КИБЕРПРОТЕКТ

КИБЕР Файлы

Версия 9.0

Руководство администратора

Редакция: 03.04.2024

Содержание

1 Введение

Данное руководство предназначено для администраторов ПО Кибер Файлы.

1.1 О программном продукте Кибер Файлы

Кибер Файлы – это решение для безопасного доступа, синхронизации и совместного использования файлов организации. Решение позволяет ИТ-отделу организации контролировать безопасность передаваемого контента и соблюдение нормативных требований.

Кибер Файлы можно использовать на настольных компьютерах, ноутбуках, планшетах и смартфонах. Можно обмениваться файлами не только внутри компании, но и с внешними доверенными лицами, например, клиентами, партнерами и поставщиками.

Функциональные возможности программы можно разделить на две основные категории: доступ и синхронизация данных и совместное использование

1.2 О функции Sync & Share

Функция Sync & Share – единственное в отрасли решение для совместного использования и синхронизации корпоративных файлов, которое сочетает простоту и эффективность для конечных пользователей с безопасностью, управляемостью и гибкостью для корпоративных ИТ-отделов.

Кибер Файлы дает корпоративным ИТ-отделам контроль над доступом к файлам и позволяет определять, соответствуют ли действия по обмену файлами нормативным требованиям и требованиям безопасности организации. Также Кибер Файлы обеспечивает уровень видимости и мониторинга, недоступный для потребительских решений.

2 Быстрый запуск

Это руководство предназначено для быстрой установки и запуска Кибер Файлы. Оно не содержит информации о пользовательской настройке. Подробные сведения и инструкции для каждого компонента см. в соответствующих разделах полной документации.

2.1 Установка

2.1.1 Использование установщика

1. Скачайте установщик Кибер Файлы.
2. Отключите все антивирусное ПО на компьютере, иначе оно может прервать процедуру установки.
3. Дважды щелкните по исполняемому файлу программы установки.
4. Нажмите кнопку **Далее**, чтобы начать установку.
5. Прочитайте и примите лицензионное соглашение.
6. Нажмите кнопку **Установить**.
7. Нажмите кнопку **OK**, чтобы использовать для главной папки Кибер Файлы путь по умолчанию.
8. Задайте пароль для пользователя Postgres и запишите его. Этот пароль понадобится для резервного копирования и восстановления базы данных.
9. Откроется окно с отображением всех компонентов, которые будут установлены. Нажмите **OK**, чтобы продолжить.
10. После завершения установки Кибер Файлы нажмите **Выйти**
11. Автоматически запустится средство конфигурации, позволяющее завершить установку.

2.1.2 Использование средства конфигурации

Примечание
Параметры в средстве конфигурации можно будет изменить позже.

Оставьте значения по умолчанию для каждой вкладки и нажмите кнопку «OK», чтобы запустить Кибер Файлы.

2.2 Начальная настройка

Мастер настройки поможет администратору выполнить ряд шагов, чтобы обеспечить работу базовых функций сервера.

Примечание
После выполнения программы настройки на первый запуск сервера уйдет 30-45 секунд.

Перейдите к веб-интерфейсу Кибер Файлы, указав IP-адрес сетевого адаптера и нужный порт. Будет выдан запрос на установку пароля для учетной записи администратора по умолчанию.

Примечание
При запуске Кибер Файлы с сертификатами по умолчанию вместо использования сертификатов из центра сертификации отображается ошибка с сообщением о недоверенном сервере.

Примечание
Ко всем параметрам, отображаемым на странице «Начальная настройка», можно будет получить доступ и после ее закрытия. Дополнительные сведения обо всех параметрах см. в статье Администрирование сервера.

2.2.0.1 Лицензирование

Для запуска пробной версии выполните следующие действия.

Выберите **Начать пробное использование**, введите необходимую информацию и нажмите кнопку **Продолжить**.

2.2.0.2 Для лицензирования экземпляра Кибер Файлы:

1. Выберите **Ввод лицензионных ключей**.
2. Введите лицензионный ключ и установите флажок.
3. Нажмите кнопку **Сохранить**.

2.2.0.3 Общие настройки

1. Введите имя сервера.
2. Укажите корневое DNS-имя или IP-адрес, с помощью которых пользователь может получить доступ к веб-сайту (начинается с http:// или https://).
   Выберите язык по умолчанию для **Журнала аудита**.
3. В настоящее время доступны: **английский, немецкий, французский, японский, итальянский, испанский, чешский, русский, польский, корейский, традиционный и упрощенный китайский**.
4. Нажмите кнопку **Сохранить**.

2.2.0.4 SMTP

Примечание
Можно пропустить этот раздел и настроить SMTP позже.

1. Введите DNS-имя или IP-адрес сервера SMTP.
2. Введите порт SMTP-сервера.

3. Если вы не используете сертификаты для SMTP-сервера, снимите флажок **Использовать защищенное подключение?**.
4. Введите имя, которое будет отображаться в поле «От» сообщений электронной почты, отправляемых сервером.
5. Введите адрес, на который сервер будет отправлять сообщения.
6. Если вы применяете проверку подлинности на основе имени пользователя и пароля для SMTP-сервера, установите флажок **Использовать проверку подлинности SMTP?** и введите учетные данные.
7. Нажмите кнопку **Отправить тестовое письмо**, чтобы отправить тестовое сообщение, настроенное на шаге 5.
8. Нажмите кнопку **Сохранить**.

2.2.0.5 LDAP

Примечание
Можно пропустить этот раздел и настроить LDAP позже, но до этого времени некоторые функции Кибер Файлы будут недоступны.

1. Установите флажок **Включить LDAP**.
2. Введите DNS-имя или IP-адрес сервера LDAP.
3. Введите порт сервера LDAP.
4. Если для подключений к серверу LDAP используется сертификат, установите флажок **Использовать защищенное LDAP-подключение**.
5. Введите свои учетные данные LDAP с доменом (например, Cyberprotect\hristo).
6. Введите базу поиска LDAP.
7. (например, чтобы включить проверку подлинности LDAP для учетной записи с адресом **joe@glilabs.com**, нужно ввести **glilabs.com**).
8. Введите требуемый домен или домены для проверки подлинности LDAP
9. Нажмите кнопку **Сохранить**.

2.2.0.6 Локальный сервер шлюза

Чтобы служба KCD работала через мобильные клиенты, необходимо зарегистрироваться на локальном шлюзе. Он установлен на той же машине, что и сервер Tomcat, который им управляет. Тогда шлюз будет направлять эти запросы на данный сервер управления Tomcat.

1. Задайте DNS-имя или IP-адрес для локального сервера шлюза.
2. Нажмите кнопку **Сохранить**.

Примечание
Если сервер шлюза и сервер Кибер Файлы устанавливаются на одном компьютере, то сервер Кибер Файлы обнаружит сервер шлюза автоматически и будет им управлять. Появится запрос для настройки DNS-имени или IP-адреса, по которому локальный сервер шлюза будет доступен клиентам. Этот адрес можно изменить позднее.

Файловый репозиторий

Выберите тип хранения файла. Выберите **Файловая система**, чтобы хранить файлы на своих компьютерах, либо любой из следующих вариантов, чтобы файлы хранились в облаке: **Swift S3**, **Ceph S3** или **Другое S3-совместимое хранилище**.

Примечание
Вариант **Другое S3-совместимое хранилище** можно использовать для поставщиков хранилищ S3, не указанных в списке, но правильная работа всех функций не гарантируется.

Примечание
Тип хранилища MinIO S3 поддерживается и может быть настроен как **Другое S3-совместимое хранилище**, однако мы не поддерживаем его использование через незащищенное подключение HTTP.

1. Введите DNS-имя или IP-адрес службы файлового репозитория.

   Примечание
   Программа настройкиКибер Файлы служит для указания адреса, порта и местоположения хранилища файлов репозитория. Настройка «Конечная точка репозитория хранения файлов» должна соответствовать настройкам на вкладке «Файловый репозиторий» средства конфигурации. Чтобы просмотреть или изменить эти настройки, запустите файл Cyber Files Configuration Utility.exe, который обычно находится в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\Configuration Utility на сервере конечной точки.

2. Выберите уровень защиты. Выберите один из следующих вариантов: **Нет**, **Низкий**, **Высокий**, **ГОСТ 28147-89**.
3. Укажите минимальное пороговое значение свободного места на диске, прежде чем сервер начнет отправлять предупреждения.
4. Нажмите кнопку **Сохранить**.

2.3 Мобильный доступ

2.3.1 Настройка политики по умолчанию

Функции всех клиентов, зарегистрированных в системе управления веб-сервером Кибер Файлы, будут управляться и контролироваться пользовательской или групповой политикой. Политика по

умолчанию создается автоматически при установке и имеет наименьший приоритет (наибольший приоритет имеет индивидуальная пользовательская политика), но она применяется ко всем пользователям без индивидуальной политики, не являющимся членами групповой политики. Политика по умолчанию изначально включена.

2.3.1.1 Настройка политики по умолчанию

1. Откройте веб-интерфейс Кибер Файлы.
2. Выберите **Мобильный доступ** -> **Политики** -> **Политики для групп**.
3. Убедившись, что флажок в поле **Включено** установлен, щелкните политику **По умолчанию**.
4. Просмотрите настройки и внесите изменения при необходимости.

2.3.2 Мобильные клиенты

При первом запуске приложения Кибер Файлы необходимо зарегистрироваться на сервере вашей компании. После появления экрана приветствия выберите **Использовать сервер компании**.

1. Введите адрес сервера, PIN-код (если требуется), имя пользователя и пароль.
2. После заполнения всей формы нажмите кнопку **Зарегистрироваться**.
3. В зависимости от конфигурации сервера компании вы можете получить предупреждение, что сертификат безопасности сервера управления не является доверенным. Чтобы принять предупреждение и продолжить, нажмите кнопку **Все равно продолжить**.
4. Если для мобильного приложения Кибер Файлы требуется пароль блокировки приложения, вам будет предложено установить его. Возможно наличие требований к сложности пароля, которые будут показаны при необходимости.

Может быть показано окно подтверждения, если ваша политика управления ограничивает хранение файлов в Кибер Файлы или запрещает добавление отдельных серверов из мобильного приложения Кибер Файлы. Если файлы хранятся локально в приложении Кибер Файлы, то будет запрошено подтверждение на удаление всех файлов в локальном хранилище **Мои файлы**. Если выбрать «Нет», то процесс регистрации в системе управления будет отменен и файлы останутся без изменений.

2.3.3 Руководства по клиентам

Сведения об использовании клиентов Кибер Файлы см. в Руководстве пользователя.

2.3.3.1 Клиент для Android

Приложение работает на смартфонах и планшетах с ОС Android 7.0 и новее. Устройства с архитектурой процессора x86 не поддерживаются.

Скачать клиент можно в веб-интерфейсе в меню профиля пользователя и на странице обновления продукта.

2.4 Синхронизация и общий доступ

2.4.1 Источник данных синхронизации и общего доступа

После установки и настройки Кибер Файлы будет автоматически создан источник данных с именем **Sync & Share**, а в список назначенных пользователей и групп будет по умолчанию добавлена группа **Пользователи домена**. Администраторы могут в любой момент изменить или удалить папку этого источника данных.

Этот источник данных по умолчанию будет доступен всем новым пользователям, входящим в группу **Пользователи домена**, при работе через мобильный клиент, клиент для настольных ПК или веб-клиент.

2.4.1.1 Открытие общего доступа к содержимому для пользователей

Чтобы открыть общий доступ к существующему содержимому, достаточно настроить для него источник данных и назначить этот источник нужным пользователям или группам.

Создание источника данных

1. Откройте веб-интерфейс Кибер Файлы.
2. Откройте вкладку **Мобильный доступ**.
3. Откройте вкладку **Источники данных**.
4. Перейдите в **Папки**.
5. Нажмите **Добавить новую папку**.
6. Введите отображаемое имя папки.
7. Выберите сервер шлюза, который будет предоставлять доступ к этой папке.
8. Выберите расположение данных. Они могут находиться на самом сервере шлюза, на другом сервере SMB, на узле или в библиотеке SharePoint или же на сервере синхронизации и общего доступа.

   Примечание
   Папку со съемного носителя нельзя использовать в качестве общей папки. Выберите папку в другом месте.

   Примечание
   При выборе Sync & Share обязательно введите полный путь к серверу с указанием номера порта, например https://mycompany.com:3000

9. В зависимости от выбранного расположения введите путь к папке, серверу, сайту или библиотеке.
10. Выберите тип **синхронизации** для этой папки.

11. Установите параметр **Показывать при просмотре сервера**, если этот источник данных должен отображаться при просмотре мобильными клиентами Кибер Файлы содержимого сервера шлюза.

    Примечание
    При создании источников данных SharePoint можно включить отображение отслеживаемых сайтов SharePoint.

12. Нажмите кнопку **Сохранить**.

2.4.1.2 Разрешение пользователям веб-клиентов доступа к файловым серверам и т. п.

По умолчанию пользователи не могут открывать устройства NAS, файловые серверы и ресурсы SharePoint из веб-клиента. Но эту возможность легко включить и дать большую свободу веб-пользователям.

1. Откройте веб-интерфейс и найдите раздел **Мобильный доступ** --> **Политики**. (Обратите внимание, что, хотя политики в основном касаются мобильного приложения, настройка веб-доступа производится там же.)
2. Выберите политику, которую нужно изменить. Если вы не создавали новых политик, выберите политику **По умолчанию** .
3. На вкладке **Политика сервера** установите флажок **Разрешить доступ к файловому серверу, NAS и SharePoint из веб-клиента**.
4. При желании можно также включить для выбранной политики синхронизацию с настольным компьютером с помощью вложенных параметров **Разрешить клиентскому приложению для настольных ПК синхронизацию с папками файлового сервера, NAS и SharePoint** и **Разрешить клиентскому приложению для настольных ПК двустороннюю синхронизацию с папками файлового сервера, NAS и SharePoint**.
5. Выберите **Сохранить**.

Эта возможность реализована в виде параметра, применяемого к отдельным политикам, для большей гибкости. Параметр можно включить для другой группы или конкретных политик.

2.4.2 Подготовка LDAP

Включение распределения LDAP позволит пользователям выполнять вход со своими учетными данными LDAP и автоматически создавать для них учетные записи вместо индивидуального приглашения каждого пользователя (или группы) администратором. Эти учетные записи занимают лицензию из пула лицензий, поэтому необходимо выбрать определенную группу (или группы) LDAP для распределения.

2.4.2.1 Включение распределения LDAP

1. Откройте веб-интерфейс Кибер Файлы.
2. Выберите **Sync & Share** -> **Распределение LDAP**.
3. Введите имя группы (или нескольких групп) LDAP.
4. Выберите нужные группы и нажмите кнопку **Сохранить**.

