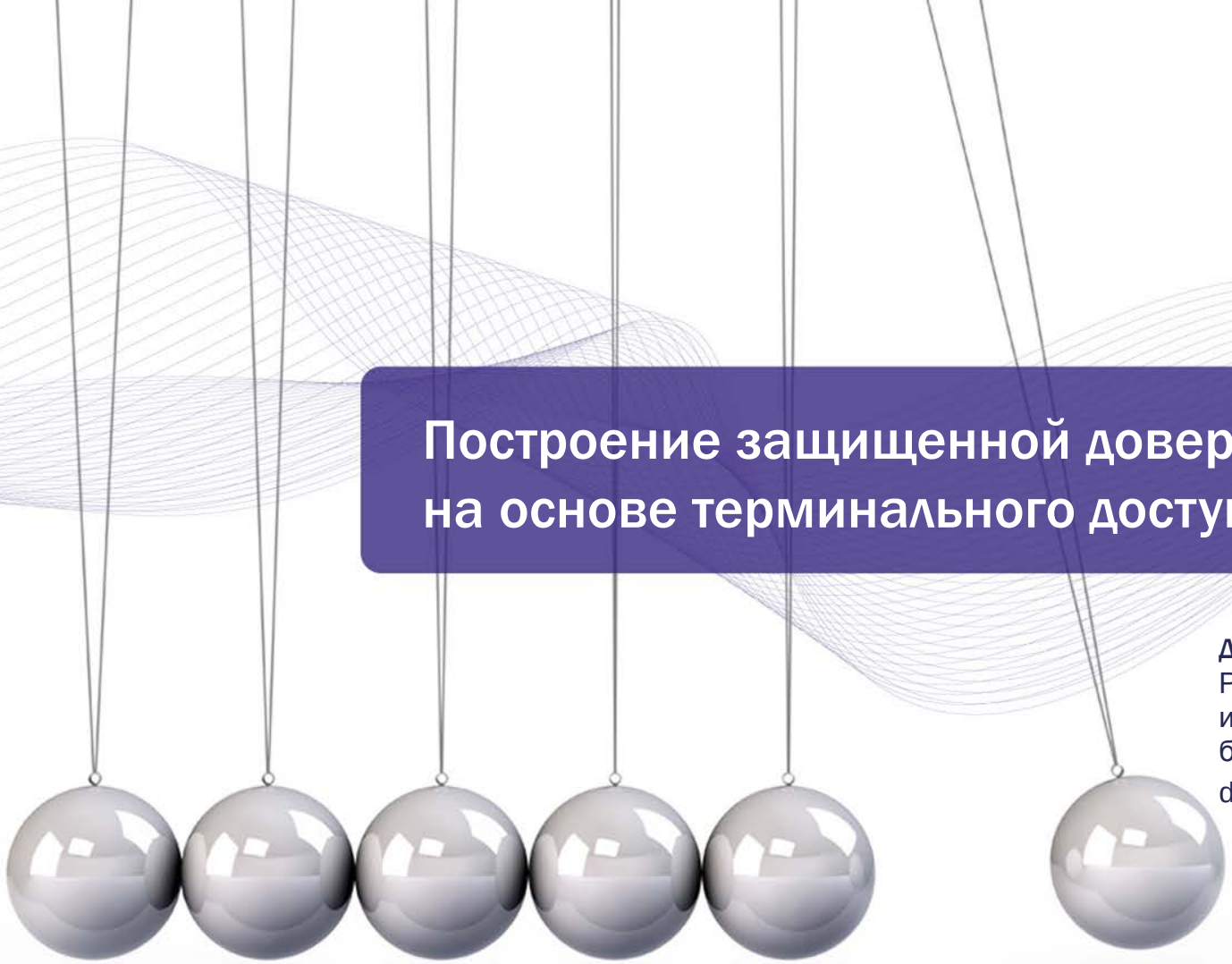
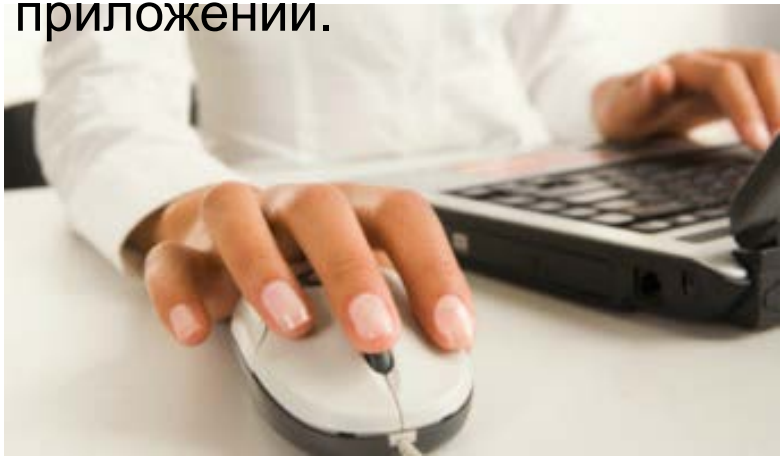
Построение защищенной доверенной среды на основе терминального доступа



