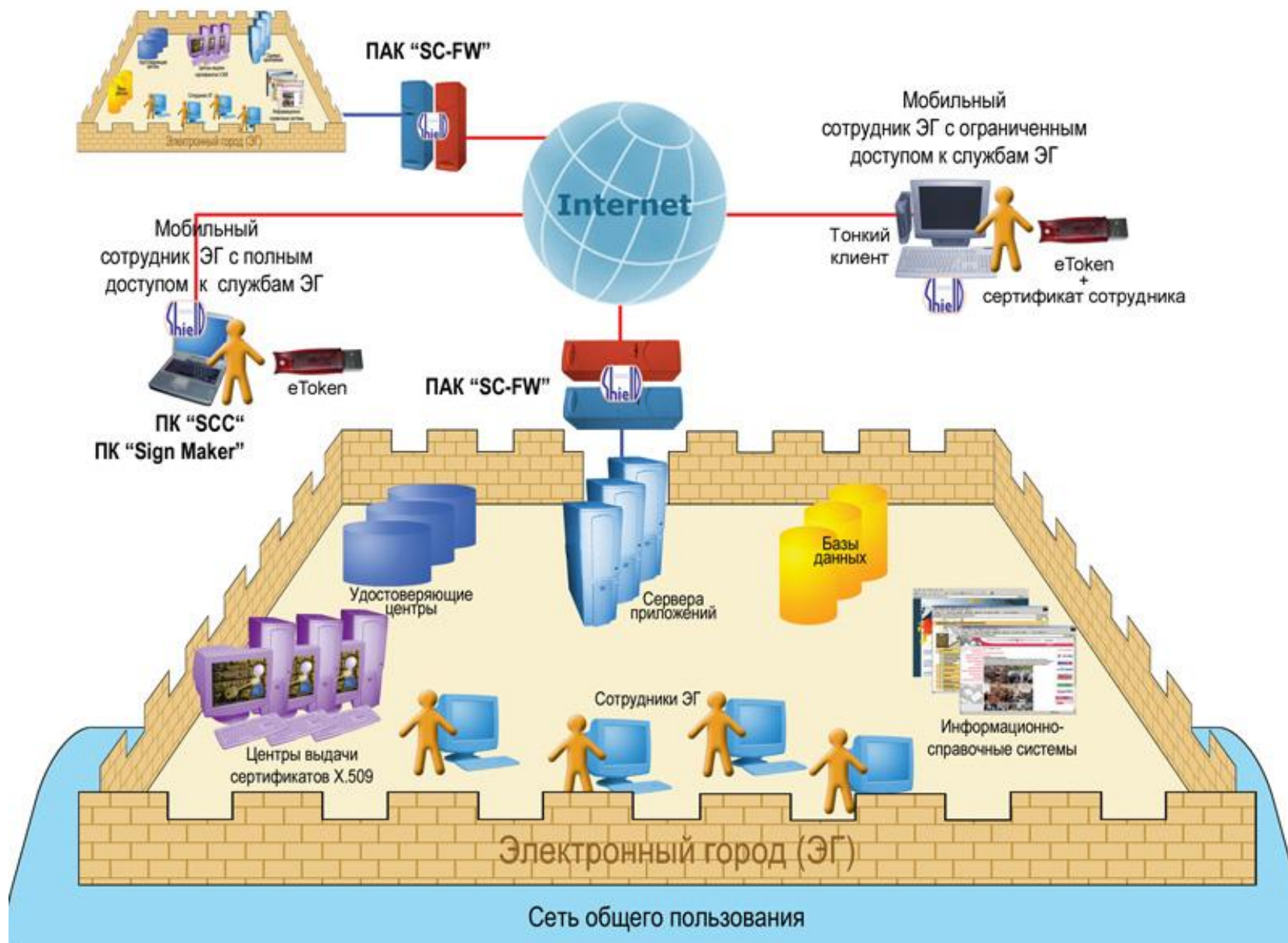
Формирование ESP(IPSEC) пакетов

Контроль целостности ПО по ГОСТ Р34.11-94

Шифрование и контроль целостности по ГОСТ 28147-89



Доступ мобильных сотрудников в электронный город

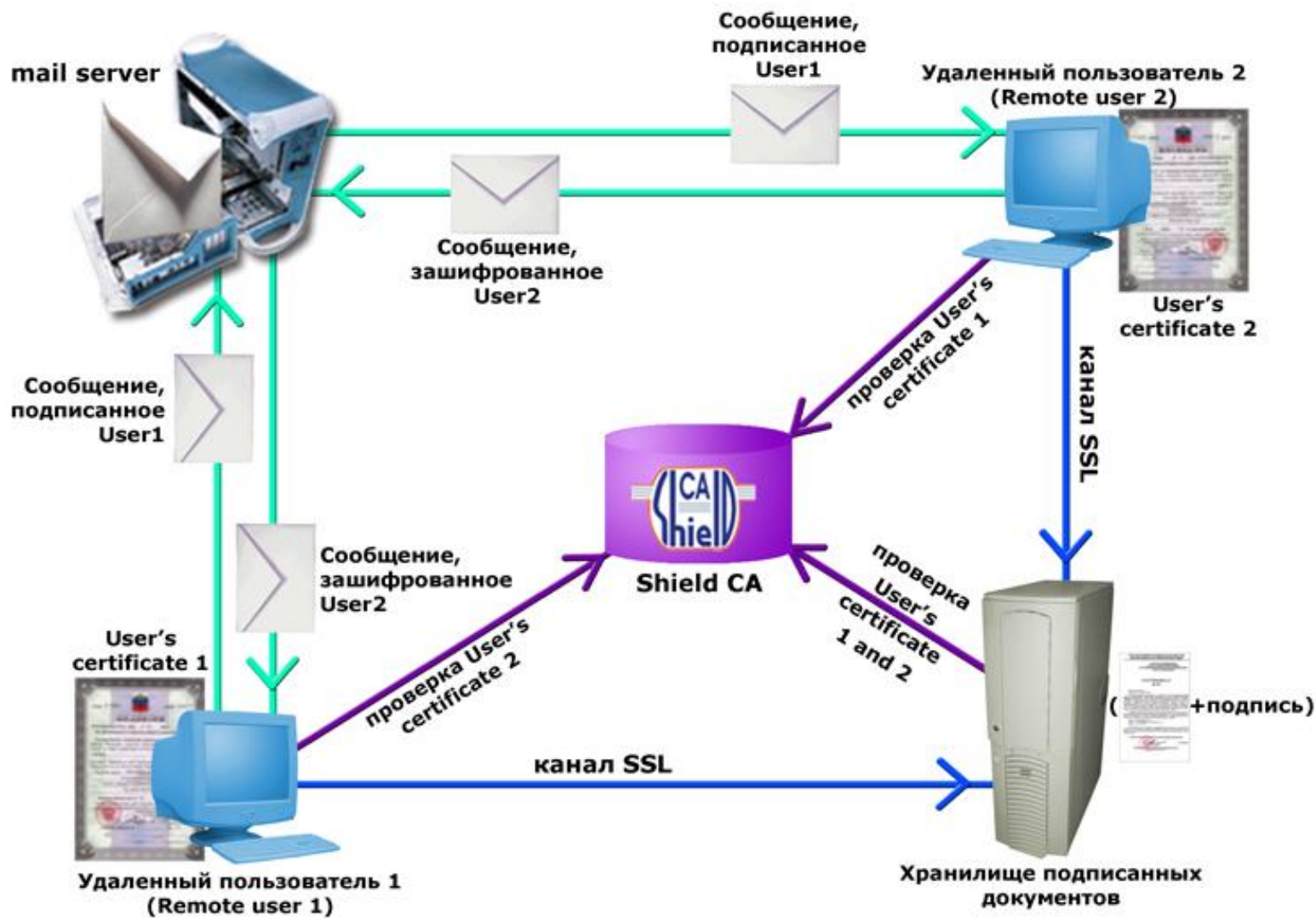


Составляющие системы защищенного документооборота

Компоненты:

- Цифровые сертификаты X.509
- Инфраструктура открытых ключей PKI (Удостоверяющий центр Shield CA)
- Средства организации защищенного документооборота (SignMaker)

Принципы функционирования системы защищенного документооборота



Цифровые сертификаты X.509

Использование сертификатов позволяет :

- Осуществлять идентификацию и аутентификацию пользователей;
- Обеспечить конфиденциальность передаваемой информации за счет ее шифрования;
- Реализовать механизм «неотказуемости» от документа;
- Обеспечить юридическую значимость электронных документов;
- Совместно со средствами защиты от НСД к ресурсам ПК осуществлять управление доступом к информации

Удостоверяющий центр Shield CA:

□ Центр регистрации:

- обработка запросов на выдачу сертификатов и секретных ключей;
- проверка подлинности сертификатов (идентификация пользователей);
- управление сертификатами;

□ Центр сертификации:

- Создание и хранение сертификатов и закрытых ключей
- Ведение списка отозванных сертификатов

Схема функционирования Shield CA



- ✓ Иерархическая структура интерфейсов (служб)
- ✓ Гибкая схема обмена данными между интерфейсами
- ✓ Кроссплатформенность
- ✓ Интернационализация
- ✓ Поддержка различных баз данных и хранилищ
- ✓ Гибкое конфигурирование
- ✓ Веб интерфейс

Shield CA – запрос на сертификат

ЗАЩИЩЕННЫЙ
УДОСТОВЕРЯЮЩИЙ
ЦЕНТР

Общая информация

Информация ЦС

Пользователь

Сертификаты

Запросы

Язык

Запросить сертификат

Получить запрошенный сертификат

Проверить сертификат

Отозвать сертификат

Запросить сертификат

Для того чтобы запросить сертификат используйте одну из следующих ссылок. Вам будет предложена форма для заполнения и подтверждения введенных данных. После подачи заявки вы должны пойти на выбранный ЦР для подтверждения запроса.

Запросить сертификат, используя автоматическое определение браузера.