Для пользователей в выбранных группах будут автоматически создаваться учетные записи Кибер Файлы при попытке входа в Кибер Файлы с учетными данными LDAP.

2.5 Клиент для ПК и веб-клиент

- Веб-клиент позволяет всем пользователям с допустимыми учетными данными Кибер Файлы открывать папки и файлы и делиться ими прямо в удобном для них браузере.
- Клиент для ПК позволяет легко обмениваться большими файлами и обеспечивать их актуальность.

3 Установка

3.1 Требования

Перед установкой Кибер Файлы необходимо выполнить вход от имени администратора. Убедитесь, что выполняются следующие требования.

3.1.1 Требования к операционной системе

3.1.1.1 Веб-сервер Кибер Файлы

Поддерживаются следующие серверные операционные системы:

- Windows Server 2012, 2012 R2, 2016, 2019 – выпуски Standard и Datacenter
- Альт Сервер 10
- РЕД ОС 7.3 и новее
- Astra Linux SE 1.7 и новее

3.1.1.2 Сервер шлюза

Поддерживаются следующие серверные операционные системы:

- Windows Server 2012, 2012 R2, 2016, 2019 – выпуски Standard и Datacenter

3.1.2 Рекомендуемое оборудование

3.1.2.1 Примеры развертываний

Цифры в примерах подразумевают, что все компоненты Кибер Файлы работают на одной виртуальной машине или физическом сервере.

Примечание
Рекомендуемое дисковое пространство предполагает настроенную очистку старых и удаленных версий в файловом репозитории.

Примечание
Рекомендуемый размер диска является отправной точкой, и может потребоваться его увеличение в зависимости от размера и количества файлов, синхронизируемых пользователями.

Примечание
Кибер Файлы Web Server можно установить на виртуальных машинах.

Примечание
Убедитесь, что дискового пространства достаточно для запуска установщика Кибер Файлы. Для этого потребуется 1 ГБ дискового пространства.

Примечание
Эти значения рекомендуются для производственной среды. Если вы планируете запуск пробной версии или установку Кибер Файлы для тестирования, требования к оборудованию могут быть снижены в зависимости от тестовой нагрузки.

Небольшие развертывания

- До 25 пользователей
- ЦП: Intel класса i7 Xeon с 4 ядрами или эквивалент от AMD.
- ОЗУ: 16 ГБ
- Дисковое пространство: 100 ГБ

Средние развертывания

- До 500 пользователей
- ЦП: Intel класса i7 Xeon с 8 ядрами или эквивалент от AMD.
- ОЗУ: 40 ГБ
- Дисковое пространство: 2 ТБ RAID

Крупные развертывания

- До 2500 пользователей
- ЦП: Intel класса i7 Xeon с 16 ядрами или эквивалент от AMD.
- ОЗУ: 64 ГБ
- Дисковое пространство: 10 ТБ RAID

Примечание
Для развертываний на более 2500 пользователей рекомендуется кластерная конфигурация серверов. По поводу таких развертываний обратитесь в службу поддержки пользователей Cyberprotect.

3.1.3 Сетевые требования

- Один статический IP-адрес. Для определенных конфигураций может потребоваться два IP-адреса.
- Необязательно, но рекомендуется: DNS-имена, соответствующие IP-адресам, указанным выше.
- Сетевой доступ к контроллеру домена, если планируется использовать Active Directory (LDAP).

- Сетевой доступ к SMTP-серверу для уведомлений и приглашений по электронной почте.
- Адрес 127.0.0.1 используется мобильным приложением для внутренних целей и не должен участвовать в туннелях какого-либо вида: VPN, MobileIron и т. д.
- Все компьютеры, на которых работает веб-сервер Кибер Файлы или сервер шлюза, необходимо привязать к Windows Active Directory.

Два компонента обрабатывают HTTPS-трафик: сервер шлюза и веб-сервер Кибер Файлы. Сервер шлюза используется мобильными клиентами для доступа к файлам и общим ресурсам источников данных. Веб-сервер Кибер Файлы предоставляет веб-интерфейс для клиентов Sync & Share, а также служит консолью администрирования мобильного доступа, синхронизации и общего доступа.

Для большинства развертываний рекомендуется назначить обоим серверам один IP-адрес, но с разными портами и отдельными DNS-записями. Конфигурация с одним IP-адресом подойдет для большинства установок. Сервер можно настроить на использование отдельных IP-адресов для каждого компонента, если этого требует конкретная модель развертывания или установки.

Если нужно предоставлять доступ мобильным устройствам за пределами брандмауэра, существует несколько вариантов.

- **Доступ по порту 443**. Кибер Файлы использует HTTPS для зашифрованной передачи данных, поэтому его пропускают стандартные правила брандмауэра, разрешающие HTTPS-трафик по порту 443. Если разрешается доступ к веб-серверу Кибер Файлы по порту 443, то авторизованные клиенты iPad могут подключиться к нему в области действия брандмауэра и за ее пределами. Приложение также можно настроить для использования любого другого порта.
- **VPN**. Мобильное приложение Кибер Файлы поддерживает доступ через VPN-подключение. Поддерживаются сторонние VPN-клиенты. Профили управления iOS при необходимости можно применить к устройствам с помощью систем управления мобильными устройствами (MDM) или средства конфигурации Apple iPhone, чтобы настроить функцию iOS **VPN по запросу** на основе сертификатов. Это позволит легко предоставить доступ к веб-серверам Кибер Файлы и другим корпоративным ресурсам.
- **Обратный прокси-сервер**. Если настроен обратный прокси-сервер, то клиенты на iPad смогут подключаться без открытия порта брандмауэра или VPN-подключения. Мобильное приложение Кибер Файлы поддерживает сквозную проверку подлинности обратного прокси-сервера, проверку подлинности на основе имени пользователя и пароля, проверку подлинности с ограниченным делегированием Kerberos и проверку подлинности на основе сертификатов.

Сертификаты: Кибер Файлы поставляется и устанавливается с самозаверенными сертификатами для тестирования. В производственных развертываниях необходимо использовать сертификаты ЦС.

Примечание
Некоторые веб-браузеры отображают предупреждающие сообщения при использовании самозаверенных сертификатов. Эти сообщения можно пропустить, после чего системой можно пользоваться без каких-либо проблем. Использование самозаверенных сертификатов в производственных условиях не поддерживается.

Примечание
При включении функции защищенного LDAP-подключения Кибер Файлы требует, чтобы полное доменное имя сервера LDAP присутствовало в сертификате как общее имя (CN) или альтернативное имя субъекта (SAN).

3.1.4 Требования клиента для ПК

3.1.4.1 Системные требования

Поддерживаемые операционные системы

- Windows 7, 8, 8.1, 10 и 11

  Примечание
  Кибер Файлы не поддерживает Windows Server 2008 R2 (ссылка на официальное уведомление Microsoft).

- macOS X версий 10.13-10.15 с Mac, совместимые с 64-битным ПО
- macOS 11 Big Sur и macOS 12 Monterey с 64-битными x86 процессорами Intel и Apple Silicon

  Примечание
  При установке клиента для ПК Кибер Файлы убедитесь, что созданная папка синхронизации не вложена в папку, которая синхронизируется другим программным обеспечением. Список известных конфликтов см. на странице Вызывающее конфликты программное обеспечение.

Поддерживаемые веб-браузеры:

- Mozilla Firefox 60 и более поздние версии
- Microsoft Edge 42 или более поздние версии
- Google Chrome 64 и более поздние версии
- Safari 12 и более поздние версии
- Opera 72 и более поздние версии

3.1.4.2 Дополнительные требования

Для установки потребуется следующее.

- Кибер Файлы – исполняемый файл установщика клиента для ПК и соответствующие права для его запуска.
- Адрес сервера, который будет использоваться (предоставляется администратором или по электронной почте).
- Учетные данные для сервера (полученные из Active Directory, предоставленные администратором или по электронной почте).

3.2 Установка на Linux

В данном разделе приведены шаги по установке веб-сервера Кибер Файлы на поддерживаемые ОС Linux.

3.2.1 Установка на Альт Сервер

Выполните следующие шаги:

1. Настройте использование команды sudo, как описано в ALT Linux Wiki.
2. Обновите список пакетов:

   ```
   $ sudo apt-get update
   ```

3. Установите пакет Кибер Файлы, например:

   ```
   $ sudo apt-get install cyberfiles-9.0.0.alt.rpm
   ```

4. Инициализируйте и запустите службы Postgres и Tomcat. В данной конфигурации используется незащищенное локальное подключение к Postgres, обеспеченное настройками пакета по умолчанию.

   ```
   $ sudo /etc/init.d/postgresql initdb
   $ sudo systemctl enable --now postgresql.service
   $ sudo -u postgres psql -c "create database cyberfiles_production"
   $ sudo systemctl enable --now cyberfiles-tomcat.service
   ```

Веб-интерфейс сервера будет доступен по адресу https://localhost. Загрузка первой страницы после перезапуска сервера может занимать 1-2 минуты.

3.2.1.1 Удаление

Выполните следующие шаги:

1. Остановите службы репозитория и Tomcat:

   ```
   $ sudo systemctl stop cyberfiles-repository.service
   $ sudo systemctl stop cyberfiles-tomcat.service
   ```

2. Удалите пакеты Кибер Файлы:

   ```
   $ sudo apt-get remove cyberfiles
   ```

3.2.2 Установка на РЕД ОС

Выполните следующие шаги:

1. Установите Postgres и создайте базу данных. Вместо <password> укажите пароль для пользователя postgres.

```
$ sudo dnf install postgresql-server
$ sudo postgresql-setup --initdb --unit postgresql
$ sudo sed  -i '1i host cyberfiles_production postgres samehost md5' /var/lib/pgsql/data/pg_
hba.conf
$ sudo systemctl enable --now postgresql.service
$ sudo -iu postgres psql -c "ALTER USER postgres WITH PASSWORD '<password>'"
$ sudo -iu postgres psql -c "CREATE DATABASE cyberfiles_production"
```

2. Установите пакет Кибер Файлы, например:

```
sudo rpm -i cyberfiles-9.0.0.red.rpm
```

Укажите пароль для пользователя postgres, созданный на предыдущем шаге, в конфигурационном файле /opt/cyberprotect/cyberfiles/tomcat/webapps/access-server/WEB-INF/cyberfilessrv.cfg в значении параметра DB_PASSWORD и перезапустите службу Tomcat, чтобы изменения вступили в силу:

```
$ sudo systemctl restart cyberfiles-tomcat.service
```

3.2.2.1 Удаление

Выполните следующие шаги:

1. Остановите службы репозитория и Tomcat:

```
$ sudo systemctl stop cyberfiles-repository.service
$ sudo systemctl stop cyberfiles-tomcat.service
```

2. Удалите пакеты Кибер Файлы:

```
$ sudo rpm -e cyberfiles
```

3.2.3 Установка на Astra Linux SE

Выполните следующие шаги:

1. Отключите МКЦ (мандатный контроль целостности):

```
$ astra-mic-control disable
```

2. Обновите систему до последней версии:
   a. Замените в адресах репозиториев "https" на "http" в файле sources.list. Для его редактирования понадобятся привилегии sudo, например:

```
$ sudo nano /etc/apt/sources.list
```

b. Выполните следующие команды:

```
$ sudo apt-get update
$ sudo apt-get install astra-update
$ sudo astra-update -A -r
```

3. Установите Java Development Kit (JDK). Скачать установочный пакет можно из Центра загрузок Axiom JDK. Кроме того, можно использовать альтернативные репозитории:
   a. Создайте файл /etc/apt/sources.list.d/lab50.list с привилегиями sudo, например:

   ```
   $ sudo nano /etc/apt/sources.list.d/lab50.list
   ```

   Укажите в нем адрес альтернативного репозитория:

   ```
   deb http://packages.lab50.net/alse/ alse17 main
   deb-src http://packages.lab50.net/alse/ alse17 main
   ```

   b. Добавьте цифровой ключ подписи в APT. Сделать это можно командой

   ```
   $ wget -qO - http://packages.lab50.net/lab50.asc | sudo apt-key add -
   ```

   Также можно обновить кэш и установить пакет lab50-archive-keyring из используемого альтернативного репозитория. Например:

   ```
   $ aptitude update
   $ aptitude -y install lab50-archive-keyring
   ```

   c. Убедитесь, что переменная окружения JAVA_HOME указывает на директорию с установленным JDK версии 1.8. Например, имеет значение /usr/lib/jvm/java-8-openjdk-amd64 в файле /lib/systemd/system/cyberfiles-tomcat.service.
4. Установите Postgres и создайте базу данных. Вместо <password> укажите пароль для пользователя postgres.

   ```
   $ sudo apt update
   $ sudo apt install postgresql-11
   $ cd /var/lib/postgresql
   $ sudo -u postgres psql -c "ALTER USER postgres WITH password '<password>'"
   $ sudo -u postgres psql -c "CREATE DATABASE cyberfiles_production"
   ```

5. Установите пакет Кибер Файлы, например:

   ```
   $ sudo apt install ./cyberfiles-9.0.0.astra.deb
   ```

   Укажите пароль для пользователя postgres, созданный на предыдущем шаге, в конфигурационном файле /opt/cyberprotect/cyberfiles/tomcat/webapps/access-server/WEB-INF/cyberfilessrv.cfg в значении параметра DB_PASSWORD и перезапустите службу Tomcat, чтобы изменения вступили в силу:

   ```
   $ sudo systemctl restart cyberfiles-tomcat.service
   ```

При установке пакетов из файлов с помощью команды apt пакеты и их зависимости устанавливаются автоматически, но при успешном завершении установки выдается предупреждение:

> Загрузка выполняется от лица суперпользователя без ограничений песочницы, так как файл «...» недоступен для пользователя «_apt». - pkgAcquire::Run (13: Отказано в доступе)

Это предупреждение о том, что программа установки, не имея прав доступа к текущему каталогу, была вынуждена получить привилегии root для выполнения установки. Установка при этом завершается успешно, и предупреждение можно игнорировать.

Веб-интерфейс сервера будет доступен по адресу https://localhost. Загрузка первой страницы после перезапуска сервера может занимать 1-2 минуты.

3.3 Запустите Кибер Файлы на вашем сервере

Следующие шаги позволяют выполнить установку с нуля и проверку Кибер Файлы с поддержкой HTTPS с использованием предоставленного самозаверенного сертификата.

Примечание
Указания по обновлению см. в разделе Обновление.

Примечание
Инструкции по установке в кластере см. в разделе Балансировка нагрузки.

Три шага установки Кибер Файлы.

