



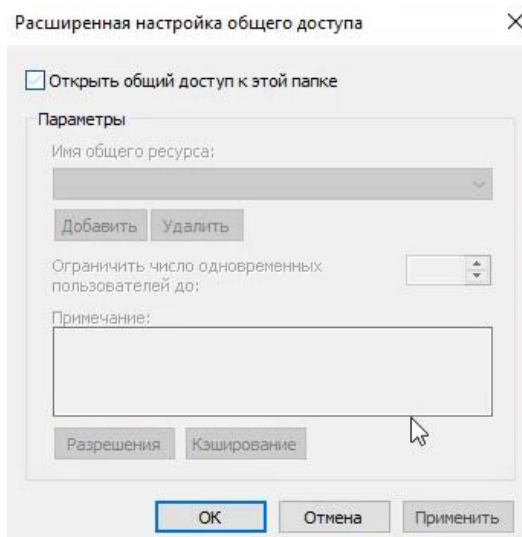
Защита файлов от копирования по локальной сети



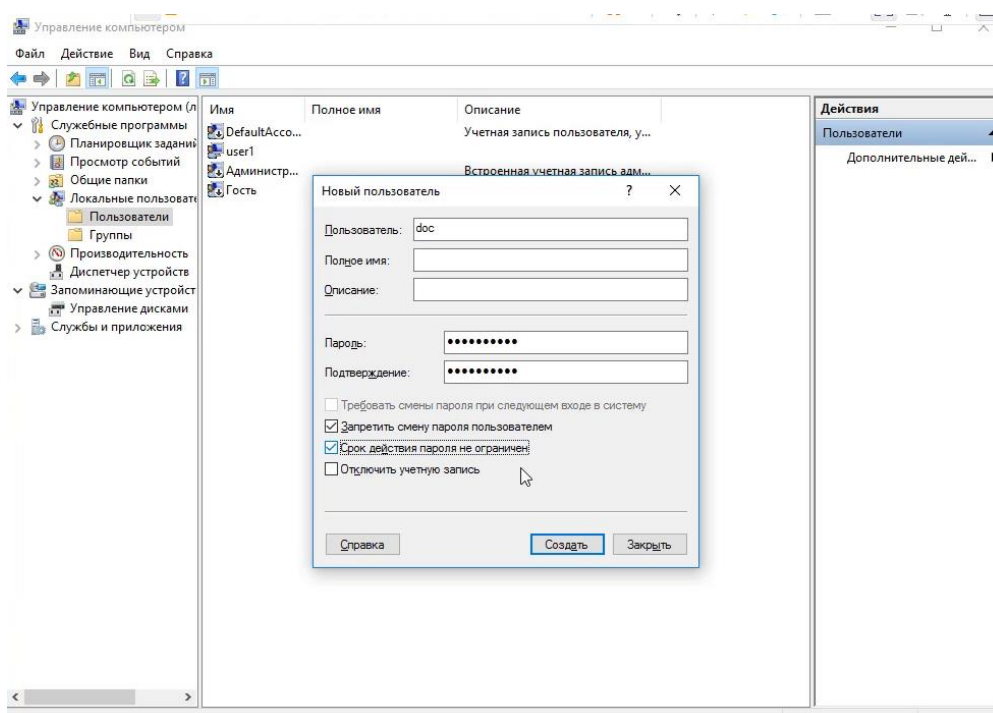
Инструкция Антона Севостьянова

Создание терминального сервера

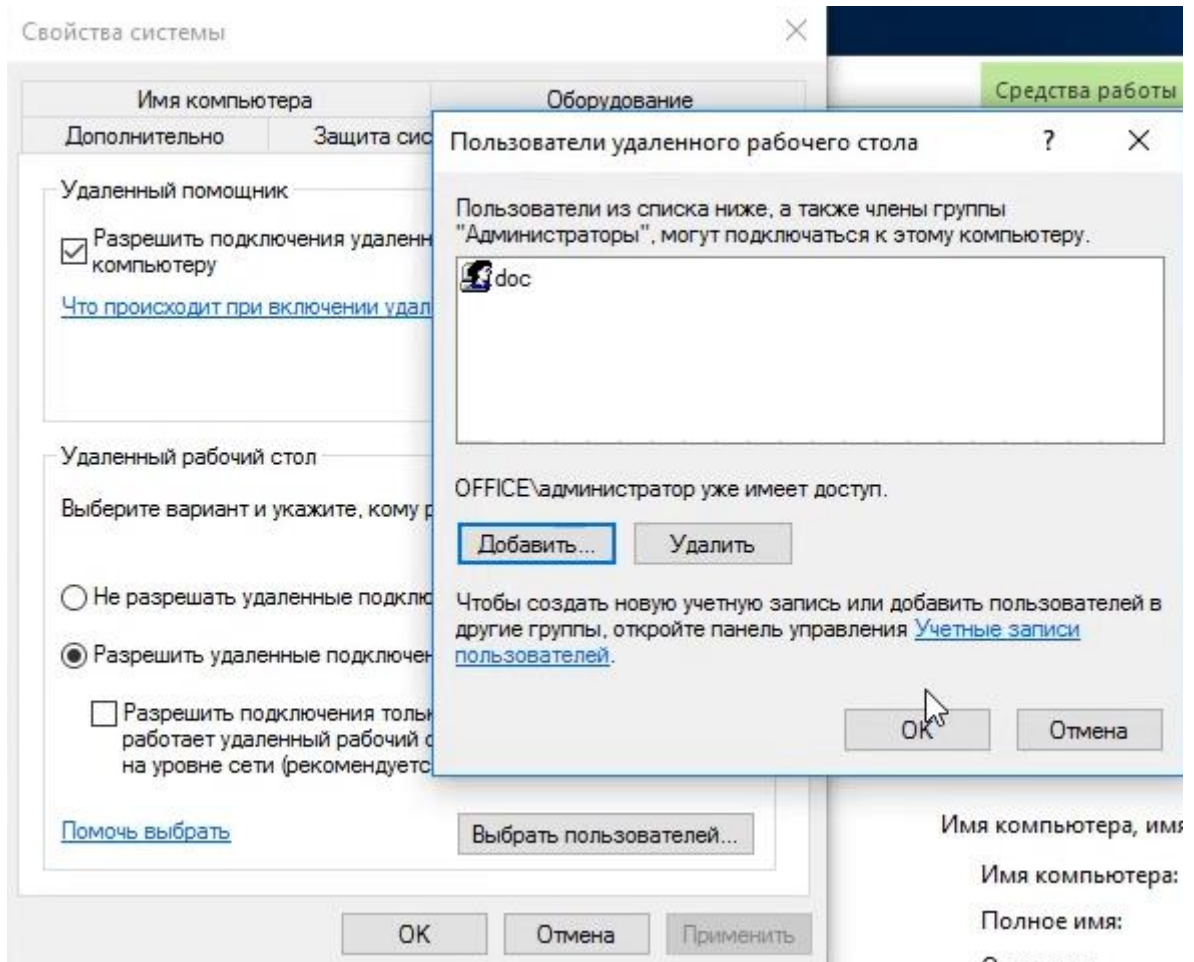
1) Убираем все доступы к нашему хранилищу документации (ПКМ \ Свойства \ Доступ \ Расширенная настройка \ Убираем галочку: Открыть общий доступ к этой папке \ ОК)



2) Создадим локального пользователя, под которым сотрудник будет получать доступ к файлам (Этот компьютер \ ПКМ \ Управление компьютером \ Локальные пользователи \ Пользователи \ ПКМ \ Новый пользователь \ Пользователь: doc \ Пароль \ Запретить смену пароля пользователем \ Срок действия пароля не ограничен \ Создать \ Закрыть)