[Используйте эту ссылку, если вы не знаете что надо делать]

Стандартный запрос

[Создание ключа и запроса на сервере]

Токен запрос

[Запросить аппаратный токен для авторизации регистрации]

Netscape запрос

[Запрос через браузер пользователя - SPKAC]

Internet Explorer запрос

[Запрос через браузер пользователя - Microsoft]

Серверный запрос

[PKCS#10 PEM форматированный Запрос]

[Общая информация](#)[Активные CSR](#)[Активные CRR](#)[Информация](#)[Утилиты](#)[Язык](#)[По умолчанию](#)[German](#)[Greek](#)[English](#)[Spanish](#)[French](#)[Italian](#)[Japanese](#)[Polish](#)[Slovene](#)[Russian](#)[Vietnamese](#)

Серверная Информация для ShieldCA

Среда 16 Марта 14:27:44 UTC

Модуль	Версия
LIR-SSL	1.0
Tools	0.4.3
DB	0.9.115.2.5
Configuration	1.5.3
TRISateCGI	1.5.5
REQ	0.9.61
X509	0.9.57
CRL	0.9.24
PKCS7	0.9.19

ЗАЩИЩЕННЫЙ
УДОСТОВЕРЯЮЩИЙ
ЦЕНТР

Общая информация **Администрирование** Утилиты Журнал Язык

Остановить демонов крипто токенов Инициализация сервера **Обмен данными** Резервное копирование и восстановление База данных

Отправить данные на низший уровень иерархии

- Все
- Сертификаты
- CRL
- Конфигурация
- Batchprocessors

Получить данные с низшего уровня иерархии

- Все
- Запросы
- CRR

Загрузить данные с высшего уровня иерархии

- Все
- Сертификаты
- CRL
- Конфигурация
- Batchprocessors

Загрузить данные на высший уровень иерархии

- Все
- Запросы
- CRR

Shield CA – интерфейс ПОЛЬЗОВАТЕЛЯ

ЗАЩИЩЕННЫЙ
УДОСТОВЕРЯЮЩИЙ
ЦЕНТР

Общая информация

Информация ЦС

Пользователь

Сертификаты

Запросы

Язык

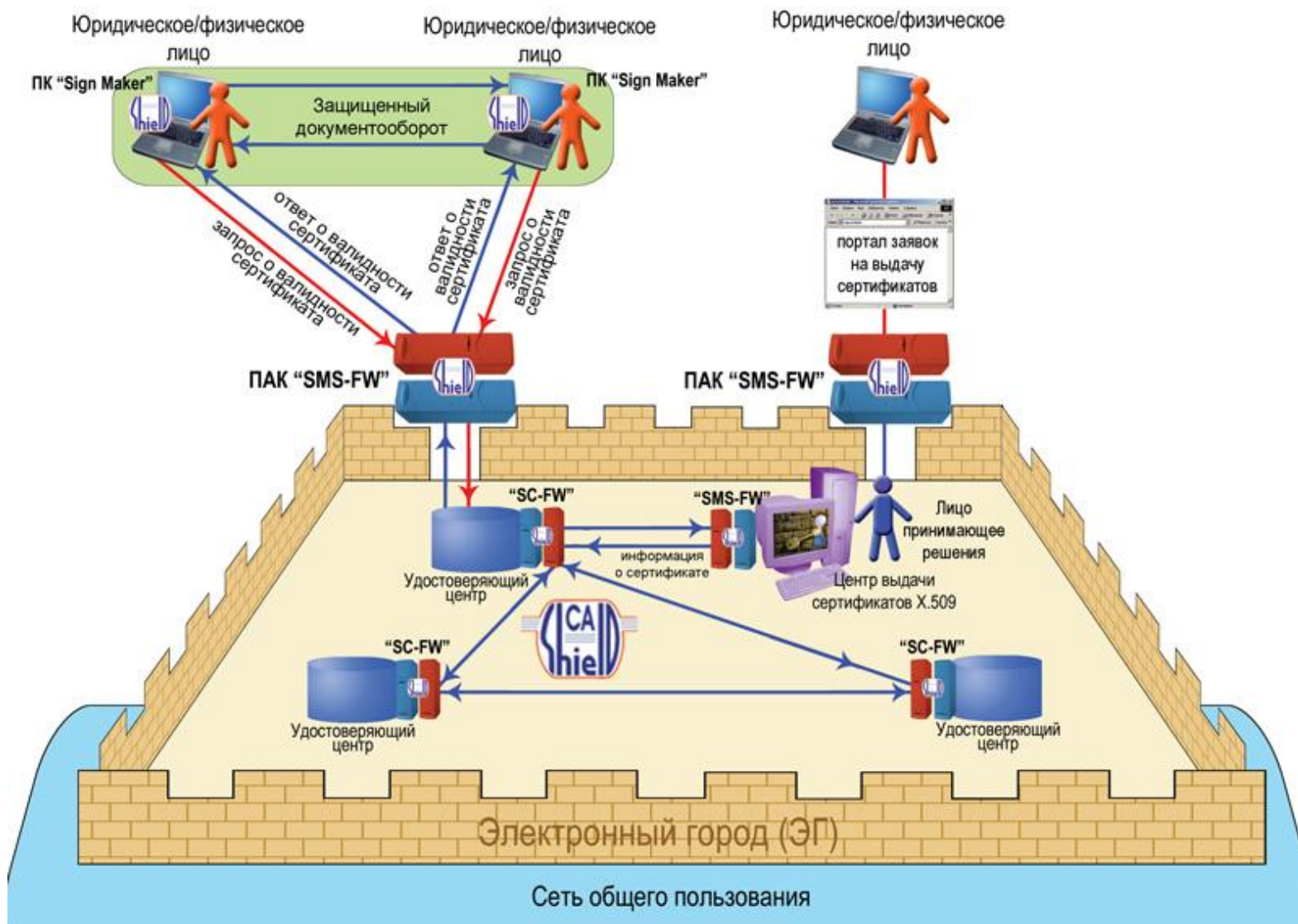
Выход

Серверная Информация для ShieldCA

Среда 16 Марта 14:35:08 UTC

Модуль	Версия
LIR-SSL	1.0
Tools	0.4.3
DB	0.9.115.2.5
Configuration	1.5.3
TRISStateCGI	1.5.5
REQ	0.9.61
X509	0.9.57
CRL	0.9.24
PKCS7	0.9.19

