Не просто ТОНКие клиенты

Михаил Ушаков, *генеральный директор ООО "Группа Компаний ТОНК"*


Фото: ГК ТОНК

В этом году Группа Компаний ТОНК отмечает свое 15-летие. Прошедшие годы, полученный опыт, успешные реализованные проекты, поиски новых решений и нестандартные задачи позволяют формировать собственный профессиональный взгляд на бизнес. В этой небольшой статье мы представляем свою позицию о продуктах и решениях, которые разрабатываем, производим и поставляем последние 15 лет. Сотни партнеров, тысячи благодарных заказчиков, сотни тысяч устройств, работающих долгие годы, свидетельствуют, что 15 лет прошли не зря.

Практически все устройства ТОНК поддерживают работу с различными аппаратными и программными модулями доверенной загрузки.

Возникающие и бурно развивающиеся современные технологии, экспоненциально растущие киберугрозы, отчаянное снижение компетенций и нехватка кадров несут нам новые вызовы. Привычное понятие "тонкий (терминальный) клиент" претерпевает трансформацию, и даже то, о чем мы говорили несколько лет в период бурного роста решений удаленной работы, требует переосмысления. Возможно, некоторым наш (ТОНКовский) взгляд на современную проблематику покажется преждевзятым, а кому-то сложным, но не судите строго.

Тонкий клиент предназначен для удаленных вычислений (Remote Computing), доступа к удаленным приложениям, рабочим столам и инфраструктуре виртуальных рабочих столов (Virtual Desktop Infrastructure – VDI). Тем не менее последние пару лет профессионалы по организации ИТ-инфраструктур предпочитают использовать термин "безопасное бизнес-подключение", или SBC (Secure Business Connection). Действительно, конечному пользователю, реализующему повседневные бизнес-задачи, абсолютно все равно, где физически находятся приложения и информационные ресурсы, самое важное – непрерывность работы, надежность и безопасность. Ключевое понятие в SBC именно Secure – безопасность, которую предоставляют нетрадиционные, современные подходы к построению корпоративных информационных систем.

Текущие реалии – зарубежные игроки ИТ-рынка ушли, и, наконец, стала очевидной важность импортозамещения и цифрового суверенитета. Внезапно стало понятно, что не стоит покупать всем сотрудникам компьютеры в Этой Большой Американской (любой другой) Фирме (ЭБАФ) только потому, что это делали последние 30 лет. И ноутбуки ЭБАФ, которые всем подряд покупали регулярно каждые два-три года, уже не выглядят таким безупречным решением. Увы, нет гармонии в опенспейсе, в котором сгорбившиеся редкие сотрудники всматриваются в 13-дюймовые экраны, совершая неловкие движения попадания пальцем в клавиатуру.

На фоне нехватки кадров явно не решается вопрос производительности труда. В поле информационной безопасности тоже все не очень хорошо. Сотрудники ИБ-подразделений продолжают бегать за злоумышленниками, которые ежедневно совершают сотни тысяч кибератак, вместо того чтобы использовать принципиально другой подход, либо создавать исходно безопасные (Secure by Design) ИТ-системы и устройства, либо использовать в качестве "клиентских" компьютеры, атака на которые не имеет никакого смысла.

Сегодня мы говорим о тонких клиентах как о защищенных компьютерах именно для безопасных бизнес-подключений. В ТОНК мы привыкли говорить о том, что не разрабатываем какие-то там компьютеры или тонкие клиенты, а целенаправленно предлагаем заказчику конечные устройства для их пользователей – для эффективного, надежного и безопасного выполнения бизнес-задач. Конечно, существуют и специальные решения.

Практически все устройства ТОНК поддерживают работу с различными аппаратными и программными модулями доверенной загрузки. Мы широко практикуем технологическое партнерство с компаниями – лидерами в сфере информационной безопасности и предоставляем заказчикам право самостоятельного выбора дополнительных решений.

Тонкий клиент ТОНК TN2900 со снятой боковой стенкой

В линейке устройств ТОНК – специализированные тонкие клиенты с поддержкой двух сетевых адаптеров (изолированная работа в доверенной сети), оптико-волоконных сетевых карт и встроенных аппаратных средств многофакторной аутентификации.

Необходимо понять важный принцип: набор непонятных устройств (каких-то компьютеров) с разнородным ПО, отсутствие контроля над клиентскими устройствами разрушают контур цифровой безопасности предприятия. Часто уже принятые стандарты ИБ, регламенты многофакторной (аппаратной) аутентификации не могут быть реализованы на наспех приобретенном оборудовании. Устройства и приложения, используемые удаленными сотрудниками, на которых не применяются общие и единые политики, не могут быть включены в единую систему предотвращения, обнаружения и нейтрализации атак и угроз.

Вернемся к термину SBC, безопасное бизнес-подключение, и посмотрим со стороны бизнеса. Бесспорно, бизнес – это деятельность, направленная на систематическое получение прибыли. Экономика опирается на современный бизнес, а передовые бизнес-модели – рачительный подход к ведению хозяйственной деятельности – определяют успех современных предприятий.

Мы часто наблюдаем полное отсутствие экономического подхода в архитектуре современных ИТ-систем. При расчетах совокупной стоимости владения (Total Cost of Ownership – TCO) и возврата вложений (Return of Investment – ROI) происходит манипулирование капитальными расходами (CAPEX – Capital Expenditure) и операционными затратами (OPEX – Operational Expenditure).

Программное обеспечение и системы виртуализации стоят недешево, система лицензирования часто сложна и запутанна, модернизация информационной системы иногда происходит как переход с нелицензионного ПО, да еще и могут потребоваться существенные инвестиции в серверную часть (ядро ИТ-системы). Лица, принимающие решения, не понимающие преимуществ "отложенной" экономической выгоды (наступит через 5–6 лет), уверены в том, что "гром не грянет", и преисполнены надежд о неразрушимости бизнеса.

Вспомним многие (довольно известные) разрушенные в 2023–2024 гг. бизнесы, казалось бы, стабильных и крепких компаний в различных сферах, миллионные утечки данных и прочие стихийные бедствия. Часто даже владельцы бизнеса сами отвергают любые предложения сделать простой и понятной (уж, по крайней мере, для себя), прозрачной ИТ-систему. Нередко в качестве эксперта приглашают "того самого парня", технаря, своего в доску, и предлагают взять потестировать тонкий клиент. И вот "тот самый парень" решает заведомо предопределенную для себя задачу, потому что тонкие клиенты сокращают численность ИТ-службы и затраты на ИТ.

Установленные вместо персональных компьютеров на рабочих местах тонкие клиенты не выходят из строя. Прекращаются закупки запчастей для ремонта и антивирусных программ. Сеть относительно крупной (сотни АРМ) организации может обслуживать внешняя ИТ-служба – у пользователей нет проблем на рабочих местах, а ядро информационной системы, размещенной в центре обработки данных, и всю систему в целом в состоянии поддерживать ограниченная команда инженеров.

Впрочем, у пользователей все же есть "проблема": из-за отсутствия неполадок с АРМ сотрудники все свое рабочее время "вынуждены" уделять исключительно работе, выполнению своих прямых функциональных обязанностей.

Получается, что тонкие клиенты спасут бизнес от всех напастей? Скорее всего, нет. Но давайте вспомним другие их преимущества.

- Быстрое масштабирование. Компания знает ресурс ядра своей системы, частного или публичного облака, в котором развернуты приложения и рабочие столы сотрудников. При необходимости можно наращивать этот ресурс и закупать дополнительное количество новых тонких клиентов.
- Снижение затрат на электроэнергию и покупку ИБП на рабочие места. В пике тонкий клиент потребляет 6–7 Вт, использование энергосберегающих устройств – настоящее спасение там, где не хватает выделенной электрической мощности. Тонкие клиенты не зависят от скачков или пропадания электропитания (при работе с удаленными вычислительными ресурсами). Восстановление электроснабжения позволит быстро восстановить подключение с удаленным рабочим столом или приложением и продолжить работу.
- Гармония и удовлетворенность всех вовлеченных в работу. Руководство меньше тратит средств на поддержку ИТ, закупку и ремонт парка компьютеров. Сэкономленные средства будут направлены на развитие бизнеса, а это значит, что компании, использующие тонкие клиенты, – более успешные. Развитие, целеустремленность обеспечивает и ИТ-департамент (служба поддержки и эксплуатации ИТ-систем), инженеры занимаются инновациями, а не ремонтами и решением проблем или ликвидациями аварий. Да и самим сотрудникам нравится эргономика новых устройств – прежний шум, зависания, ошибки их перестают беспокоить. Важно разъяснить сотруднику принцип эффективной работы, невозможность потери критически важной информации.

Осознание методов безопасной и эффективной совместной работы ведет к существенному увеличению производительности труда, а в конечном счете – к росту, развитию и процветанию любой компании и ее сотрудников. ●

Тонкий клиент в современном офисе

Установленные вместо персональных компьютеров на рабочих местах тонкие клиенты не выходят из строя. Прекращаются закупки запчастей для ремонта и антивирусных программ.

Из-за отсутствия неполадок с АРМ сотрудники все свое рабочее время "вынуждены" уделять исключительно работе, выполнению своих прямых функциональных обязанностей.

Ваше мнение и вопросы присылайте по адресу is@groteck.ru

Кибериммунитет для тонких клиентов

Михаил Левинский, *старший менеджер по продукту, "Лаборатория Касперского"*

Лаборатория Касперского

Есть разные взгляды на тонкие клиенты и принципы построения их архитектуры. И хотя самих тонких клиентов на российском рынке не так много, решение "Лаборатории Касперского" явно выделяется среди всех за счет заложенной в нем кибериммунности. Разберемся, что это означает на практике и какие инструменты для контроля и управления это дает для специалистов по информационной безопасности.

Существует миф, что тонкий клиент – априори безопасная система, ведь никакая информация на нем не хранится и не обрабатывается, а значит, злоумышленникам нет смысла пытаться туда проникнуть.

Это заблуждение активно поддерживается глобальными вендорами, которые при описании преимуществ своих тонких клиентов обязательно добавляют пункт Secure – мол, безопасный.

