

Особенности прозрачной виртуализации небезопасных и уязвимых систем для упрощенного администрирования учебных классов

Д. Костюк, А. Приступчик

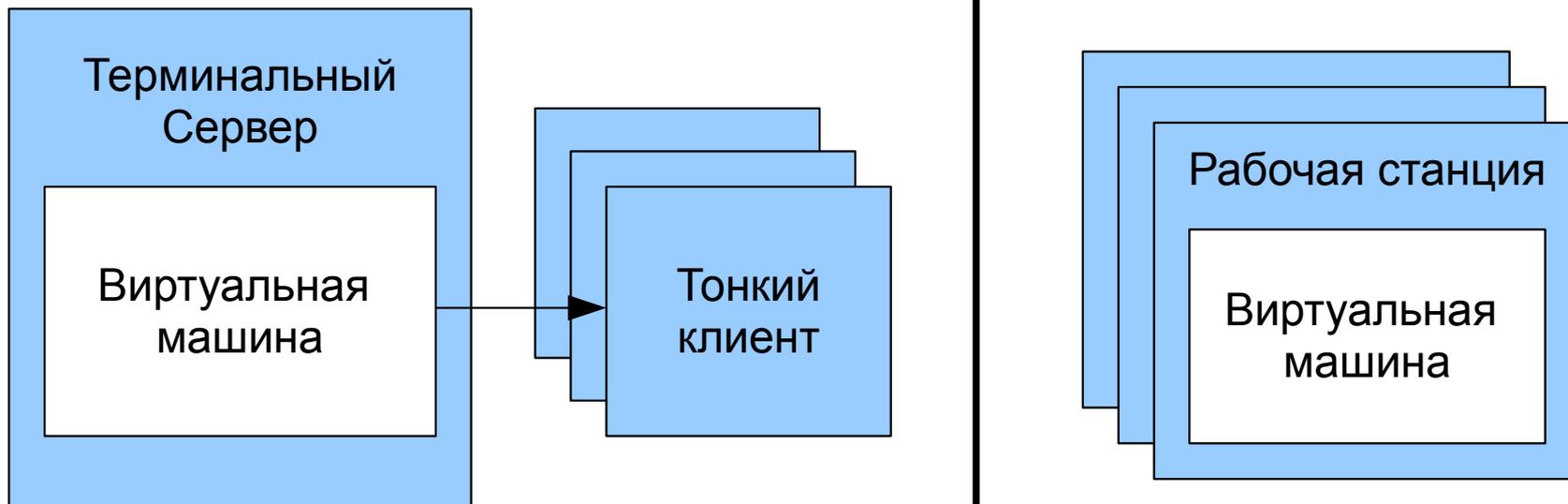
Брестский государственный технический
университет

Зачем нужна виртуализация рабочих окружений

- Гостевая ОС абстрагирована от разнообразия компьютерных комплектующих
- Меньше влияние внешних угроз безопасности
- Мгновенное восстановление от сбоев и нарушения работоспособности (snapshots)
- Легкая тиражируемость, быстрое развертывание готового к работе виртуализованного окружения.

Виртуализация

Desktop Virtualization (виртуализация рабочих станций)



