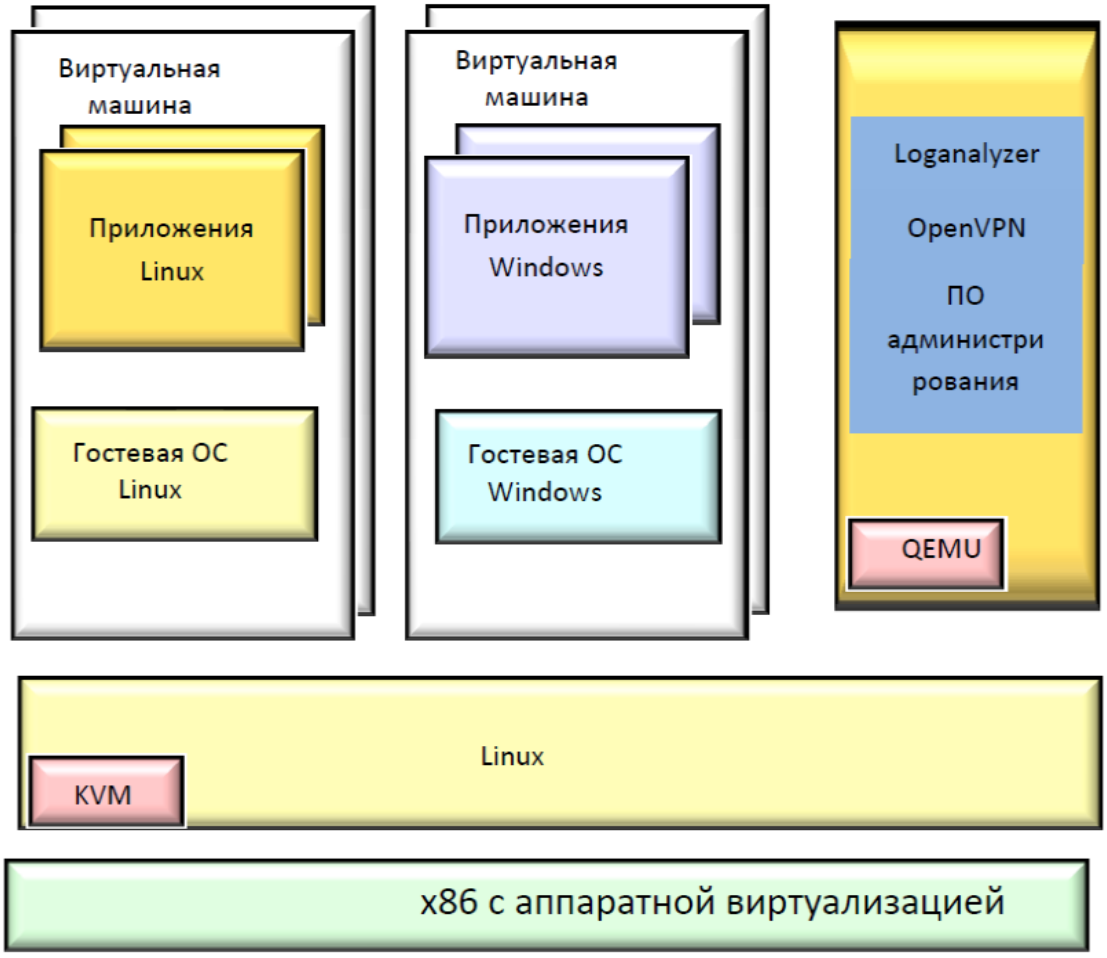
4. Минимизация сложности и количества используемого оборудования, минимизация архитектуры применяемых информационно-технических средств, максимально упрощенное физическое обслуживание, удаленное обслуживание и администрирование.
5. Обеспечение возможности использования электронной подписи в режимах:
    - Подпись локально на рабочем месте;
    - Облачная подпись.
6. Возможность работы со всеми виртуальными ресурсами предприятия, включая электронный документооборот.
7. Возможность повторного использования уже имеющегося оборудования.