Дмитрий Огородников
Руководитель направления информационной безопасности
d_ogorodnikov@in-line.ru

«Тонкий клиент»

Тонким клиентом называется устройство ввода и отображения информации (терминал). Физически тонкий клиент это компактный компьютер без жесткого диска, загрузка основной операционной системы которого происходит на сервере. Все пользовательские приложения выполняются на терминальном сервере приложений.

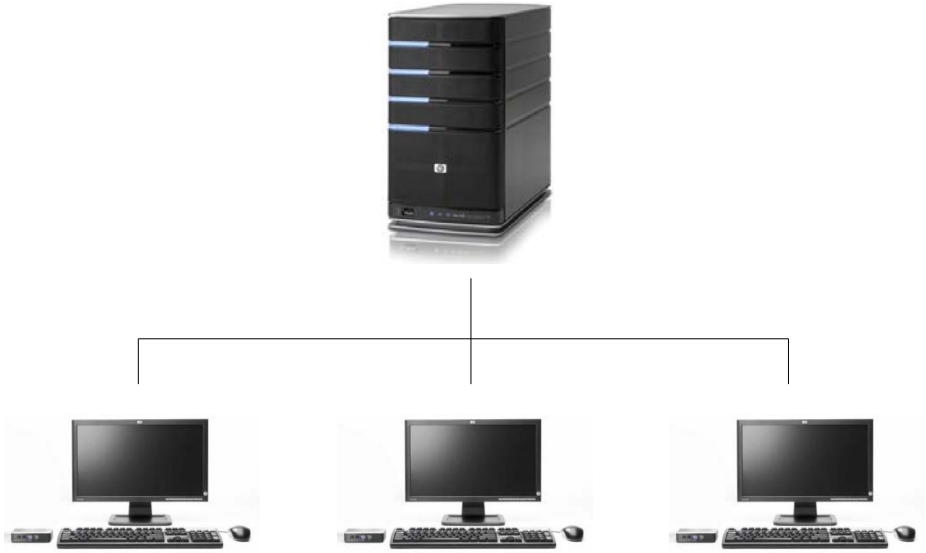


Области применения – замена стандартных персональных компьютеров.

Тонкий клиент предназначен для широкого круга офисных программ.

Сравнение

Сеть состоит из полнофункциональных рабочих станций и файлового сервера, все процессы выполняются на рабочих станциях пользователей.
Управление не централизовано.

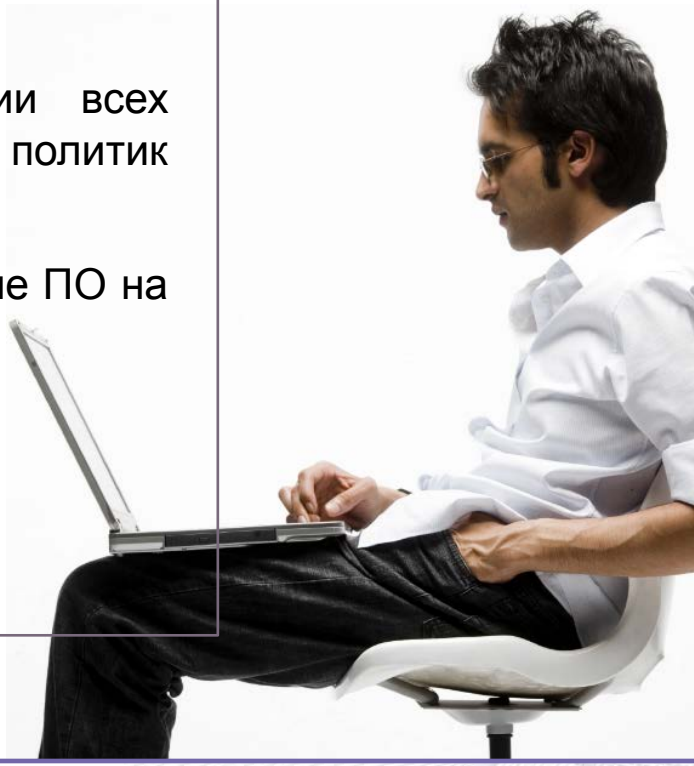


Альтернатива – сеть, построенная с использованием технологии тонких клиентов. Все функции централизованы. Тонкий клиент служит средством ввода и отображения информации.