Прозрачная виртуализация

А) Запуск немодифицированной гостевой ОС в виртуальной машине

- в таком смысле термин используется VMWare;
режим распространен на десктопе

Б) Пользователь «не видит» виртуальной машины и/или ОС хост-системы

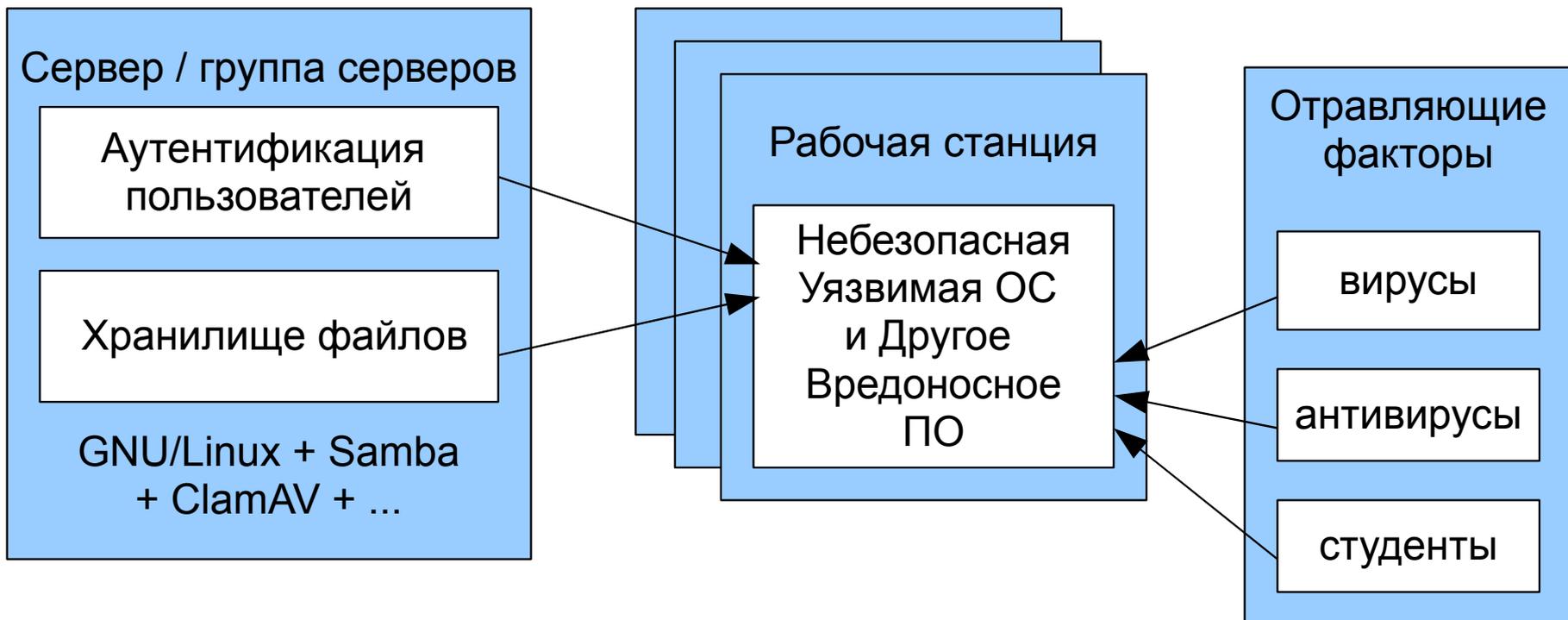
- непонятно, кем используется термин, но
другого названия у подхода все равно нет

- подход похож на виртуализацию приложений
(application-level virtualization)

Когда не выгодны тонкие клиенты

- Уже имеется класс из офисных компьютеров
- Слабый ценовой разрыв между офисным компьютером и терминалом
- Нецелесообразно использовать устаревшее оборудование в качестве тонких клиентов
- Дополнительные требования к производительности сетевого оборудования

