Технология «тонкого клиента» для защиты информации в системах терминального доступа

Сергей Александрович Буров,
ЗАО «Фирма НТЦ КАМИ»

2 ноября 2010 г.,
г. Ярославль

План презентации

1. Базовые принципы решения
2. Архитектура решения
3. Возможности решения
   3.1. Стандартные возможности
   3.2. Принципиально новые
4. Система защиты информации
   4.1. Принципы реализации
   4.2. Динамика
5. Преимущества решения «КАМИ-Терминал»
6. Экономические аспекты
7. Успешные внедрения
8. Вопросы

1. Базовые принципы решения

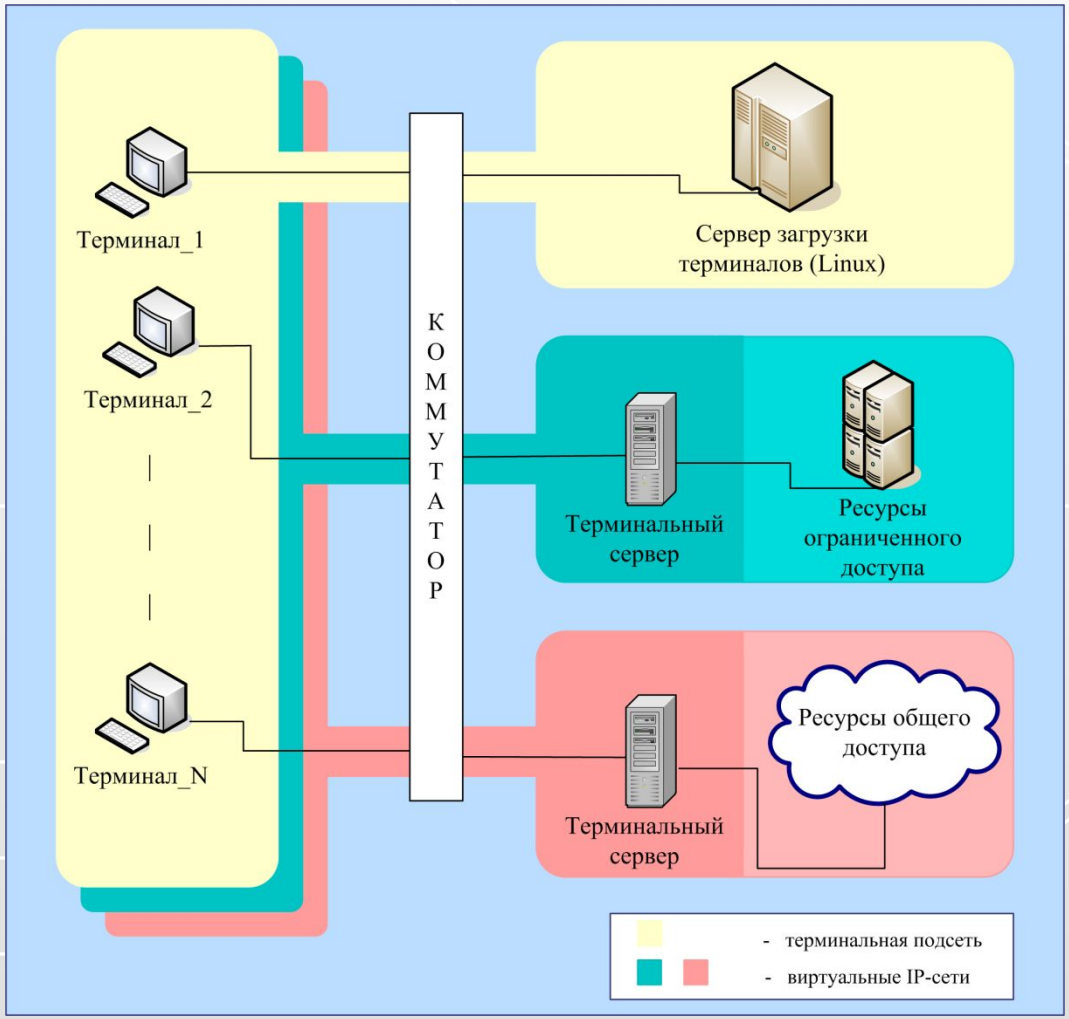
- безопасность;
- надёжность;
- масштабируемость;
- модульность архитектуры;
- экономическая привлекательность.

2. Архитектура решения

Система включает в себя:

- терминальные станции (тонкие клиенты);
- выделенный сервер загрузки терминалов;
- подсеть терминалов;
- терминальные серверы;
- сегменты существующей информационной системы с различными уровнями доступа (защиты) информации.