Преимущества использования

Простота администрирования

- только серверное администрирование
- нет необходимости в постоянном обслуживании всех рабочих станций организации и контроле политик безопасности на рабочих местах
- централизованная установка программ и обновление ПО на сервере
- быстрое создание новых рабочих мест
- простота замены и установки нового оборудования
- возможность удаленного администрирования



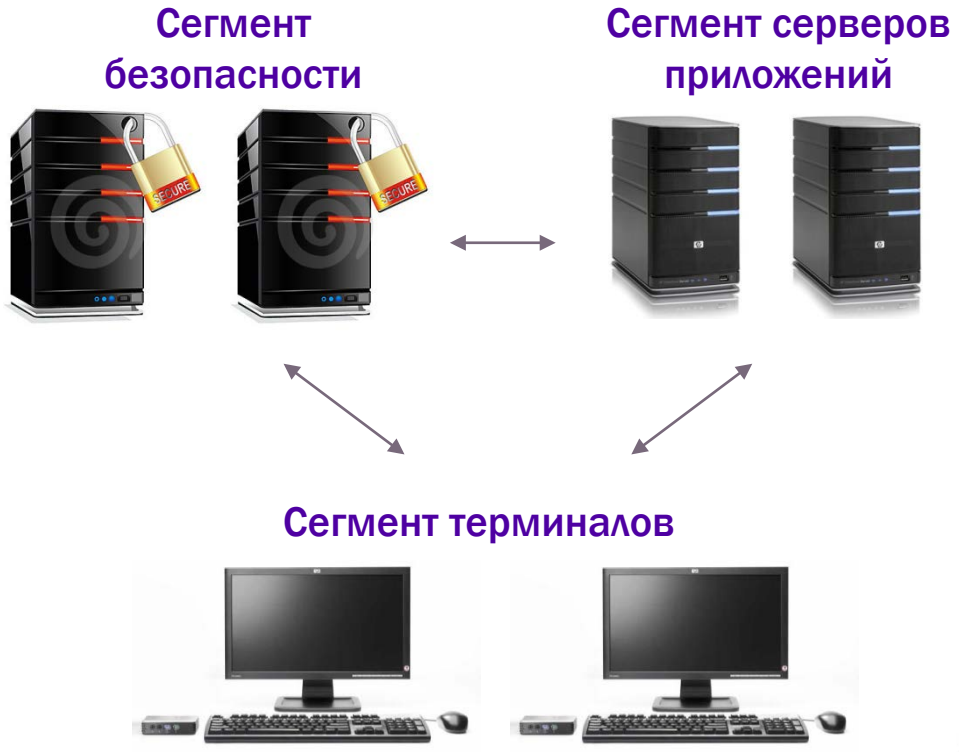
ПАК «Тринити»

Программно-аппаратный комплекс (ПАК) «Тринити» представляет собой устройство, предназначенное для реализации технологии защищенного терминального доступа, обеспечивающей обработку информации в замкнутой и доверенной аппаратно-программной среде.

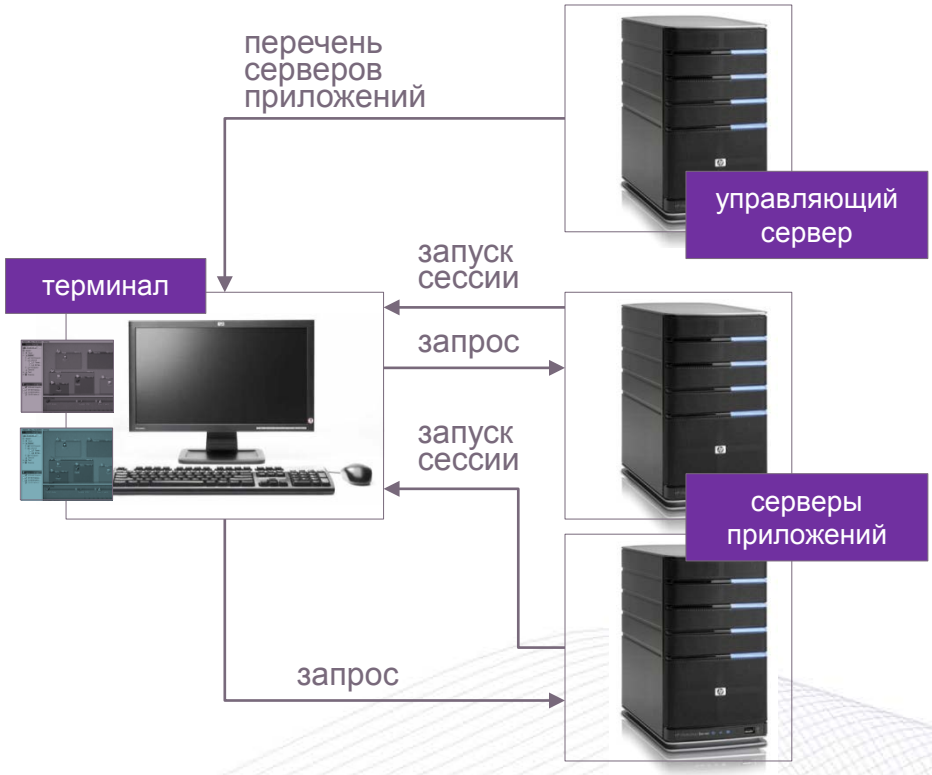
Является собственной разработкой компании «Setec»