Без виртуализации



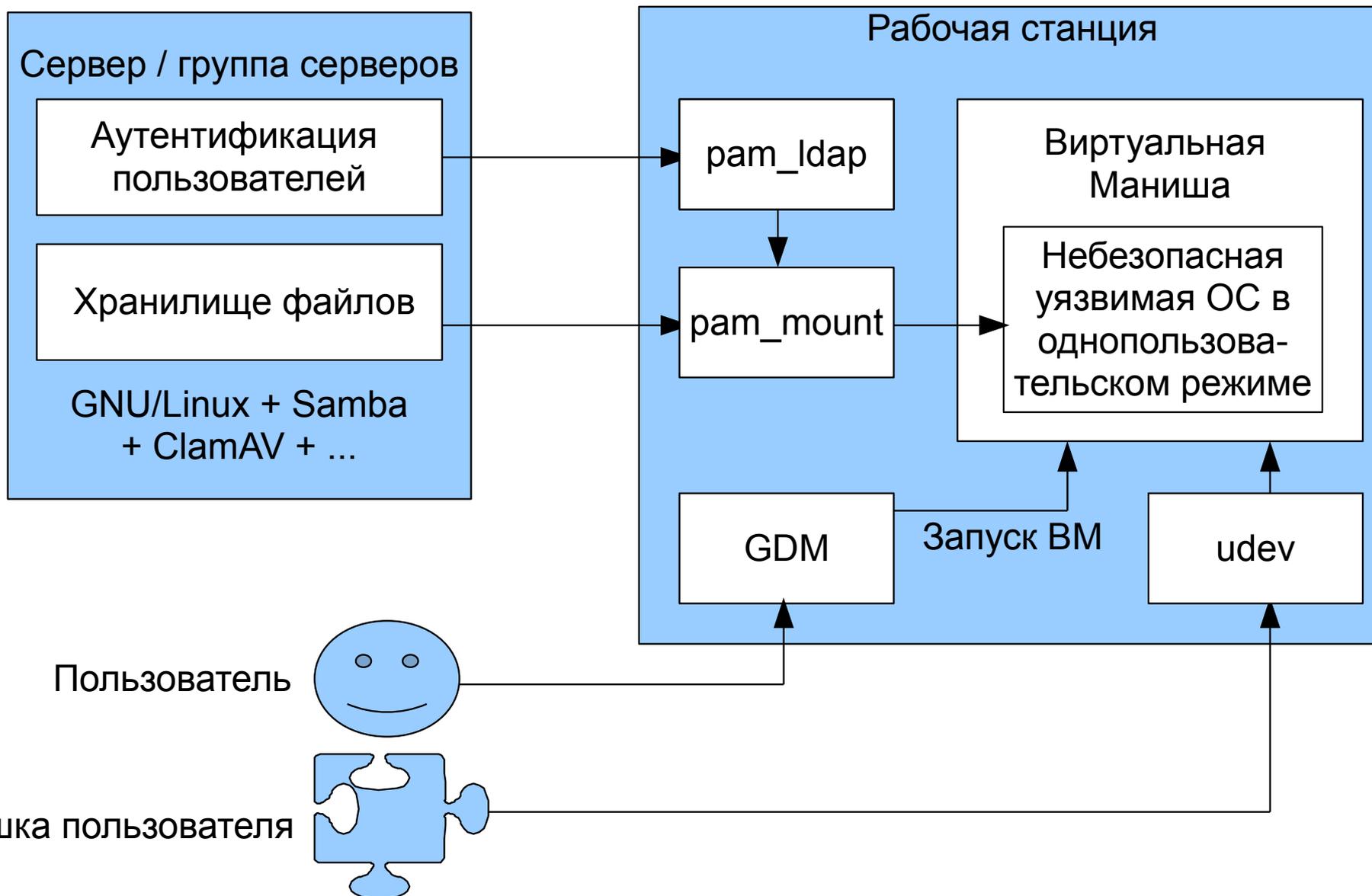
Помещение ОС от Microsoft в песочницу виртуальной машины

- Избавляет от необходимости восстановления после сбоев
- Избавляет от необходимости в антивирусном мониторе на рабочей станции
- Осложняет непредусмотренную учебным процессом активность (multi-play)
- Позволяет сделать образы рабочих станций идентичными

Выбор виртуальной машины

- Критерии
 - Работа без аппаратной поддержки виртуализации
 - Высокая производительность
 - Поддержка проброса USB-носителей и сети
 - Свободная лицензия
- VirtualBox — практически без вариантов

Изоляция ОС от Microsoft



Последовательность действий

- Настройка рабочей станции на GNU/Linux
 - Аутентификация через `ram_idap`
 - Монтирование сетевых дисков через `ram_mount`
- Настройка VirtualBox для многопользовательской работы с виртуальной машиной
 - перенос «`.VirtualBox/`» в общедоступную область
 - помещение символической ссылки на него в шаблон домашнего каталога `/etc/skel/`

Запуск виртуальной машины как сеанса из GDM

- Запуск виртуальной машины (VBoxManage)
- Проброс сетевых дисков в виртуальную машину через механизм Shared Folders
 - выполняется только на запущенной виртуальной машине
- Ожидание завершения работы виртуальной машины

Дополнительные опции

- Фиксация дискового образа виртуальной машины для потери изменений при перезапуске (immutable disk image)
- Настройка udev на хост-системе для автоматического проброса USB-storage в виртуальную машину
- Добавление полноэкранного оконного менеджера в скрипт запуска

По итогам

- Преимущества
 - Решение, прозрачное для пользователя
 - Реализует мечту «все виртуализировать и забыть о проблемах»
- Недостатки
 - Нет готового пакета чтобы «все и сразу»
 - Требуется разбираться с нестандартной настройкой ряда пакетов
 - В конце начинает казаться, что вывести пользователю ярлык виртуальной машины на рабочий стол — не так красиво, но много проще