Но реальная безопасность тонких клиентов заключается в наборе используемых технологий и в первую очередь – в операционной системе, как правило, базирующейся на Linux. Впрочем, есть и другой подход.

KasperskyOS – другой подход к безопасности

KasperskyOS – это микроядерная операционная система, на базе которой разрабатываются кибериммунные продукты. Она разработана по принципу Secure by Design, то есть безопасна уже по своей природе и не требует наложенных средств защиты. Это результат серьезного научного исследования, в которое "Лаборатория Касперского" вложила 15 лет работы.

Одно из практических продуктов KasperskyOS – специализированная операционная система для тонких клиентов Kaspersky Thin Client. В данный момент в России она устанавливается на платформе TONK TN1200. За рубежом это решение известно под названием Centerm F620 и уже доступно с предустановленной ОС Kaspersky Thin Client в Малайзии, Индонезии, Швейцарии, Австрии, ОАЭ, Королевстве Саудовской Аравии и других странах.

Кибериммунный тонкий клиент – это практическое подтверждение того, что можно строить системы, безопасные по дизайну. А главный вклад в кибериммунность дает микроядерная архитектура KasperskyOS.

Микроядро для сокращения поверхности атаки

Обычный подход, в том числе и мировой, при разработке операционных систем для применения в тонких клиентах – усечение образа монолитного ядра операционных систем Linux и Unix, размер которых исчисляется гигабайтами. Поэтому для сокращения объема часть компонентов вырезается из образа, попутно образуя риски для стабильности работы.

Микроядерная архитектура строится в обратном направлении – на суперкомпактное и выверенное ядро накладываются только компоненты, необходимые для конкретного применения. Микроядро контролирует все компоненты вокруг себя и их взаимодействия с другом.

Дело в том, что в монолитной архитектуре взаимодействие между компонентами происходит напрямую, а при микроядерном подходе все запросы проходят через ядро. Это дает богатейшие возможности по контролю безопасности.

За счет добавления только необходимых компонентов сокращается поверхность атаки. Для сравнения: ядро Linux содержит 35 млн строк кода, а в KasperskyOS – всего несколько десятков тысяч. Почти 90% уязвимостей, которые присущи монолитным ядрам, на микроядре или просто не будут существовать или будут иметь низкую степень критичности с точки зрения безопасности.

Компактное ядро и проблема обновлений

Размер образа ОС Kaspersky Thin Client версии 2.0, развернутого на тонком клиенте, составляет не более 700 Мбайт, а дистрибутив (сжатый образ) для доставки из источника обновления до тонких клиентов – не более 300 Мбайт. Это достаточно маленький объем даже в сравнении с другими операционными системами для тонких клиентов. Отсюда следуют несколько важных особенностей.

Во-первых, устройства под управлением Kaspersky Thin Client становятся нетребовательными к аппаратным ресурсам. Сейчас операционная система для тонких клиентов "Лаборатории Касперского" работает на аппаратной платформе TONK TN1200. Но компактный образ Kaspersky Thin Client позволяет им работать и на другом оборудовании, в том числе с довольно скудной аппаратной спецификацией.

Во-вторых, решается проблема с обновлениями. Высокая периодичность обновлений на операционных системах с монолитным ядром объясняется необходимостью доставки патчей безопасности, а это огромная нагрузка на сеть. Особенно это критично для слабых каналов в регионах, а надо отметить, тонкие клиенты часто используются в географически распределенных инфраструктурах.

Благодаря кибериммунности регулярные обновления для Kaspersky Thin Client в принципе не нужны. Следствием минимальности поверхности атаки является полное отсутствие патчей безопасности. Единственный случай, когда необходимы обновления, – если заказчик хочет получить новую функциональность.

Посмотрим на пример. Ретейл и банки – частые пользователи тонких клиентов. Если в каком-либо магазине или банке парк тонких клиентов не заведется только из-за того, что образ в несколько гигабайт не обновился за ночь, это – серьезные потери для бизнеса. В случае использования Kaspersky Thin Client такая ситуация исключена.

На что распространяется кибериммунность?

Используя тонкие клиенты "Лаборатории Касперского", заказчик не просто

приобретает компактный ПК, но выстраивает инфраструктуру тонких клиентов.

Кибериммунность означает не только защищенность конкретной конечной точки – безопасность связана со всем жизненным циклом тонких клиентов и полным стеком технологий в их инфраструктуре. Например, есть задачи, связанные с распределением сертификатов для подключения к виртуальным рабочим столам, и от надежности этого механизма также будут зависеть характеристики безопасности кибериммунного тонкого клиента. Все подобные аспекты учитываются при расчете модели угроз и при планировании свойств кибериммунности.

Конечно, тонкие клиенты не могут впрямую отвечать за VDI-инфраструктуру, но ее безопасность могут обеспечивать другие продукты "Лаборатории Касперского", начиная с уровня хранения "золотых" образов до защиты гипервизора, виртуальных машин и т.д.

Точно можно утверждать, что на кибериммунном тонком клиенте нет необходимости в установке, например, антивируса, потому что он построен таким образом, что через него злоумышленник не сможет провести кибератаку. Но для решения дополнительных задач кибербезопасности, например, обеспечения двухфакторной аутентификации или защиты конфиденциальной информации, передаваемой по каналам связи, потребуются средства защиты.

Управление тонкими клиентами

В процессе разработки проявилось еще одно технологическое преимущество тонких клиентов помимо свойств кибериммунности. На сегодняшний день "Лаборатория Касперского" защищает сотни миллионов конечных точек по всему миру. Большая их часть – корпоративные рабочие места, и для централизованного управления агентами, установленными на защищаемых объектах, используется Kaspersky Security Center.

Естественным образом это решение применяется и при управлении кибериммунными тонкими клиентами. Если в компании уже работает хотя бы один корпоративный продукт "Лаборатории Касперского", значит, де-факто система централизованного управления тонкими клиентами уже есть. Для этого в Kaspersky Security Center нужно добавить еще один модуль.

В результате для начала использования кибериммунных тонких клиентов достаточно просто подключить их к корпоративной сети через Ethernet-разъем, а дальше Kaspersky Security Center увидит новый кибериммунный продукт Kaspersky Thin Client, выдаст все необходимые конфигурации – и рабочее место готово к использованию.

Благодаря автоматической настройке Kaspersky Thin Client можно подключить к инфраструктуре всего за две минуты.

Мониторинг и контроль

Тонкие клиенты, появляющиеся вместо обычных рабочих мест, несут риск ухода в область Shadow Hardware, теневое аппаратное обеспечение, скрытое от глаз безопасников. Первое, что обеспечивает Kaspersky Security Center, – это необходимая видимость: в консоли могут работать как айтишники, в задачи которых входит внедрение тонких клиентов, так и безопасники, например для сопровождения антивирусных средств защиты или работы с крупными продуктами, такими как KUMA или KATA.

Изображение: Лаборатория Касперского

Второе – поддержка с помощью Kaspersky Security Center специфических настроек безопасности: например, разрешения или запрета на подключение подключаемых USB-носителей или возможности для пользователя изменять параметры подключения устройства.

Таким образом Kaspersky Security Center позволяет органично вписать использование и сопровождение тонких клиентов в привычный для ИТ и ИБ сценарий.

Совместимость с VDI-решениями

RDP – базовый протокол в Kaspersky Thin Client, и любое VDI-решение, которое его поддерживает, будет совместимо.

Из российских VDI-производителей поддерживается Basis WorkPlace, а в версии 2.0 анонсирована возможность подключения по HTML5 к Citrix и VMware. Доступен также режим доставки отдельных приложений.

Тонкие клиенты для АСУ ТП

Промышленный сегмент – это очень интересная область использования тонких клиентов.

Устройства в промышленном сегменте работают, как правило, в затрудненных условиях эксплуатации: пыль, влажность, электростатика и другие негативные факторы. Поэтому в сегмент АСУ ТП ставятся только компактные рабочие станции в промышленном исполнении.

Тонкие клиенты хороши как раз тем, что в них нет движущихся частей, и вероятность их выхода из строя под воздействием неблагоприятных факторов среды крайне мала.

Вторая важная особенность сегмента АСУ ТП – нишевой сценарий использования. Чаще всего это подключение к удаленной или виртуализованной SCADA-системе. Для работы со SCADA не нужны мощные производительные протоколы – как правило, достаточно обычного RDP, чтобы инженер мог осуществлять мониторинг технологического процесса или управлять им.

Но важно минимизировать время простоя конечной рабочей станции. Если происходит неполадка с традиционным промышленным компьютером, потребуется значительное время, чтобы устранить неполадку или заменить одну рабочую станцию на другую.

В случае с тонким клиентом процесс подключения нового тонкого клиента занимает две минуты с холодным стартом, а горячий старт будет еще быстрее. Поэтому интерес к форм-фактору тонкого клиента на АСУ ТП исходит не только от безопасников, но и от айтишников.

Важное преимущество в заключение

Важное преимущество Kaspersky Thin Client заключается в том, что продукт полностью закрывает задачи как для обычных пользователей, так и ИТ-администратора, а также не создает дополнительной головной боли для ИБ-администраторов. В том числе и за это в 2022 г. Kaspersky Thin Client получил международную награду как одна из лучших технологических инноваций на World Internet Conference.

В 2023 г. решение было отмечено на "Инфофоруме-Сочи" и победило в номинации "Защищенный гражданин". В этой категории участники конкурса соревновались за звание лучшего защищенного решения в сфере финансовых услуг, цифрового здравоохранения, цифрового образования и цифрового социального обеспечения в регионах России.

Интегративный подход GETMOBIT к работе с тонкими клиентами и пользовательскому опыту в сложной корпоративной инфраструктуре заказчика

Василий Шубин, *руководитель центра развития продукта и компетенций GETMOBIT*
Александр Тарасов, *главный архитектор технологической платформы GETMOBIT*


Фото: GETMOBIT


Фото: GETMOBIT

Существует распространенное мнение, что тонкий клиент – это маленькая коробочка с любой, в том числе стандартной, операционной системой, работающей в режиме киоска и запускающей тот или иной клиент удаленного доступа. Верно ли это? Разберемся, какие бывают тонкие клиенты, что же делает устройство тонким клиентом и какая инфраструктура обеспечивает эффективность, стабильность и удобство работы с парком таких устройств.