1. Установка инсталлятора веб-сервера Кибер Файлы.
2. Настройка сетевых портов и сертификатов SSL, используемых веб-сервером Кибер Файлы.
3. Использование веб-мастера установки для настройки сервера для дальнейшего использования.

3.3.1 Установка Кибер Файлы

Установку Кибер Файлы нужно производить с правами администратора.

1. Скачайте установщик Кибер Файлы.
2. Отключите все антивирусное ПО на компьютере, иначе оно может прервать процедуру установки.
3. Дважды щелкните по исполняемому файлу программы установки.
4. Нажмите кнопку **Далее**, чтобы начать установку.
   Прочитайте и примите лицензионное соглашение.
5. Нажмите кнопку**Установить**.
   .

Примечание
Если развертывается несколько серверов Кибер Файлы или устанавливается нестандартная конфигурация, то можно указать устанавливаемые компоненты, нажав кнопку **Выборочная установка**.

6. Оставьте путь по умолчанию или выберите новый путь для главной папки Кибер Файлы и нажмите кнопку **OK**.
7. Задайте пароль для пользователя Postgres и запишите его. Этот пароль понадобится для резервного копирования и восстановления базы данных.
8. Откроется окно с отображением всех компонентов, которые будут установлены. Нажмите **OK**, чтобы продолжить.
9. После завершения установки Кибер Файлы нажмите **Выйти**
10. Автоматически запустится средство конфигурации, позволяющее завершить установку.

Сведения об использовании средства конфигурации см. на странице Использование средства конфигурации.

3.4 Использование средства конфигурации

В состав программы установки Кибер Файлы входит средство конфигурации, которое поможет легко и быстро настроить доступ к серверу шлюза, файловому репозиторию и веб-серверу Кибер Файлы.

Примечание
Дополнительные рекомендации по настройке IP-адресов для Кибер Файлы см. в разделе Требования к сети.

Примечание
Сведения о добавлении сертификата в хранилище сертификатов Microsoft Windows см. в статье Использование сертификатов.

3.4.1 Обзор программы настройки

Параметры средства конфигурации можно изменить в любое время, запустив программу и внеся необходимые изменения. Она автоматически изменит необходимые файлы конфигурации и перезапустит соответствующие службы.

3.4.1.1 Вкладка Веб-сервер

Веб-сервер Кибер Файлы предоставляет веб-интерфейс для клиентов Кибер Файлы, а также служит консолью администрирования мобильного доступа и Sync & Share.

- **Адрес** – укажите IP-адрес своего веб-интерфейса или выберите **Все адреса** для прослушивания всех доступных интерфейсов.

- **Порт** – порт веб-интерфейса.
- **Сертификат** – путь к сертификату для веб-интерфейса. Сертификат можно выбрать из хранилища сертификатов Microsoft Windows.

  Примечание
  Используемый сертификат должен содержать свой закрытый ключ. Убедитесь, что при импорте ключа был установлен флаг **Пометить этот ключ как экспортируемый**. Подробнее про установку и требования к сертификатам см. в разделе " Установка сертификата в хранилище сертификатов Windows" (стр. 204).

- **Сертификат цепочки** – путь к промежуточному сертификату для веб-интерфейса. Сертификат можно выбрать из хранилища сертификатов Microsoft Windows. Этот сертификат необходим только в случае, если центр сертификации также выдал промежуточный сертификат.
- **Перенаправлять запросы с порта 80**. Если выбрать этот вариант, Tomcat будет прослушивать входящий трафик на незащищенном порту 80 и перенаправлять его на порт HTTPS, указанный выше. Если другая программа прослушивает порт 80, то не устанавливайте данный флажок.
- **Учетная запись службы** позволяет запускать службу веб-сервера Кибер Файлы в контексте другой учетной записи. При обычной установке задавать этот параметр обычно не требуется.

3.4.1.2 Вкладка Мобильный шлюз

Сервер шлюза используется мобильными клиентами для доступа как к файлам, так и к общим ресурсам.

- **Адрес** – укажите IP-адрес своего сервера шлюза или выберите **Все адреса** для прослушивания всех интерфейсов.
- **Порт** – порт сервера шлюза.
- **Сертификат** – путь к сертификату сервера шлюза. Сертификат можно выбрать из хранилища сертификатов Microsoft Windows.
- **Учетная запись службы** – позволяет запускать службу сервера шлюза в контексте другой учетной записи. При обычной установке задавать этот параметр обычно не требуется.
- **Использовать прокси-сервер для запросов к серверу Кибер Файлы**. Если эта настройка включена, пользователи будут подключаться к серверу шлюза, который затем будет перенаправлять их на сервер Кибер Файлы. Доступно, если имеются Кибер Файлы Server и сервер шлюза, установленные на одном компьютере.
- **Перенаправлять запросы с порта 80**. Если выбрать этот вариант, Tomcat будет прослушивать входящий трафик на незащищенном порту 80 и перенаправлять его на порт HTTPS, указанный выше. Если другая программа прослушивает порт 80, то не устанавливайте данный флажок.

3.4.1.3 Вкладка Файловый репозиторий

Файловый репозиторий используется функцией Sync & Share. Если этот компонент еще не включен, то можно принять значения по умолчанию. Если Sync & Share используются, то путь к

хранилищу файлов должен указывать местоположение на диске, которое будет использоваться в качестве хранилища.

- **Адрес –** укажите IP-адрес своего файлового репозитория или выберите **Все адреса** для прослушивания всех интерфейсов. Если указан IP-адрес или DNS-адрес, то этот же адрес должен быть указан в разделе **Файловый репозиторий** в веб-интерфейсе. Дополнительные сведения о нем см. в статье Репозиторий файлов.
- **Порт –** порт файлового репозитория. Этот же порт следует указать в разделе **Файловый репозиторий** в веб-интерфейсе. Дополнительные сведения о нем см. в статье Репозиторий файлов.
- **Путь к хранилищу файлов –** путь в UNC-формате к хранилищу файлов. При изменении пути к хранилищу файлов НЕОБХОДИМО вручную скопировать все файлы из исходного хранилища в новое место.

  Примечание
  Если вы переместили хранилище файлов в новое место, следует отправить туда новый файл, чтобы проверить правильность работы нового хранилища. Также стоит скачать какой-либо файл, который был в старом хранилище, и убедиться, что все файлы из старого хранилища доступны и в новом.

- **Учетная запись службы –** если хранилище файлов репозитория расположено на удаленном сетевом ресурсе, то необходимо настроить учетную запись службы, у которой есть разрешения на работу с этим сетевым общим ресурсом. Эта учетная запись также должна иметь права для чтения и записи в папке Repository (например, C:\Program Files (x86)\Cyberprotect\Cyber Files\File Repository\Repository), чтобы иметь возможность записи в файл журнала.

  Примечание
  Если для службы используется конкретная учетная запись вместо **учетной записи локальной системы**, то необходимо перейти на панель управления **Службы**, открыть свойства службы **Файловый репозиторий Кибер Файлы** и изменить параметры на вкладке **Вход**. Необходимо вручную ввести учетную запись и ее пароль в соответствующие поля.

3.4.2 Переход к мастеру настройки

После заполнения всех необходимых полей нажмите **Применить** или **OK**. Службы, в настройки которых были внесены изменения, будут перезапущены.

Примечание
Сервер Кибер Файлы станет доступен через 30-45 секунд после запуска служб.

1. После начальной установки средства конфигурации веб-браузер автоматически открывает веб-интерфейс Кибер Файлы.
2. На странице входа вы получите запрос ввести пароль **администратора**, после чего мастер установки поможет выполнить остальные шаги процесса установки.

Запишите пароль администратора, так как в случае утери восстановить его будет невозможно.

3.5 Использование мастера настройки

После установки программного обеспечения и запуска средства конфигурации для выбора сетевых портов и сертификатов SSL следующим действием администратора будет настройка сервера Кибер Файлы. Мастер настройки поможет администратору выполнить ряд шагов, чтобы обеспечить работу базовых функций сервера.

Примечание
После запуска средства конфигурации на первый запуск сервера уйдет 30-45 секунд.

Если вы не настроили учетную запись администратора на предшествующем шаге, на странице входа вы получите запрос ввести пароль **администратора**.

Запишите пароль администратора, так как в случае утери восстановить его будет невозможно.

3.5.1 Выполнение процесса начальной настройки

Перейдите к веб-интерфейсу Кибер Файлы, указав IP-адрес и порт, которые были заданы в средстве конфигурации. Будет выдан запрос на установку пароля для учетной записи администратора по умолчанию.

Примечание
Дополнительные учетные записи администраторов можно будет настроить позже, подробнее см. в разделе Администрирование сервера.

Этот мастер поможет настроить основные параметры работы продукта.

- Раздел **Общие настройки** содержит настройки работы самого веб-интерфейса, такие как язык, цветовая схема, имя сервера, используемое в уведомлении администратора, параметры лицензирования и список администраторов.
- Раздел **Настройки LDAP** позволяет задать учетные данные, правила и политики Active Directory в продукте.

Раздел **Настройки SMTP** относится к работе функций мобильного доступа и Sync & Share. SMTP-сервер используется для рассылки приглашений для регистрации в системе мобильного доступа. Функции Sync & Share используют SMTP-сервер для отправки приглашений к папкам, предупреждений и сводок по ошибкам.

Ко всем параметрам, отображаемым на странице **Начальная настройка**, можно будет получить доступ и после ее закрытия. Дополнительные сведения обо всех параметрах см. в статье Администрирование сервера.

3.5.1.1 Лицензирование

Для запуска пробной версии выполните следующие действия.

Выберите **Начать пробное использование**, введите необходимую информацию и нажмите кнопку **Продолжить**.

3.5.1.2 Для лицензирования экземпляра Кибер Файлы:

1. Выберите **Ввод лицензионных ключей**.
2. Введите лицензионный ключ и установите флажок.
3. Выберите **Сохранить**.

3.5.1.3 Общие настройки

1. Введите имя сервера.
2. Укажите корневое DNS-имя или IP-адрес, с помощью которых пользователь может получить доступ к веб-сайту (начинается с http:// или https://).
3. Выберите язык по умолчанию для **Журнала аудита**. В настоящее время доступны: английский, немецкий, французский, японский, итальянский, испанский, чешский, русский, польский, корейский, традиционный и упрощенный китайский.
4. Выберите **Сохранить**.

3.5.1.4 SMTP

Примечание
Можно пропустить этот раздел и настроить SMTP позже.

1. Введите DNS-имя или IP-адрес сервера SMTP.
2. Введите порт SMTP-сервера.
3. Если вы не используете сертификаты для сервера SMTP, снимите флажок **Использовать защищенное подключение?**.
4. Введите имя, которое будет отображаться в поле «От» сообщений электронной почты, отправляемых сервером.
5. Введите адрес, на который сервер будет отправлять сообщения.
6. Если вы применяете проверку подлинности для SMTP-сервера на основе имени пользователя и пароля, установите флажок **Использовать проверку подлинности SMTP?** и введите учетные данные.
7. Нажмите кнопку **Отправить тестовое письмо**, чтобы отправить тестовое сообщение, настроенное на шаге 5.
8. Выберите **Сохранить**.

3.5.1.5 LDAP

Примечание
Можно пропустить этот раздел и настроить LDAP позже, но до этого времени некоторые функции Кибер Файлы будут недоступны.

1. Установите флажок **Включить LDAP**.
2. Введите DNS-имя или IP-адрес сервера LDAP.
3. Введите порт сервера LDAP.
4. Если вы используете сертификат для подключений к серверу LDAP, установите флажок **Использовать защищенное LDAP-подключение**.
5. Введите свои учетные данные LDAP вместе с доменом (например, Cyberprotect\hristo).
6. Введите базу поиска LDAP.
7. Введите требуемый домен или домены для проверки подлинности LDAP (чтобы включить аутентификацию LDAP для учетной записи с адресом joe@glilabs.com, следует ввести glilabs.com).
8. Выберите **Сохранить**.

3.5.1.6 Локальный сервер шлюза

Чтобы служба KCD работала через мобильные клиенты, необходимо зарегистрироваться на локальном шлюзе (который установлен на той же машине, что и сервер Tomcat, который им управляет). Тогда шлюз будет направлять эти запросы на данный сервер управления Tomcat.

Примечание
Если сервер шлюза и сервер Кибер Файлы установлены на одном компьютере, то последний обнаружит сервер шлюза автоматически и будет управлять им. Появится запрос для настройки DNS-имени или IP-адреса, по которому локальный сервер шлюза будет доступен клиентам. Этот адрес можно изменить позднее.

1. Задайте DNS-имя или IP-адрес для локального сервера шлюза.
2. Нажмите кнопку **Сохранить**.

3.5.1.7 Файловый репозиторий

1. Выберите тип хранения файла. Выберите **Файловая система**, чтобы хранить файлы на своих компьютерах, либо любой из следующих вариантов, чтобы файлы хранились в облаке: **Swift S3**, **Ceph S3** или **Другое S3-совместимое хранилище**.

Примечание
Вариант **Другое S3-совместимое хранилище** можно использовать для поставщиков хранилищ S3, не указанных в списке, но правильная работа всех функций не гарантируется.

Примечание
Тип хранилища MinIO S3 поддерживается и может быть настроен как **Другое S3-совместимое хранилище**, однако мы не поддерживаем его использование через незащищенное подключение HTTP.

2. Введите DNS-имя или IP-адрес службы файлового репозитория.

Примечание
Средство конфигурации Кибер Файлы используется для указания адреса, порта и расположения хранилища файлов репозитория. Настройка «Конечная точка репозитория хранения файлов» должна соответствовать настройкам на вкладке «Файловый репозиторий» средства конфигурации. Чтобы просмотреть или изменить эти настройки, запустите файл Cyber Files Configuration Utility.exe, который обычно находится в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\Configuration Utility на сервере конечной точки.

3. Выберите уровень защиты. Выберите один из следующих вариантов: **Нет**, **Низкий**, **Высокий**, **ГОСТ 28147-89**.
4. Укажите минимальное пороговое значение свободного места на диске, прежде чем сервер начнет отправлять предупреждения.
5. Выберите **Сохранить**.

3.6 Кластеризация Кибер Файлы

Кибер Файлы предусматривает конфигурацию установки в режиме высокой доступности без необходимости в стороннем ПО для кластеризации. Все эти конфигурации управляются через сервер Кибер Файлы.

Дополнительные сведения и инструкции по настройке кластерной группы см. в статье Кластерные группы.

Хотя рекомендуется использовать встроенную функцию кластеризации, Кибер Файлы поддерживает также отказоустойчивую кластеризацию Майкрософт; дополнительные сведения см. в разделе Вспомогательные материалы.

3.7 Балансировка нагрузки Кибер Файлы

Кибер Файлы поддерживает балансировку нагрузки. Дополнительные сведения приведены в разделах Установка Кибер Файлы в конфигурации с балансировкой нагрузки, Миграция на конфигурацию с балансировкой нагрузки.