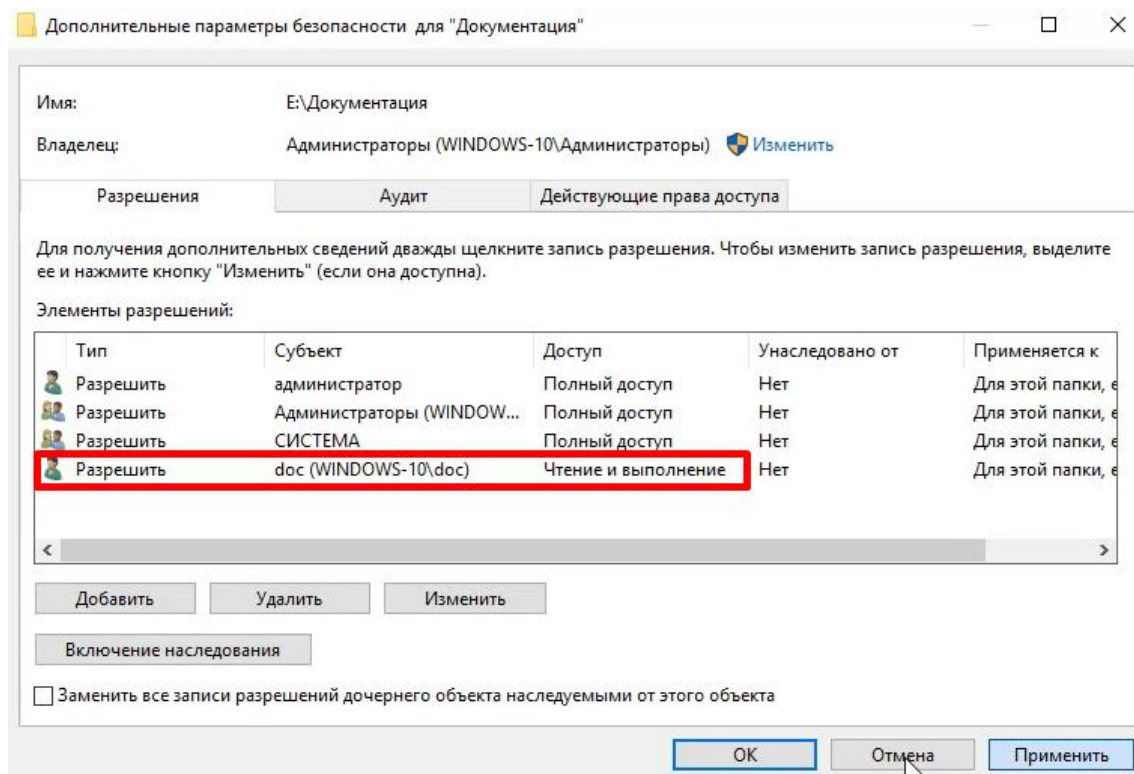


3) Разрешаем подключение через удаленный рабочий стол по протоколу RDP (Этот компьютер \ Свойства \ Настройка удаленного доступа \ Разрешить удаленное подключение а этому компьютеру \ Электропитание \ Отключаем режим сна \ ОК \ Убираем галочку: Разрешить подключения только с проверкой подлинности \ Выбрать пользователей \ Добавить \ Размещение: Этот компьютер \ Пользователь: doc \ ОК \ ОК)