GETMOBIT – сравнительно молодая российская технологическая компания, совершившая революцию на рынке тонких клиентов.

Компания представляет интегральную аппаратно-независимую платформу для системной организации и администрирования многофункциональных рабочих пространств с повышенными требованиями безопасности удаленного доступа сотрудников к корпоративным информационным ресурсам. В ее составе оригинальная док-станция, встроенное системное программное обеспечение и система управления клиентскими устройствами корпоративного уровня, а также специализированные программные компоненты.

Тонкий клиент или ПК?

Говоря о том, что такое тонкий клиент, необходимо учитывать различные смыслы этого понятия.

Тонкий клиент:

- аппаратная часть, так называемое "легкое железо", – отдельный тип и форм-фактор оборудования. Физически тонкий клиент – это облегченный компактный и бесшумный компьютер без жесткого диска (и без вентиляторов);
- дистрибутив, который устанавливается на оборудовании. Загрузка основной операционной системы тонкого клиента происходит на сервере. Все пользовательские приложения выполняются на терминальном сервере (сервере приложений), но для пользователя это совершенно прозрачно. Вся вычислительная нагрузка ложится на сервер, поэтому тонкий клиент обладает минимальной аппаратной конфигурацией без какого-либо ущерба производительности.

Обеспечивает базовый функционал работы клиента: начальную загрузку, корректную работу видеоадаптера, аудио, работу периферийных устройств подключенных непосредственно к терминальному клиенту (мышь, клавиатура, локальные принтеры, USB-флеш накопители). Операционная система тонкого клиента может содержать в своем составе интернет-браузер, который может работать автономно (без терминального сервера).

При переходе в терминальный режим клиент начинает работать с серверной операционной системой, индивидуальный сеанс которой запускается на терминальном сервере. С этого момента терминал становится просто средством отображения и ввода информации.

Переход к инфраструктуре виртуальных рабочих столов (VDI) позволяет перенести корпоративные данные, образы операционных систем и запускать приложения на серверах компании. Таким образом, пользователи, подключаясь удаленно к среде VDI, получают полноценный доступ к своему рабочему окружению из любого места и с любого устройства.

Наличие такой инфраструктуры дает бизнесу возможность избавиться от необходимости обслуживать парк персональных компьютеров с размещенными на них данными и приложениями и перейти на легкую и гибкую инфраструктуру "тонких клиентов".

Тонкий клиент или телефон?

Тонкий клиент GM-Box G1, разработанный GETMOBIT, отличается ото всех тонких клиентов, что вы видели ранее. Внешне и по содержанию.

GM-Box G1 – оригинальная многофункциональная док-станция, заменяющая тонкий клиент и видеотелефон, с защищенным доступом к инфраструктуре вир-

туальных рабочих мест, веб-сервисам и IP-телефонии, с возможностью аутентификации пользователя с помощью смартфона, смарт-карт, токенов.

Средства защиты информации встроены в аппаратное решение. Вместе с программными инструментами управления и интеграции образуют единую среду для создания и экономной эксплуатации корпоративных рабочих мест как в офисах, так и удаленно.

Док-станция GM-Box обладает достаточным количеством интерфейсов для подключения периферии (принтеров, внешних носителей информации и других устройств, использующих USB-интерфейс).

Устройство задает единый унифицированный стандарт рабочего места по принципу all-in-one, позволяющий реализовать множество специальных режимов работы сотрудников организации с помощью универсального набора технических средств и ПО.


Фото: GETMOBIT

Один тонкий клиент GETMOBIT вместо нескольких ПК

Часто встречается ситуация, когда пользователь должен с одного рабочего места работать в двух независимых информационных системах, условно "открытой" и "защищенной". Традиционно таким пользователям выдают два ПК или ТК с дублирующим набором устройств (иногда на разных столах, чтобы пользователь не запутался, где он работает). GETMOBIT предлагает иной подход.

Универсальная док-станция GM-Box выпускается в двух модификациях: GM-Box BASE – с одной системной платой (одним вычислительным модулем) и GM-Box DUO – с двумя физически независимыми системными платами (двумя вычислительными модулями) в одном корпусе.

Для обеспечения использования одного комплекта устройств ввода/отображения информации в GM-Box DUO встроен аппаратный программно-управляемый KVM-переключатель, обеспечивающий одновременный безопасный доступ сотрудника к двум изолированным информационным контурам с одного рабочего места – GM-Box Duo.

ПАК GM SMART KVM имеет Сертификат ФСТЭК № 4800. Чтобы обеспечить безопасность, используется механизм однонаправленного переключения, который позволяет передавать информацию только на другой вычислительный модуль, но не обратно. Таким образом, нарушитель не сможет переключить устройства ввода и отображения информации на свой модуль из-за особенностей схемотехники KVM-переключателя.

Лицензия ФСТЭК России подтверждает, что GM SMART KVM соответствует "Требованиям по безопасности информации, устанавливающим уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий" по 4-му уровню доверия, а также техническим условиям на программно-аппаратный комплекс. Простыми словами: ПАК соответствует повышенным требованиям к обеспечению безопасности данных в организациях, где используются два информационных контура.

Тонкий клиент. Что остается за кадром?

Аппаратная часть важна, но конечное устройство – "вишенка на торте". Главная особенность тонкого клиента – способность уверенно работать не только на маломощном оборудовании, но и на слабых каналах. Под работой подразумевается не только доставка виртуального рабочего места по протоколам удаленного доступа, но и вопросы обновления, настройки и безопасной работы устройства с учетом удаленности его месторасположения.

Устройство становится полноценным тонким клиентом, только когда на нем есть специализированная прошивка (Firmware), учитывающая все особенности эксплуатации данного класса устройств. Она (прошивка) выполняет роль операционной системы и может базироваться на разных ОС общего назначения, именно она обладает теми свойствами, которые отличают ПК от ТК.

При плохом канале задачи управления обновления операционной системы и приложений становятся практически невыполнимыми для персональных компьютеров с ОС общего назначения. Читатель прекрасно знает, обновления какого объема приходят для Windows. Обновления Linux, хотя и меньше, но тоже достаточно значительные. А стоит пропустить очередную версию – и прилетят уже сотни мегабайт.

Например, на устройство, находящееся за спутниковым каналом, в реальной жизни такие масштабные обновления никогда "не накатятся", в противном случае возникнет существенный риск получения не соответствующей корпоративным требованиям конфигурации ПО. Получится фрагментация версий ПО, высокая сложность поддержки парка устройств, риски и проблемы с информационной безопасностью, поскольку обновления почти всегда несут в себе устранение уязвимостей.

Прошивка для тонкого клиента проектируется с учетом максимального уменьшения поверхности атаки. Там, где у обычного ПК останется возможность взлома, у тонкого клиента окажется стена – отсутствие интерфейсов, через которые можно попытаться провести атаку.

Уменьшение размера образа и минимизация поверхности атаки стали возможны за счет установки прошивки нового поколения GETMOBIT, базирующейся на сборке Linux, переработанной разработчиками GETMOBIT (находится в реестре Минцифры России по классу встроенного и системного ПО).

Система управления – мозг инфраструктуры тонких клиентов

Степень готовности тонкого клиента к выполнению своих задач гораздо выше, чем у обычного ПК, что достигается благодаря максимальному отказу от локального управления устройствами конечных пользователей. GETMOBIT уделяет большое внимание возможностям централизованного управления и интеграции для обеспечения сквозной эффективности в единой цифровой среде.

Используя эту особенность, интеллектуальная система управления GM Smart System позволяет масштабировать инфраструктуру тонких клиентов,

подстраиваясь под разные задачи заказчиков.

В состав платформы входит универсальный сервер управления GM Workspace Factory, который учитывает установленные тонкие клиенты с подходящей прошивкой и автоматически обнаруживает новые. При этом не требуется ручная настройка устройств – все индивидуальные и групповые настройки отправляются централизованно. Конфигурация прошивки позволяет работать с широким спектром как иностранных VDI-инфраструктур (VMware, Citrix, Microsoft), так и российских (Termidesk, Space, Basis WorkPlace, Горизонт-ВС).

Платформа позволяет тонкому клиенту работать и в режиме веб-клиента, для этих целей в прошивке имеется встроенный браузер.

Практически любой компьютер с архитектурой Intel или AMD, можно превратить в тонкий клиент, управляемый GM Smart System.

Почему тонкие клиенты – это безопасно?

Идея работы любых тонких клиентов заключается в том, чтобы обеспечить информационную безопасность за счет централизованной обработки данных.

В информационной системе, построенной по архитектуре "клиент-сервер" с применением VDI/RDP, обработка защищаемой информации осуществляется в VDI-среде сервера информационной системы. Такой способ разрешен приказом ФСТЭК России № 17 от 11.02.2013 г., а также приказом ФСТЭК России № 239 от 25.12.2017 г. Централизованное управление настройками устройств пользователей позволяет еще больше сократить возможную поверхность атак и вместе с этим при использовании большого парка устройств позволяет свести к минимуму локальное администрирование конечных устройств, что не только повышает издержки на администрирование, но и создает дополнительные риски. Особенно это актуально для территориально распределенных инфраструктур, где оперативный доступ к устройствам пользователей не всегда просто обеспечить.

Эксперты GETMOBIT используют нетривиальные инструменты, минимизирующие поверхность атаки в GM Smart System. Защита предусмотрена на трех уровнях инфраструктуры: аппаратная часть, прошивка и системное ПО.

В самих устройствах GM-Box реализованы различные методы идентификации и аутентификации пользователей, которые в совокупности с мерами по управлению доступом обеспечивают однозначную идентификацию и аутентификацию субъекта доступа, а также разграничение прав доступа субъектов доступа. Кроме того, в случае установки в док-станцию GM-Box G1 сертифицированного средства доверенной загрузки (аппаратно-программного модуля доверенной загрузки), например ПАК "Соболь", как правило, осуществляется дополнительная идентификация и аутентификация пользователя.

