



СОВРЕМЕННЫЕ ПОДХОДЫ ПОСТРОЕНИЯ ЗАЩИЩЁННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ НА БАЗЕ ОТЕЧЕСТВЕННЫХ ПРОИЗВОДИТЕЛЕЙ

Гилязов Руслан Раджабович
Руководитель центра разработки средств защиты
информации
ООО "СиТек"

- Развитие современных технологий позволяет строить продукты нового уровня в сфере информационной безопасности. Это, в свою очередь, более качественно поддерживает концепцию AIC-триады (Availability, Integrity, Confidentiality).
- Текущие потребности бизнеса требуют от средств защиты информации большей гибкости, функциональности и удобства не в ущерб моделям минимизации рисков.
- Развитие телекоммуникационного оборудования, сетей и аппаратных платформ позволяет на практике применять технологии терминального доступа. Это, в свою очередь, даёт возможность строить более совершенные средства защиты информации.

ПАК «Тринити» - «коробочное»
решение компании Setec

Программно-аппаратный комплекс (ПАК) «Тринити»
реализация комплексного решения защищенного
терминального доступа

Назначение: построение современных, масштабируемых
автоматизированных систем трехзвенной архитектуры
(тонкий клиент – сервер приложений – база данных, портал,
другие сервисы) с высоким уровнем информационной
безопасности (вплоть до защиты ГТ).



Изделие, предназначенное для реализации технологии защищенного терминального доступа, обеспечивающей обработку информации в замкнутой и доверенной аппаратно-программной среде.

Защищенность этой технологии происходит за счёт реализации комплекса доверенных механизмов и функций безопасности, обеспечивающих замкнутую и доверенную программно-аппаратную среду и сертифицированных по требованиям действующей нормативной базы регулирующих органов в области защиты информации.

Тонкий клиент – сетевое устройство для связи пользователя с вычислительным ресурсом.

Особенности ПАК «Тринити»



«Тринити-АПМДЗ» – аппаратно-программный модуль доверенной загрузки.

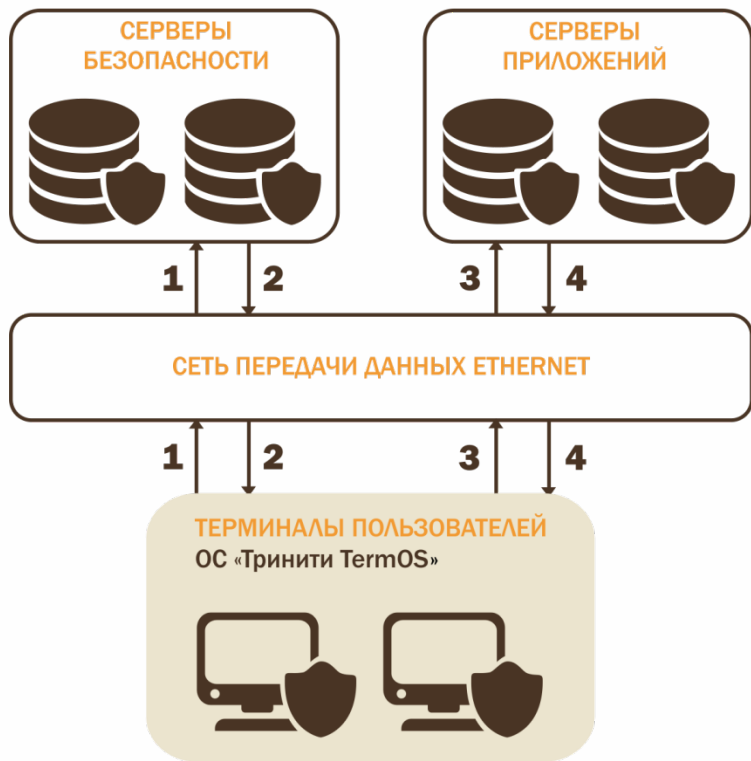


- усиленная аутентификация оборудования и пользователей
- защита от загрузки с внешних носителей
- обеспечение целостности операционной системы
- обеспечение целостности аппаратной конфигурации
- сторожевой таймер
- удаленное управление

Покомпонентный состав



Логика работы ПАК «Тринити»



1. Аутентификация пользователя и терминала в системе;
2. При успешной аутентификации по сети на терминал загружается образ собственной операционной системы;
3. Терминал формирует запросы к серверам приложений на установление защищенной терминальной сессии;
4. Серверы обеспечивают запуск и трансляцию защищенных терминальных сессий на терминал.