4 Обновление

4.1 Обновление кластеров шлюза

Для обновления кластеризованной конфигурации Кибер Файлы понадобится обновить как веб-сервер Кибер Файлы, так и серверы шлюза в кластерной группе.

Примечание
Сведения об обновлении конфигурации отказоустойчивой кластеризации Майкрософт см. в разделе Вспомогательные материалы.

Примечание
Инструкции по обновлению веб-сервера Кибер Файлы см. в статье Обновление Кибер Файлы

Для каждого сервера шлюза необходимо будет выполнить следующую операцию обновления.

Перед обновлением просмотрите наши статьи по резервному копированию и сохраните копию конфигурации.

Примечание
Перед обновлением просмотрите минимальные требования к оборудованию.

Примечание
В зависимости от развертывания некоторые пути, указанные в этой статье, могут отличаться от ваших. Структура папок может измениться при обновлении предыдущих версий Кибер Файлы или пользовательской установке.

4.1.1 Обновление сервера шлюза

1. Запустите программу установки Кибер Файлы на требуемом сервере.
2. Нажмите кнопку **Далее** на экране **Приветствие**.
3. Прочитайте и примите лицензионное соглашение.
4. Выберите **Пользовательская** .
5. Выберите только компонент **Сервер шлюза Кибер Файлы** и нажмите кнопку **Далее**.
6. Проверьте компоненты и нажмите кнопку **Установить**.
7. После завершения установки проверьте **сводку** и закройте программу установки.
8. Появится запрос на открытие **программы настройки**. Откройте ее, чтобы проверить, сохранились ли ранее сделанные настройки сервера шлюза. При необходимости внесите изменения и нажмите кнопку **OK**.

4.2 Обновление конфигураций с балансировкой нагрузки

Это руководство предназначено для установок с балансировкой нагрузки Кибер Файлы и всех его компонентов.

Перед обновлением просмотрите наши статьи по резервному копированию и сохраните копию конфигурации.

Примечание
Перед обновлением просмотрите минимальные требования к оборудованию.

Примечание
В зависимости от развертывания некоторые пути, указанные в этой статье, могут отличаться от ваших. Структура папок может измениться при обновлении предыдущих версий Кибер Файлы или пользовательской установке.

4.2.1 Перед началом работы

Предупреждение
Кибер Файлы не поддерживает те версии Tomcat, Java и PostgreSQL, которые являются более новыми, нежели версии, предоставляемые с каждым выпуском.

Примечание
Мы настоятельно рекомендуем вам запустить тестовое обновление за пределами вашей рабочей среды.

Все пути к файлам, перечисленные на этой странице, соответствуют расположениям по умолчанию. Ваши пути могут отличаться, если вы выполняли обновление версии или пользовательскую установку. В этих случаях по записи Windows Services [имя службы] найдите точное расположение папки исполняемого модуля программы.

Важный момент, который следует учитывать в зависимости от текущей конфигурации.

- Серверы Кибер Файлы и PostgreSQL расположены на одной машине?
- На каком порту работает PostgreSQL?
- Какая локализация у текущей установки PostgreSQL? Чтобы проверить, откройте средство администрирования PostgreSQL и щелкните по базе данных cyberfiles_production. Справа в разделе **Свойства** отобразятся **Кодировка** и **Тип символов**.

Предупреждение
Убедитесь, что в новой установке PostgreSQL те же **Кодировка** и **Тип символов**, иначе обновление выполнить не удастся.

- Какой IP-адрес и/или DNS-имя у машины с PostgreSQL?
- Какой номер версии PostgreSQL у текущего сервера. Самый простой способ узнать версию – посмотреть имя подпапки внутри основной папки PostgreSQL (по умолчанию: C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\PostgreSQL). Имя подпапки представляет собой номер основной версии PostgreSQL (например, 9.2; 9.3; 9.4).
- Убедитесь, что настроены все необходимые разрешения в файловых системах.

Выберите один из веб-серверов Кибер Файлы в качестве **основного**. Этот узел будет **основным** только в том смысле, что он будет обновлен первым, а затем перенесет все изменения и настройки в базу данных PostgreSQL. Если база данных очень большая, перенос может занять несколько минут.

Предупреждение
НЕ обновляйте другие серверы Tomcat до тех пор, пока не будет обновлен **Основной** сервер, и до того, как можно будет выполнить вход в веб-интерфейс для проверки.

4.2.1.1 Чистка базы данных

Это ускорит процесс резервного копирования и восстановления за счет оптимизации базы данных.

1. Откройте программу Кибер Файлы PostgreSQL Administrator (также может называться PgAdmin). Оно находится в меню «Пуск» Windows в папке Кибер Файлы. Дважды щелкните **localhost** для подключения к серверу.
2. Щелкните правой кнопкой по базе данных cyberfiles_production и выберите **Обслуживание**.
3. Выберите **ЧИСТКА** и установите для параметра **АНАЛИЗ** значение «Да».

   Предупреждение
   Чистка может занять некоторое время. Этот процесс следует запускать в периоды низкой загрузки сервера.

4. Нажмите кнопку**OK**.
5. После завершения процесса **чистки** нажмите кнопку **Готово**.
6. Закройте средство PostgreSQL Administrator.

4.2.2 Резервное копирование компонентов с балансировкой нагрузки

Подробные сведения о процедурах резервного копирования и восстановления см. в статье** Резервное копирование и восстановление Кибер Файлы **.

4.2.2.1 Резервное копирование базы данных PostgreSQL

1. Остановите все службы Кибер Файлы Tomcat.
2. Откройте средство Кибер Файлы PostgreSQL Administrator. Оно находится в меню «Пуск» Windows в папке Кибер Файлы. Подключитесь к серверу базы данных. Может потребоваться ввести пароль для пользователя postgres .
3. Разверните раздел **Базы данных** и щелкните правой кнопкой базу данных cyberfiles_production.
4. Выберите **Обслуживание**.
5. Выберите **ЧИСТКА** и установите для параметра **АНАЛИЗ** значение «Да».
6. Нажмите кнопку**OK**.
7. Разверните базу данных, раздел **Схемы** и раздел **Общедоступные**. Обратите внимание на число в разделе **Таблицы** . Это может помочь удостовериться в успешности восстановления базы данных.
8. Закройте средство PostgreSQL Administrator и откройте командную строку с повышенными привилегиями.
9. В командной строке перейдите в папку bin PostgreSQL.
   например, "C:\Program Files(x86)\Cyberprotect\Cyber Files\Common\PostgreSQL\<version>\bin"

Примечание
Необходимо будет изменить путь, чтобы он указывал на папку PostgreSQL, если это старая или выборочная установка (например, C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\PostgreSQL\9.4\bin\).

1. Введите следующую команду: pg_dumpall --host localhost --port 5432 --username postgres --file alldbs.sql
   - alldbs.sql будет именем файла резервной копии, сохраненной в каталоге bin PostgreSQL. Вы можете использовать путь в приведенной выше команде, если хотите сохранить его в другом месте, например, измените последнюю часть приведенной выше команды следующим образом: --file D:\Backups\alldbs.sql
   - Если используется порт, отличный от порта по умолчанию, замените 5432 на нужный номер порта.
   - Если вы по умолчанию не используете учетную запись администратора PSQL postgres, то в приведенной выше команде измените postgres на имя вашей учетной записи администратора.
   - В процессе этого вам потребуется несколько раз ввести пароль пользователя postgres . При каждом запросе вводите пароль и нажимайте клавишу «Ввод».

   Примечание
   Ввод пароля никак не отражается в окне командной строки.

2. Скопируйте файл резервной копии в надежное место.
3. **НЕ** отключайте службу Postgres, иначе обновление PostreSQL не будет выполнено.

4.2.2.2 Резервное копирование важных дополнительных компонентов

1. Создайте резервные копии папок Tomcat **conf** и **logs**. По умолчанию они расположены в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\apache-tomcat-<version>\

   Примечание
   Замените <version> номером версии вашего экземпляра Кибер Файлы Tomcat, например \apache-tomcat.70.0.70\

2. Создайте резервную копию файла **cyberfilessrv.cfg**. По умолчанию он расположен в папке . C:\Program Files (x86)\Cyberprotect\Cyber Files\Access Server
3. Сделайте резервные копии всех файлов **web.xml**. Они по умолчанию расположены в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Access Server\Web Application\WEB-INF\.
4. Создайте резервную копию файла **newrelic.yml**. Он находится там, куда вы его сохранили ранее. Этот шаг можно пропустить, если вы не используете мониторинг New Relic.

4.2.2.3 Резервное копирование баз данных серверов шлюза

1. Отключите все службы шлюза Кибер Файлы
2. Перейдите в папки базы данных шлюза, по умолчанию расположенные в C:\Program Files (x86)\Cyberprotect\Cyber Files\Gateway Server\database
3. Создайте резервную копию файла **mobilEcho.sqlite3**.
4. Повторите эти шаги для каждого сервера шлюза.

4.2.2.4 Остановите все службы Кибер Файлы на всех машинах

Крайне важно перед обновлением остановить все службы Кибер Файлы Tomcat. Рекомендуется также остановить все остальные службы Кибер Файлы, кроме службы PostgreSQL, которая должна работать.

4.2.3 Обновление файлового репозитория

Обновите файловый репозиторий первым, независимо от его расположения.

1. Скопируйте установщик Кибер Файлы на машину с компонентом «Файловый репозиторий» и запустите.

   Примечание
   Если у вас несколько служб файлового репозитория, повторите эти шаги для всех репозиториев перед тем, как приступать к остальным компонентам.

2. На экране **приветствия** нажмите кнопку **Далее**.

3. Примите условия лицензионного соглашения.
4. Выберите **Настроить**, затем выберите обновление только **< Кибер Файлы - Файловый репозиторий** .
5. Щелкните **Далее**, проверьте устанавливаемые компоненты и нажмите кнопку **Установить**.
6. После завершения обновления нажмите кнопку **Выйти**. Когда запустится средство конфигурации, нажмите кнопку **OK**.
7. Далее обновите **основной** сервер Кибер Файлы на соответствующей машине.

4.2.4 Обновление основного сервера Кибер Файлы

1. Скопируйте программу установки Кибер Файлы на компьютер **основного** веб-сервера Кибер Файлы.
2. Запустите программу установки Кибер Файлы на **основном** узле.
3. На экране приветствия нажмите кнопку **Далее**, а затем **Настроить**. Это позволит обновить только необходимые службы, уже установленные на машине, без установки других служб.
4. Выберите службы Кибер Файлы, которые необходимо обновить. Выбирайте только веб-сервер Кибер Файлы и те компоненты, которые уже установлены на машине.
5. Нажмите кнопку **Установить**, подождите завершения работы установщика и запустите **Средство конфигурации**.

   Примечание
   Не меняйте никакие настройки в **средстве конфигурации**! Изменение настроек конфигурации может вызвать проблемы.

6. Когда средство конфигурации запустит все необходимые службы и перенос баз данных завершится, убедитесь, что веб-интерфейс Кибер Файлы на **основном** сервере работает нормально. Автоматически запустится веб-браузер, и отобразится окно входа на сервер Кибер Файлы.
7. Выполните вход как администратор и проверьте, что параметры те же и нет никаких изменений или проблем.
8. Оставьте этот экземпляр Кибер Файлы работать во время обновления всех остальных компонентов.

Предупреждение
Не обновляйте и не запускайте другие серверы Tomcat, пока не возобновит работу основной сервер Tomcat и вы не убедитесь, что он работает правильно.

4.2.5 Обновление серверов шлюза

1. Скопируйте установщик Кибер Файлы на любую машину с сервером шлюза и запустите его.
2. На экране приветствия нажмите кнопку **Далее**.
3. Примите условия лицензионного соглашения.

4. Выберите **Настроить**, затем выберите обновление только сервера шлюза Кибер Файлы.
5. Щелкните **Далее**, проверьте устанавливаемые компоненты и нажмите кнопку **Установить**.
6. После завершения обновления нажмите кнопку **Выйти**. Когда запустится средство конфигурации, нажмите кнопку **OK**.

4.2.6 Обновление всех остальных узлов

Успешно обновив основной узел Кибер Файлы, все серверы файловых репозиториев и все серверы шлюза, обновите остальные серверы Кибер Файлы.

1. Скопируйте программу установки Кибер Файлы на нужный узел и запустите ее.
2. На экране приветствия нажмите кнопку **Далее**, а затем **Настроить**. Это позволит обновить только необходимые службы, уже установленные на машине, без установки других служб.
3. Выберите службы Кибер Файлы, которые необходимо обновить. Выбирайте только те службы, которые установлены на машине.
4. Нажмите кнопку **Установить**, подождите завершения работы установщика и запустите **Средство конфигурации**.

   Примечание
   Не меняйте никаких настроек в **средстве конфигурации**. Изменение настроек конфигурации может вызвать проблемы.

5. После того как средство конфигурации запустит все необходимые службы, убедитесь, что компоненты Кибер Файлы на этом узле работают нормально.

5 Мобильный доступ

Этот раздел описания веб-интерфейса относится ко всем параметрам и настройкам, которые затрагивают пользователей мобильных устройств.

5.1 Понятия

Кибер Файлы мобильные клиенты подключаются напрямую к вашему серверу, а не к сторонним службам, позволяя вам контролировать ситуацию. Сервер Кибер Файлы можно установить в той же сети, что и существующие файловые серверы, чтобы устройства типа iPad, iPhone и Android могли получать доступ к файлам, расположенным в этой сети. Обычно это те же файлы, что доступны на ПК при использовании общего доступа к файлам Windows и на компьютерах Mac через Files Connect Server.

Клиенты получают доступ к серверам Кибер Файлы с помощью учетной записи пользователя Active Directory. Дополнительные учетные записи в Кибер Файлы настраивать не требуется. Приложение Кибер Файлы также поддерживает доступ к файлам с использованием локальных учетных записей компьютера, настроенных на сервере Windows, на котором работает Кибер Файлы. Это необходимо, если требуется предоставить доступ пользователям вне AD. Для применения возможностей управления клиентами, описанных ниже, требуются учетные записи пользователей AD.

Минимальное развертывание состоит из одного сервера Windows с установкой Кибер Файлы по умолчанию. В эту стандартную установку входит компонент Кибер Файлы Server и локальный сервер шлюза Кибер Файлы. Такой сценарий дает пользователям Кибер Файлы возможность подключаться к этому файловому серверу, а также позволяет управлять клиентами на мобильных устройствах. Если управления клиентами не требуется, то на локальном сервере шлюза можно настроить источники данных, при этом мобильные клиенты Кибер Файлы смогут получить доступ к ним, но пользователи будут сами контролировать настройки приложения.