Электронный документооборот между юридическими и физическими лицами



Средство организации
защищенного документооборота
программный комплекс
«SignMaker»

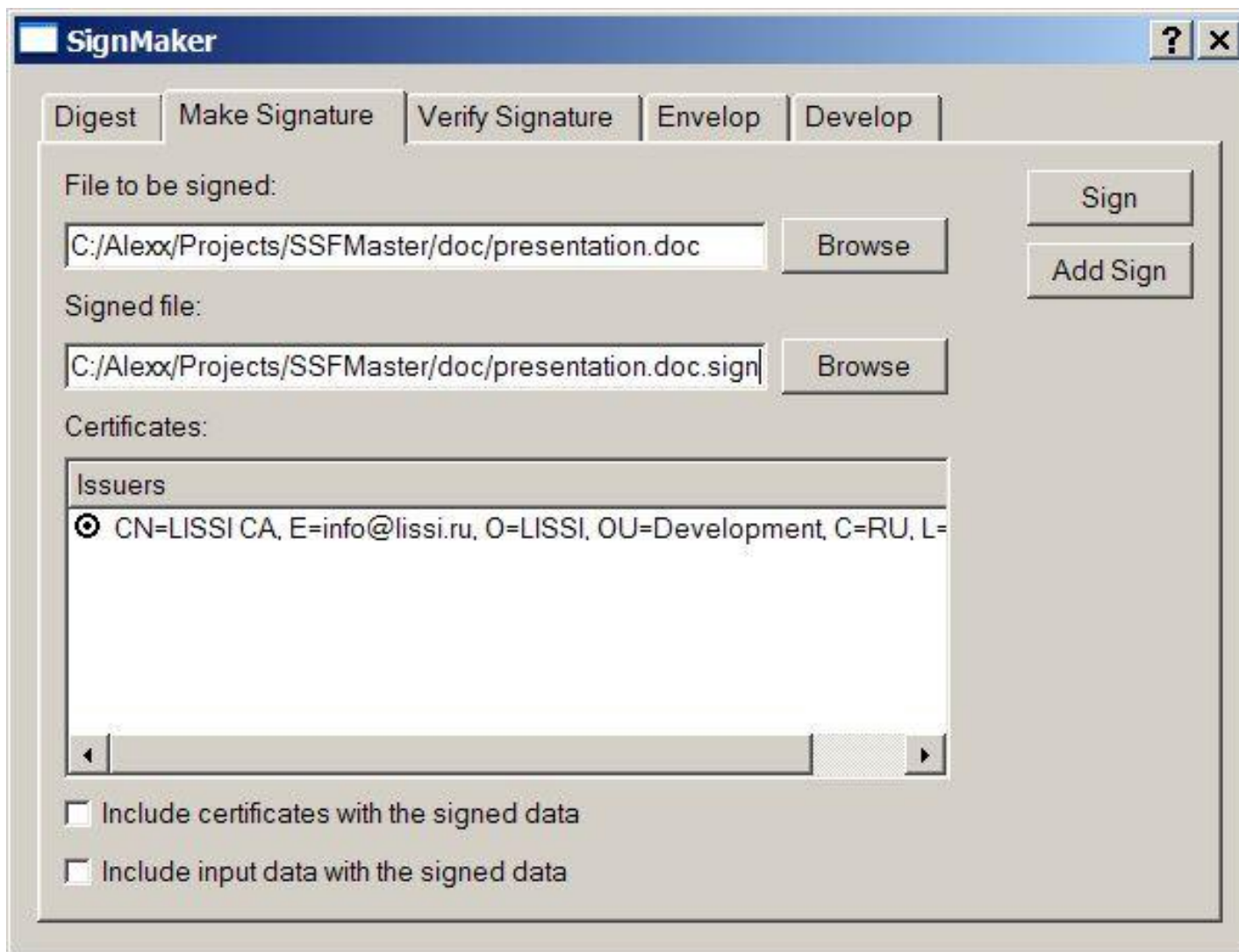
Возможности ПК «SignMaker»

- ✓ Подпись электронных документов несколькими лицами
- ✓ Проверка подписи электронных документов
- ✓ Формирование цифровых конвертов (шифрование и подпись электронных документов) для нескольких адресатов
- ✓ Извлечение электронных документов из цифровых конвертов
- ✓ Вычисление дайджеста (хэш-функции) электронного документа
- ✓ Развитый графический интерфейс

