

ОПЫТ ОРГАНИЗАЦИИ УДАЛЕННОЙ РАБОТЫ С 3D САПР В АО «КОНЦЕРН «ЦНИИ «ЭЛЕКТРОПРИБОР»

А.Г. Баженов, Е.Н. Карташев (Санкт-Петербург)

Введение

Пандемия 2020 года заставила многие организации перевести своих сотрудников на дистанционный режим работы, при этом необходимо было обеспечить доступ сотрудников к программному обеспечению и данным как при работе в офисе. Наиболее распространенный подход для решения указанной задачи является подключение личных вычислительных устройств пользователей к корпоративным сервисам с использованием протокола удаленного рабочего стола (RDP – remote desktop protocol). Данный подход успешно применяется более полутора десятков лет для организации подключений территориально удаленных пользователей. Одной из проблем, которую долго не удавалось разрешить, это организация в таком режиме работы с приложениями, производящими интенсивную обработку графической информации. Примерами таких приложений являются системы автоматизированного проектирования (САПР), работающие с трехмерными изображениями, пакеты архитектурного моделирования и дизайна и т. п. На современном приборостроительном предприятии инженеры, работающие в САПР, являются ключевыми сотрудниками, приносящими прибыль компании, и организация их дистанционной работы является крайне актуальной. Программное обеспечение, работающее с трехмерными изображениями, предъявляет высокие требования к аппаратному обеспечению. Кроме того, передача лицензии на программное обеспечение для работы на домашнем компьютере не всегда допустима, поэтому идея работы даже 10 инженеров в режиме удаленного рабочего стола уже становится привлекательна и с финансовой точки зрения.

Особенностью корпоративной вычислительной сети (КВС) «Концерн ЦНИИ «Электроприбор» является ее изолированность от открытых глобальных сетей. Однако в нынешней непростой ситуации, когда многие ключевые специалисты вынуждены по разным причинам оставаться дома, необходимость выполнения производственного плана вынуждает предоставить инструмент доступа к ресурсам КВС тем сотрудникам, которые оказались в изоляции. В тоже время требуется обеспечить конфиденциальность их работы с вычислительными ресурсами, находящимися внутри КВС [1 – 5].

Организация терминального доступа

Для обеспечения удалённых расчётов были выделены специальные «терминальные» серверы в «демилитаризованной» зоне КВС. Демилитаризованная зона – сегмент сети, отделённый от частных сервисов, но содержащий общедоступные. «Терминальный» сервер – предоставляющий клиентам вычислительные ресурсы (процессорное время, память, дисковое пространство) для решения задач. В качестве средства криптографической защиты информации, которое обеспечивает шифрование канала в «виртуальной частной сети», было использовано “S-Terra”. Ключи шифрования для канала были переданы пользователям при помощи зашифрованных архивов.

После включения зашифрованного канала и подключения к серверу процесс работы не отличается от обычного. Для реализации такого подхода имеются различные способы реализации, начиная с механизма удаленного стола и кончая способами, базирующегося на построения механизма тонкого клиента.

Описание используемого решения

Удалённый доступ — это технология, позволяющая пользователю подключиться к компьютеру на расстоянии с помощью другого устройства и управлять им так, как если бы он сам сидел за этим компьютером. Это может быть и подключение к рабочей машине из дома, и помощь другу с установкой программ — вариантов много. Главное условие — наличие на обоих устройствах выхода в интернет/интранет¹ и специальной программы (Radmin, Splashtop, TeamViewer, AeroAdmin UltraVn, Ammyy Admin).

Для организации удалённого доступа существует множество программ, как сложных, так и очень простых. Устройство в сети удалённого доступа может играть две роли: хост — компьютер, к которому предоставляется доступ (например, рабочий компьютер, на котором нужно поработать из дома); клиент — машина, осуществляющая доступ к другим устройствам. Один и тот же компьютер в разных ситуациях может использоваться и как хост, и как клиент — но не одновременно.