Архитектура

Комплекс обеспечивает защиту от НСД к информации в автоматизированных системах, работающих в архитектуре тонкого клиента по протоколу RDP на основе терминального сервера Microsoft Terminal Services версии 2008 и более поздних версиях.



Логика работы



в процессе загрузки операционной системы с управляющего сервера терминальная станция получает перечень серверов приложений и набор клиентских приложений для связи с ними

терминалы формируют запросы для серверов приложений

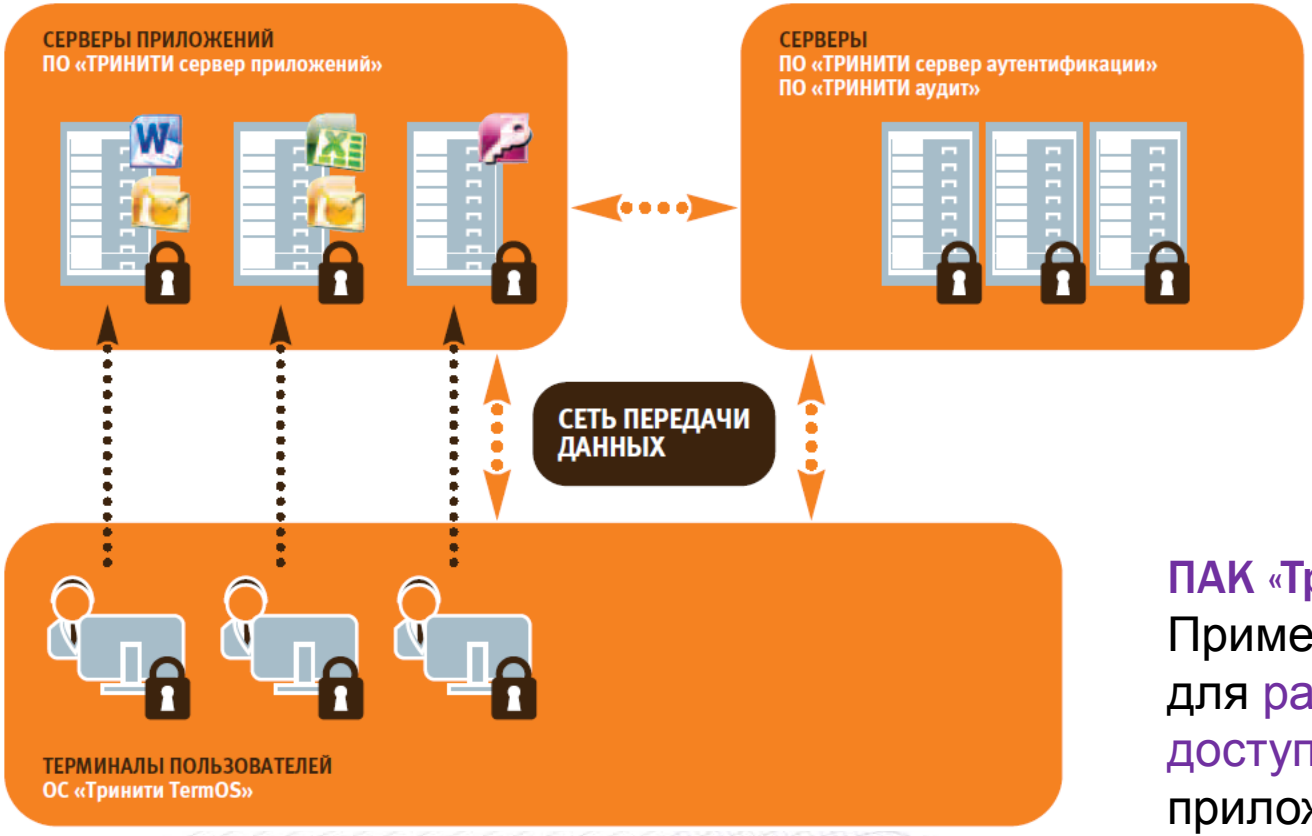
серверы обеспечивают запуск и трансляцию сессий на терминал

сессии отображаются на различных независимых виртуальных консолях, что позволяет исключить возможность взаимодействия между ними

Функциональные возможности

- удаленный запуск и завершение прикладных приложений пользователя на терминальном сервере
- возможность подключения к терминалу различных периферийных устройств
- возможность работы пользователей в различных контурах, в которых может обрабатываться информация разного уровня конфиденциальности
- возможность работы со съемными носителями, принтерами, сканерами
- возможность блокировки и разблокировки сеансов работы
- Возможность балансировки приложений

Возможности использования



ПАК «Тринити»
Пример использования для разграничения доступа к ресурсам и приложениям

Возможности использования

Коммерческие организации

Формирование технологии защищенного удаленного доступа сотрудников компании к внутрикорпоративным ресурсам. Возможность обеспечения безопасности удаленной работы.