2. Архитектура решения



3.1. Стандартные возможности решения

- обеспечение высокой надёжности СТД за счёт развёртывания кластерных систем, состоящих как из терминальных серверов, так и серверов загрузки и управления;
- масштабируемость системы до уровня ИС предприятия при практически отсутствующей потребности существенной модернизации терминальных станций и клиентского СПО;
- использование серверных платформ RedHat Enterprise Linux или SuSE Linux Enterprise Server, позволяющих обеспечить высокую готовность и производительность сервера загрузки и управления;
- поддержка возможности использования на терминальном устройстве внешних USB-накопителей (флэш-дисков), USB-устройств типа floppy и CD-ROM, принтеров;
- поддержка звука на терминальном устройстве.

3.2. Принципиально новые возможности решения

- построение системы разграничения доступа к информационным ресурсам с различными уровнями защиты информации с использованием идеологии виртуальных IP-сетей (VLAN);
- формирование образа загружаемой на терминале ОС в адаптивном режиме в соответствии с полномочиями пользователя и характером решаемых задач;
- предоставление пользователю одновременного запуска нескольких Windows сессий (протоколы ICA, RDP) на клиентском рабочем месте с переключением между ними в процессе работы. Каждая сессия запускается на отдельной виртуальной консоли;
- создание многоуровневой системы защиты информации, начиная с формирования среды доверительной загрузки ОС терминала на локальном уровне (сразу после включения питания).

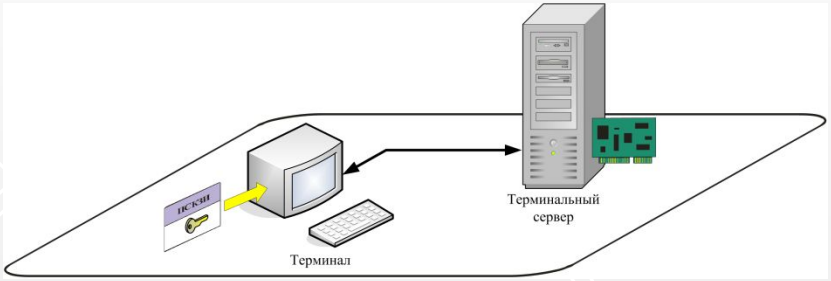
4. Система защиты информации (вариант терминала)

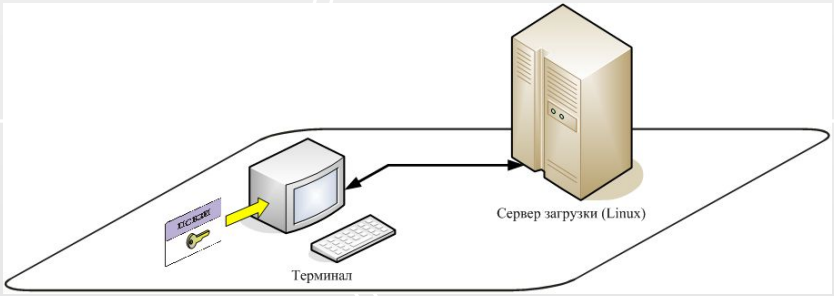
4.1. Система защиты информации (принципы реализации)

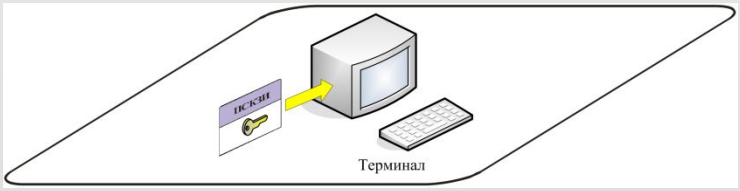
	Клиентское рабочее место	Серверная система
Аппаратный уровень (конфигурация)	▪ Исключение устройств долговременного хранения данных; ▪ Минимальное необходимое количество портов ввода/вывода.	—
Аппаратно-программный уровень	▪формирование среды доверительной загрузки ОС (КАМИ-BIOS); ▪ аутентификация пользователя терминала и затем пользователя Windows при обращении к терминальному серверу ▪(ПСКЗИ).	▪Сервер загрузки терминалов (Linux) ▪ Верификация процесса «отгрузки» образа ОС на терминал; ▪ Терминальные серверы (Windows) ▪ Разграничение полномочий администратора СТД и администратора информационной безопасности СТД. ▪ (АМДЗ + СПО)
Программный уровень	• Минимальный слой ПО, необходимый для подключения к серверу загрузки терминалов и обеспечения функциональности СКЗИ; • Усеченный вариант загружаемого ядра ОС (Linux); • Работа ОС терминала только в ОЗУ.	▪ Сервер загрузки терминалов (Linux) ▪ Предоставление загружаемых на терминалы образов ОС в соответствии с полномочиями пользователей («принцип минимума полномочий»); ▪ Аудит работы терминалов ▪Терминальные серверы (Windows) ▪ Выполнение роли «посредника» для доступа к информационным ресурсам.