Протокол Remote Desktop создан компанией Microsoft для обеспечения удаленного доступа к серверам и рабочим станциям Windows. Протокол RDP рассчитан на использование ресурсов высокопроизводительного сервера терминалов многими менее производительными рабочими станциями. В настоящее время RDP является основным протоколом удаленного доступа для операционных систем семейства Windows, а клиентские приложения существуют как для ОС от Microsoft, так и для Linux, FreeBSD, MAC OS X и др. В настоящее время RDP является основным протоколом удаленного доступа для систем семейства Windows, а клиентские приложения существуют как для ОС от Microsoft, так и для Linux, FreeBSD, MAC OS X и др. Говоря об истории появления RDP, нельзя не упомянуть компанию Citrix (основана в 1989 г.). Права на ICA (Independent Computing Architecture), прикладной протокол взаимодействия тонких клиентов с сервером приложений Citrix, остались за Citrix Systems, а протокол Microsoft RDP строился на базе ITU T.120.

На основании последнего режима предлагается построение работы пользователей с терминальным сервером. При этом у клиента появляется изображение стола сессии, запущенной на сервере «демилитаризованной» зоны предприятия. Пользователь не имеет доступа к своим ресурсам на персональном компьютере, а передает и принимает данные из тех папок, которые доступны ему на сервере. Защита портов серверов обеспечивается модулями S-Terra Client (см рис. 1). Последние годы набирает популярность инфраструктура виртуальных рабочих столов (VDI), предлагающая каждому пользователю собственную виртуальную машину в дата-центре.

Ускорить их работу на обычном терминальном сервере можно установкой мощной видеокарты. Например, при использовании RemoteFX видеокарта AMD FirePro S10000 поддерживает до 70 пользователей [6]. Помимо графических приложений, ускорение GPU² используется при работе даже обычных офисных пакетов MS Office, LibreOffice. Если сотрудники жалуются на производительность офисных приложений, установка видеокарты может исправить ситуацию. Решением проблемы может стать перевод требовательных пользователей на VDI³ вместо простого терминала. Потребовалась операционная система с поддержкой аппаратного ускорения графики. Терминальный сервер в этом случае состоял из трёх основных компонентов:

¹ Интранет (Intranet, также употребляется термин интрасеть) — в отличие от Интернета, это внутренняя частная сеть организации или крупного ведомства. Как правило, интранет — это корпоративная вычислительная сеть предприятия.

² Графический процессор (graphics processing unit, GPU) — отдельное устройство персонального компьютера или игровой приставки, выполняющее графический рендеринг.

³ Инфраструктура виртуальных рабочих столов.

многоядерный сервер для централизованного хостинга ресурсов; протокола для связи с удалёнными рабочими столами пользователей RDP, который управляет передачей данных между сервером и клиентом, а также клиентская программа на каждом пользовательском устройстве, которая позволяет ему подключаться к серверу по протоколу RDP. Кроме того, необходима служба лицензирования терминалов (Terminal Services Licensing Service), которая представляет серверу клиентские лицензии служб терминалов TS CAL (Terminal Services Client Access License), чтобы они могли к нему подключаться. Список сессий при этом сохраняется в службе Sessions Directory Service. Список индексируется по имени пользователя, что позволяет ему всё время подключаться к одному и тому же серверу. С 2016 года это умеют большинство операционных систем, установленных на терминальном сервере. Для проброса видекарты нужно проверить соответствие системы ряду требований (рис. 2).