Абонентский облачный терминал

Программное средство общего назначения с встроенными средствами защиты «Абонентский облачный терминал» (АОТ) решает задачу путём совмещения на одной аппаратной единице, персональном компьютере, произвольного количества разнородных, изолированных, не зависимых друг от друга рабочих мест. Программный комплекс АОТ концептуально схож по архитектуре с Qubes OS, но выполнен на других программных платформах. Реализация АОТ основана на применении технологии виртуализации. Программное обеспечение состоит из модуля KVM, выполняемого на уровне ядра Linux, как представлено на рисунке ниже (См. Рисунок 1) Для эмуляции аппаратного обеспечения процессоров Intel x86 и устройств ввода-вывода виртуальных рабочих мест используется QEMU.



исунок 2 Архитектура программного комплекса АОТ

Модуль KVM ядра Linux позволяет QEMU, выполняющемуся в пространстве пользователя, использовать возможности аппаратной виртуализации, предоставляемые современными x86-совместимыми процессорами, для повышения производительности виртуальных рабочих мест.

Каждое рабочее место работает под управлением своей операционной системы, в своём программном и сетевом окружении, включая возможность полной изоляции от сети. Администратор, контролирующий АОТ локально или удаленно из центра управления, конфигурирует комплекс, в том числе настраивает доступ пользователей

к локальным настройкам АОТ, которые отвечают их служебным обязанностям и соответствуют принятой политике безопасности.

АОТ реализует в своем составе работу тонкого клиента в режиме удаленного терминального доступа. Помимо тонкого клиента АОТ совмещает на одной аппаратной единице несколько одновременно работающих полностью изолированных друг от друга виртуальных АРМ, каждое из которых может работать как автономно, так и, при наличии сетевого соединения, в своём домене. Время переключения между различными АРМ составляет не более двух секунд. Реализация этого компонента также возможна на выносном USB-носителе, подключаемом практически к любому современному персональному компьютеру, допускающему загрузку с внешнего диска. При этом доступ к внутреннему диску этого компьютера с установленных на внешнем диске АРМ может быть исключён.

Администрирование АОТ может осуществляться централизованно с рабочего места администратора в инфраструктуре предприятия, либо локально. Также возможен мониторинг работы пользователя, в том числе файлового обмена между виртуальными машинами с анализом содержимого файлов. Содержимое файла может передаваться в автоматическом режиме на сервер для более детального анализа в зависимости от требований и настроек политик безопасности. Журнальные записи действий пользователя, включая действия внутри виртуальных рабочих мест, передаются для анализа в оригинальном и/или предобработанном виде в Центр оперативной безопасности предприятия для дальнейшего интегрального анализа.

АОТ компенсирует следующие риски:

1. Риски, вызванные необходимостью наличия постоянного надёжного широкополосного сетевого соединение клиентского рабочего места со службами централизованной (облачной) вычислительной структуры предприятия (далее - ЦВС).

АОТ наряду с обеспечением работы в терминальном режиме допускает работу автономно, без использования постоянного соединения с информационной инфраструктурой предприятия. В этом случае, сетевое соединение требуется исключительно для обмена пользовательскими данными, а также в случае необходимого обновления конфигурации рабочего места в технологические периоды, когда каналы связи менее всего загружены. Администрирование, аудит и контроль рабочих мест осуществляется централизовано администраторами ЦВС.

2. Отсутствие шифрования канала в классических терминальных решениях.

АОТ обеспечивает защищенный канал с ЦВС, что позволяет при необходимости использовать открытые каналы связи.

3. Недостаточно проработанные вопросы обеспечения безопасности клиентского места.

Изоляция рабочих мест, находящихся под управлением АОТ, допускает сертификацию регулятора ввиду сравнительно небольшого объёма исходного кода.