В дальнейшем можно добавить любое число серверов шлюза и настроить их для доступа через клиенты Кибер Файлы.

Примечание
Сведения об установке Кибер Файлы см. в разделе Установка настоящего руководства.
Настройка серверов шлюза и источников данных описана в разделе Мобильный доступ.

Если нужно удаленно управлять мобильными клиентами, средство Кибер Файлы Management позволяет создавать политики для отдельных пользователей и групп Active Directory. Требуется всего один сервер Кибер Файлы. Эти политики могут:

- задавать общие параметры приложения;
- назначать серверы, папки и домашние каталоги, которые будут отображаться в клиентском приложении;
- ограничивать действия, которые можно выполнять с файлами;

- ограничивать сторонние приложения, в которых можно открывать файлы Кибер Файлы;
- задавать требования безопасности (частоту входа на сервер, пароль блокировки приложения и т. д.);
- отключать возможность хранения файлов на устройстве;
- отключать возможность добавлять файлы Кибер Файлы в резервные копии iTunes;
- удаленно сбрасывать пароль блокировки приложения пользователя;
- удаленно очищать локальные данные и настройки мобильного приложения;
- настраивать дополнительные параметры конфигурации и безопасности.

Обычная сеть с поддержкой функций управления клиентами содержит один сервер с сервером Кибер Файлы и сервером шлюза Кибер Файлы, а также несколько дополнительных серверов шлюза, которые действуют как файловые серверы. В этом сценарии все мобильные клиенты управляются сервером Кибер Файлы и будут связываться с ним при каждом запуске приложения Кибер Файлы для проверки изменения параметров, сброса пароля блокировки и удаленной очистки данных.

Клиентам Кибер Файлы можно назначить список серверов, отдельных папок в общих томах и домашних каталогов в соответствующей политике управления. Эти ресурсы будут автоматически отображаться в приложении Кибер Файлы, а клиентское приложение будет напрямую связываться с этими серверами при необходимости доступа к файлам.

Примечание
Сведения о включении и настройке управления клиентами см. в разделах Политики и Управление мобильными устройствами данного руководства.

5.2 Политики

Кибер Файлы позволяет назначать политики группам Active Directory. Политики групп обычно реализуют все или большинство требований для управления клиентами. Список политик групп отображается в порядке очередности, при этом у первой группы в списке самый высокий приоритет. Когда пользователи обращаются к серверу Кибер Файлы, то их настройки определяются политикой группы с наивысшим приоритетом, в которую они входят.

Политики пользователей применяются, когда необходимо применить определенные параметры к пользователю вне зависимости от групп, в которых он состоит, так как приоритет политик пользователей обычно выше, чем у политик групп. Политики пользователей переопределяют все политики групп.

Примечание

Советы по управлению группами.

Чтобы назначить всем или большинству пользователей одинаковые параметры политики, можно использовать групповую политику **По умолчанию**. Все пользователи, которые не входят в какую-либо политику группы и которым не назначена явная политика пользователя, станут членами группы **По умолчанию**. Изначально группа **По умолчанию** включена. Чтобы запретить группе пользователей доступ к функциям управления Кибер Файлы, убедитесь, что они не являются участниками настроенных групповых политик. Если учетная запись пользователя не входит ни в одну групповую политику, он не сможет зарегистрироваться в средстве управления клиентами Кибер Файлы.

5.2.1 Добавление новой политики

5.2.1.1 Чтобы добавить новую групповую политику, выполните следующие действия.

1. Откройте вкладку **Политики для групп**.
2. Нажмите кнопку **Добавить новую политику**, чтобы добавить новую групповую политику. При этом откроется страница **Добавление новой групповой политики**.
3. В поле **Найти группу** введите полностью или частично имя группы Active Directory, для которой создается политика. В группах Active Directory можно производить поиск типа **начинается с** или **содержит**. Поиск «начинается с» работает намного быстрее, чем поиск типа «содержит».
4. Нажмите кнопку **Поиск**, затем найдите в отобразившихся результатах имя нужной группы и щелкните его.
5. Задайте необходимые настройки на вкладках Безопасность, Приложение, Синхронизация, Домашние папки и Сервер, а затем нажмите **Сохранить**.

5.2.1.2 Чтобы добавить новую политику пользователей, выполните следующие действия.

1. Откройте вкладку **Политики для пользователей**.
2. Нажмите кнопку **Добавить новую политику**, чтобы добавить новую политику пользователей. При этом откроется страница **Добавление новой пользовательской политики**.
3. В поле **Найти пользователя** введите полностью или частично имя пользователя Active Directory, для которого создается политика. Среди пользователей Active Directory можно производить поиск типа **начинается с** или **содержит**. Поиск «начинается с» работает намного быстрее, чем поиск типа «содержит».
4. Нажмите кнопку **Поиск**, затем найдите в отобразившихся результатах имя нужного пользователя и кликните на него.
5. Задайте необходимые настройки на вкладках Безопасность, Приложение, Синхронизация, Домашние папки и Сервер, а затем нажмите **Сохранить**.

5.2.2 Изменение политик

Существующие политики можно изменить в любое время, Изменения будут применены к соответствующим пользователям мобильного приложения при следующем его запуске.

Примечание

Требования к подключению Клиенты

Кибер Файлы должны иметь сетевой доступ к серверу Кибер Файлы, чтобы получать обновления профиля, команды на удаленный сброс пароля или удаленную очистку данных. Если для доступа к Кибер Файлы клиенту необходимо VPN-подключение, то это подключение необходимо и для приема команд управления.

5.2.2.1 Изменение политики группы

1. Щелкните **Политики группы** в верхней строке меню.
2. Выберите группу, которую необходимо изменить.
3. Внесите необходимые изменения на странице **Изменить политику группы** и нажмите **Сохранить**.
4. Чтобы временно отключить политику, снимите флажок в столбце **Включено** для нужной группы. Это изменение вступает в силу немедленно.
5. Чтобы изменить приоритет группы, щелкните по стрелке вверх или вниз в списке «Управление профилями групп». Это приведет к тому, что группа поднимется или опустится в списке на один уровень.

5.2.2.2 Изменение политики пользователя

1. Откройте вкладку **Политики для пользователей**.
2. Выберите пользователя, которого необходимо изменить.
3. Внесите необходимые изменения на странице **Изменить политику пользователя** и нажмите **Сохранить**.
4. Чтобы временно отключить политику, снимите флажок в столбце **Включено** для нужного пользователя. Это изменение вступает в силу незамедлительно.

5.2.3 Настройки политик

5.2.3.1 Политика безопасности

- **Создание пароля приложения** – в мобильном приложении можно настроить пароль блокировки, который необходимо ввести перед запуском приложения.
  - **Необязательно** – при применении этого параметра пользователям не придется задавать пароль блокировки приложения, но они смогут настроить его в меню **Настройки** приложения, если потребуется.

- **Отключено** – этот параметр отключает возможность настройки пароля блокировки приложения в меню **Настройки** в приложении. Это может быть полезно при использовании общих мобильных устройств, чтобы запретить пользователю задавать пароль и блокировать доступ других пользователей к мобильному приложению.
- **Обязательно** – при применении этого параметра пользователям необходимо задать пароль блокировки приложения, если это еще не сделано. Требования к сложности пароля и удаление данных при превышении числа неудачных попыток ввода пароля применяются, только если для параметра **Создание пароля приложения** задано значение **Обязательно**.
  - **Приложение будет заблокировано** – этот параметр задает льготный период для пароля приложения. Когда пользователь переключается с мобильного приложения Кибер Файлы на другое приложение на устройстве, ему не придется вводить пароль, если он вернется в мобильное приложение до истечения определенного периода времени. Чтобы требовать ввода пароля всегда, выберите параметр **Сразу после выхода**. Чтобы разрешить пользователю изменять параметр **Приложение заблокирует** в настройках мобильного приложения, выберите параметр **Разрешить пользователю менять этот параметр**.
  - **Минимальная длина пароля** – минимальная разрешенная длина пароля блокировки приложения.
  - **Минимальное число сложных символов** – минимальное число небуквенных и нецифровых символов в пароле блокировки приложения.
  - **Требовать одну или несколько букв** – при использовании этого параметра пароль приложения должен содержать по крайней мере одну букву.
  - **Мобильное клиентское приложение будет очищено, когда число неудачных попыток ввода пароля достигнет X** – если этот параметр включен, настройки и данные мобильного приложения будут удалены после указанного числа неудачных попыток ввода пароля.
- **Очистить или заблокировать после потери связи** – включите этот параметр, чтобы мобильное приложение автоматически удаляло данные или блокировалось, если оно не связывалось с этим сервером Кибер Файлы в течение заданного числа дней.

  Предупреждение
  Если приложение по какой-либо причине не сможет пройти проверку подлинности, его контакт с сервером не будет зарегистрирован, даже если сервер доступен.

  - Заблокированные клиенты будут разблокированы автоматически, если они в дальнейшем успешно свяжутся с сервером.
  - После очистки все локальные файлы будут автоматически удалены из мобильного приложения, политика управления клиентами будет удалена и будут восстановлены настройки по умолчанию. Этих клиентов нужно будет заново зарегистрировать в средстве управления, чтобы получить доступ к серверам шлюза.
  - **Мобильное клиентское приложение будет заблокировано/очищено через X дн. после неудачной попытки связаться с сервером Кибер Файлы этого клиента** – задает действие по умолчанию, которое выполняется, если клиенту не удается связаться с сервером Кибер Файлы в течение заданного количества дней.

- **Предупреждать пользователей за [ ] дн.** – приложение Кибер Файлы может предупреждать пользователя о предстоящей очистке данных или блокировке в случае потери связи. Это позволяет восстановить сетевое подключение, чтобы приложение Кибер Файлы связалось с сервером Кибер Файлы и блокировка или очистка была отменена.

- **Отчеты о сбоях приложения** – отправка отчета в Киберпротект при сбое мобильного приложения. Отчеты не содержат конфиденциальных данных и личной информации.
  - **Никогда не отправлять отчеты**
  - **Отправлять отчеты по выбору пользователя**
  - **Всегда отправлять отчеты**
- **Разрешить iTunes и iCloud создавать резервные копии локальных файлов Кибер Файлы files**. Если этот параметр отключен, то мобильное приложение не позволит iTunes или iCloud создавать резервные копии своих файлов. Таким образом, файлы в безопасном хранилище Кибер Файлы не будут копироваться в резервные копии.
- **Пользователь может удалить мобильный клиент из списка управляемых элементов**. Включите этот параметр, чтобы разрешить пользователям Кибер Файлы удалять политику управления из Кибер Файлы. Это позволит восстановить все функции приложения и все настройки, измененные политикой.
  - **Очистить все данные Кибер Файлы при удалении**. Этот параметр можно выбрать, если пользователю разрешено удалять политики. Если он включен, то все локальные данные в мобильном приложении будут удалены, когда оно будет удалено из списка управляемых устройств, чтобы обеспечить отсутствие корпоративных данных на неуправляемом клиенте.

5.2.3.2 Политика приложения

- **Требовать подтверждения при удалении файлов** – если этот параметр включен, то у пользователя будет каждый раз запрашиваться подтверждение при удалении файла. Чтобы разрешить пользователю в дальнейшем изменять эту настройку, выберите **Разрешить пользователю менять этот параметр**.
- **Задать действие для файла по умолчанию** – этот параметр определяет, что произойдет, когда пользователь коснется файла в Кибер Файлах. Если он не установлен, то по умолчанию в клиентском приложении открывается **Меню действий**. Чтобы разрешить пользователю в дальнейшем изменять эту настройку, выберите **Разрешить пользователю менять этот параметр**.
- **Разрешить хранение файлов на этом устройстве** – этот параметр включен по умолчанию. Если он включен, то файлы будет разрешено хранить на устройстве в пределах изолированного хранилища Кибер Файлы. Отдельные компоненты, которые хранят файлы локально (папка «Мои файлы», синхронизируемые папки, кэширование недавно использованных файлов), можно включить или отключить с помощью дополнительных настроек политики. Если этот параметр отключен, то файлы не будут храниться на устройстве, что гарантирует отсутствие корпоративных данных на устройстве в случае его утери или кражи. Если параметр отключен, то пользователь не сможет сохранять или синхронизировать файлы для автономного использования, кэшировать файлы для повышения производительности, а также отправлять

файлы из других приложений в мобильный клиент Кибер Файлы с помощью функции «Открыть в».

  - **Разрешить пользователю хранить файлы в папке My Files на устройстве** – если этот параметр включен, то файлы можно копировать в папку «Мои файлы» для автономного доступа и редактирования. Это хранилище общего назначения в пределах изолированного хранилища Кибер Файлы на устройстве.
  - **Кэшировать недавно использованные файлы на устройстве** – если этот параметр включен, то серверные файлы, к которым недавно осуществлялся доступ, будут сохраняться в локальном кэше на устройстве для использования в случае повторного доступа без изменений, что способствует повышению производительности и экономии пропускной способности сети. Можно указать **Максимальный размер кэша**, а также при необходимости разрешить пользователю изменять эту настройку.
- **Срок действия содержимого в папках My Files и File Inbox истекает через X дн.** – если этот параметр включен, то файлы в папке **Мои файлы** будут удаляться с устройства через заданное количество дней.
- **Блокировать загрузку файлов и папок больше, чем X MB** – при включенном параметре файлы или папки, чей размер превышает заданную величину, не будут загружены мобильными приложениями.

Разрешить

Эти настройки позволяют отключить некоторые компоненты и возможности мобильного приложения. Все настройки копирования, создания, перемещения, переименования и удаления применяются к файлам и папкам, расположенным на серверах шлюза. Файлы в локальной папке «Мои файлы» мобильного клиента хранятся на устройстве и не затрагиваются. Все прочие настройки применяются к любым файлам – как серверным, так и хранящимся локально на клиенте.

Операции с файлами

- **Копирование/создание файла** – если этот параметр отключен, то пользователь не сможет сохранять файлы из других приложений или из библиотеки фотографий iPad на сервере шлюза. Кроме того, пользователи не смогут копировать или создавать новые файлы или папки на сервере шлюза. Эта настройка имеет больший приоритет, чем любые разрешения NTFS для клиента, которые могут разрешать создание файлов.
- **Удаление файлов** – если этот параметр отключен, то пользователь не сможет удалять файлы с сервера шлюза. Эта настройка имеет больший приоритет, чем любые разрешения NTFS для клиента, которые могут разрешать удаление файлов.
- **Перемещения файлов** – если этот параметр отключен, пользователь не сможет перемещать файлы из одного местоположения в другое на сервере шлюза, равно как и с сервера в локальное хранилище «Мои файлы». Эта настройка имеет больший приоритет, чем любые разрешения NTFS для клиента, которые могут разрешать перемещения файлов или папок.