Финансы

Перевод дополнительных офисов, отделений и филиалов банка на защищаемый терминальный доступ с целью снижения затрат на обслуживание ИТ-инфраструктуры и повышения уровня безопасности удаленных площадок банка. Создание защищенного платежного сегмента банковской ИС.

Промышленность

Перевод инфраструктуры операторов АСУТП на инфраструктуру тонких клиентов ПАК «Тринити».

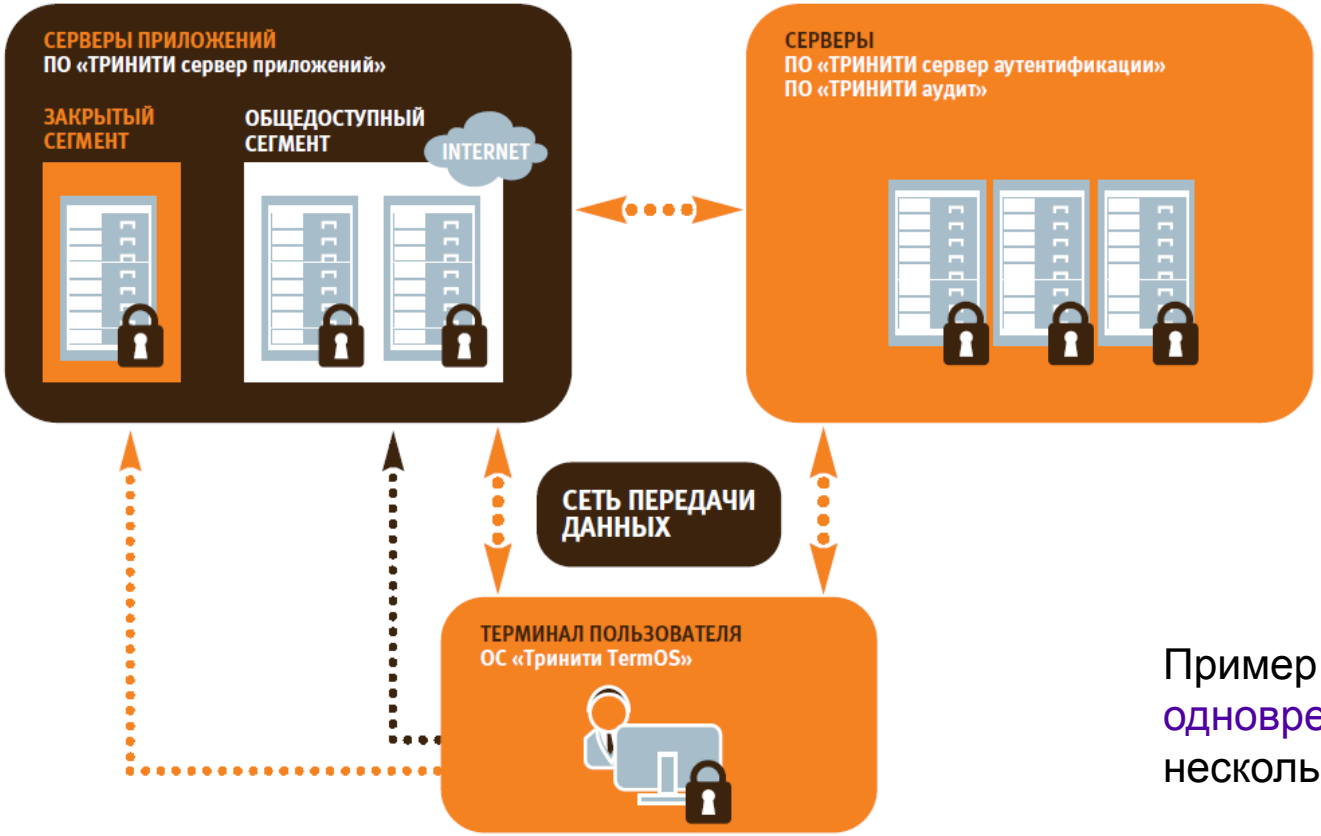
Государство

Миграция на инфраструктуру тонких клиентов с целью унификации и стандартизации рабочих мест, а также выполнения требований законодательства и действующей нормативной базы регуляторов.

