РЕШЕНИЕ ДЛЯ ВАШЕГО БИЗНЕСА

защищенные терминальные станции в корпоративной сети

В крупных компаниях, как правило, складывается разветвленная и разнородная ИТ-инфраструктура, поддержание которой поглощает большой объем ресурсов и создает ряд проблем.
Такую систему сложно защищать и поддерживать технически в силу неоднородности (разные аппаратные конфигурации и программное обеспечение) и нецентрализованного хранения ценной информации.

Программно-аппаратный комплекс “Тринити” – решение, реализованное на базе технологий терминального доступа, благодаря которым информационные системы приобретают практически полную неуязвимость как для внешних злоумышленных атак, так и для враждебной деятельности инсайдеров. Решение обеспечивает эффективный контроль информационной среды и высокий уровень защиты за счет централизации программ и данных, усиленной аутентификации, многоуровневого разграничения доступа, аудита событий и контроля каналов распространения информации, включая средства печати и USB-носители.

Концепция ПАК “Тринити” основана на концентрации всех данных и программного обеспечения в центре обработки данных. Таким образом, вся корпоративная информация, в том числе и составляющая коммерческую тайну, хранится не на рабочих местах, а на центральном сервере. Благодаря этому риск несанкционированного доступа к данным или утечки информации существенно снижается.

За счет уникальных технологий, используемых в решении, обеспечивается многоконтурность, т.е. безопасная одновременная работа в Интернете и с различными сегментами корпоративных систем. При переключении между сегментами осуществляется смена виртуальных рабочих столов с помощью нажатия комбинации горячих клавиш. Встроенные механизмы безопасности исключают возможность обмена информацией между контурами с различными политиками безопасности. Благодаря гибкой системе разграничения пользовательских прав, доступ к тем или иным данным и приложениям предоставляется только сотрудникам, имеющим соответствующее разрешение. При таком подходе можно сформировать замкнутую среду без доступа к командной строке, реестру и другим критичным системным ресурсам. Криптографическая защита всей передаваемой информации в рамках взаимодействия «клиент-сервер» позволяет существенно увеличить эффективность защиты корпоративных ресурсов.

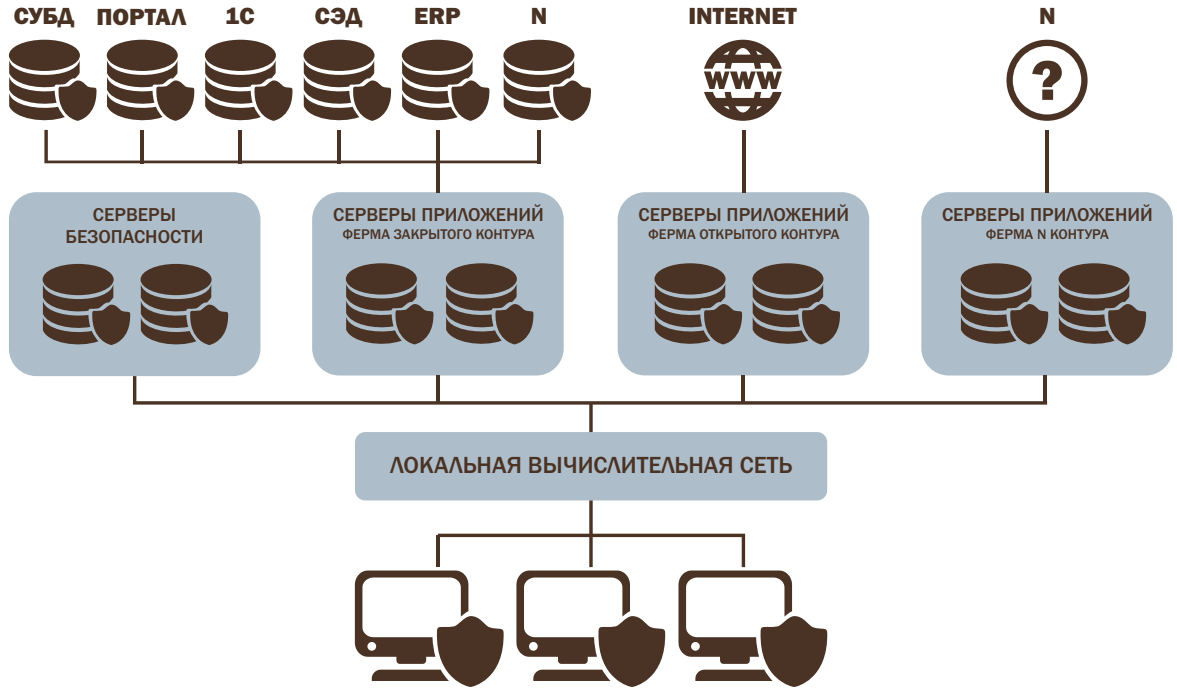

Схема «Одновременная работа в нескольких контурах»

Все пользователи и оборудование аутентифицируются в системе с применением средств криптографической защиты. Для повышения требований безопасности и реализации двухфакторной аутентификации в решении может использоваться собственный аппаратно-программный модуль доверенной загрузки (Тринити-АПМДЗ). За счет этого модуля обеспечивается целостность операционной системы, а гибкий и эффективный контроль использования периферийных устройств и USB-накопителей решает проблему утечки данных через съемные носители. Одновременно с этим решается задача сохранения «стерильности» среды корпоративной информационной системы.

С финансовой точки зрения, ПАК «Тринити» также имеет ряд немаловажных достоинств по сравнению с персональными компьютерами. К их числу можно отнести снижение затрат на приобретение и внедрение решения за счет возможности использования имеющихся или устаревших ПК или замены их на бездисковые терминалы, экономию на пользовательских лицензиях программного обеспечения, технической поддержке и модернизации.

Благодаря технологическим преимуществам, экономичности внедрения и обслуживания, простоте эксплуатации, а, главное, высокому уровню информационной безопасности, ПАК «Тринити» является выгодной и достойной альтернативой персональным компьютерам в корпоративных информационных сетях. В решении реализованы все необходимые требования законодательства РФ по защите персональных данных, конфиденциальной информации и коммерческой тайны.

127521, Москва,
ул. Октябрьская, д. 103

info@setec.ru
www.setec.ru