4. Даже при полном выполнении всех требований по скорости и качеству соединения для большинства пользователей, останутся категории рабочих мест, для которых качества и скорости будет не хватать. Число рабочих мест с повышенными требованиями к средствам коммуникации с развитием цифровых технологий будет только расти. Единственная альтернатива – перевод рабочих мест

для обслуживания основных бизнес-процессов на алфавитно-цифровые терминалы, но это уже невозможно. Принципиальная невозможность оперативной предварительной обработки первичных данных на рабочих местах приводит к непропорциональному увеличению загрузки коммуникационных линий и выделенных серверов для обработки этих данных. А объём таких данных будет только расти. В условиях терминального решения, первичная предобработка таких данных практически исключена.

Единственным выходом из ситуации представляется возможность локальной предварительной обработки данных в автономном режиме с последующей отложенной синхронизации с ЦВС в специально выбранные технологические периоды. Не исключается применение открытых сетей при условии защиты канала связи на транспортном уровне модели OSI и использовании провайдера СКЗИ.

5. Проблема подключения пользователей к сети Интернет централизованно приводит к росту нагрузки на каналы связи, децентрализовано - усложняет архитектуру программно-аппаратных средств на местах. При этом требование использования отдельного компьютера для доступа к сети Интернет в обоих случаях ведет к усложнению архитектуры и дополнительным затратам.

Изоляция рабочих мест, находящихся под управлением АОТ, позволяет в решении использовать локальные подключения к открытым сетям. Контроль за исполнением политик информационной безопасности и мониторинг обмена между

рабочими местами, включая семантический анализ передаваемой между рабочими местами информации, лежит на администраторах ЦВС.

6. Как показывает практика, конечные пользователи не отказываются от использования персональной вычислительной техники, а значит:

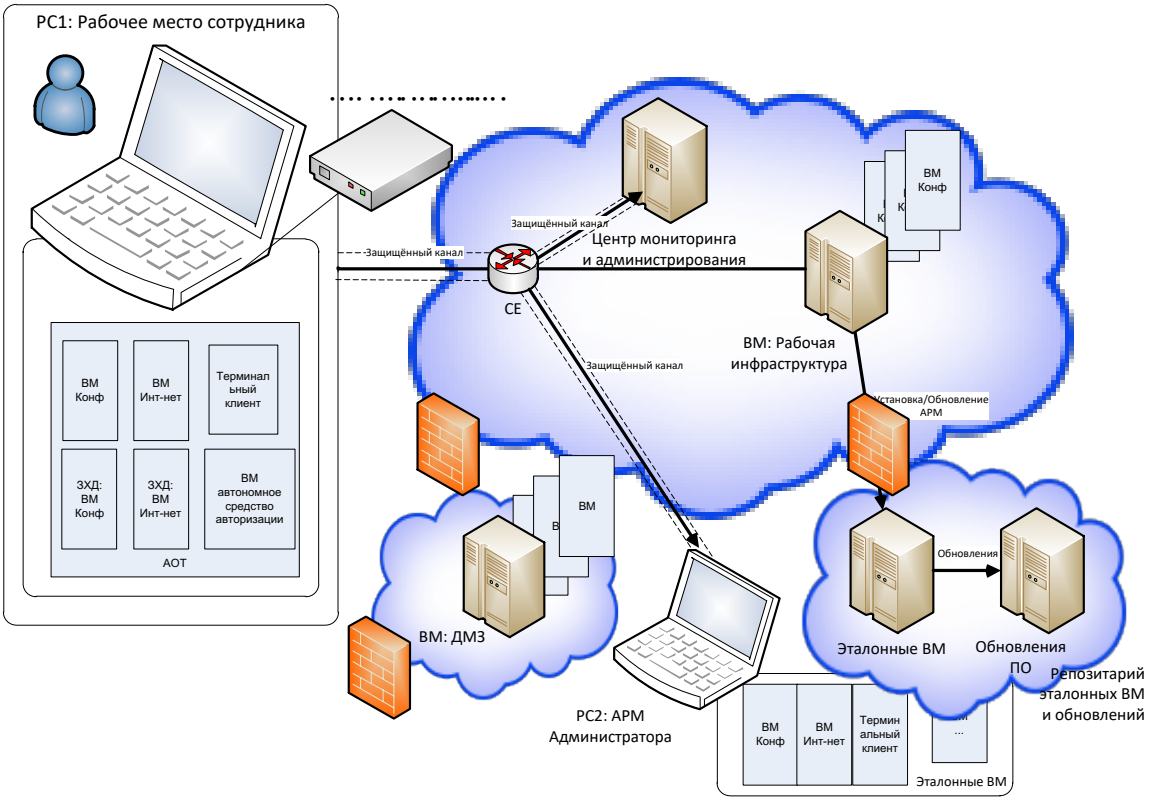
– Будут использоваться различные каналы для работы с данными вне защищённого контура на неконтролируемом оборудовании