Ритейл

Миграция существующих киосков самообслуживания на технологию защищенных тонких клиентов, создание защищенной мобильной сети торговых представителей.

Возможности использования



Пример организации одновременной работы в нескольких контурах

Возможности использования

Государство

Создание нескольких контуров обработки информации, разделяемых по виду информации, уровню ее конфиденциальности и требований к защите с возможностью работы с ними переключая виртуальные рабочие столы.

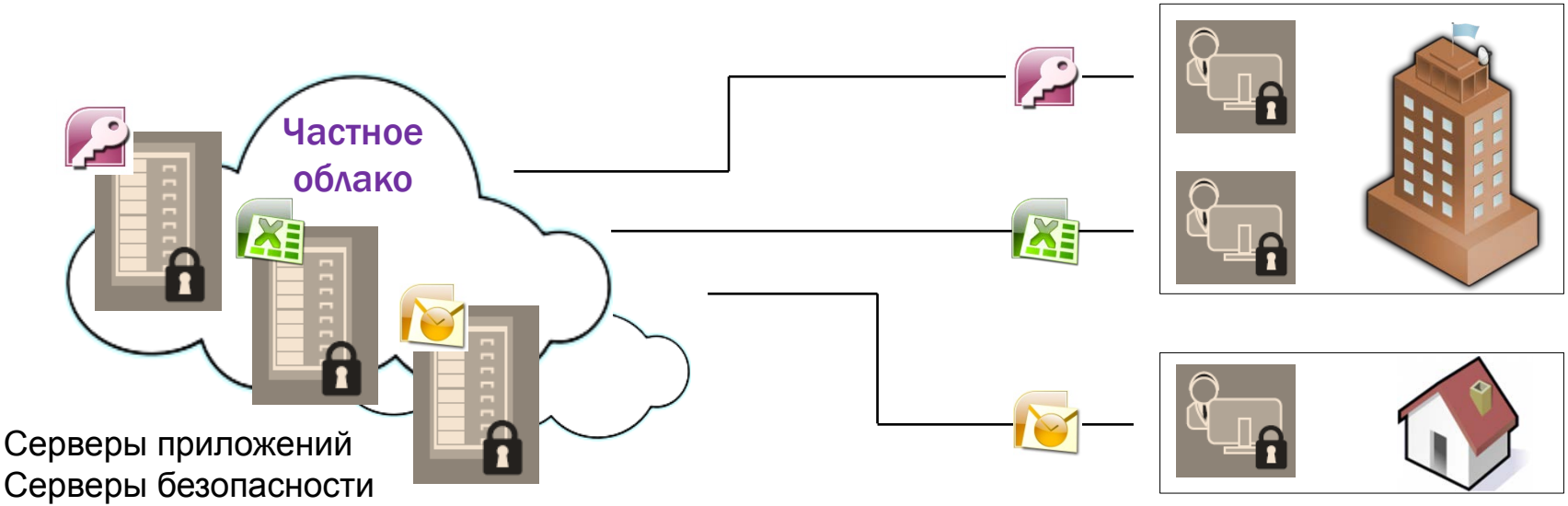
Финансы

Использование одного терминального устройства пользователя для доступа к различным банковским автоматизированным системам: АБС, корпоративные сервисы, электронный документооборот, процессинг, казначейские системы, торговые площадки, биржи и т.д.
Новый уровень безопасности, удобства и сервиса при взаимодействии с клиентами юридическими лицами по системе типа Клиент-Банк.

Промышленность

Организация изолированных друг от друга контуров корпоративной информационной системы, доступ к ресурсам которых пользователь получает со своего терминала. Таких контуров может быть несколько: контур для доступа в Интернет, технологический сегмент – САПР, суперЭВМ, математическое моделирование, производство, расчеты, испытания, контур для общекорпоративных сервисов – бухгалтерия, финансовый учет, заявки в бюро пропусков, система ЭДО, складской учет и пр.

Возможности использования



Организация удаленного доступа к приложениям, размещенными в облачной инфраструктуре.

Состав комплекса

ТЕРМИНАЛ	КОНСОЛЬ АДМИНИСТРАТОРА	СЕРВЕР ХРАНЕНИЯ ДАННЫХ ПОЛЬЗОВАТЕЛЯ	СЕРВЕР ПРИЛОЖЕНИЙ	СЕРВЕР БЕЗОПАСНОСТИ
Модуль доверенной загрузки «Тринити-АПМДЗ»				
Операционная система терминала			Система разграничения доступа	Сервис распространения ОС
				Сервис аутентификации
Модуль безопасности	Консоль администратора	Данные пользователя	Сервис администрирования	Сервис балансировки нагрузки
Модуль аудита				
СКЗИ				