- **Переименования файлов** – если этот параметр отключен, то пользователь не сможет переименовывать файлы с сервера шлюза. Эта настройка имеет больший приоритет, чем любые разрешения NTFS для клиента, которые могут разрешать переименования файлов.

Операции с папками

- **Копии папки** – если этот параметр отключен, то пользователь не сможет копировать папки на сервер шлюза или в его пределах. Эта настройка имеет больший приоритет, чем любые разрешения NTFS для клиента, которые могут разрешать создание папок. Для включения этой настройки необходимо включить **Копирование/создание файла**.
- **Удаление папок** – если этот параметр отключен, то пользователь не сможет удалять папки с сервера шлюза. Эта настройка имеет больший приоритет, чем любые разрешения NTFS для клиента, которые могут разрешать удаление папок.
- **Перемещение папок** – если этот параметр отключен, то пользователь не сможет перемещать папки из одного расположения в другое на сервере шлюза, равно как и с сервера в локальное хранилище «Мои файлы». Эта настройка имеет больший приоритет, чем любые разрешения NTFS для клиента, которые могут разрешать перемещения файлов или папок. Для включения этой настройки необходимо включить **Копии папки**.
- **Переименования папок** – если этот параметр отключен, то пользователь не сможет переименовывать папки на сервере шлюза. Эта настройка имеет больший приоритет, чем любые разрешения NTFS для клиента, которые могут разрешать переименования папок.
- **Добавление новых папок** – если этот параметр отключен, то пользователь не сможет создавать новые пустые папки на сервере шлюза.
- **Добавление папок в закладки** – если этот параметр отключен, то пользователь не сможет добавлять в закладки папки на устройстве или сервере Кибер Файлы для быстрого доступа к ним.

Ссылки на файлы mobilEcho

- **Отправка ссылок на файлы mobilEcho по электронной почте** – если этот параметр отключен, то пользователи не смогут отправлять URL-адреса mobilEcho:// для файлов или папок Кибер Файлы другим пользователям. Эти ссылки функционируют только при открытии с устройства, на котором у получателя установлен клиент Кибер Файлы, настроенный с указанием сервера или назначенной ему папки с доступом к расположению ссылки. Кроме того, у пользователя должно быть разрешение на чтение этого элемента на уровне файла или папки.
- **Открытие ссылок на файлы mobilEcho** – если этот параметр отключен, то пользователям будет запрещено открывать URL-адреса mobilEcho:// для файлов или папок Кибер Файлы.

Гиперссылки в документах

- **Разрешить открывать ссылки в документах** – если этот параметр включен, то пользователи смогут открывать любые ссылки, сохраненные в документах.
  - **Разрешить пользователю изменять эти параметры** – если этот параметр включен, то пользователи смогут включать или отключать эту функцию по своему усмотрению.

  Открывать в:

- **Встроенный браузер** – гиперссылки будут открываться непосредственно в приложении Кибер Файлы.
- **Браузер по умолчанию** – гиперссылки будут открываться по умолчанию в браузере, выбранном на устройстве.
- **MobileIron Web@Work** – гиперссылки будут открываться в приложении MobileIron Web@Work.
- **BlackBerry Access** – гиперссылки будут открываться в приложении BlackBerry Access.

Защита от утечки данных

- **Открытие файлов Кибер Файлы в других приложениях** – если этот параметр отключен, мобильное приложение не будет показывать кнопку **Открыть в** и не позволит открывать файлы Кибер Файлы в других приложениях. Открытие файла в другом приложении приводит к копированию файла в хранилище данных этого приложения без контроля Кибер Файлы.
  - **Белый/черный список приложения**. Выберите предварительно настроенный список разрешений или список блокировки, который определяет, в каких сторонних приложениях на устройстве можно открывать файлы Кибер Файлы. Чтобы создать белый или черный списки, выберите **Разрешенные приложения** в верхней строке меню.
- **Разрешить использование поставщика документов** – этот параметр позволяет мобильным устройствам использовать расширение поставщика документов для Кибер Файлы. Расширение поставщика документов зависит от следующих конфигураций:
  a. Если клиент находится под управлением старого сервера, то расширение поставщика документов включено, если только не **отключен** параметр **Открытие файлов Кибер Файлы в других приложениях** или не включен список разрешений/блокировки.
  b. Если клиент находится под управлением нового сервера (версии 7.3.1 и выше) и параметр **Разрешить использование поставщика документов** включен, то, даже если отключено **Открытие файлов Кибер Файлы в других приложениях** или включены списки разрешений/блокировки, пользователи все равно смогут обмениваться файлами с другими приложениями. В том числе с заблокированными.
  c. Если параметр **Разрешить использование поставщика документов** включен, но запрещено создание файлов, то расширение поставщика документов будет работать, но пользователи не смогут сохранять файлы из других приложений в любые источники данных Кибер Файлы.
- **Отправка файлов в Кибер Файлы из других приложений** – если этот параметр отключен, Кибер Файлы не будут принимать файлы, отправленные с помощью функции **Открыть в** других приложений.
- **Импорт файлов из камеры/библиотеки фотографий** – если этот параметр включен, то пользователи смогут импортировать фотографии и видеозаписи из библиотеки фотографий устройства непосредственно в Кибер Файлы.
- **Отправка файлов из Кибер Файлы по электронной почте** – если этот параметр отключен, мобильное приложение не будет показывать кнопку **Отправить файл по электронной почте** и не позволит отправлять файлы в Кибер Файлы по электронной почте из приложения.

Примечание
Платформа Android не имеет встроенного приложения эл. почты или подобной функции, которая может быть отключена. Чтобы запретить пользователям отправлять файлы по эл. почте, вместо этого нужно отключить функцию открытия файлов Кибер Файлы в других приложениях.

- **Печать файлов из Кибер Файлы** – если этот параметр отключен, мобильное приложение не будет показывать кнопку **Печать** и не позволит печатать файлы из Кибер Файлы.
- **Копирование содержимого из открытых файлов** – если этот параметр отключен, то мобильное приложение не разрешает пользователям выделять текст в открытых документах для операций копирования и вставки. Это предотвращает копирование данных в другие приложения.

Предупреждение
Если активна политика MobileIron, то ее настройка Разрешить копирование/вставку имеет приоритет над этой настройкой.

Редактирование файлов

- **Редактирование и создание файлов Office** – если этот параметр отключен, то пользователям не будет разрешено редактировать документы с помощью встроенного редактора SmartOffice.
  - **Редактирование файлов, защищенных паролем** – если этот параметр отключен, то пользователю не будет разрешено редактировать файлы, защищенные паролем.
- **Редактирование и создание текстовых файлов** – если этот параметр отключен, то пользователю не будет разрешено редактировать TXT-файлы с помощью встроенного текстового редактора.

Аннотации и редактирование PDF

- **Разрешить редактирование PDF** – если этот параметр включен, то пользователи будут иметь доступ к различным функциям редактирования PDF-файлов, таким как создание страниц, дублирование страниц, копирование и вставка, изменение порядка, поворот, удаление, а также создание нового документа из выбранных страниц.
- **Разрешить аннотации в PDF** – если этот параметр отключен, то мобильному приложению не будет разрешено добавлять аннотации в PDF-файлы.
  - **Разрешить создание пустых PDF-файлов** – если этот параметр включен, то пользователи смогут создавать пустые PDF-файлы, которые можно редактировать с помощью аннотаций.
- **Применить пользовательские параметры просмотра PDF** – если этот параметр включен, то все подпараметры будут применены для всех пользователей и всех PDF-файлов.
  - **Разрешить пользователю изменять эти параметры** – если этот параметр включен, то пользователи смогут изменять свои параметры просмотра PDF.
  - **По ширине** – если этот параметр включен, размер страницы будет подгоняться под ширину экрана устройства.
  - **Ночной режим** – если этот параметр включен, устройство будет использовать цветовую схему ночного режима для более комфортного просмотра в условиях плохой освещенности.

- **Направление прокрутки** – позволяет выбрать смену страниц по горизонтали или по вертикали.
- **Переход по страницам** – позволяет выбрать визуальные эффекты при переходе по страницам. **Скольжение** – простая смена страниц; **Непрерывно** – прокрутка страниц в виде одного непрерывного листа; **Переворачивание** – перелистывание страниц, как в книге.
- **Режим отображения страницы** – позволяет выбрать режим просмотра с отображением одной или двух страниц на экране.
- **Эскизы** – задает размер эскизов PDF-страниц. Можно выбрать **Мелкие**, **Крупные** или **Нет**.
- **Поиск** – позволяет настроить формат отображения результатов поиска во встроенном средстве просмотра. Существует три типа представления результатов поиска.
  - **Простой** – результаты будут выделены, и по ним можно будет перемещаться с помощью значков со стрелками.
  - **Расширенный** – отображает раскрывающийся список всех результатов, по которым можно перемещаться касанием.
  - **Динамический** – устанавливает тип отображения **Простой** для устройств iPhone и **Расширенный** для устройств iPad.
- **Выделение гиперссылок** – позволяет выбрать цвет для выделения гиперссылок. Либо можно отключить выделение, выбрав вариант **Отключено**.

5.2.3.3 Политика синхронизации

- **Разрешить пользователю создавать папки синхронизации** – разрешает пользователю создавать собственные синхронизируемые папки.
  - **Разрешить создание папок только односторонней синхронизации** – пользователи смогут создавать синхронизируемые папки только для односторонней синхронизации.
  - **Тип синхронизируемой папки по умолчанию** – устанавливает односторонний или двусторонний тип синхронизируемых папок по умолчанию.
- **Клиенту предлагается подтвердить операцию перед скачиванием синхронизированных файлов** – выберите условия, при которых пользователь должен давать подтверждение перед скачиванием файлов в синхронизированных папках. Возможные варианты: **Всегда**, **Только при подключении к сотовым сетям** или **Никогда**. Если включен параметр **Разрешить пользователю менять этот параметр**, то клиенты смогут изменять параметры подтверждения.
- **Разрешить синхронизацию файлов только при подключении к WiFi-сетям**. Если этот режим включен, то Кибер Файлы не будет разрешать синхронизацию файлов по сотовой связи. Если включен параметр **Разрешить пользователю менять этот параметр**, то клиенты смогут включать или отключать автоматическую синхронизацию файлов при подключении к сетям WiFi.
- **Интервал автоматической синхронизации**. Если этот параметр включен, то Кибер Файлы будет выполнять автоматическую синхронизацию при следующих условиях: **никогда**, **только при запуске приложения** или через определенные **интервалы времени**.
  - **Разрешить пользователю менять этот параметр**. Если этот параметр включен, то пользователи смогут изменять интервал времени из мобильного приложения Кибер Файлы.

- **Разрешить автоматическую синхронизацию файлов только при подключении к WiFi-сетям** – если этот параметр включен, то автоматическая синхронизация не будет выполняться, если только пользователь не подключен посредством сети WiFi.

- **Не допускать перехода устройства в спящий режим во время синхронизации файлов** – если этот параметр включен, то поддерживающие его устройства не будут переходить в режим блокировки или спящий режим при запущенной синхронизации файлов. Если включен параметр **Разрешить пользователю менять этот параметр**, то клиенты смогут изменять параметры подтверждения.

5.2.3.4 Домашние папки

- **Отображать домашнюю папку пользователя** – с помощью этого параметра можно включить отображение личного домашнего каталога пользователя в приложении Кибер Файлы.
  - **Показать имя, отображаемое в клиенте** – задает отображаемое имя элемента домашней папки в приложении Кибер Файлы. Чтобы включить имя пользователя в отображаемое имя папки, используйте подстановочное значение %USERNAME%.

    Примечание
    Подстановочное значение %USERNAME% нельзя использовать для отображения имени пользователя в других типах источников данных. Его можно использовать только для назначенных домашних папок Active Directory.

  - **Назначенная домашняя папка Active Directory** – домашняя папка, отображаемая в приложении Кибер Файлы, ведет к серверу и пути, указанным в профиле учетной записи пользователя в AD.
    Домашняя папка будет доступна через выбранный шлюз.
  - **Настраиваемый путь к домашнему каталогу** – домашняя папка, отображаемая в приложении Кибер Файлы, ведет пользователя к серверу и пути, определенным в данном параметре. Чтобы включить имя пользователя в путь к домашней папке для источника данных любого типа, используйте подстановочное значение %USERNAME%. %USERNAME% необходимо вводить в верхнем регистре.
  - **Синхронизация с мобильным клиентом** – этот параметр устанавливает тип синхронизации домашнего каталога.

    Примечание
    Этот параметр **НЕ** отражается на возможности пользователя синхронизировать свою домашнюю папку с клиентом для рабочего стола.

5.2.3.5 Политика сервера

- **Требуемая частота входа для ресурсов, назначенных этой политикой** – задает частоту, с которой пользователь должен выполнять вход на серверы, назначенные ему политикой.
  - **Один раз, затем сохранить для будущих сеансов** – пользователь вводит свой пароль при первой регистрации в системе управления. Затем этот пароль сохраняется и используется

для любых последующих подключений к файловому серверу, которые он инициирует.
    - **Один раз за сеанс** – после запуска мобильного Кибер Файлы пользователю требуется вводить пароль во время подключения к первому серверу. Пока пользователь не выйдет из мобильного приложения Кибер Файлы, он сможет подключаться к дополнительным серверам без необходимости повторного ввода пароля. Если пользователь выйдет из мобильного приложения Кибер Файлы на некоторое время, а затем вернется, ему снова будет необходимо ввести пароль для подключения к первому серверу.
    - **Для каждого подключения** – пользователю необходимо вводить пароль каждый раз при подключении к серверу.
- **Разрешить пользователю добавлять отдельные серверы**. Если этот параметр включен, пользователи смогут вручную добавлять серверы из мобильного приложения Кибер Файлы, пока у них имеется DNS-имя или IP-адрес сервера. Если нужно, чтобы для пользователя была доступна только политика **Назначенные серверы**, оставьте этот параметр отключенным.
    - **Разрешить сохраненные пароли для настроенных пользователем серверов** – если пользователю разрешено добавлять отдельные серверы, этот вложенный параметр определяет, разрешено ли ему сохранять пароль для такого сервера.
- **Разрешить доступ к файловому серверу, NAS и Sharepoint из веб-клиента** – если этот флажок включен, то пользователи веб-клиента будут иметь доступ также и к мобильным источникам данных.
    - **Разрешить клиентскому приложению для настольных ПК синхронизацию с папками файлового сервера, NAS и SharePoint** – когда эта настройка включена, клиенты для настольных ПК получат возможность односторонней синхронизации с данными, которые передаются через **Сеть**.
        - **Разрешить клиентскому приложению для настольных ПК двустороннюю синхронизацию с папками файлового сервера, NAS и SharePoint** – когда эта настройка включена, клиенты для настольных ПК получат возможность двусторонней синхронизации с данными, которые передаются через **Сеть**.