Доступ в настройки BIOS GM-Box и других тонких клиентов закрыт, настройки не позволяют загружаться с USB-устройств или из сети. Прошивка тонких клиентов работает в режиме read-only, на диск устройства ничего не может быть записано, кроме как через сервер управления. Это исключает возможность пользователю или вредоносному ПО записать в долговременную память устройства произвольное, в том числе и вредоносное ПО. Установка на тонкий клиент дополнительных средств защиты не требуется, так как обработка защищаемой информации на тонком клиенте не производится. Возможности удаленного подключения, существующие в обычных операционных системах, например SSH, отключены по умолчанию. Оставлен минимальный набор открытых сетевых портов.


Фото: GETMOBIT

В состав прошивки включены сертифицированные средства защиты – Крипто Про и VipNET, обеспечивающие шифрование трафика по требованиям ГОСТ.

Система управления поддерживает политики разрешения и запрета работы с разными типами устройств (флешнакопителями, веб-камерами и т.п.). Плагины, обеспечивающие подключение к средам VDI, или другие компоненты прошивки, могут доставляться только с сервера управления, а также собраны в проприетарном формате. Локальная установка каких-либо программных пакетов невозможна. Кроме того, в GM Smart System встроены развитые функции логирования и мониторинга. Сбор этой информации происходит централизованно на сервере управления, затем события могут быть отправлены в SIEM для анализа и выявления инцидентов.

С точки зрения архитектуры всей АИС должна быть обеспечена защита среды виртуализации, включая серверные и гостевые ОС, а также прикладные системы. В частности, должны быть обеспечены наличие и запуск на серверах информационных систем только разрешенного ПО.

Для передачи информации между серверами информационных систем и тонкими клиентами используются алгоритмы шифрования. Если применение сертифицированных СКЗИ предусмотрено законодательными и иными нормативными правовыми актами Российской Федерации, то могут быть применены дополнительные программно-аппаратные средства криптографической защиты, сертифицированные ФСБ России.

"Транзитные" технологии GETMOBIT

Таким образом, становится возможным построение системы транзитных архитектур для доступа конечных пользователей к разнородной инфраструктуре сервисов виртуальных рабочих мест на базе российских и зарубежных платформ VDI через единую витрину инфраструктурных сервисов, эксплуатируемых в организации. В платформе GM Smart System – буквально витрина для доступа конечных пользователей к инфраструктурным сервисам, определяемая на уровне шаблонов в соответствии с функциональными задачами пользователя в организации.

За счет поддержки совместимости с широко распространенными на российском рынке зарубежными решениями VDI (VMWare Horizon, Citrix XenDesktop, Microsoft VDI, HUAWEI FUSION, Cisco, Avaya, Siemens и др.), а также с технологиями российских производителей VDI-платформ (Space, Горизонт-ВС, Базис,

VDI VeIL, Термидеск, Ovirt, РУСТЭК, СКАЛА-Р и др.), IP-телефонии и ВКС (CommuniGate Pro, IVA, РТУ, Элтекс, TrueConf, VideoMost и др.), а также информационной безопасности (АПМДЗ "Соболь", ПАК "Соболь", сертифицированная ОС Альт 8 СП, СКЗИ "КриптоПро CSP", VipNet Client 4U for Linux), технологии GETMOBIT выступают своеобразным "трансфером" данных к конечному пользователю практически вне зависимости от того, какими инструментами пользуется организация.

Централизованное управление существующего парка сторонних ПК / ТК / ноутбуков

Распространена ситуация, когда заказчик накопил большой парк унаследованных устройств, от использования которого отказываться экономически нецелесообразно. При этом сотрудники, поддерживающие инфраструктуру, сталкиваются с рядом вызовов:

- трудоемкость процесса технической поддержки;
- невозможность миграции на российские VDI;
- многообразие инструментов управления (ручная работа, SCCM, HPDM),
- невозможность оперативно реагировать на требования регуляторов и бизнеса;
- ограничения по развитию и обновлению парка пользовательского оборудования.

У GETMOBIT есть ответ для конвертации унаследованных устройств в "свои", и встраивание их в единую управляемую инфраструктуру.

Старт конвертации настраивается с помощью "родных" средств управления, под которыми ранее работали тонкие клиенты иностранных вендоров. Конвертация одного устройства происходит примерно в течение шести минут – из сети берется прошивка GM 3rd Party Kit, и устройство перепрошивается.

То есть через шесть минут, без вмешательства пользователя в устройстве начинает работать прошивка GM Smart System. Она автоматически обнаружит сервер управления, получит настройки, которые содержат возможность работы с иностранным или с российским VDI, и все – пользователь может работать.

В подавляющем большинстве случаев на конечном рабочем месте не требуется вмешательство ни пользователя, ни администратора – все делается автоматически.

Таким образом, решается сразу несколько актуальных задач: продление срока эксплуатации текущего парка СВТ и возможность использования различных сред VDI отечественных разработчиков.

Кроме того, реализовано удаленное подключение к экрану конечного устройства для службы HelpDesk, чтобы она могла решить вопросы поддержки в реальном времени.

А как работать компаниям, чьи филиалы географически распределены?

На этом можно было бы остановиться, но разработчики GETMOBIT решили еще одну важную задачу. Дело в том, что большинство заказчиков, использующих инфраструктуру терминального доступа или VDI, имеют географически распределенную структуру с большим количеством филиалов в отдаленных регионах страны и ограничены в количестве ИТ-специалистов. При этом бизнесу требуются ускоренное развертывание и маневренный контроль.

В платформе GM Smart System модуль, конвертирующий устройства, получил роль прокси для доставки новых "прошивок" и обновлений для VDI-клиентов. Теперь не надо гнать по магистральному каналу потоки обновлений для сотен и тысяч устройств. Достаточно доставить обновления до прокси, который распределит их оптимальным образом по близким к нему устройствам.

Так заказчик получает возможность простого поэтапного перехода к единому стандарту информационной среды пользователя во всех подразделениях и филиалах, с единообразием и контролируемой версионностью программных компонентов, что, как мы помним, слабо или практически нереализуемо для "классических" ОС и систем управления ими.

Выводы о тонких клиентах

В нескольких предложениях. Рабочие места в инфраструктуре тонких клиентов – это не просто суперпозиция какого-то "железа" и какого-то ПО. Это, в первую очередь, решение задач бизнеса и производственных процессов: безопасное, предсказуемое, эффективное и с опережением. При условии комплексной увязки возможностей системного и прикладного ПО с преимуществами современных и доступных аппаратных архитектур.

Тонкий клиент – это когда:

- конечное устройство не привязано к пользователю и не содержит пользовательских или корпоративных данных. У любого пользователя есть возможность войти в систему с любого тонкого клиента в организации и получить удаленный доступ к своим данным и приложениям, практически не ощущая разницы по сравнению с работой на "обычном" ПК. Это облегчает реализацию концепции современных "гибких" офисных пространств;
- радикально сокращается время подготовки новых рабочих мест сотрудников. Пользовательское окружение настраивается на стороне VDI и системы управления тонкими клиентами. Пользователю выдается устройство в состоянии "как есть", с минимальным участием ИТ-специалистов для предварительной настройки. Это повышает готовность компаний к оперативному найму новых сотрудников. А для организаций с региональной филиальной структурой, значительно упрощает и ускоряет процесс запуска новых отделений и филиалов в регионах;
- многократно повышается производительность труда сотрудников группы ИТ по поддержке рабочих мест. Система управления тонкими клиентами позволяет осуществлять мониторинг и вносить изменения в настройки устройств в режиме реального времени. Это дает возможность централизованно управлять десятками тысяч тонких клиентов, географически распределенных по всей стране, в том числе при ограничениях пропускной способности каналов связи;
- практически исключается время простоев из-за неисправностей пользовательских устройств. В случае поломки тонкого клиента достаточно его заменить на аналогичный. Как правило, это не требует участия ИТ-специалиста, и пользователь возвращается к работе за считанные минуты. Не происходит потери выполненной работы в приложениях, так как они размещены на серверах компании, а не на конечном устройстве;
- становится значительно проще обеспечивать безопасность пользовательских устройств. Тонкие клиенты по своей архитектуре менее подвержены угрозам по сравнению с ПК, работающими под управлением операционных систем общего назначения, и позволяют гибко применять политики и ограничения. Это помогает выполнять требования регуляторов и упрощает решение ряда задач бизнеса, например перевод сотрудников на "гибридный" режим работы;
- выбор форм-фактора и конфигурации пользовательских устройств остается за заказчиком, что освобождает от привязки к конкретному бренду оборудования. Система управления тонкими клиентами дает возможность единого управления разными аппаратными платформами, включая существующий парк компьютеров разных моделей и тонкие клиенты сторонних производителей. При этом обеспечивается минимизация требований к производительности конечных устройств.

Все эти возможности должны быть реализованы с учетом возрастающей сложности и разнородности современных ИТ-инфраструктур, а также растущих потребностей к многозадачной работе пользователей и критичности обеспечения позитивного пользовательского опыта. Ожидания рынка направлены на предоставление описанных выше возможностей гибкого управления, а также интеграцию с изменяющимся ландшафтом ИТ-систем, где параллельно могут функционировать как зарубежные, так и отечественные VDI-среды. ●

Termidesk 5.0: универсальное решение для организации удаленных рабочих мест

Termidesk — это российское решение по виртуализации ПК и приложений, обеспечивающее безопасный удаленный доступ к виртуальному рабочему месту из любой точки мира и с любого устройства.

Termidesk разрабатывает компания "Увеон – облачные технологии" – одна из крупнейших российских команд разработчиков систем данного класса. VDI-решения очень популярны у заказчиков по нескольким причинам:

- они позволяют централизованно управлять и предоставлять доступ к данным и приложениям, а используя дополнительные возможности по ограничению проброса периферии, существенно снижают риск утечек и несанкционированного доступа;
- позволяют легко масштабировать число рабочих мест и быстро открывать новые филиалы, что дает возможность компаниям быстро адаптироваться к изменяющимся потребностям бизнеса.