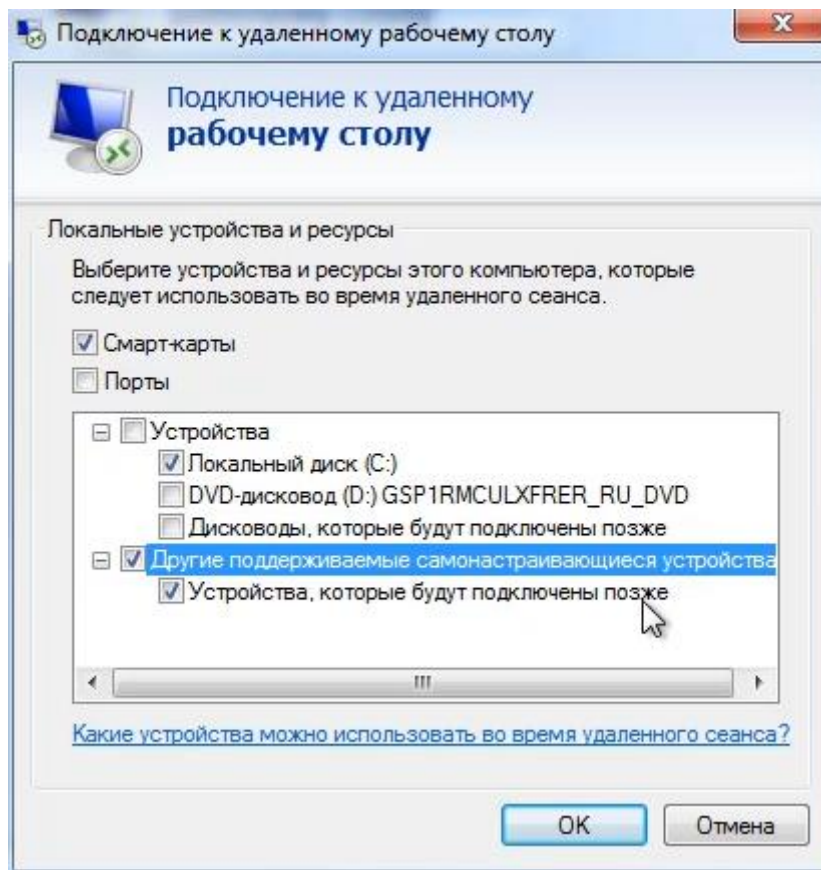
Запрет на изменение файлов

Запретим изменение файлов, чтобы с психа он не удалил документы или не внес какие-то изменения в техническую документацию. Да, бывают и такие сотрудники, когда их вроде как не справедливо увольняют. (Документация \ ПКМ \ Свойства \ Безопасность \ Дополнительно \ Изменить разрешения \ Удаляем лишние группы и пользователей \ Добавить \ Выберите субъект \ Размещение: Этот компьютер \ Пользователь: doc \ ОК \ ОК)



Проверим подключение через удаленный рабочий стол (Клиентский компьютер \ Пуск \ Удаленный рабочий стол \ Windows-10 \ Имя пользователя: Windows-10\doc \ Подключиться \ Создавать и удалять документы мы не можем)

Но, тут появляется ряд уязвимостей, которыми могут воспользоваться. Если мы зайдём в параметры подключения к удаленному рабочему столу, то увидим, что в терминальный сеанс можно пробрасывать Принтеры, Буфер обмена, локальные диски и даже устройства которые будут подключены во время удаленного сеанса.

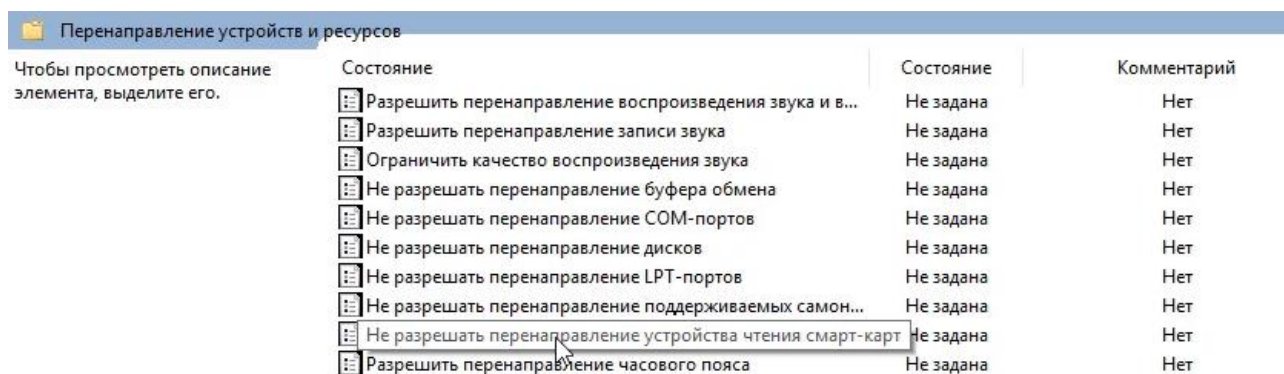


В итоге, мы можем просто скопировать файл и вставить его на наш компьютер, либо скопировать его на подключенный диск.