– Имеются риски потери и нарушения целостности данных, утечки информации

– Возникают нарушения политик информационной безопасности.

Как указано выше, применение АОТ не только не ограничивает использование открытых сетей с рабочего компьютера, но и повышает эргономику такой работы, не нарушая при этом политик информационной безопасности организации.

Таким образом, предлагаемое решение позволяет компенсировать изложенные выше недостатки, сократить операционные и капитальные затраты, возникающие в процессе эксплуатации.



Составные части:

- Хранилище эталонных ВМ и обновлений;
- Инфраструктура ЦВС;
- Демилитаризованная зона.

Хранилище эталонных ВМ и обновлений содержит эталонные ВМ, серверы с обновлениями ПО. Задачи, решаемые в этой части ЦВС: формирование проверенных, согласованных, безопасных эталонных рабочих мест в виде контейнеров с типовыми ВМ.

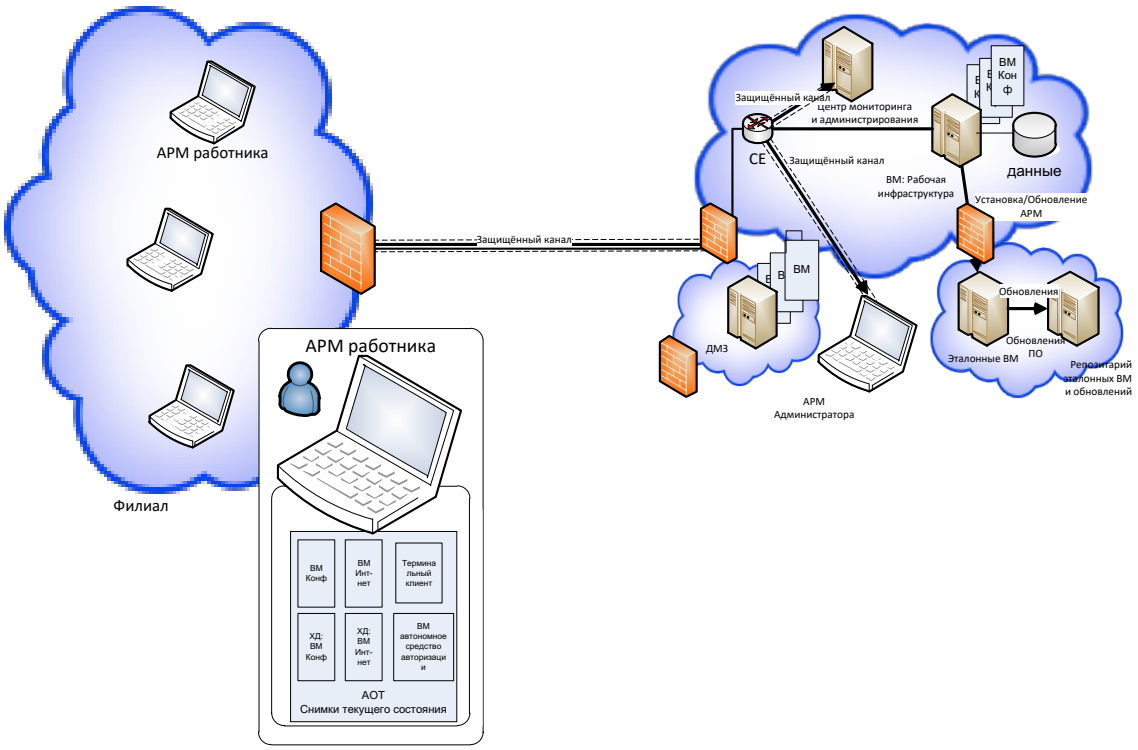
Рабочая инфраструктура ЦВС – продукционный ландшафт, состоящий из компонентов информационной инфраструктуры, элементов, услуг и ВМ, прошедших принятую на предприятии процедуру внедрения в постоянную эксплуатацию. В этой части ЦВС находятся в том числе серверы с ВМ, реализующими рабочие места сотрудников.