Termidesk поставляется в виде готовых и преднастроенных образов виртуальных машин (Virtual Applience), таким образом существенно уменьшается порог входа по изучению продукта и значительно снижаются затраты на его первоначальную настройку и внедрение.

Как устроен Termidesk

Termidesk построен на основе клиент-серверной архитектуры. На серверной стороне работают два основных компонента: диспетчер и шлюз. Диспетчер отвечает за управление сессиями пользователей и распределение ресурсов, в то время как шлюз обеспечивает безопасное подключение и передачу данных. Разработчики рекомендуют развертывать серверные компоненты с использованием Virtual Appliance – специализированного виртуального модуля, который упрощает установку и управление системой.

Клиентская часть Termidesk включает в себя агенты, которые отвечают за доставку и эксплуатацию рабочих мест. Они бывают нескольких типов:

- виртуальные машины, которые поставляют рабочие места на базе виртуальных машин;
- узел виртуализации, на который можно устанавливать и запускать виртуальные машины;
- сессионные агенты, обеспечивающие доставку терминальных приложений, позволяя пользователям работать с этими приложениями удаленно.

Пользователь взаимодействует с системой через клиентское приложение Termidesk, которое можно установить на любую из поддерживаемых операционных систем. Для бездисковых рабочих станций и тонких клиентов доступен Termidesk Live, обеспечивающий подключение к инфраструктуре через сетевую загрузку.

Рабочие места VDI

Виртуальные рабочие места – это развернутая на виртуальной машине полноценная операционная система с установленным агентом Termidesk и необходимым прикладным программным обеспечением. Подключение к рабочему месту происходит при помощи протоколов удаленного доступа RDP, SPICE и Loudplay.

Доступ к виртуальному рабочему месту может осуществляться из веб-браузера с использованием HTML5 либо из программы-вьювера, которую запускает клиентское приложение программного комплекса. Пользовательские данные не привязываются к виртуальной машине, что дает возможность повысить еще больше эффективность использования VDI-инфраструктуры. Вся информация и файлы, с которыми работает пользователь, сохраняются не на его устройстве, а на корпоративном сервере или в облаке. Механизм политик безопасности позволяет гибко настроить параметры доступа пользователей к своим рабочим местам.

Терминальный доступ к приложениям

Когда нет необходимости в полноценных виртуальных ОС, а нужно только обеспечить пользователей определенным набором приложений или доступом к ресурсам сервера, рекомендуется сделать выбор в пользу терминального доступа. Для этого не нужна виртуализация, а необходим лишь сервер с установленной Astra Linux (STAL) или Windows Server.

Предоставляя пользователю терминальный сервис с помощью Termidesk, можно одновременно подключаться к рабочему столу и приложениям под управлением Linux или Windows.

Новая версия Termidesk 5.0

В мае компания "Увеон – облачные технологии" представила новую версию продукта Termidesk 5.0, в которой было реализовано несколько важных обновлений.

Обновленный "Шлюз"

"Шлюз" в его текущей реализации не требует наличия Apache-сервера, как это было в предыдущих версиях Termidesk. У него теперь имеется свой порт, через который он принимает соединения и туннелирует их. Изменился механизм запуска "Шлюза", он стал проще и удобнее. Улучшились количественные характеристики "Шлюза". Теперь поддерживается до 10 тыс. конкурентных соединений. На одном шлюзе можно использовать не 250, как раньше, а 1000 RPM.

Удаленный помощник

Инструмент "Удаленный помощник", позволяющий службе поддержки оказывать помощь пользователям в удаленном режиме. Инженеры техподдержки подключаются к RPM пользователей, что значительно ускоряет и упрощает процесс решения проблем.

Интеграция с облаками

Оркестратор Termidesk позволяет интегрировать систему как в частные, так и в публичные облака. Это дает возможность масштабировать инфраструктуру в зависимости от потребностей бизнеса, обеспечивая гибкость и надежность.

Протоколы доставки рабочих мест

Termidesk 5.0 включает значительные улучшения в области протоколов доставки рабочих мест. Для работы с 3D-графикой используется протокол Loudplay, который теперь полностью интегрирован в клиент Termidesk. Обновления на серверной стороне поддерживают новые параметры подключения клиента Loudplay, что улучшает качество и стабильность работы с графически насыщенными приложениями. Одним из главных новшеств можно назвать реализацию собственного экспериментального протокола доставки рабочих мест TERA, над которым разработчики трудились последние девять месяцев. Это было сделано по той причине, что компания RedHat отказалась считать протокол SPICE перспективным. Соответственно, на поддержку сообщества рассчитывать уже не приходится. В основе нового протокола TERA лежит модернизированный SPICE, и теперь этот протокол перенесен в гостевую операционную систему. Протокол TERA пока работает в экспериментальном режиме, поэтому его функциональность несколько ограничена. На данный момент поддерживаются базовые возможности (экран, клавиатура, мышь, видеокамера). Все ограничения протокола разработчики

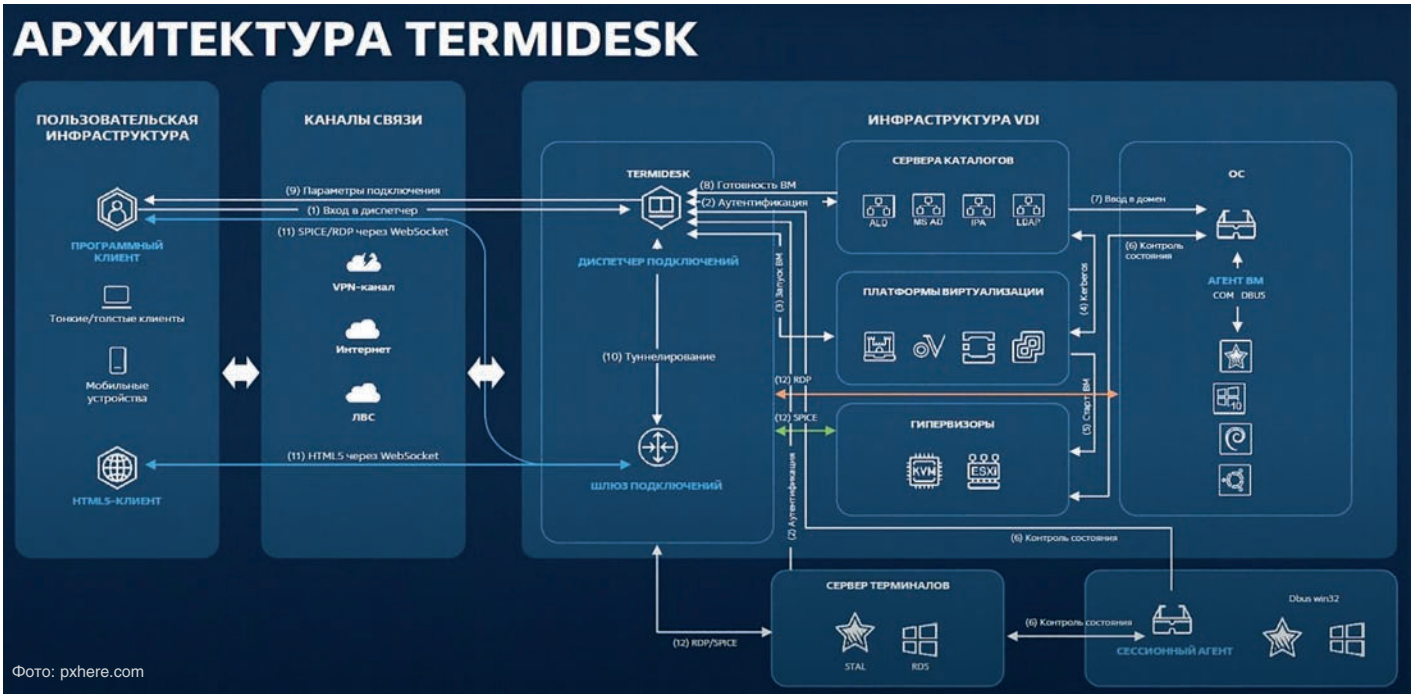

Фото: pxhere.com

обещают снять к выходу следующей версии Termidesk 5.1, которая увидит свет осенью. В ряде сценариев протокол TERA выигрывает у SPICE и RDP. В работе с офисными документами, при веб-серфинге и просмотре видео достигается существенная экономия полосы пропускания по сравнению со SPICE.

Новые поставщики ресурсов и улучшение уже имеющихся

Выросло количество поддерживаемых поставщиков ресурсов, то есть платформ виртуализации, на которых можно размещать ВРМ. Прежде всего это VMmanager – продукт "Группы Астра". Имеется механизм, который определяет доступность узлов VMmanager, размер хранилища, а также связанные клоны. Добавлены по отдельности платформы "Ред Виртуализация" и zVirt. Ранее они использовались под одним коннектором. Обновлены механизмы работы с метапоставщиком, обеспечивающим работу терминальных сессий. Для платформы VMware добавлена возможность автоматического переназначения сетей и хранилищ.

ГУСИ и УИЗР

ГУСИ (глобальный уникальный сессионный идентификатор) обеспечивает управление пользовательскими сессиями. Планируется, что в будущих версиях пользователь, запустив сессию на одном устройстве, в дальнейшем сможет ее продолжить на другом без потери приложений. ГУСИ записывает всю пользовательскую сессию, все действия пользователя. В дальнейшем это может помочь и в поиске неисправностей.

УИЗР (универсальный идентификатор запуска ресурсов) связан с конкретным приложением, которое использует пользователь. Фиксирует всю информацию для дальнейшего анализа.

Безопасность

В "Диспетчере" добавилась возможность управления политиками хранения логина и пароля в клиенте. Администратор может запретить пользователю сохранять логин и пароль при подключении к "Диспетчеру". Реализована возможность взаимной аутентификации компонентов, например работает протокол mTLS для подключения к СУБД.

Усовершенствована ролевая модель. Администратор может назначить роли не только для отдельных пользователей, но и для групп пользователей. Теперь можно вручную назначить пользователю конкретную ВМ, которая будет за ним закреплена.