Весь трафик в системе шифруется



Совместное решение – это:

- Программно-аппаратный комплекс на базе отечественной платформы «Байкал»;
- Защищенный сертифицированный терминальный доступ;
- Масштабируемая система с высоким уровнем информационной безопасности;
- Разграничение доступа к конфиденциальной и открытой информации;
- Усиленная аутентификация пользователей и идентификация оборудования в системе.

- Консолидация аппаратных ресурсов на единой удаленной площадке (сервера безопасности и сервера приложений различных контуров);
- Единая система подключения к стандартному окружению удаленных рабочих столов вне зависимости от используемой инфраструктуры виртуализации;
- Универсальное решение для подключения терминальных станций, персональных компьютеров и мобильных рабочих мест.

Мобильное защищенное рабочее место



- **Мобильность.** Возможность использования из произвольного места при наличии сетевой связанности;
- **Унификация.** Возможность использования недоверенного произвольного APM;
- **Отказоустойчивость.** Вероятность потери данных в случае поломки или утери RuToken равна 0;
- **Масштабирование.** Высокая скорость развертывания нового рабочего места;
- **Безопасность.** Все ключи и сертификаты хранятся в защищенной области памяти;
- **Экономия.** Низкая совокупная стоимость владения мобильным APM.

Решение “Тринити-Флеш”

- В случае мобильной работы (командировки, служебные выезды и т.п.) обеспечивается доступ к привычному окружению, корпоративным сервисами, средствам разработки и внутренней коммуникации.
- Позволяет использовать амортизированные персональные компьютеры в качестве терминальных решений в рамках ПАК «Тринити», что позволяет существенно уменьшить экономические затраты на покупку нового оборудования.

Повышение удобства работы с разноткатегорийной информацией

Возможность одновременной безопасной работы с одного АРМ с разными сегментами:

- сеть Интернет;
- проектный (НИОКР);
- производственный (АСУТП);
- управленческий (PLM);
- сегмент различных корпоративных сервисов (СЭД, внутренний портал, информационные банки данных и другие).

Объединение в единую информационную систему всех подразделений: филиалы, представительства, ведомственные учреждения.

Единая безопасная VDI платформа:

- Интеграция «из коробки» в существующую инфраструктуру, включая существующие VDI решения: **Citrix, VMware, Microsoft**, предприятий, подключаемых к единой системе.
- Совокупное интеграционное решение позволит параллельно работать с различными VDI платформами, соблюдая требования регуляторов в сфере информационной безопасности.

Решение позволяет формировать изолированные и защищенные системы для взаимодействия между смежными предприятиями при разработке и модернизации образцов вооружений и техники:

- Совместная конструкторская работа (в т.ч. НСИ);
- Электронный юридически значимый ДО;
- Система управленческого учета и финансового мониторинга;
- Защищенная ВКС (в т.ч. межведомственная).

Эффективное сервисное обслуживание

Возможность безболезненного перехода на сервисную модель эксплуатации пользовательской ИТ-инфраструктуры, использование единого центра управления и эксплуатации. Особенно важно при наличии ИТ-активов, консолидирующих в себе ключевые ИТ-компетенции. Данный подход позволит существенно повысить эффективность сервисных услуг на фоне их удешевления.

АПМДЗ:

- АПМДЗ-С на ТУ и соответствие требованиям ФСТЭК по 3 уровню контроля отсутствия НДВ;
- АПМДЗ на ТУ и соответствие требованиям ФСТЭК по 4 уровню контроля отсутствия НДВ;
- на соответствие требованиям ФСБ к АПМДЗ класса 2Б и 3Б соответственно.

СРД:

- на соответствие требованиям ФСТЭК по 4 уровню контроля отсутствия НДВ и ТУ (1Г и 1 и 2 уровни защищенности персональных данных в государственных информационных системах и информационных системах персональных данных);
- на соответствие требованиям ФСБ к АИС класса АК2.

СКЗИ:

- корректность встраивания CryptoPro CSP (сертифицировано по КС2).

Спасибо за внимание!

email: info@setec.ru | web: www.setec.ru