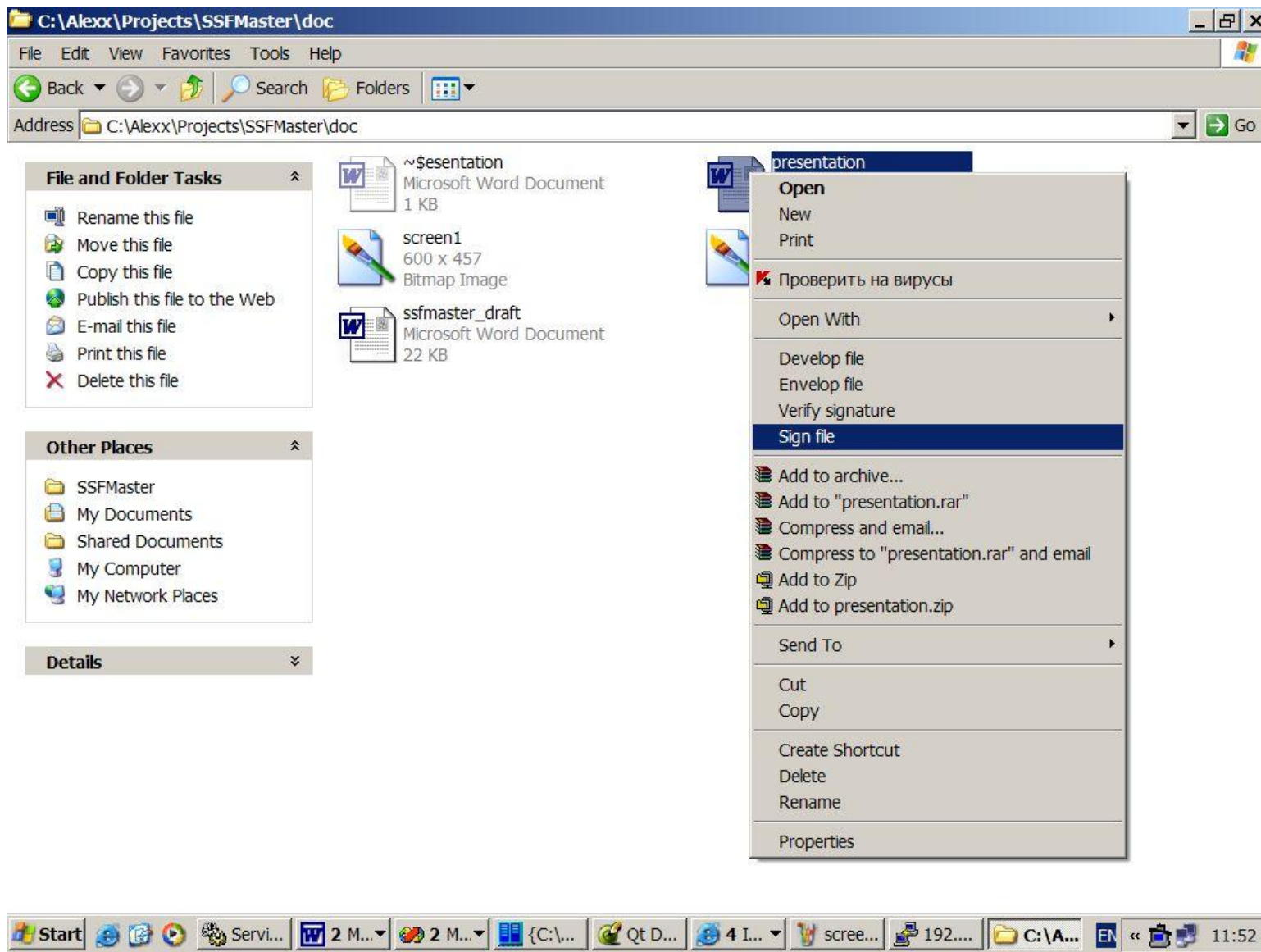
Отличительные особенности программного комплекса «SignMaker»

- ✓ Кроссплатформенность
- ✓ Использование российских криптоалгоритмов:
 - ГОСТ 28147-89
 - ГОСТ Р 34.10-2001
 - ГОСТ Р 34.11-94
- ✓ Поддержка стандартов
 - X.509 v3
 - PKCS#7
 - PKCS#9
- ✓ Использование электронных ключей для хранения ключевой информации (eToken, ruToken)