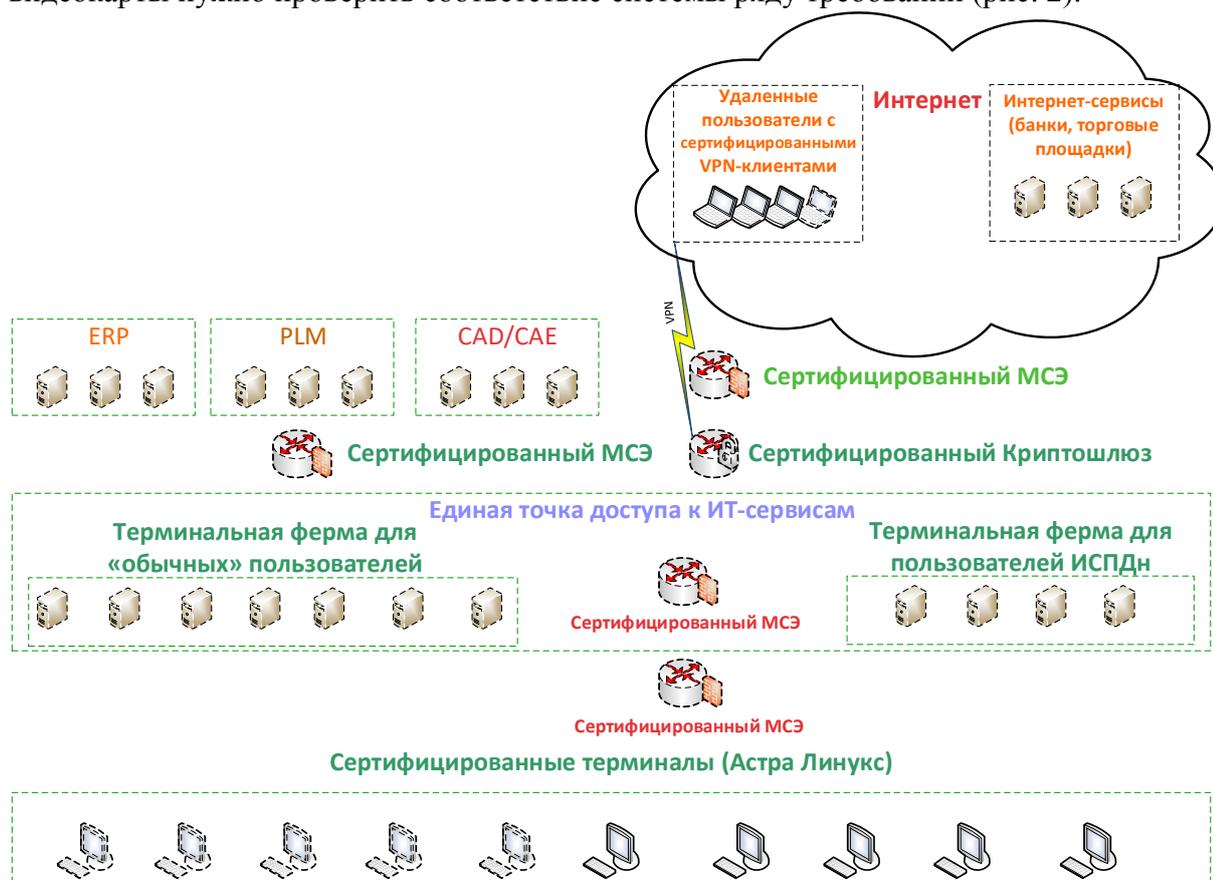


Рисунок 1 – Схема построения удаленной работы в защищенном сегменте

Терминальные серверы дают возможность централизованного хостинга приложений и данных предприятия вне зависимости от расположения и платформы устройств конечных пользователей, давая доступ к ним через терминальные клиентские устройства. Эта концепция позволила реализовать много преимуществ: доступ к цифровым ресурсам предприятия из любого места, в любое время и практически с любого устройства; наличие единой точки мониторинга, позволяющей контролировать всю инфраструктуру с центрального пульта; приложения устанавливаются однократно и регулярно обновляются в терминальном сервере централизованно, то есть нет необходимости делать это на каждом компьютере в сети; наличие одновременной централизованной лицензии вместо лицензирования каждого устройства, что снижает стоимость лицензирования.