Поэтому данную систему нужно доработать!

Отключаем проброс буфера обмена и локальных дисков

Отключить проброс буфера обмена и подключение дисков можно через групповую политику (Windows-10 \ Логинимся под админом \ Win+R \ gpedit.msc \ Конфигурация компьютера \ Административные шаблоны \ Компоненты Windows \ Службы удалённых рабочих столов \ Узел сеансов удалённых рабочих столов \ Перенаправление устройств и ресурсов : Запрещаем все \ Перенаправление принтеров: Запрещаем все \ Win+R \ cmd \ groupdate /force – применяем групповую политику)



The screenshot shows the Group Policy Editor window titled 'Перенаправление устройств и ресурсов'. The left pane shows the tree structure: 'Перенаправление устройств и ресурсов' > 'Узел сеансов удалённых рабочих столов' > 'Перенаправление устройств и ресурсов'. The right pane displays a list of policies. The policy 'Не разрешать перенаправление поддерживаемых самон...' is selected and highlighted with a mouse cursor. The 'Состояние' column for this policy is 'Не задана', and the 'Комментарий' column is 'Нет'.

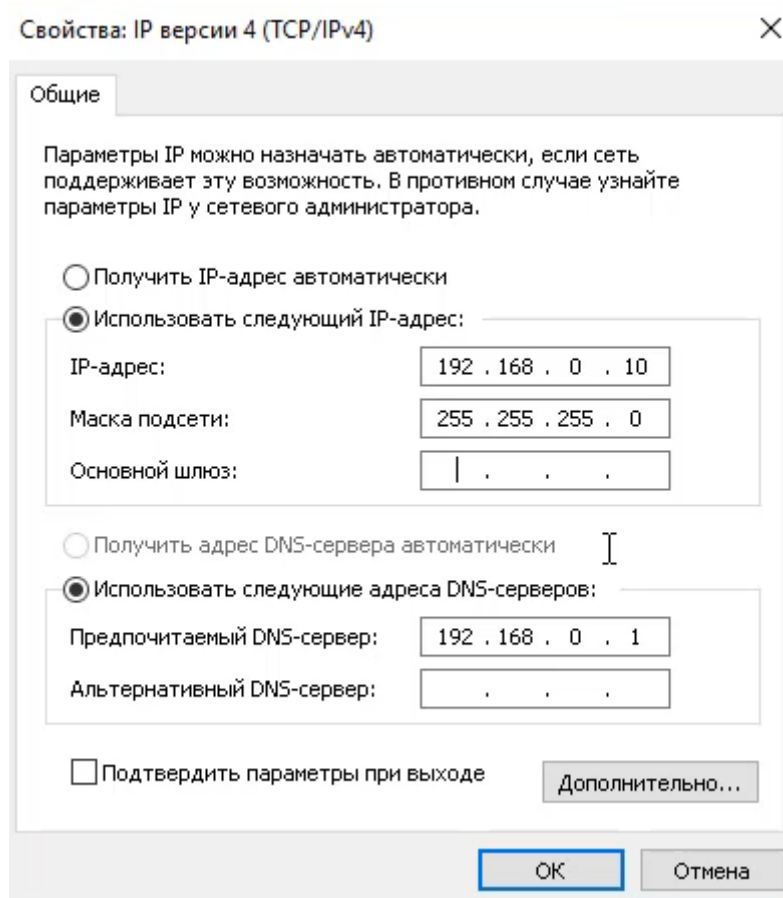
Состояние	Состояние	Комментарий
Разрешить перенаправление воспроизведения звука и в...	Не задана	Нет
Разрешить перенаправление записи звука	Не задана	Нет
Ограничить качество воспроизведения звука	Не задана	Нет
Не разрешать перенаправление буфера обмена	Не задана	Нет
Не разрешать перенаправление COM-портов	Не задана	Нет
Не разрешать перенаправление дисков	Не задана	Нет
Не разрешать перенаправление LPT-портов	Не задана	Нет
Не разрешать перенаправление поддерживаемых самон...	Не задана	Нет
Не разрешать перенаправление устройства чтения смарт-карт	Не задана	Нет
Разрешить перенаправление часового пояса	Не задана	Нет

Подключаемся и видим, что теперь мы не можем через буфер обмена копировать файлы, а также отключились локальные диски от терминального сеанса.