Virtual Appliance

Обновился модуль Virtual Appliance. Наряду с диалоговыми окнами в терминальном режиме у него появился веб-интерфейс. Это означает, что администрировать и управлять Termidesk можно через обычный веб-браузер.

Termidesk Live

Новая возможность, реализованная в новой версии Termidesk. Он загружает рабочее место по сети. Используются портированные специально собранные приложения appimage, которые размещаются на сетевом ресурсе, затем их подмонтирует Termidesk Live, после чего пользователи могут работать с ними. Плюс в том, что передаются не все приложения, которые есть, а только те, что загружает пользователь. Перегрузки сетевого канала при этом не происходит.

Акценты будущего развития Termidesk

Разработчики намерены сосредоточить усилия на развитии масштабируемости, что актуально для больших внедрений и крупных заказчиков. Приоритетом является отказоустойчивость, которая подразумевает как стабильную работу в рамках одного ЦОД, так и поддержку катастрофоустойчивых георасределенных конфигураций. Важным направлением можно также назвать мультиплатформенность (платформы виртуализации, ОС, службы каталогов). Наконец, это пользовательский опыт – улучшение интерфейса и эргономических показателей всех компонентов Termidesk.

Что касается технологических планов, то большое будущее ждет протокол TERA. Разработчики намерены до конца нынешнего года сделать его стандартом для VDI-рабочих мест, а в следующем году внедрить этот стандарт не только для VDI, но и для терминального доступа.

Будет развиваться и терминальный сервер STAL, разработчики сосредоточат усилия на задачах в области доставки приложений, проброса периферии и двухфакторной аутентификации.

Еще одно направление – профили и слои. Эти компоненты будут реализованы с акцентом на Linux, но поддержка Windows разработчиками также обещана.

В этом году ожидается выпуск нового компонента – Termidesk Агрегатор, который будет представлять собой единую точку входа и масштабирования для множества приложений в рамках одного ЦОД. Наконец, на основе уже упомянутого нового компонента "Шлюз" будет реализована балансировка с поддержкой механизмов GSLB и L4+L7. ●

Российские решения для организации

Название решения	ТОНК TOS CDMS
Компания-разработчик, страна	ООО "Группа Компаний ТОНК", Россия
Год появления на российском рынке	2007
Поддержка интерфейса на русском языке	Да
Поддержка интерфейса на других языках	Английский, китайский
Сертификаты, патенты и лицензии	RU C-RU.HA83. A00287/20
Позиционирование	Тонкие клиенты для корпоративного сегмента
Актуальная версия	TOS4000 .1.00.04, CDMS 7.0.0.0000.43272
Аппаратные тонкие клиенты	
Модели ТК собственной разработки	TN1000V, TN1500, TN1200, TN1700, TN1900, TN1800, TN2000, TN2900
Используемые ТК других производителей	Нет
Операционная система, используемая для ТК	TOS4000 (на базе Linux), MS Win10IoT
Возможности подключения к..	Терминальным серверам, приложениям, рабочим столам и VDI
Поддерживаемые VDI-решения	Microsoft RDS, Hyper-V, VMware Horizon, Citrix Workspace, Termidesk, SPICE
Другие важные возможности ТК	Операционная система имеет нулевой интерфейс, который не позволяет работать с локальными приложениями и сохранять информацию на тонком клиенте. Графический интерфейс позволяет пользователю подключаться исключительно к удалённым приложениям, рабочим столам и VDI. Тонкие клиенты не имеют движущихся частей, это увеличивает срок службы устройства до 9 лет. В линейке есть бюджетные ТК с процессорами ARM
Платформа для управления ТК	
Название платформы	CDMS (Centralized Desktop Management System)
Поддерживаемые серверные ОС для установки	MS Server, Desktop OS, Linux
Централизованное управление парком ТК	Да
Развертывание ТК	Да
Авто обнаружение ТК	Да
Обновление ТК	Да
Мониторинг конфигурации и состояния ТК	Да
Мониторинг действий пользователя ТК	Да
Встроенные отчеты	Да
Другие важные функции платформы управления	Система управления позволяет управлять тонкими клиентами с TOS4000 (x86/ARM) и MS Win10IoT. Система управления позволяет снять настройки с одного тонкого клиента и быстро распространить эти настройки на сотни и тысячи подобных устройств. Максимальное количество управляемых устройств – до 250 тыс., ТК управляются из единого центра системой управления ТОНК CDMS
Сайт с подробностями решения	https://tonk.ru

инфраструктуры тонких клиентов

Kaspersky Thin Client	GM SMART SYSTEM
"Лаборатория Касперского", Россия	GETMOBIT, Россия
2022	2017
Да	Да
Английский, португальский бразильский, испанский	Английский
Реестр российского ПО	Реестр российского ПО, сертификат ФСТЭК России, патенты
Кибериммунная, управляемая и функциональная инфраструктура тонких клиентов	Экосистема продуктов на базе комплекса программных средств и оригинальной линейки оборудования для безопасного и унифицированного подключения пользователей к виртуальным рабочим столам и сервисам унифицированных коммуникаций
Kaspersky Thin Client 2.0	Система управления: 3.15.1, встроенное ПО GM CORE KIT 2.4.0
Нет	GM-Box G1 Base, GM-Box G1 Duo
TONK TN1200, Centerm F620	Возможна установка встроенного и системного ПО на ТК, ПК и ноутбуки других производителей
Kaspersky Thin Client (на базе микроядерной KasperskyOS)	GM CORE KIT
Терминальным серверам, удаленным виртуальным машинам, VDI-инфраструктуре, удаленным физическим ПК или серверам, серверам приложений	VDI, терминальным серверам, терминальным станциям, веб-сервисам, SIP АТС, SIP ВКС
Microsoft Remote Desktop Services, Базис WorkPlace, Citrix и VMware Horizon	VDI SPACE, VDI VeiL, Горизонт-ВС, Термидеск, BASIS, Huawei Fusion, VMware Horizon, Citrix, Microsoft RDP/RDS
Настраиваемая панель управления Kaspersky Thin Client. Настройки интерфейса в соответствии с индивидуальными предпочтениями. Расширенная система уведомлений. Детализированные сообщения об ошибках с советами по их устранению. Автоматическое переподключение к удаленному рабочему столу в случае разрыва соединения. Поддержка аудиоконференций в решениях VideoMost, IVA Technologies и SPIRIT DSP. Перенаправление периферийных устройств, подключенных к тонкому клиенту. Образ обновления составляет не более 300 Мбайт. Обеспечение защиты тонких клиентов на уровне архитектуры без необходимости установки дополнительных средств защиты информации СЗИ	Централизованное управление устройствами пользователей в т.ч. в георазпределённых сетях. Возможность работы в нескольких контурах с одного устройства (в модификации GM-Box DUO). Замена тонкого клиента, видеотелефона, WiFi, LTE модулей, проводной и беспроводной зарядки в одном устройстве. Вариативные способы идентификации и аутентификации. Мобильное приложение для аутентификации на устройствах GM-Box (доступно для ОС Аврора, Android, iOS)
Платформа для управления ТК Kaspersky Security Center 14	GM Workspace Factory
MS Windows (64), Linux (64), Astra Linux, Альт Сервер, РЕД ОС Сервер	Astra Linux, Ред ОС, Ubuntu
Да	Да
Да	Да
Да	Да
Да	Да
Да	Да
Да	Да
Да	Да
Быстрая интеграция тонких клиентов в инфраструктуру. Контроль сетевых подключений к удаленным рабочим столам. Настройка языков интерфейса и ввода: выбор только необходимых пользователю раскладок клавиатуры. Разграничение прав доступа к настройкам администрирования. Гибкое управление периферийными устройствами тонкого клиента. Управление энергосбережением тонкого клиента. Авторизация критичных действий пользователя на тонком клиенте. Управление настройками подключений к удаленным рабочим столам	Интеграция со службами каталогов ALD Pro, FreeIPA, MS Active Directory. Автоматическое профилирование пользовательских устройств. Интеграция с syslog/SIEM. Логирование событий ИБ системы управления
https://os.kaspersky.ru/solutions/kaspersky-thin-client/	https://getmobit.ru/

Представленные в таблице данные предоставлены соответствующими компаниями.
Редакция выполнила работу по сбору данных, но не проверяла их соответствие действительности.

Тонкие клиенты для гибкой информационной безопасности

Круглый стол производителей

В современном бизнес-ландшафте тонкие клиенты становятся важным элементом инфраструктуры благодаря своей способности обеспечивать эффективное управление ресурсами и высокую степень безопасности данных. Использование тонких клиентов способствует повышению безопасности, так как данные хранятся на сервере, а не на пользовательских устройствах, что минимизирует риски потери или краж.
Редакция поинтересовалась у экспертов, как наиболее эффективно использовать такую инфраструктуру и как уберечься от типовых ошибок.

Сергей Даниэльян, *руководитель отдела системной разработки GETMOBIT*
Михаил Левинский, *старший менеджер продукта, "Лаборатория Касперского"*
Александр Тарасов, *главный архитектор технологической платформы GETMOBIT*
Михаил Ушаков, *генеральный директор ООО "Группа Компаний ТОНК"*
Василий Шубин, *руководитель центра развития продукта и компетенций GETMOBIT*

Топ-3 основных вызовов для заказчика, ответом на которые может быть использование инфраструктуры тонких клиентов.

Михаил Ушаков, ТОНК:

1. Надежность бизнеса. Собственная производственная линия, полный контроль качества продукции, налаженная логистика – все это позволяет нам закрывать потребности наших клиентов в период санкций без ущерба в сроках поставки.

2. Информационная безопасность. Защитить сервер (кластер) проще, исключаются утечки данных, любой пользователь информационной системы находится под строгим контролем.

3. Снижение затрат. Переход на тонкие клиенты кардинально снижает затраты на поддержку ИТ-инфраструктуры.

Михаил Левинский, Лаборатория Касперского:

Главные вызовы:

1. Низкая скорость и высокая стоимость масштабирования и технического сопровождения географически распределенных подразделений организации.

2. Высокие затраты на администрирование инфраструктуры состоящей их традиционных рабочих станций.