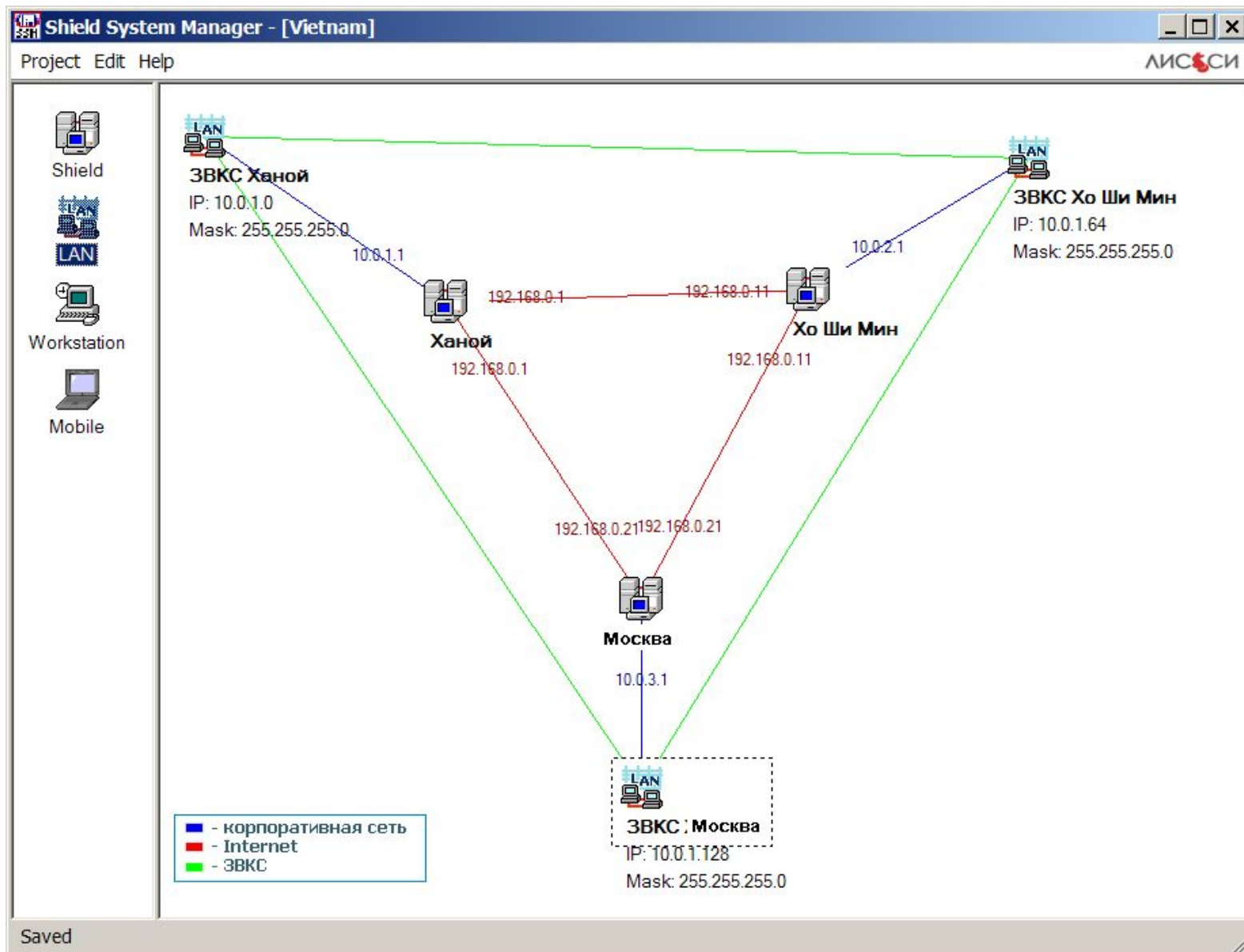
Интерфейс программного комплекса «SignMaker»



Интерфейс программного комплекса «SignMaker»



Проектирование защищенной виртуальной сети электронного города (Shield System Manager SC-FW)



Конфигурирование ЗВКС электронного города

Shield System Manager - [Vietnam*]

Project Edit Help

ЛИССИ

Shield
LAN
LAN
Workstation
Mobile

ЗВКС Ханой
IP: 10.0.1.0
Mask: 255.255.255.0

Ханой

ЗВКС Хо Ши Мин
IP: 10.0.1.64
Mask: 255.255.255.0

Хо Ши Мин

■ SecurityPolicy

Name: ЛВС_Ханой-ЛВС_Хо_Ши_Мин

ЗВКС Ханой
Gate internal server IP: 10.0.1.1
Gate external server IP: 192.168.0.1

ЗВКС Хо Ши Мин
Gate internal server IP: 10.0.2.1
Gate external server IP: 192.168.0.11

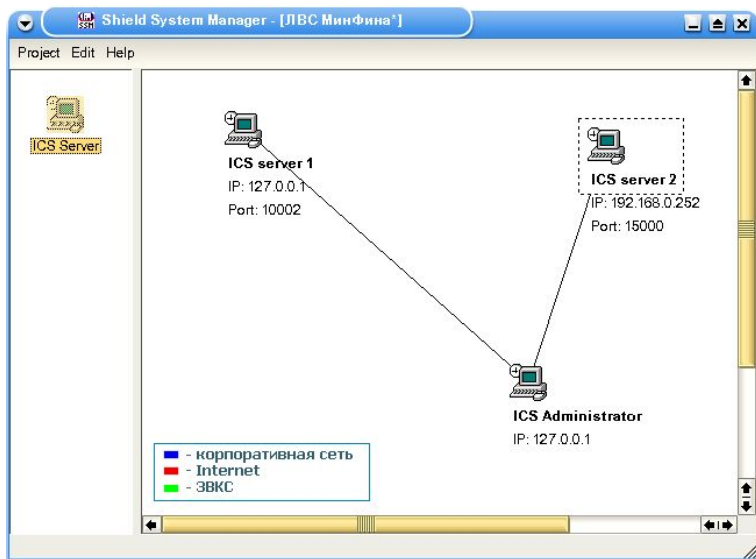
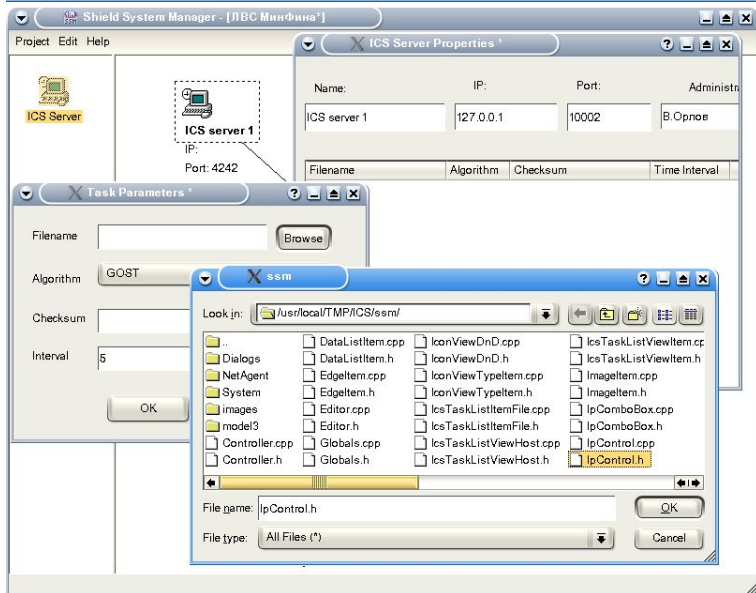
■ ESP
 Enabled Keying type: Automatic
 Authentication: Crypto:
 MD5 GOST 28147-89
 Authentication key file: Ханой-ЛВС_Хо_Ши_Мин.auth Crypto key file: аной-ЛВС_Хо_Ши_Мин.crypto
 AuthKeyLength: 128 CryptoKeyLength: 256
 Security parameters index: 0
 IPsec SA lifetime: 28800