ДМЗ (демилитаризованная зона) – для размещения ВМ для работы с открытыми сетями.

На рабочем месте находится АОТ, задача которого:

- Работа в терминальном режиме без скачивания контейнера с ВМ по выделенным или защищённым каналам с использованием открытых сетей.
- Безопасный терминальный доступ к VDI Рабочей инфраструктуры ЧОБР.
- Безопасный терминальный доступ к VDI ДМЗ.
- Репликация эталонной ВМ Рабочей инфраструктуры на персональный компьютер.
- Репликация эталонной ВМ ДМЗ на персональный компьютер.
- Репликация ВМ из Рабочей инфраструктуры ЦВС на персональный компьютер при необходимости работы off-line в условиях, где соединение с информационной инфраструктурой сильно затруднено или невозможно, например, дома, в командировке, местах без наличия выхода в интернет. После выполнения работы в режиме off-line и возвращения к работе с сетью предприятия ВМ вместе с результатами работы перемещается в Рабочую инфраструктуру.
- Безопасная одновременная работа во всех перечисленных выше режимах
- Создание VPN канала.
- Электронная подпись.

Один из существенных недостатков типового решения состоит в том, что для размещения на персональном компьютере образа виртуальной машины с установленной на ней полноценной ОС, например, MS Windows 10, необходимо скопировать и передать по сети около 40 Gb, что выливается в длительную процедуру обновления и приводит к «коллапсу» системы связи.



Возможны несколько вариантов компенсации сформулированного выше недостатка:

– Вариант 1. На установленном на рабочем месте АОТ при начальной конфигурации установить на встроенный диск персонального компьютера актуальные эталонные образы виртуальных машин из ЦВС (см. диаграмму выше). В процессе эксплуатации обновления/изменения установленных ВМ проводятся инкрементально с использованием механизма снимка состояния жёсткого диска ВМ, состоящего из измененных блоков. Размер устанавливаемого снимка ВМ существенно меньше размера самой ВМ, а проксирование трафика позволит значительно оптимизировать использование каналов с ЦВС в процессе обновления ВМ.

– Вариант 2. При необходимости использовать оборудование, которое по ряду причин не обладает нужным объёмом встроенного диска, при начальной конфигурации расположить образы виртуальных машин на индивидуальном внешнем носителе, например, SD карте или ином USB-устройстве. Для оптимизации процесса первоначальной конфигурации внешние носители допускают клонирование любым из доступных способов. Требования по скорости обмена с таким устройством не предъявляются, так как оперативная работа виртуальной машины происходит с использованием встроенных средств хранения информации, расположенных локально на рабочих местах так, что хранятся лишь изменения к этим образам в допускающем хранение изменений формате дискового образа (например, Qcow2). Это позволяет существенно понизить требования к объёму непосредственно жёсткого диска рабочего места или замещающего его устройства хранения информации в АРМ до 12-16 Gb. В свою очередь, это даёт теоретическую возможность использовать имеющиеся в распоряжении организации терминальные устройства типа «тонкий клиента».
– Вариант 3. Этот вариант предполагает комбинацию перечисленных выше подходов в зависимости от конкретных сложившихся обстоятельств и может быть предложен после проведения анализа и согласования условий эксплуатации.

При тестировании варианта 2 было выявлено, что для доступа к образу диска виртуального рабочего места по сети приемлемым является применение протокола NBD при следующих условиях:

пропускная способность канала от 200 мбит/с, круговая задержка до 10 мс.