4.2. Система защиты информации (динамика)

1. Локальные процессы
2. Сетевая загрузка ОС
3. Запуск клиентских приложений

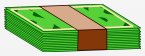






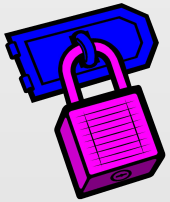
«КАМИ-Терминал» – комплексное системное решение, предназначенное для создания защищенных автоматизированых систем, и обеспечивающее эффективный и безопасный доступ к сетевым информационным ресурсам на принципах технологии терминального доступа.

5. В чем преимущества решения КАМИ-Терминал?



Вы экономите средства:
- на техническую поддержку
- на программное обеспечение
- на модернизацию парка оборудования

Вы экономите время:
- на восстановление работоспособности оборудования на рабочих местах пользователей
- на установку программного обеспечения и оборудования



Вы обеспечиваете сохранность Вашей информации:
- централизованно управляя доступом к ней
- централизованно защищая от потери в случае выхода из строя оборудования и действий вредоносных программ
-программный комплекс «Ками-Терминал» сертифицирован ФСТЭК России по 4 уровню НДВ и на 5 класс РД СВТ

Вы получаете квалифицированную техническую поддержку разработчика:
- если терминал что-то «не умеет» – мы постараемся «научить» его согласно Вашим потребностям!
- решение разработано компанией «Фирма НТЦ КАМИ»

kami
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

Продукт сертифицирован согласно требованиям безопасности информации:

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 2013

Выдан 14 января 2010 г.
Действителен до 14 января 2013 г.

Настоящий сертификат удостоверяет, что **программный комплекс «КАМИ-Терминал»** разработанный и производимый ЗАО «Фирма Научно-технический центр КАМИ» в соответствии с техническими условиями ШСКД.00033-01 93, реализующий терминальный доступ по протоколам ICA, RDP, X11, является программным средством защиты от несанкционированного доступа к информации, не содержащей сведения, составляющие государственную тайну, и соответствует требованиям руководящих документов «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) - по **5** классу защищенности и «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) - по **4** уровню контроля.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ЗАО «НПП «БИТ» (аттестат аккредитации от 11.09.2003 № СЗИ RU.473.Б022.047) – техническое заключение от 06.11.2009, и экспертного заключения от 16.11.2009 органа по сертификации ФГУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 26.04.2005 № СЗИ RU.840.A92.007).

Заявитель: ЗАО «Фирма Научно-технический центр КАМИ»
Адрес: 125480, г. Москва, ул. Героев Панфиловцев, д. 10
Телефон: (495) 948-4330

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль её соответствия требованиям указанных в настоящем сертификате руководящих документов осуществляется испытательной лабораторией ЗАО «НПП «БИТ».

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

А.Гапонов

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации 14 января 2010 г.

6. Экономические аспекты

- сбалансированная стоимость терминальной станции и решения в целом;
- возможность использования имеющегося парка Intel-совместимых персональных компьютеров , что дает возможность сохранения уже вложенных в инфраструктуру инвестиций;
- применение ОС Linux;
- снижение затрат на проведение плановой модернизации ИС за счёт обновления программной и аппаратной составляющих, используемых исключительно на серверной стороне;
- практическое полное исключение затрат на «локальное администрирование».

7. Успешные внедрения

- Пятилетний опыт реализации систем терминального доступа в подразделения Министерства Обороны (на базе ОС МСВС);

- Выполнение опытно-конструкторской работы по созданию СТД в информационно коммуникационной системе Совета Федерации (2006 – 2008 гг.).

- Решение Центрального Банка России о принятии решения Ками-Терминал в качестве типового терминального решения в информационной структуре (2008год). Начало внедрения в управлениях территориальных подразделений банка (2008-2010 гг.).

8. Ваши вопросы ?

kami
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

Наши координаты

Россия,
125480 г. Москва, ул. Героев Панфиловцев, д. 10
Тел.: (495) 948-43-30
150000 г. Ярославль, ул. Чайковского, д. 40а,
Тел.: (4852) 727-555
www.kami.ru
info@kami.ru

kami
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

Спасибо за внимание !