3. Низкий уровень обеспечения защиты корпоративных данных, расположенных на рабочих станциях пользователей.

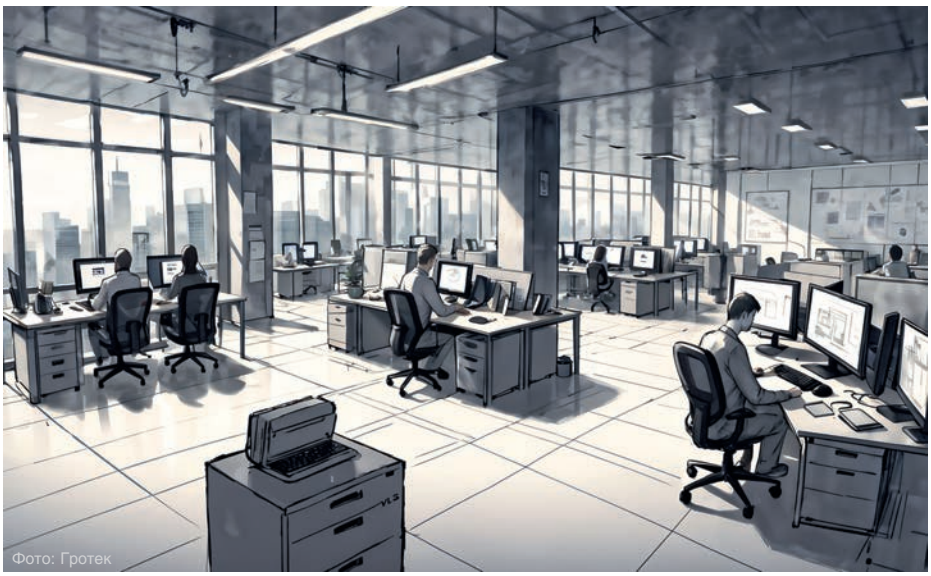

Фото: Гротек

Александр Тарасов, GETMOBIT:

1. Наличие каналов связи с ограниченной пропускной способностью между рабочими местами и датацентром, подходящих для работы протоколов удаленного доступа, но не подходящих под "толстые" обновления ОС общего назначения и ее приложений. Инфраструктура ТК позволяет гарантированно управлять РМ вне зависимости от канала подключения.

2. Безопасность рабочего места по подходу к архитектуре системы, а не по количеству наложенных средств безопасности. Дизайн ОС ТК имеет минимальную поверхность атаки, благодаря чему количество инцидентов стремится к нулю.

3. Необходимость эффективно работать с большим количеством сред VDI, решений VPN и ВКС. Усилия вендоров тонких клиентов направлены на совершенствование специализированных прошивок и систем, что позволит одновременно взаимодействовать с множеством ИТ-систем и предоставит инструмент для плавного и предсказуемого перехода с зарубежных на российские среды VDI без потери стабильности бизнес-процессов.

Как внедрение тонких клиентов влияет на общие затраты на ИТ-инфраструктуру и поддержку по сравнению с использованием персональных компьютеров?

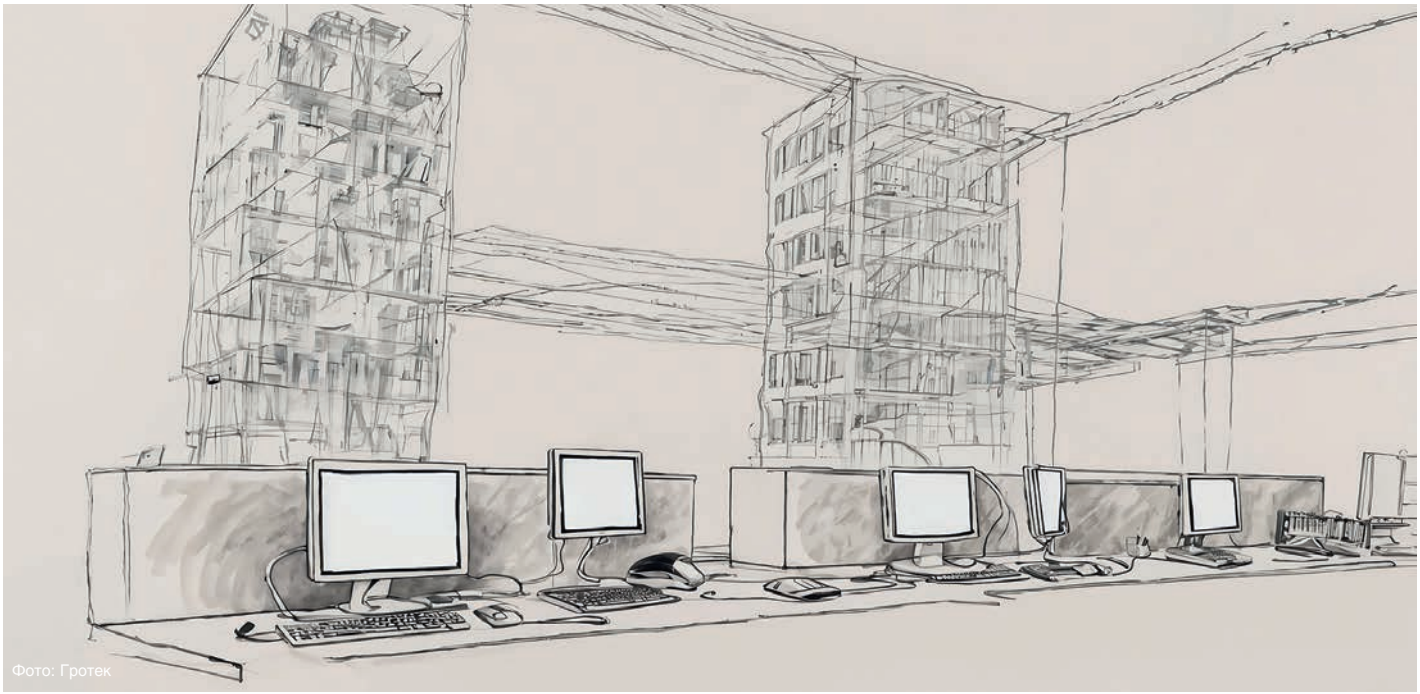
Фото: Гротек

Михаил Левинский, Лаборатория Касперского:

Использование тонких клиентов существенно сокращает стоимость владения рабочим местом пользователя за счет сокращения затрат:

- на обеспечение средств кибербезопасности конечных устройств пользователей;
- на масштабирование и администрирование тонких клиентов, особенно расположенных в географически удаленных точках;
- на техобслуживание тонких клиентов, которые реже выходят из строя, чем традиционные рабочие станции и имеют более длительный срок эксплуатации;
- на коммунальные платежи за электроэнергию;
- на услуги высококвалифицированных специалистов, способных обслуживать тонкие клиенты в отдельных бизнес-юнитах организации.

Сергей Даниэльян, GETMOBIT:

Переход на инфраструктуру тонких клиентов позволяет снизить как капитальные затраты на ИТ-инфраструктуру (CAPEX), так и операционные (OPEX). Устройства для доступа к инфраструктуре требуют гораздо меньших вычислительных возможностей по сравнению с ПК, что позволяет сократить расходы на оборудование рабочих мест. Устройства ТК быстро конфигурируются и обновляются, настройка одного тонкого клиента приравнивается к настройке десятка обычных устройств по трудозатратам за счет возможности использования шаблонов. Учитывая неизменяемость и файловую систему read-only, снижаются затраты на управление парком устройств. Кроме того, количество инцидентов в техподдержке за счет безопасного дизайна ТК становится минимальным.

Михаил Ушаков, ТОНК:

Затраты на поддержку ИТ-инфраструктуры снижаются в несколько раз. Известно, что персональный компьютер утраивает свою стоимость в течение пяти лет эксплуатации. Инфраструктура, построенная на виртуализации, требует 8–10% ежегодных затрат от первоначальной стоимости внедрения. Многочисленные исследования свидетельствуют о снижении и прямых и косвенных затрат – тонкие клиенты имеют более длительный жизненный цикл и потребляют меньше электроэнергии.

Возможна ли для заказчика плавная миграция с персональных компьютеров на тонкие клиенты?

Михаил Ушаков, ТОНК:

Именно так и происходит в реальности! Заказчик или уже имеет избыточные серверные ресурсы, на которых разворачиваются виртуальные АРМ и приложения для безопасного доступа, или вводит новые, позволяющие масштабировать инфраструктуру предприятия. Сегментарно часть ПК превращаются в тонкие клиенты и по мере вывода их из эксплуатации заменяются на тонкие клиенты. Часто новые филиалы (подразделения) сразу оснащаются тонкими клиентами.

Михаил Левинский, Лаборатория Касперского:

Да, миграция возможна. Как правило она происходит плавно и без ущерба основному бизнесу организации. В этом случае традиционные рабочие станции, которые устаревают, выходят из строя или требуют дополнительных капитальных вложений, заменяются на тонкие клиенты.

Василий Шубин, GETMOBIT:

Этот вопрос стоит разбить на две части.

Во-первых, переход на инфраструктуру VDI (или публикация приложений на терминальных серверах), во-вторых, перевод АРМ в архитектуру тонких клиентов.

Первая задача давно и успешно решается благодаря продуктам разработчиков систем VDI. Вторая задача часто пугала заказчиков, так как представлялась как необходимость сиюминутной замены всего парка АРМ с одного типа устройств на другое.

С решением GETMOBIT плавная миграция с инфраструктуры классических АРМ становится возможной за счет автоматизированной и централизованной конвертации существующих устройств в управляемые тонкие клиенты без существенных трудозатрат.

Топ-3 ошибок заказчика, которые снизят эффективность использования инфраструктуры тонких клиентов и ваши рекомендации, как их избежать.