Терминал пользователя

- функционирует под управлением собственной доверенной ОС, созданной на базе ядра Linux
- устанавливает RDP сессии с серверами приложений. Отображает окно приложения, запущенного пользователем
- поддержка режима многоконтурной работы. Достигается за счет использования виртуальных рабочих столов полностью изолированных друг от друга
- встроенные криптографические функции на базе СКЗИ «КриптоПРО CSP». Обеспечивают криптографическую защиту данных, передаваемых по каналу связи

Аппаратные средства терминала

Параметр	Конфигурация 1	Конфигурация 2
Процессор	VIA Eden ULV Processor 500Mhz / 1GHz	Intel® AtomTM Processor N270 1.6GHz
Оперативная память	1GB DDR2 667MHz SDRAM	2GB DDR2 667MHz SDRAM
Порты ввода-вывода	4 USB, 1 x DVI port и др.	6 USB, 1 x VGA (DB-15), 1 x DVI port
Ehternet	1 порт RJ-45 (Gigabit LAN)	2 порт RJ-45 10/100/1000 Mbps (Gigabit LAN)
Максимальное разрешение	до 1920 x 1080 @ 60Hz	до 1920 x 1080 @ 60Hz
ДхШхВ	155.8 мм x 33.5 мм x 186.8 мм	243мм x 55 мм x 198 мм
Вес	860 грамм	860 грамм

Модуль безопасности

Модуль безопасности – прошивка терминала.
Может быть установлен в произвольный ПК или USB-носитель.

Функции:

- аутентификация пользователей
- доверенная загрузка образа операционной системы по сети
- проверка целостности программных и аппаратных средств терминала
- шифрование каналов связи средствами КриптоПРО CSP 3.6

Консоль администратора

Консоль администрирования представляет собой графический интерфейс и интерфейс командной строки для предоставления всех необходимых функций администрирования системы.
Администрирование системы может производиться с любого терминала.

- создание, удаление и модификация профилей пользователей, терминалов, серверов, приложений
- сбор информации об установленных приложениях на каждом сервере приложений
- публикация для пользователя или пользователей приложения или группы приложений
- привязка пользователей к терминалам
- назначение пользователям прав доступа и т.д.

Сервер хранения данных

Сервер хранения данных предоставляет сервис для хранения пользовательских профилей, файлов и папок.

Создан на основе OpenLDAP
Возможна интеграция с Active Directory

Функции:

- хранение профилей пользователей
- хранение данных (файлов и папок) пользователей
- предоставление сервиса доступа к данным пользователей по протоколу SMB.

Сервер приложений

- защищенный сервер приложений. Обеспечивает контролируемый запуск пользовательских приложений на сервере.
- разграничение доступа к ресурсам сервера приложений. Обеспечивает разграничение доступа к ресурсам сервера приложений.
- публикация приложений. Пользователю можно назначить набор доступных ему приложений. Другие приложения, установленные в системе будут не только не доступны, но и не видны для пользователя.
- кластеризация серверов приложений. Возможность кластеризации и балансировки нагрузки на серверы приложений.

Аппаратные средства

сервера приложений

Конфигурация сервера приложений для поддержки одновременной работы 50 пользователей

Процессор:
2x Intel Xeon E5640 (2,66GHz, LGA1366, 12288Kb)

Оперативная память:
12GB DDR-III PC3-10600 ECC Registered

Ehternet:
2x Intel® 82574L Gigabit Ethernet

Форм-фактора:
1U Rackmount

Средняя цена – 130 000 рублей

Сервер безопасности

- сервис аутентификации
- сервис балансировки нагрузки
- сервис распределения операционной системы

Сервер аутентификации (сервер безопасности)

Единственная точка входа в систему. Точка входа в систему всех пользователей. Обеспечивается аутентификация и авторизация пользователей.

Аутентификация компонентов системы. Обеспечивает аутентификацию пользователей, серверов приложений и терминалов в системе.

Привязка пользователя к терминалу. Пользователь может работать только с того терминала, который ему назначил администратор.

Аудит. Обеспечивает протоколирование событий безопасности, происходящих в системе.

Сервис балансировки нагрузки

Обеспечивает балансировку нагрузки на серверы приложений и сервис аутентификации.

- Инициатором соединения всегда является клиент сервиса балансировки
- После установки соединения общение с сервисом происходит по схеме «запрос-ответ»
- При выполнении любого запроса происходит проверка идентификатора сессии пользователя, используя сервис аутентификации

Сервис распределения ОС

Компонент обеспечивает передачу операционной системы на терминал пользователя. При этом обеспечивается контроль целостности операционной системы.

Благодаря тому, что сервис распространения ОС терминала является независимым от других компонентов, то возможно его кластеризовать в режиме балансировки нагрузки.