          Примечание
          Чтобы включить двустороннюю синхронизацию данных, которые передаются через **Сеть**, для настольных клиентов, необходимо предварительно разрешить следующие действия с файлами и папками на вкладке **Политика приложения**: **создание** (**добавление** для папок), операции **копирования**, **удаления**, **перемещения** и **переименования**.
- **Разрешить пользователю добавлять сетевые папки с помощью UNC-пути или URL-адреса** – если этот параметр включен, пользователи мобильного клиента смогут добавлять и открывать сетевые папки и узлы SharePoint, которые им не назначены или недоступны посредством существующих источников данных. Выбранный сервер шлюза должен иметь доступ к таким общим папкам SMB или узлам SharePoint.
    - **Блокировать доступ к определенным сетевым путям.** Если эта функция включена, то администратор может создавать и использовать списки блокировки сетевых путей, которые пользователям запрещено самостоятельно настраивать.

- **Разрешить этому мобильному клиенту подключение только к серверам с подписанными третьей стороной сертификатами SSL**. Если этот параметр включен, то клиенту Кибер Файлы будет разрешено подключаться только к серверам с сертификатами SSL, подписанными третьей стороной.

  Примечание
  Если у сервера управления нет сертификата от третьей стороны, клиент не сможет связаться с сервером управления после начальной настройки. При включении этого параметра убедитесь в наличии сертификатов от третьих сторон на всех ваших серверах шлюза.

- **Предупреждать клиента при подключении к серверам с недоверенными SSL-сертификатами** – если ваши пользователи регулярно подключаются к серверам, которые будут использовать самозаверенные сертификаты, то по выбору можно отключить диалоговое окно с предупреждением на стороне клиента, которое открывается при подключении к таким серверам.
- **Время ожидания клиента для неотвечающих серверов** – этот параметр устанавливает время ожидания подключения при входе клиента для серверов, которые не отвечают на запросы. Если клиент пользуется очень медленным подключением для передачи данных либо полагается на решение «VPN по запросу» для первоначального установления соединения, прежде чем сервер шлюза станет доступным, нужно задать время ожидания, которое больше значения по умолчанию – 30 секунд. Если вам нужно, чтобы клиент мог изменять эту настройку с помощью мобильного приложения Кибер Файлы, установите флажок **Разрешить пользователю менять этот параметр**.

5.2.4 Создание списка блокируемых путей

Вы можете создать списки блокировки путей, которые не должны быть доступны пользователям для самостоятельной настройки на мобильных устройствах. Эти списки должны быть назначены групповой или пользовательской политике и действительны только для самостоятельно предоставляемых путей. После создания и назначения списка подходящим пользователям или группам нужно включить функцию **Блокировать доступ к определенным сетевым путям** для каждой нужной пользовательской или групповой политики.

5.2.4.1 Чтобы создать список, выполните следующие действия.

1. Откройте веб-интерфейс от имени администратора.
2. Откройте страницу Политики.
3. Выберите нужную пользовательскую или групповую политику.
4. Откройте вкладку Политика сервера.
5. Установите флажок **Блокировать доступ к определенным сетевым путям**.

Примечание
Это действие нужно выполнить для каждой пользовательской/групповой политики, которой необходимо назначить список блокировки.

6. Нажмите **Добавить/отредактировать списки**.
7. На странице **Списки блокированных путей** нажмите **Добавить список**.
8. Введите имя списка.
9. Введите путь или набор путей, которые будут блокироваться. Каждую запись следует вводить на новой строке.
10. Откройте вкладку **Применить к пользователю или группе**.
11. Назначьте список нужным пользователям и группам.
12. Нажмите кнопку **Сохранить**.

5.2.4.2 Чтобы применить список блокировки к пользовательской или групповой политике, выполните следующие действия.

1. Откройте веб-интерфейс от имени администратора.
2. Откройте страницу Политики.
3. Выберите нужную пользовательскую или групповую политику.
4. Откройте вкладку Политика сервера.
5. Установите флажок **Блокировать доступ к определенным сетевым путям**.

Примечание
Это действие нужно выполнить для каждой пользовательской/групповой политики, которой необходимо назначить список блокировки.

6. Выберите требуемый список из раскрывающегося меню.

Примечание
При нажатии кнопки **Обновить списки** будут обновлены параметры раскрывающегося меню.

7. Нажмите кнопку **Сохранить**, чтобы сохранить политику и выйти.

5.2.5 Разрешенные приложения

Кибер ФайлыСлужба управления клиентами позволяет создавать белые и черные списки, которые ограничивают Кибер Файлы возможность мобильного устройства открывать файлы в других приложениях на мобильном устройстве. Они используются как гарантия того, что любые файлы, к которым осуществляется доступ через мобильное устройство Кибер Файлы, будут открываться только в надежных и доверенных приложениях.

Белые списки позволяют задать список приложений, в которых разрешается открывать файлы Кибер Файлы. Всем другим приложениям доступ запрещается.

Черные списки позволяют задать список приложений, в которых запрещается открывать файлы Кибер Файлы. Всем другим приложениям доступ разрешается.

Чтобы программа Кибер Файлы могла идентифицировать конкретное приложение, необходим **идентификатор пакета** данного приложения. Список распространенных приложений с их идентификаторами пакетов по умолчанию входит в состав веб-интерфейса Кибер Файлы. Если приложение, которое следует включить в список разрешений или блокировки, отсутствует в этом списке, необходимо его добавить.

Примечание
Включение приложений в белые и черные списки в настоящее время не поддерживается мобильным приложением Кибер Файлы для Android.

Списки

Добавьте белые и черные списки. После создания белые и черные списки можно назначать любой политике пользователей или групп в Кибер Файлы. Они будут применяться только к указанным вами политикам пользователей или групп.

- **Имя** – показывает имя списка, заданное администратором.
- **Тип** – показывает тип списка (разрешений/блокировки).
- **Добавить список** – открывает меню «Добавить белый список» список или «Добавить черный список».

5.2.5.1 Добавление приложений, доступных для списков

Чтобы добавить приложение, которое можно будет включать в список разрешений или блокировки, выполните следующие действия.

1. Щелкните **Разрешенные приложения** на верхней панели меню.
2. Щелкните **Добавить приложение** в разделе **Приложения, доступные для списков**.
3. Введите **Имя приложения**. Это может быть как имя приложения, под которым оно предлагается в магазине приложений, так и другое имя по вашему выбору.
4. Введите **Идентификатор пакета**. Этот параметр должен в точности совпадать с идентификатором пакета соответствующего приложения, иначе оно не будет включено в разрешенный или запрещенный список.
5. Выберите **Сохранить**.

Идентификатор пакета можно найти, просмотрев файлы на устройстве, а также в библиотеке iTunes.

5.2.5.2 Определение идентификатора пакета приложения

Определение идентификатора пакета приложения путем просмотра файлов на устройстве

Если используется программное обеспечение, которое позволяет просматривать содержимое хранилища вашего устройства, можно найти приложение на устройстве и определить его **идентификатор пакета**. Одно из приложений, которое позволяет это сделать, — iExplorer.

1. Подключите устройство к компьютеру через USB и запустите iExplorer или подобную утилиту.
2. Откройте папку Apps на устройстве и найдите требуемое приложение.
3. Откройте папку этого приложения и найдите в ней файл **iTunesMetadata.plist**.
4. Откройте этот PLIST-файл в текстовом редакторе.
5. Найдите в списке ключ **softwareVersionBundleId**.
6. Значение типа **string** — идентификатор пакета, который потребуется ввести для приложения в Кибер Файлы. Обычно идентификаторы имеют следующий формат: **com.companyname.appname.**

Поиск идентификатора пакета приложения в библиотеке iTunes

Если устройство синхронизируется с iTunes, а требуемое приложение либо находится на вашем устройстве, либо было загружено через iTunes, то оно также находится на жестком диске вашего компьютера. Можно найти его на жестком диске и определить по файлам в приложении **идентификатор пакета**.

1. Перейдите в библиотеку iTunes и откройте папку **Мобильные приложения**.
2. На компьютере Mac обычно она находится в домашнем каталоге пользователя: ~/Music/iTunes/Mobile Applications/
3. На ПК под управлением Windows 7 это обычно папка C:\Users\username\My Music\iTunes\Mobile Applications/
4. Если приложение недавно установлено на устройство, перед продолжением убедитесь, что после этого уже производилась синхронизация iTunes.
5. Найдите требуемое приложение в папке **Mobile Applications** (Мобильные приложения).
6. Скопируйте файл и измените расширение копии на .ZIP.
7. Распакуйте только что созданный ZIP-файл, и будет создана папка под тем же именем, что и у приложения.
8. В этой папке имеется файл **iTunesMetadata.plist**
9. Откройте этот PLIST-файл в текстовом редакторе.
10. Найдите в списке ключ **softwareVersionBundleId**.

11. Значение типа **string** – идентификатор пакета, который потребуется ввести для приложения в Кибер Файлы. Обычно идентификаторы имеют следующий формат: **com.companyname.appname.**

5.3 Начало работы с мобильными устройствами

Чтобы начать работу с мобильным приложением Кибер Файлы, пользователю необходимо установить его из соответствующего магазина приложений: iTunes или Google Play. Если в вашей компании используется управление клиентами, то пользователям надо будет также зарегистрировать мобильное клиентское приложение Кибер Файлы со своего устройства на сервере Кибер Файлы. После регистрации конфигурацией мобильного клиента, его возможностями и настройками безопасности управляет соответствующая политика пользователей или групп в Кибер Файлы.

Политики управляют следующими настройками и функциями мобильного приложения.

- Требуется ли задание пароля блокировки приложения Кибер Файлы
- Требования к сложности пароля приложения
- Возможность удаления приложения Кибер Файлы из системы управления
- Разрешение отправки по электронной почте и печати файлов из приложения Кибер Файлы
- Разрешение сохранять файлы на устройстве
- Разрешение включения файлов, находящихся на устройстве с Кибер Файлы, в резервные копии iTunes
- Разрешение отправки файлов в Кибер Файлы из других приложений
- Разрешение открытия файлов Кибер Файлы в других приложениях
- Ограничение списка приложений, в которых можно открыть файлы Кибер Файлы
- Разрешение аннотирования PDF
- Разрешение создания, переименования и удаления файлов и папок
- Разрешение перемещения файлов
- Запрос подтверждения при удалении
- Можно указать серверы, папки и домашние каталоги, которые будут автоматически отображаться в приложении Кибер Файлы
- Для указанных папок можно настроить выполнение односторонней или двухсторонней синхронизации с сервером

5.3.1 Процедура регистрации на стороне сервера

1. Откройте Кибер Файлы веб-интерфейс.
2. Выполните вход от имени администратора.
3. Откройте вкладку **Мобильный доступ**.

4. Откройте вкладку **Настройки**.
5. Выберите необходимые требования при регистрации устройства

5.3.1.1 Параметры регистрации

Разрешить мобильным клиентам, восстановленным на новых устройствах, автоматически регистрироваться без PIN-кода. Если этот параметр включен, то пользователи, управляемые более старыми версиями мобильного приложения Кибер Файлы, смогут зарегистрироваться на новом сервере без указания PIN-кода.

Использовать имя участника-пользователя (UPN) для проверки подлинности на серверах шлюза – если этот параметр включен, то пользователи будут проходить проверку подлинности на серверах шлюза по имени UPN (в формате user@company.com). Если этот параметр отключен, то пользователи будут проверяться по имени домена и имени пользователя (в формате ДОМЕН/ПОЛЬЗОВАТЕЛЬ).

5.3.1.2 Режим регистрации устройства

В Кибер Файлы реализовано два варианта режимов регистрации устройств. Этот режим используется для регистрации всех клиентов. Вам необходимо выбрать вариант, который соответствует вашим требованиям.

- **PIN-код + имя пользователя и пароль Active Directory** – для активации приложения Кибер Файлы и получения доступа к серверам Кибер Файлы пользователь должен ввести одноразовый PIN-код, имеющий ограниченный срок действия, а также действующие учетные данные в Active Directory. Эта процедура гарантирует, что пользователь может зарегистрировать только одно устройство и только после получения PIN-кода, выпущенного ИТ-администратором системы. Рекомендуется использовать этот параметр, когда требуется обеспечить повышенную безопасность за счет двухфакторной регистрации устройств.
- **Только имя пользователя и пароль Active Directory** – пользователь может активировать свой экземпляр приложения Кибер Файлы с помощью только имени пользователя и пароля Active Directory. Этот вариант позволяет пользователю зарегистрировать одно или несколько устройств в любой момент времени в будущем. При этом необходимо сообщить пользователям только имя сервера Кибер Файлы или URL-адрес, указывающий на сервер Кибер Файлы. Этот адрес можно разместить на веб-сайте или отправить по электронной почте, что упрощает регистрацию в Кибер Файлы для большого количества пользователей. Этот вариант предпочтительнее использовать в средах, где двухфакторная регистрация не требуется и множеству пользователей может потребоваться доступ к Кибер Файлы в любое время, например при развертывании среди студентов.

5.3.1.3 Приглашение пользователя на регистрацию

Обычно пользователь получает приглашение на регистрацию на сервере Кибер Файлы в сообщении по электронной почте, которое отправляется администратором Кибер Файлы. Если требуется сервером, то в сообщении электронной почты содержится одноразовый PIN-код,

действующий в течение времени, определенного параметром. PIN-код может использоваться для регистрации приложения Кибер Файлы только на одном устройстве. Если у пользователя много устройств, то для каждого из устройств, которым необходимо предоставить доступ, придется отправить отдельное письмо по электронной почте. Это письмо содержит ссылку на мобильное приложение в App Store (если потребуется сначала установить приложение). Оно также содержит вторую ссылку, при открытии которой на устройстве открывается мобильный клиент Кибер Файлы и автоматически заполняются поля формы регистрации клиента, указывающие имя сервера Кибер Файлы, уникальный PIN-код регистрации и имя пользователя. Пользователю остается только ввести пароль своей учетной записи, чтобы завершить регистрацию клиента.

- После создания приглашения для регистрации список приглашенных пользователей отображается на странице **Приглашения для регистрации**. Указывается PIN-код каждого из пользователей (если потребуется сообщить его пользователю не в автоматическом сообщении электронной почты, а каким-либо другим способом).
- После того как пользователь успешно зарегистрировал мобильное приложение Кибер Файлы с помощью одноразового PIN-кода, этот код исключается из списка.
- Чтобы отозвать PIN-код приглашения пользователя, удалите код из списка, нажав кнопку Delete.

