«Организация доменной инфраструктуры в общеобразовательной школе на базе решений Базальт СПО»

ШКОЛА, ГДЕ НАЧИНАЕТСЯ БУДУЩЕЕ!

Муниципальное автономное общеобразовательное учреждение средняя общеобразовательная школа №100 города Нижний Тагил, была построена в 2019 году.

Оснащение школы обучающими материалами, средствами, и компьютерной техникой соответствовало действующим на тот момент стандартам. В связи с этим, компьютерный парк школы превышает 500 единиц.

Для централизованного управления таким количеством техники, возникла необходимость создания домена.

В виду неизбежного перехода государственных и муниципальных организаций на отечественное ПО, в качестве основы доменной инфраструктуры была выбрана ОС Альт Сервер. Средствами данной ОС, был создан домен Active Directory.

Первоначально, в составе домена работало 48 ПК с ОС Альт Образование. После заключения договора о сотрудничестве с Базальт СПО и получения по этому договору дополнительных лицензий на Альт Образование, количество ПК в домене было увеличено до 168.

В виду неизбежного перехода государственных и муниципальных организаций на отечественное ПО, в качестве основы доменной инфраструктуры была выбрана ОС Альт Сервер. Средствами данной ОС, был создан домен Active Directory.

Первоначально, в составе домена работало 48 ПК с ОС Альт Образование. После заключения договора о сотрудничестве с Базальт СПО и получения по этому договору дополнительных лицензий на Альт Образование, количество ПК в домене было увеличено до 168.

Для ПК не используемых непосредственно в учебном процессе, были куплены лицензии Альт Рабочая станция и Альт 8 СП. ПК с Альт Рабочая станция были сразу без проблем интегрированы в домен. С ОС Альт 8 СП возникли проблемы с работой групповых политик, исправленные после очередного обновления. Таким образом, на текущий момент, в состав домена входит 186 ПК с разными дистрибутивами ОС Альт.

Поддержка групповых политик реализованная в Альт Сервер, облегчает процесс настройки прав и рабочего окружения пользователей домена. В частности, активно используются инструменты установки домашней страницы браузеров, создания ярлыков программ и сетевых папок, правил подключения usb-дисков, параметров удаленного доступа, и установки дополнительного ПО.

В связи с тем, что большая часть пользователей ПК, на которых установлены ОС Альт – это школьники, которые часто очень склонны к всяким экспериментам с настройками техники которой они пользуются, самыми востребованными в школе групповыми политиками являются те, которые задают ограничения на изменение графического оформления системы – обоев, заставки, темы и так далее.

Но на данный момент, эти политики влияют только на ПК, с графической оболочкой Mate. В ОС Альт Образование, установленной на ученические ПК, используются графические оболочки xfce и kde. Поэтому ведутся поиски альтернативных методов блокировки настроек рабочей среды на ученических ПК.

Поскольку почти две трети компьютерного парка школы - это ноутбуки, весьма важным вопросом является ограничение доступа в сеть посторонних устройств. Никакие пароли не обеспечивают надежную защиту доступа в сеть. Во первых, школьники начиная с 7-8 классов прекрасно осведомлены о способах подбора пароля - например с помощью известной утилиты Reaver. Так-же, не является секретом где можно подсмотреть пароль wi-fi в настройках соединения на ПК с ОС Windows.

Первоначально, ограничение доступа обеспечивалось фильтрацией по белому списку mac-адресов. Но исчерпание емкости таблицы фильтра, вынудило перейти на другие способы аутентификации. В этом вопросе очень помогло наличие в Альт Сервер встроенного сервера FreeRadius. Тип авторизации в школьной сети был изменен на wpa enterprise, и указан адрес контроллера домена как сервера аутентификации Radius.

Помимо авторизации пользователей в ОС, доменная авторизация используется в других программных комплексах, используемых в школе: системе облачного хранилища Nextcloud, системе управления компьютерным

классом Veyon.

В случае с Nextcloud, сквозная авторизация облегчает работу пользователей - нет необходимости запоминать различные учетные данные для ПК и облака. Использование доменной авторизации в Veyon, упрощает управление каталогом клиентских компьютеров, и обеспечивает более очевидную идентификацию управляемых ПК на компьютере учителя.

Информационная безопасность обеспечивается совокупностью аппаратных и программных средств:

- аппаратным файрволом - ЛВС разделена на несколько VLAN по видам трафика (для телефонии, видеонаблюдения, wi-fi, и т. д.) которые взаимно не прозрачны. VLAN компьютерных классов и ученического wifi имеют доступ только на 2 ip из другого vlan — контроллер домена и сервер nextcloud.

- Ученические учетные записи не имеют прав запускать rpm файлы, в windows стоит запрет на установку программ и запуск приложений удаленного доступа.

- контент-фильтрацией интегрированной в канал ЕСПД — единой сети передачи данных Ростелеком, что позволяет не заботится об организации контроля доступа учащихся к запрещенным ресурсам.

- антивирусной программой clamav входящей в дистрибутив ОС Альт. Функционала данного ПО, вполне достаточно для большей части ПК школы. Единственный недостаток — отсутствие возможности централизованного управления.

- программным комплексом Kaspersky Endpoint Security установленным на ПК с повышенными требованиями безопасности, так-как его функционал шире чем Clamav, и позволяет обеспечить большую степень защиты от разного рода угроз.

-групповыми политиками ограничивающими возможность несанкционированного копирования информации — доступ к съемным носителям заблокирован у всех пользователей кроме преподавателей и административного персонала школы.

Резервное копирование данных на пока настроено на контроллере домена и сервере Nextcloud, с помощью скрипта проводящего каждые 2 дня архивирование необходимых разделов.

Сейчас для школы закуплено ещё 360 лицензий Альт Образование, для замены ОС Windows на практически 100% ПК.

Такое увеличение количества компьютеров в домене, влечет за собой обновление технической части контроллера домена – в частности переноса контроллера с обычного ПК, на стоечный сервер с существенно большими аппаратными ресурсами. Также, планируется введение вторичного контроллера.

Операции резервного копирования будут переведены с скриптового создания архивов на систему бэкапов UrBackup.

Для централизации управления антивирусной защитой ПК, производится постепенная замена антивируса clamav на Kaspersky Endpoint Security, имеющий удобную систему централизованного управления и мониторинга. Которая пока к сожалению не функционирует в ОС Альт. Ждем исправлений в новых версиях.

Также, планируется переход от использования локальных папок с данными пользователей, к использованию перемещаемых профилей (roaming profiles)

По мере увеличения функциональности встроенных средств управления доменом, в частности ADMC и GPUI, и адаптации под использование на ОС Линукс ряда спецефичных программ (випнет деловая почта, программы для проведения ВПР, ОГЭ, ЕГЭ, ПО для 3D моделирования) планируется полностью исключить из сети ПК с ОС windows и соответственно отказаться от использования RSAT