Аппаратные средства

сервер безопасности

Конфигурация сервера безопасности с установленными сервисами аутентификации, балансировки нагрузки и распространения ОС и данных пользователя для поддержки одновременной работы до 500 пользователей.

Процессор:
2x Intel Xeon E5640 (2,66GHz, LGA1366, 12288Kb)

Оперативная память:
4GB DDR-III PC3-10600 ECC Registered

Ehternet:
2x Intel® 82574L Gigabit Ethernet

Форм-фактора:
1U Rackmount

Средняя цена – 50 000 рублей

Тринити-АПМДЗ

Тринити-АПМДЗ представляет собой аппаратно-программный модуль доверенной загрузки. Он может использоваться для защиты отдельных компьютеров от НСД.

- усиленная аутентификация оборудования и пользователей в системе
- защита от загрузки с внешних носителей
- обеспечение целостности операционной системы компьютера
- обеспечение целостности аппаратной конфигурации компьютера
- сторожевой таймер
- удаленное управление

Преимущества Тринити-АПМДЗ

- Поддержка большого количества аппаратных платформ (тестирование проводилось более, чем на 20 платформах)
- Интеграция с ПАК «Тринити» (Тринити-АПМДЗ может использоваться в составе ПАК «Тринити», обеспечивая при этом единое комплексное решение по защите информации)
- Возможность работы в ноутбуках и планшетных компьютерах (благодаря наличию версии для шины miniPCI-express)
- Простота администрирования (наличие удаленного управления значительно облегчает процедуру администирования комплекса)
- Улучшенные возможности по обеспечению защиты информации (возможность двухфакторной аутентификации, контроль программной и аппаратной среды)

Ключевые особенности

- Все технологические сервисы работают под управление ОС семейства Linux
- Возможность передачи звука и видео высокой степени точности
- Поддержка IP-телефонии
- Серверы приложений функционируют под управление ОС Windows 2008 R2
- Поддержка многоконтурности - возможности обработки на одном терминале информации разного уровня конфиденциальности
- Обеспечение балансировки приложений
- Поддержка технологии VDI

Возможности по защите информации

- усиленная аутентификация пользователей
- аутентификация компонентов в системе
- разграничение доступа к приложениям, данным пользователя, съёмным носителям, периферийным устройствам и т.д.
- динамические учётные записи пользователей, пока пользователь не установил RDP-сессию с сервером приложений его учётная запись Windows на сервере приложений отсутствует
- возможность блокировки загрузки с внешних носителей
- возможность привязки пользователя к терминалу
- возможность привязки пользователей к USB-носителям
- шифрование USB-носителей

Поддерживаемое ПО

Некоторое ПО, тестированное на совместимость с ПАК «Тринити»

- Офисный пакет Microsoft Office 2007/2010/2012
- Браузеры Microsoft IE, Google Chrome, Mozilla Firefox, Opera
- Почтовые клиенты MS Outlook, LOTUS Notes.
- AutoCAD – САПР для 2D и 3D-проектирования. Тестирование проводилось как 2D моделей, так и 3D моделей.
- Avaya One X Communicator – функции IP-телефонии
- CitectSCADA - система мониторинга, управления и сбора данных

Сертификация

АПМДЗ	▪ на соответствие требованиям ФСТЭК по 3 уровню контроля отсутствия НДВ ▪ на соответствие требованиям ФСБ к АПМДЗ класса 3Б
СРД	▪ на соответствие требованиям ФСТЭК по 4 уровню контроля отсутствия НДВ и ТУ (1Г и 1 класс ИСПДн) ▪ на соответствие требованиям ФСБ к АИС класса АК2
СКЗИ	▪ на соответствие требованиям ФСБ к СКЗИ класса КС2

Развитие продукта

ПАК «Тринити-Internet»

Разработка lite-версии с урезанным функционалом для обеспечения защищённого доступа в Интернет.

ПАК «Тринити-Citrix»

Разработка аналога ПАК «Тринити» под платформу «Citrix».

ПАК «Тринити-Thin»

Разработка системы защиты толстого клиента на основе аналога технологии публикации приложений (пользователь «видит» только те приложения, которые назначены ему администратором, про остальные он даже не знает).

Компания SeTec

Компания Setec основана в 2011 году в Москве в рамках холдинга ITG.

Компания INLINE поддерживает партнерские отношения с компанией Setec, производителем средств защиты информации. INLINE занимается продвижением решений по защищенному терминальному доступу, разработчиком которых является компания Setec. Компании ведут совместную работу над проектами в области информационной безопасности, а также принимают участия в мероприятиях по тематике информационной безопасности.

Спасибо за внимание!

Дмитрий Огородников
Руководитель направления
информационной безопасности
d_ogorodnikov@in-line.ru

email: info@in-line.ru | тел: +7 495 721 35 05 | web: www.in-line.ru