Александр Тарасов, GETMOBIT:

1. Установка на ТК операционной системы общего назначения, увеличивающей затраты на внедрение и сопро-

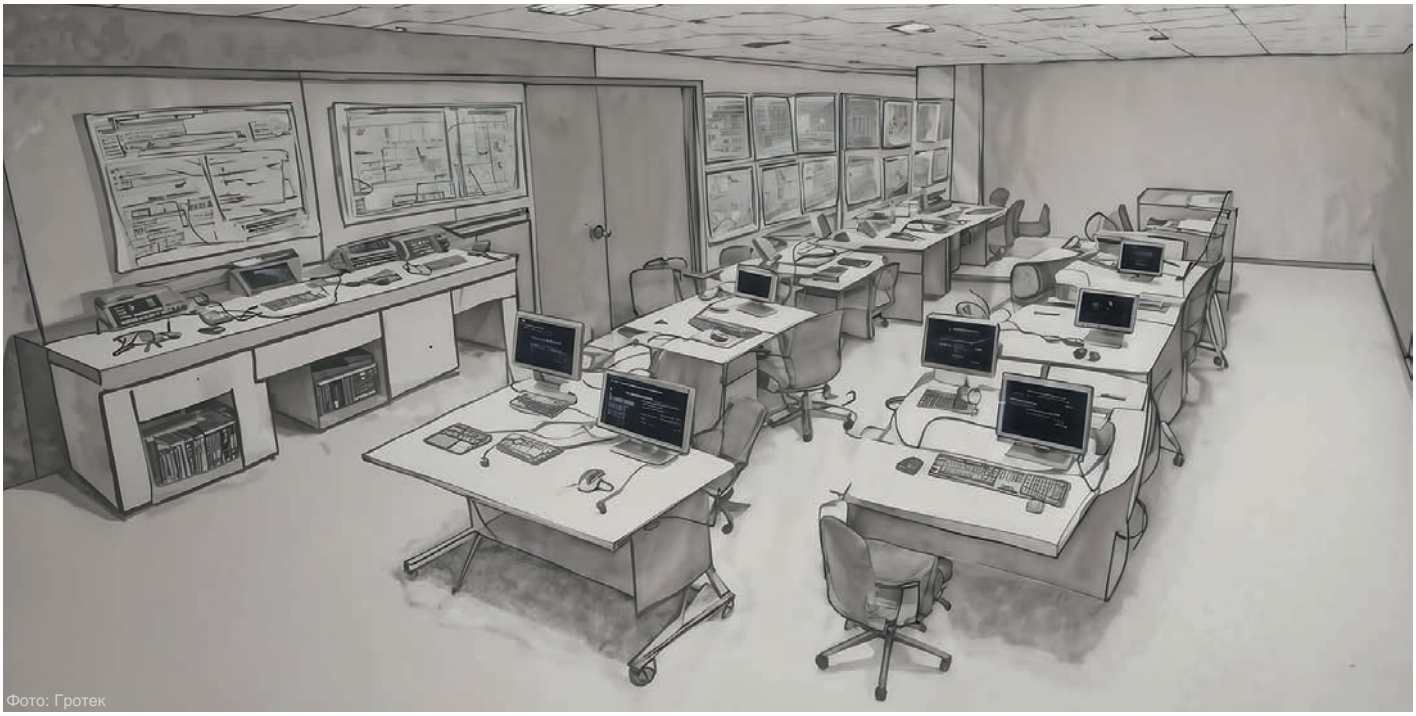
Фото: Гротек

вождение. Как избежать: выбирать решения со специализированным для ТК системным ПО, управляемой с системой (сервером), которые учитывают все особенности эксплуатации таких систем.

2. Выбор неподходящей под задачи заказчика среды VDI и протокола доступа. Ошибка с выбором может создать ограничения для продуктивной работы пользователей (скорость работы, отзывчивость интерфейса приложений, поддержка механизмов идентификации, аутентификации пользователей с применением смарт-карт и аппаратных токенов, корректность работы периферийных устройств, возможность использовать современные средства унифицированных коммуникаций и т.д.). Как избежать: тщательно анализировать возможности VDI, используемые ими протоколы, требования прикладного ПО. Проводить проектирование, пилотирование и внедрение выбранного решения с опытным квалифицированным партнером в тесном взаимодействии с вендорами ТК и VDI.

3. Слепое копирование требований ИБ с классической архитектуры ПК.

Как избежать: трезво и взвешенно анализировать требования регулятора в контексте конкретного ИТ-ландшафта и бизнеса заказчика, реализовывать возможности, предоставляемые технологией защиты среды виртуализации, оценивать влияние средств наложенной безопасности на работу протоколов удаленного доступа.

Михаил Левинский, Лаборатория Касперского:

Иногда заказчики рассматривают тонкие клиенты как традиционные персональные компьютеры и пытаются полностью или частично перенести пользовательское ПО из удаленной среды на сторону тонкого клиента. Причины этому могут быть самые разные. В большинстве случаев это решается путем правильного построения VDI-инфраструктуры и выбора пользовательского ПО, которое подходит для такого класса решений.

Михаил Ушаков, ТОНК:

Эти ошибки характеризуются следующими утверждениями: "Он ценный сотрудник, и мы ему доверяем, поэтому для него мы сделаем исключение. Мы так делали последние десять лет, и ничего не случилось." Все, что нарушает единую стратегию цифровой трансформации, стандарты ИБ и подходы к обработке критически важной информации, разрушает бизнес. В офисе рядовой сотрудник использует стационарный тонкий клиент. Дайте топ-менеджеру тонкий клиент в форм-факторе ноутбука, и если он даже его потеряет, это не приведет к катастрофе.

Какие мировые и российские тренды в развитии технологии тонких клиентов вы наблюдаете?

Михаил Ушаков, ТОНК:

Мобильность, внедрение новых технологий, отказ от обязательной работы в офисе – вот, что определяет современные тренды виртуализации рабочих мест. Citrix и VMware претерпевают трансформацию, Microsoft RDS сохраняет господствующие позиции. Вендоры идут по пути создания собственных комплексных решений (пример – HP Anywhere), больше возникает "носимых тонких клиентов". В России формируются и укрепляются отечественные решения, которые уже готовы стать альтернативой ушедшим иностранным.

Михаил Левинский, Лаборатория Касперского:

Если раньше тонкие клиенты использовались в основном для сотрудников, которые работают с текстовыми данными, то сейчас запрос на тонкие клиенты расширился в сторону потребления мультимедиа и сложной 3D-графики. Это, в свою очередь, определило высокие требования к протоколам доставки удаленного контента и компонентам аппаратной платформы тонких клиентов.

Сергей Даниэльян, GETMOBIT:

1. BYOD – превращение практически любого устройства в ТК.

2. Развитая экосистема VDI: поддержка широкого круга VDI (в том числе российских: например Термидеск, Space, Базис и др.), легкая и быстрая интеграция новых решений.

3. Наличие возможности безопасного изолированного выполнения локальных приложений на ТК (например клиенты ВКС).

4. Переход на программные средства ВКС. Увеличение количества работы с медиапотоками в среде VDI.

5. Уход от концепции нулевого или аппаратного тонкого клиента из-за их ограниченного по архитектуре функционала. ●

Ваше мнение и вопросы присылайте по адресу
is@groteck.ru

Сравнительная таблица тонких клиентов ТОНК

Модель	TN1000V	TN1200	TN1500	TN1700	TN1800	TN1900	TN2000/2900	TN4009/4010
Сегмент	Бюджетный	Базовый	Бюджетный	Премиум	Премиум	Бюджетный	Специальный	Бюджетный
Сферы использования	Офис, образование, ретейл	ГИС, банки, КИИ, офис, медицина, облака	Банки, офис, образование, ретейл, медицина	Банки, офис, медицина, строительство	Банки, офис, медицина, строительство	Банки, офис, образование, ретейл, медицина	Производство, банки, ретейл, медицина	Производство, банки, офис, образование, ретейл, медицина
Реестр РРЭП, включен в ГИСП	Нет, нет	Да, да	Нет, нет	Нет, нет	Нет, нет	Нет, да	Нет, нет	Нет, нет
Год запуска в производство	2022	2020	2016	2022	2024	2016	2016/2020	2023
Пассивное охлаждение без движущихся частей	Да	Да	Да	Да	Да	Да	Да	Да
CPU (архитектура)	RK3568 (ARM)	J4125 (x86)	GX218GL (x86)	N5105 (x86)	N200 (x86)	J1900 (x86)	J4125/N5105 (x86)	N5105
RAM установлено/максимально, Гбайт	4	4/8	4/8	4/16	8/32	4/8	4/8/16	8/16
SSD, Гбайт	8	64	64	64	128	64	64	256
Поддержка цифровых дисплеев	2	2	2	3	3	2	2/3	2
USB-C	Нет	Нет	Нет	Да	Да	Нет	Нет/Да	Нет
COM-порт	Нет	Нет	Нет	Нет	Нет	Нет	Да	Да
2 сетевых интерфейса	Нет	Нет	Нет	Нет	Нет	Нет	Да	2
Оптический сетевой интерфейс	Нет	Нет	Нет	Нет	Нет	Нет	Опционально	Нет
Беспроводная сеть	Опционально	Опционально	Опционально	Опционально	Опционально	Опционально	Опционально	Да
Поддержка аппаратных (программных) АПМДЗ	Нет	Да	Да	Да	Да	Да	Да	Да
Поддержка TOS 4000	Нет	Да	Да	Да	Да	Да	Да	Да
Поддержка российских ОС из реестра Минцифры	Нет	Да	Да	Да	Да	Да	Да	Да
Поддержка MS Win10 IoT / Win11	Нет	Да	да	Да	Да	Да	Да	Да
Поддержка ОС Kaspersky Thin Client	Планируется	Да	Нет	Нет	Планируется	Нет	Нет	Нет
Централизованная система управления	Да	Да	Да	Да	Да	Да	Да	Да
Универсальное VESA-крепление (100/75)	Да	Да	Да	Да	Да	Да	Да	Да
Форм-фактор	Ультракомпакт	Ультракомпакт	Ультракомпакт	Ультракомпакт	Ультракомпакт	Ультракомпакт	Компактный	Ультракомпакт
Гарантия стандарт/расширенная, мес.	36/нет	36/60	36/нет	36/60	36/60	36/60	36/60	36/нет

Данные предоставлены ООО "Группа Компаний ТОНК"