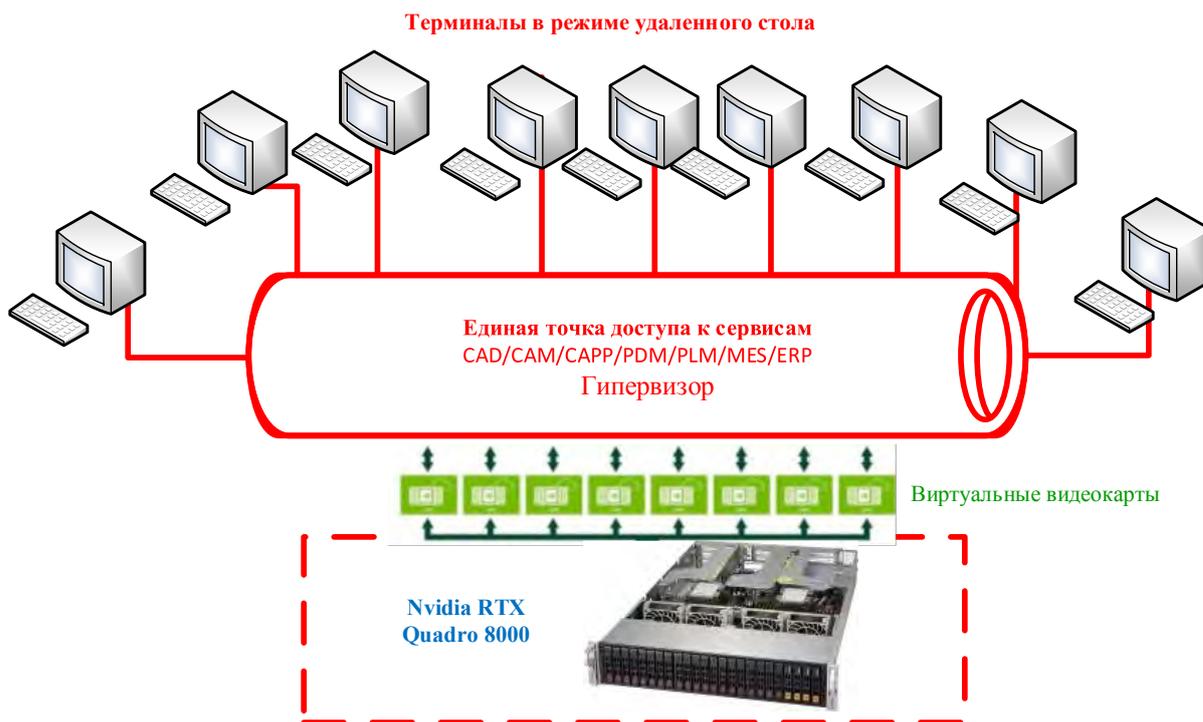


Рисунок 2 – Схема построения терминальных серверов

Особенностью работы с пакетами в области трехмерной графики было развертывание терминального сервера с видеокартой высокой производительности Nvidia Quadro RTX 8000, обеспечивающая одновременную работу до 20 пользователей на персональном компьютере под управлением механизма удаленного стола, как с операционной системой Windows - RDP, так и с отечественной средой Астра Линукс «Орел» - Remmina⁴. Интересны результаты использования терминальных режимов под управление централизованного хостинга приложений: все VDI запросили всего 48Гб оперативной памяти и обеспечили одновременно работу 20 пользователям, которые работали в графических пакетах трехмерной проекции с десятью тысячами элементов в сборке. Персональный компьютер, на котором была установлена операционная система Астра Линукс «Орел», представлял собой процессор i3 второго поколения с оперативной памятью 4Гб и двумя мониторами.

Такой подход позволяет использовать работу удаленного пользователя с практически любой операционной системой и скромными вычислительными ресурсами (не требуется установка дорогой видеокарты на компьютер пользователя).

Выводы

Описанное в статье решение позволило получить полный набор технологий для АО «Концерн «ЦНИИ «Электроприбор» для организации работы пользователей через удаленный рабочий стол. Кроме решения вопросов дистанционной работы, использование указанных технологий позволяет значительно усилить защищенность корпоративной сети от угроз, исходящих от пользовательских устройств, а также организовать при необходимости поэтапный процесс перехода к преимущественному использованию отечественного программного обеспечения (указанный переход является обязательным для организаций, у которых более 50% активов принадлежит государству).

⁴ Remmina показал образцовую производительность и продемонстрировал лучшие показатели отзывчивости среди всех клиентов.

Литература

- 1 **Карташев Е.Н., Красовский В.С.** Информационная безопасность современного предприятия ОПК // Вопросы защиты информации. 2016. №4. С.41-46.
- 2 **Карташев Е.Н., Красовский В.С.** О едином информационном пространстве в судостроительной отрасли // Навигация и гидрография. 2012. №34. С.42-46.
- 3 **Баженов А.Г., Карташев Е.Н., Красовский В.С.** Возможности проведения работ по импортозамещению программного обеспечения // XVII Всероссийская научно-практическая конференция. МОРИНТЕХ-ПРАКТИК. 2017. «Информационные технологии в судостроении-2017».
- 4 **А.Г. Баженов, Е.Н. Карташев, В.С. Красовский** «Пути импортозамещения общесистемного и офисного программного обеспечения». Доклад на конференции: XIX Международной научно-практической конференции МОРИНТЕХ-ПРАКТИК «Информационные технологии в судостроении-2018».
- 5 **Халин В.Г., Чернова Г.В.** Цифровизация и ее влияние на российскую экономику и общество: преимущества, вызовы, угрозы и риски, Санкт-Петербургский государственный университет, Санкт-Петербург, РФ; Управленческое консультирование. № 10. 2018.
- 6 <https://servermall.ru/blog/gpu-for-server/CRYSIS>. Текст «На максималках, или зачем серверу видеокарта».