■ IP compression: Enabled

■ IP defragmentation: Enabled

Help Cancel OK

■ - корпоративная сеть
■ - Internet
■ - ЗВКС

Shield System Manager - [ЛВС Минфина']

ICS Server Properties:

Name	IP	Port	Administ
ICS server 1	127.0.0.1	10002	В. Опное

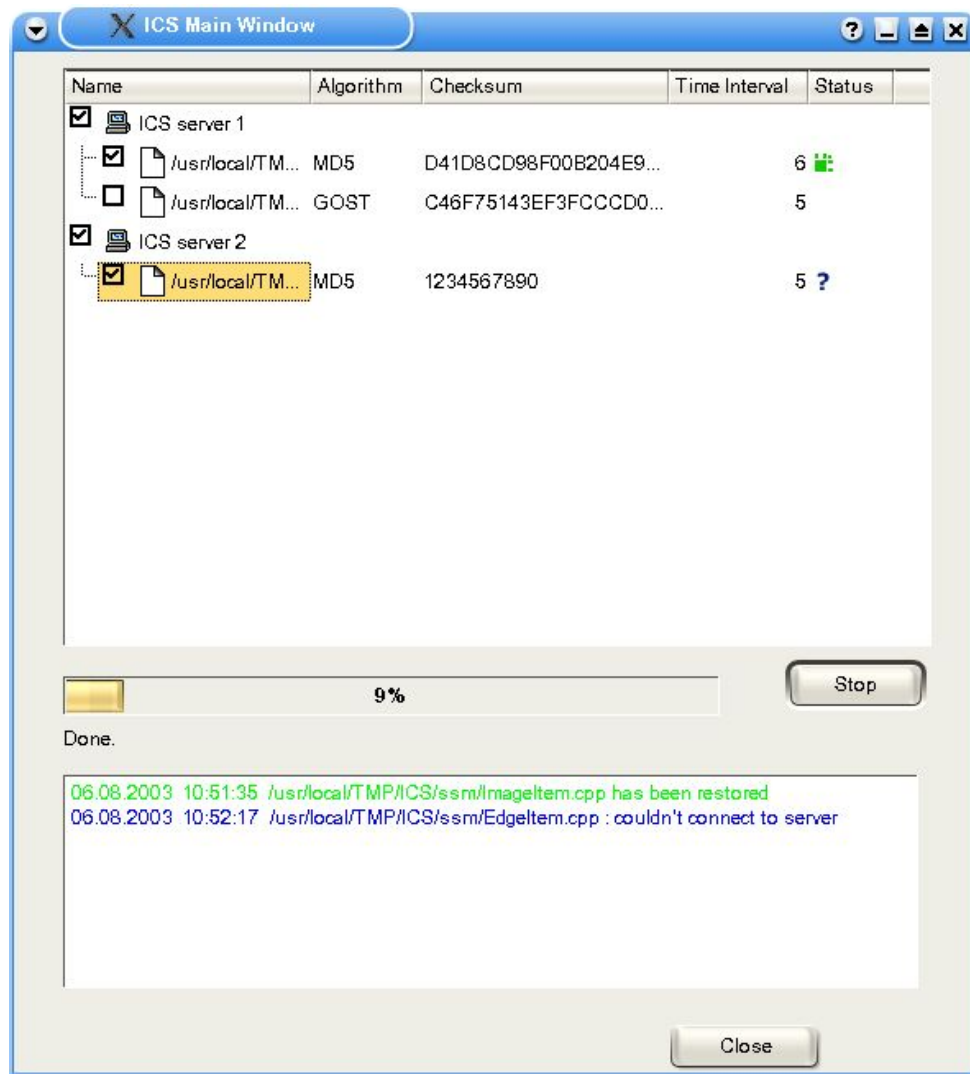
Task Parameters:

Filename	Algorithm	Checksum	Time Interval
	GOST		5

File selection dialog (Look in: /usr/local/TMP/ICS/ssm/):