Преимущества предлагаемого решения

1. Обработка информации различной категорийности на одной аппаратной единице, в том числе в режиме офф-лайн, без подключения к сети и корпоративным серверам.
2. Исполнение АОТ на внешнем жестком диске, благодаря защите от НСД носителя, каналов связи, а также наличию дополнительных средств защиты позволяет выездным сотрудникам, используя произвольную аппаратную единицу (ноутбук, стационарный компьютер и т.п.), работать с конфиденциальной информацией в условиях небезопасной среды (в заграничных командировках, в гостиницах, дома и т.п.)
3. Гибкая интеграция с другими средствами защиты информации (антивирусы, СРД, межсетевые экраны, анализаторы уязвимостей и т.п.) с целью улучшения защищенности рабочего места.
4. Минимизация возможностей для атак на рабочие места через переносимые устройства путём полного контроля подключаемых периферийных устройств с уровня гипервизора.
5. Мониторинг информационного взаимодействия. Нарушитель не может воздействовать на механизмы журналирования средствами гипервизора, что не позволяет ему скрыть следы воздействия.
6. Повышенная отказоустойчивость и доступность. За счет механизма горячего кэширования присутствует возможность полностью сохранить состояние виртуальной машины в произвольный момент времени и в случае необходимости восстановить данное состояние.

7. Мониторинг работы пользователя в части сети: скачивания файлов между контурами. Регистрируется факт, что пользователь скачал или отправил файл, администратор безопасности при желании может видеть содержимое файла. Содержимое файла может анализироваться на месте или передаваться в автоматическом режиме на сервер для более детального анализа в зависимости от требований и настроек политик безопасности. В зависимости от требований к системе анализа, для анализа можно использовать решения, начиная от простых компонент свободного распространения до самых изощрённых проприетарных современных систем с использованием искусственного интеллекта и нейронных сетей.
8. Журнальные записи всех действий пользователя включая все рабочие места, передаются для анализа в оригинальном и/или предобработанном виде в SOC для дальнейшего интегрального анализа.
9. Рабочие места, реализованные в виде виртуальных машин, централизованно администрируются из Центра при наличии сетевой связности.

Вывод

Представленное в работе решение:

1 не требует для своей работы наличия обязательного сетевого соединения со специальным сервером управления;

2 не накладывает ограничения на использование типа операционной системы для рабочего места пользователя;

3 не требует обязательной перезагрузки для переключения между сетевыми сегментами;

4 позволяет проводить необходимую пред/постобработку данных локально для выполнения требований конкретного офиса и департамента;

5 обеспечивает работу на персональных компьютерах одновременно в различных категорированных сегментах корпоративной сети, например, работа трейдеров с торговыми площадками и одновременно в защищённом периметре локальной вычислительной сети;

6 организация удалённого рабочего места сотрудников, например, из дома или в командировках;

7 безопасная работа на любом компьютере (коллективного пользования, домашний) в привычной для массового пользователя среде MS Windows;

8 использование продуктов и решений по организации защищённых виртуальных частных сетей.

9 безопасная работа с индивидуального переносного USB-диска;

10 одновременная изолированная работа нескольких виртуальных машин с остановкой всех процессов в неактивной виртуальной машине;

11 миграция ВМ из центра на рабочее место и обратно при необходимости;

12 мгновенное переключение между виртуальными машинами;

13 контроль ОС с использованием аппаратных технологий виртуализации;

14 контроль периферийных устройств компьютера, включая встроенную память и диск, с уровня гипервизора;

15 надёжная реализация функций по исключению НСД к данным и периферии на уровне гипервизора;

16 повышенная отказоустойчивость за счет механизма снимков состояния и хранилища резервных копий;

17 аудит происходящих событий;

18 контроль сетевого взаимодействия;

19 интеграция с системами обнаружения атак, например, ФОРПОСТ (РНТ);

20 организация защищенного канала на транспортном уровне модели OSI и использованием провайдера СКЗИ.

Литература

[1] Joanna Rutkowska, Rafal Wojtczuk, Qubes OS Architecture, Version 0.3, January 2010 https://www.qubes-os.org/attachment/wiki/QubesArchitecture/arch-spec-0.3.pdf