Отключаем доступ в интернет

Как вы видите, этот компьютер подключен к сети Интернет, а значит он может из самого терминального сеанса отправить файлы по почте или загрузить на какой-нибудь облачный сервис. Значит доступ в интернет нужно тоже обрубить.

Проще всего это сделать, убрав адрес шлюза из настроек сетевого подключения (Центр управления сетями и общим доступом \ Сетевое подключение \ Свойства \ IP версии 4 \ Свойства \ Шлюз \ Удаляем данные)



Проверяем доступ к интернет ресурсам (Win+R \ cmd \ ping 8.8.8.8 \ Сбой передачи)

Недостатки данной системы?

Скриншот экрана – можно снимать скриншотом данные с экрана, но, данный функционал можно отключить либо при помощи специального софта, либо через редактирование реестра. А лучше, повесить отправку уведомлений системному администратору, когда человек начинает слишком часто пользоваться кнопкой PrtScn. Так, мы сможем заранее определить не благонадежного сотрудника, пока он не придумал какой-то другой способ кражи.

Но, подобные уведомления настраиваются сторонним софтом.

Запись с экрана – можно записывать с экрана, но на это тоже можно настроить определенные ограничения, в любом случае у пользователя должны быть ограничены права на компьютере, чтобы он не смог устанавливать подобный софт.

Запись с телефона – он может сфотографировать или снять на видео то, что отображается на мониторе. Да, у всех телефоны не отберешь. Но, как вариант в одной компании мы делали следующим образом, база с архивом хранится на определенном компьютере на который была направлена видеокамера, записывающая в непрерывном формате. В таком случае, любые действия сотрудника записываются на видеокамеру и это дает очень хороший психологический эффект

Конечно же это не единственно возможный вариант, их может быть множество, в зависимости от различных бизнес процессов, функций сотрудника, удобства работы, схемы организации сети и других факторов.

Подводим итоги...

Печально то, что 100% защиты не существует, все ограничивается лишь желанием пользователя завладеть информацией.

Мы можем усложнить процесс утечки и ставить большее количество ловушек, чтобы на начальном этапе увидеть подозрительную активность и вычислить не благонадежного сотрудника, но на 100% вы все не закроете. Взять даже фильм про Сноудена, как он гениально вынес флешку с работы.

Так что, 100% варианта нет, но стремиться к 100% в любом случае стоит

А если ты хочешь пройти обучение системному администрированию под моим руководством, то буду рад тебя видеть на курсе «Комплексное обучение системному администрированию»

Вот как проходит обучение у нас:

Комплексное обучение системному администрированию проходит в следующей форме:

- ✓ обучение проходит в онлайн школе IT-Skills;
- ✓ все видеоуроки записаны и вы можете приступить к изучению в любой момент после оплаты курса;
- ✓ изучаете в удобное для вас время, но, чтобы изучить программу в 3 месяца нужно каждый день изучать по 2 видеоурока (примерно 30 минут контента);
- ✓ сопровождение и ответы на вопросы во время обучения;
- ✓ есть закрытый чат и группа ВК для студентов;
- ✓ проводим стримы для студентов с целью разбора различных вопросов.

P.S. Узнать подробное описание курса, вплоть до каждого видеоурока и модуля, можно по этой [ссылке](#)

Если у тебя возникнут какие-либо вопросы по поводу обучения, напиши мне по контактам ниже и я расскажу все более подробно:

Telegram: https://t.me/it_skills_bot

VK: <http://vk.me/club34272024>

Желаю удачи и достижения поставленных целей, уверен, что мои материалы в этом помогут. ;-)