- DataListtem.cpp
- Dialogs
- NetAgent
- System
- images
- model3
- Controller.cpp
- Controller.h
- DataListtem.h
- Edgeltem.cpp
- Edgeltem.h
- Editor.cpp
- Editor.h
- Globals.cpp
- Globals.h
- IconViewDnD.cpp
- IconViewDnD.h
- IconViewTypeItem.cpp
- IconViewTypeItem.h
- IcsTaskListtemFile.cpp
- IcsTaskListtemFile.h
- IcsTaskListViewHost.cpp
- IcsTaskListViewHost.h
- IcsTaskListViewItem.cpp
- IcsTaskListViewItem.h
- Imageltem.cpp
- Imageltem.h
- IpComboBox.cpp
- IpComboBox.h
- IpControl.cpp
- IpControl.h

File name: IpControl.h



ICS Main Window

Name	Algorithm	Checksum	Time Interval	Status
<input checked="" type="checkbox"/> ICS server 1				
<input checked="" type="checkbox"/> /usr/local/TM...	MD5	D41D8CD98F00B204E9...		6
<input type="checkbox"/> /usr/local/TM...	GOST	C46F75143EF3FCCCD0...		5
<input checked="" type="checkbox"/> ICS server 2				
<input checked="" type="checkbox"/> /usr/local/TM...	MD5	1234567890		5 ?

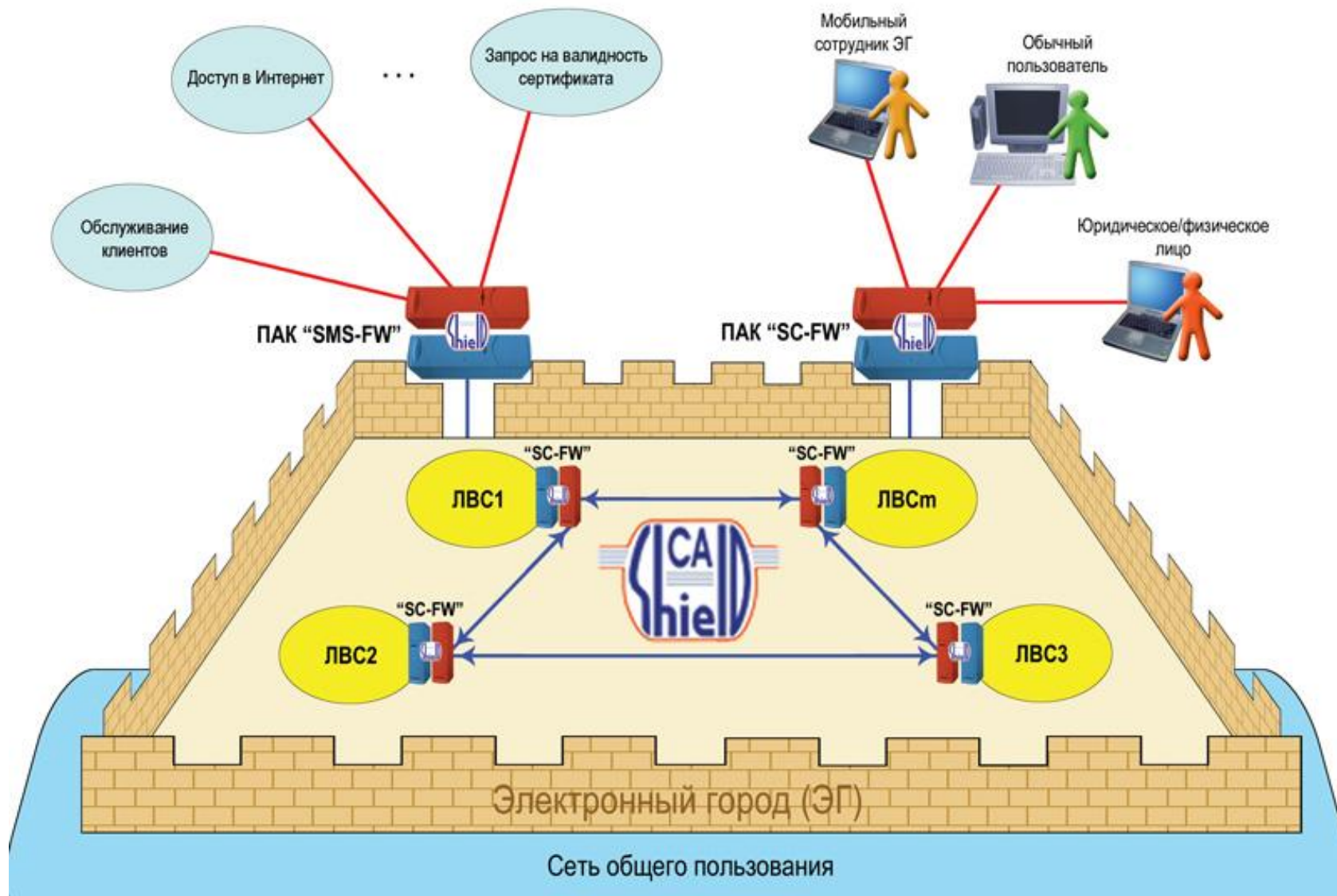
Progress: 9%

Done.

```
06.08.2003 10:51:35 /usr/local/TMP/ICS/ssm/Imageltem.cpp has been restored
06.08.2003 10:52:17 /usr/local/TMP/ICS/ssm/Edgeltem.cpp : couldn't connect to server
```

Close

Электронный город



Спасибо за внимание

Наши координаты:

<http://www.lissi.ru>

E-mail: info@lissi.ru

Тел.: +7 095 745-9988