5.3.1.4 Использование базовых URL-ссылок для регистрации, когда не требуются PIN-коды

Если на сервере не настроен запрос PIN-кодов при регистрации клиентов, то можно передать пользователю стандартный URL-адрес, который будет автоматически запускать процесс регистрации при открытии этой ссылки на мобильном устройстве.

Чтобы определить URL-адрес регистрации на своем сервере управления, перейдите на вкладку **Общие настройки** и откройте вкладку **Зарегистрировать пользователей**. На этой странице отображается URL-адрес.

Примечание
Дополнительные сведения об этих двух режимах см. в разделе Настройки.

Чтобы создать приглашение на регистрацию в Кибер Файлы, выполните следующие действия.

1. Перейдите на вкладку **Общие настройки** и откройте вкладку **Зарегистрировать пользователей**.
2. Нажмите кнопку **Отправить приглашение на регистрацию**.
3. Введите имя пользователя или группы в Active Directory и нажмите «Поиск». Если выбрана группа, то можно нажать кнопку «Добавить», чтобы внести все адреса электронной почты из этой группы в список «Приглашаемые пользователи». Таким образом, можно произвести «пакетное» приглашение всех членов группы. При необходимости перед отправкой приглашений из списка можно исключить отдельных членов группы. В группах Active Directory

можно производить поиск типа «начинается с» или «содержит». Поиск «начинается с» работает намного быстрее, чем поиск типа «содержит».

4. После добавления первого пользователя или группы можно инициировать новый поиск и продолжать добавление в список дополнительных пользователей или групп.
5. Просмотрите список «Приглашаемые пользователи». При необходимости можно удалить любых пользователей, которых нужно исключить из списка.
6. Если с учетной записью пользователя не связан адрес электронной почты, то в столбце «Адрес электронной почты» будет отображаться надпись **Адрес электронной почты не назначен — нажмите здесь для изменения**. Можно щелкнуть по любой из таких записей, чтобы вручную ввести альтернативный адрес электронной почты для соответствующего пользователя. Если пользователь останется в состоянии **Адрес электронной почты не назначен**, то для него все же будет сформирован PIN-код, который будет отображаться на странице «Зарегистрировать пользователей». Чтобы пользователь смог зарегистрировать свое мобильное приложение Кибер Файлы, этот PIN-код нужно сообщить пользователю.

   Примечание
   Если вы предпочитаете передавать PIN-коды пользователям самостоятельно, то можно снять флажок **Отправить сообщения с приглашениями на регистрацию по электронной почте каждому из пользователей с указанным адресом**. Все PIN-коды будут отображаться на странице **Приглашения для регистрации**.

7. В поле «Число дней до истечения срока действия приглашения» укажите, в течение какого времени будут действовать приглашения.
8. Укажите число PIN-кодов, которые нужно отправить каждому из пользователей, в списке приглашений. Это может оказаться полезным в тех случаях, когда у пользователя имеется два или три устройства. Пользователь получит отдельные сообщения, в каждом из которых будет указан уникальный одноразовый PIN-код.

   Примечание
   Согласно правилам лицензирования Кибер Файлы каждый из лицензированных пользователей может активировать до трех устройств. Каждое дополнительное устройство сверх трех рассматривается в контексте лицензирования как дополнительный пользователь.

9. Выберите версии мобильного приложения Кибер Файлы, которые ваши пользователи будут скачивать и устанавливать на своих устройствах.
10. Нажмите **Отправить**.

    Примечание
    Если при отправке выдается сообщение об ошибке, проверьте правильность параметров SMTP на вкладке SMTP в общих настройках. Кроме того, если используется **Защищенное подключение**, убедитесь, что используемый сертификат соответствует имени узла вашего SMTP-сервера.

5.3.2 Процесс регистрации на стороне пользователя

Каждый пользователь, которому отправляется приглашение для регистрации, получит сообщение электронной почты, которое содержит:

- ссылку для установки мобильного Кибер Файлы из магазина Apple App Store;
- ссылку для запуска приложения Кибер Файлы и автоматизации процесса регистрации;
- одноразовый PIN-код;
- адрес сервера управления.
- В сообщении представлены инструкции по установке мобильного приложения Кибер Файлы и вводу регистрационных данных.

Если это мобильное приложение уже установлено и пользователь выберет параметр «Коснитесь этой ссылки, чтобы автоматически начать регистрацию...», просматривая это сообщение на устройстве, Кибер Файлы автоматически запустится и откроется форма регистрации. В этом URL-адресе закодированы адрес сервера, PIN-код и имя пользователя, поэтому эти поля будут автоматически заполнены в форме регистрации. На этом этапе пользователь просто вводит пароль, чтобы завершить регистрацию.

Имя пользователя и пароль – это имя пользователя и пароль Active Directory. Эти учетные данные используются для сопоставления с соответствующей политикой управления пользователями или группой для доступа к серверам шлюза и, если политика управления это разрешает, сохранения учетных данных для входа на сервер Кибер Файлы.

Если политика управления требует использовать пароль блокировки приложения, то появится запрос на его ввод. Все требования к сложности пароля, настроенные в политике, будут применяться к начальному паролю и вводимым в дальнейшем паролям.

Если политика ограничивает локальное хранение файлов на устройстве, отображается предупреждение о том, что существующие файлы будут удалены. Пользователь может отменить установку, если им необходимо скопировать некоторые файлы.

5.3.2.1 **Для регистрации в системе управления выполните следующие действия.**

Автоматическая регистрация с помощью регистрационного письма

1. Откройте письмо, присланное вашим ИТ-администратором, и нажмите ссылку **Щелкните здесь, чтобы установить Кибер Файлы**, если Кибер Файлы еще не установлен.
2. После установки Кибер Файлы вернитесь к письму с приглашением на своем устройстве и нажмите ссылку **Щелкните по этой ссылке, чтобы автоматически начать регистрацию** на втором шаге письма.
3. Будет показана форма регистрации. Если вы использовали ссылку в приглашении, чтобы начать регистрацию, адрес сервера, PIN-код и имя пользователя будут заполнены

автоматически.

Примечание
Если сервер не требует ввода PIN-кода, он не будет показан в форме регистрации.

4. Введите свой пароль и нажмите **Зарегистрироваться**, чтобы продолжить.

Примечание
Имя пользователя и пароль – это ваши стандартные учетные данные в компании. Скорее всего, они совпадают с именем пользователя и паролем, который вы используете для входа на свой компьютер или в почтовый ящик.

5. После заполнения всей формы нажмите кнопку **Зарегистрироваться**.
6. В зависимости от конфигурации сервера компании вы можете получить предупреждение, что сертификат безопасности сервера управления не является доверенным. Чтобы принять предупреждение и продолжить, нажмите кнопку **Все равно продолжить**.
7. Если для мобильного приложения Кибер Файлы требуется пароль блокировки приложения, вам будет предложено установить его. Возможно наличие требований к сложности пароля, которые будут показаны при необходимости.

Может быть показано окно подтверждения, если ваша политика управления ограничивает хранение файлов в Кибер Файлы или запрещает добавление отдельных серверов из мобильного приложения Кибер Файлы. Если файлы хранятся локально в приложении Кибер Файлы, то будет запрошено подтверждение на удаление всех файлов в локальном хранилище **Мои файлы**. Если выбрать «Нет», то процесс регистрации в системе управления будет отменен и файлы останутся без изменений.

Регистрация вручную

1. Откройте приложение Кибер Файлы.
2. Откройте меню **Настройки**.
3. Нажмите **Зарегистрироваться**.
4. Введите адрес сервера, PIN-код (если требуется), имя пользователя и пароль.
5. После заполнения всей формы нажмите кнопку **Зарегистрироваться**.
6. В зависимости от конфигурации сервера компании вы можете получить предупреждение, что сертификат безопасности сервера управления не является доверенным. Чтобы принять предупреждение и продолжить, нажмите кнопку **Все равно продолжить**.
7. Если для мобильного приложения Кибер Файлы требуется пароль блокировки приложения, вам будет предложено установить его. Возможно наличие требований к сложности пароля, которые будут показаны при необходимости.

Может быть показано окно подтверждения, если ваша политика управления ограничивает хранение файлов в Кибер Файлы или запрещает добавление отдельных серверов из мобильного

приложения Кибер Файлы. Если файлы хранятся локально в приложении Кибер Файлы, то будет запрошено подтверждение на удаление всех файлов в локальном хранилище **Мои файлы**. Если выбрать «Нет», то процесс регистрации в системе управления будет отменен и файлы останутся без изменений.

5.3.2.2 Непрерывное обновление управляющей информации

После первоначальной настройки системы управления клиенты Кибер Файлы будут пытаться установить соединение с сервером управления при каждом запуске клиентского приложения. Клиентское приложение в этот момент будет принимать любые изменения настроек, назначенных серверов и папок, операции сброса пароля блокировки и удаленной очистки данных.

Примечание

Требования к подключению Клиенты

Кибер Файлы должны иметь сетевой доступ к серверу Кибер Файлы, чтобы получать обновления профиля, команды на удаленный сброс пароля или удаленную очистку данных. Если для доступа к Кибер Файлы клиенту необходимо VPN-подключение, то это подключение необходимо и для приема команд управления.

5.3.2.3 Удаление из списка управления

Есть два варианта отключения клиента Кибер Файлы от управления.

- отключить параметр «Использовать управление» (если разрешено политикой);
- удалить приложение Кибер Файлы.

В зависимости от параметров политики управления Кибер Файлы у вас могут быть права для удаления мобильного Кибер Файлы из списка управления. Вероятно, это приведет к тому, что вы не сможете получить доступ к корпоративным файловым серверам. Если у вас есть подобные разрешения, выполните следующие действия.

Для удаления устройства из списка управляемых устройств выполните следующие действия.

1. Откройте меню **Настройки**.
2. Отключите параметр **Использовать управление**.
3. Ваш профиль может потребовать удаления клиентских данных Кибер Файлы при отключении устройства от управления. На этом этапе можно отменить процесс, чтобы не потерять свои файлы.
4. Подтвердите отключение Кибер Файлы от управления, выбрав вариант **ДА** в окне подтверждения.

Примечание
Если политика Кибер Файлы не разрешает удалять клиент из списка, параметр **Использовать управление** не будет отображаться в меню **Настройки**. В этом случае единственным способом отключить это устройство от управления является удаление приложения Кибер Файлы. При этом будут удалены все существующие данные и настройки мобильного Кибер Файлы, а после переустановки будут восстановлены параметры приложения по умолчанию.

Для удаления приложения Кибер Файлы выполните следующие действия.

Для iOS:

1. Удерживайте палец на значке приложения Кибер Файлы до тех пор, пока он не начнет дрожать.
2. Коснитесь кнопки **X** в приложении Кибер Файлы и подтвердите удаление.

Для Android:

Примечание
В разных приложениях для устройств Android настройки могут немного отличаться.

1. Откройте меню приложения и выберите **Изменить/удалить**.
2. Найдите приложение Кибер Файлы и выделите его.
3. Нажмите кнопку **Удалить**.

5.4 Управление серверами шлюза

Сервер шлюза Кибер Файлы – это сервер, к которому подключаются мобильные приложения Кибер Файлы. Он обслуживает доступ и выполнение операций с файлами и папками на файловых серверах, в репозиториях SharePoint и/или томах Sync & Share. Сервер шлюза служит посредником (шлюзом) между мобильными клиентами и их файлами.

Сервер Кибер Файлы может работать с несколькими серверами шлюза, обеспечивая управление и настройку из единой консоли управления. Управляемые серверы шлюза отображаются в разделе **Серверы шлюза** в меню **Мобильный доступ**.

- **Тип** – указывает тип шлюза; на данный момент доступен только тип «Сервер».
- **Имя** – имя, присвоенное шлюзу при его создании (используется для удобства идентификации).
- **Адрес** – DNS-имя или IP-адрес шлюза.
- **Версия** – содержит версию сервера шлюза Кибер Файлы.
- **Состояние** – указывает, находится сервер в сети или вне сети (сервер недоступен).
- **Активные сеансы** – число активных в настоящий момент сеансов на этом сервере шлюза.
- **Используемые лицензии** – число используемых и число доступных лицензий.
- **Лицензия** – показывает типы текущих лицензий, используемых сервером шлюза.

Зарегистрировать новый сервер шлюза можно с помощью кнопки **Добавить новый сервер шлюза**.

В меню **Действия** для каждого сервера шлюза администратор может:

- получить подробные сведения о сервере и его работе;
- изменить его конфигурацию;
- изменить ограничения доступа для сервера;
- изменить лицензирование для сервера;
- удалить сервер.

Предупреждение
Закладки на источники данных безвозвратно исчезают при удалении сервера шлюза, на котором они расположены. Добавление сервера и связанных источников данных обратно в консоль администрирования сервера Cyber Files не восстановит закладки.

Примечание
Сервер шлюза использует службу Windows HTTP.sys и применяет соответствующие параметры Windows на данном компьютере, в том числе настройки Microsoft Secure Channel (schannel), которые управляют безопасностью протокола защиты TLS. Если пользователи хотят изменить настройки безопасности службы сервера шлюза, они должны будут использовать для управления этими параметрами Windows инструмент, отличный от, например, IIS Crypto.

5.5 Параметры поиска сервера шлюза

5.5.0.1 Требования

Кибер Файлы использует **Поиск Windows**, чтобы разрешить поиск в сетевых источниках данных. **Поиск Windows** встроен в Windows Server, но по умолчанию не включен.

Чтобы включить его, выполните следующие действия.

- Добавьте/установите роль **Файловые службы** в диспетчере сервера.
- Убедитесь, что **служба поиска Windows** включена и запущена.

Примечание
Если эти требования не соблюдены, поиск в сетевых источниках данных будет невозможен.

Поиск также *не* поддерживается в следующих случаях:

- для файловых серверов NAS, хранилищ данных CMIS и SharePoint. Однако имеется поддержка файловых серверов SMB/CIFS.
- в корневом каталоге файловых серверов (//server); поиск будет работать только в фактических общих папках внутри (//server/share)

- если учетная запись службы на машине шлюза не имеет доступа (разрешений Windows) к компьютеру, на котором размещена общая папка. Чтобы это проверить, попробуйте запустить службу шлюза с учетной записью администратора.

Поле **Поиск** неактивно, если:

- по какой-либо причине невозможно выполнить поиск
- индексированный каталог пуст

5.5.0.2 Индексировать локальные источники данных для поиска файлов по именам

Поиск по сетевым источникам данных выполняется с помощью сервера шлюза Кибер Файлы и индекса службы поиска Windows. Если индексирование службы поиска Windows включено для нужного тома и он был проиндексирован, то на нем можно выполнять как глубокий поиск, так и поиск по содержимому.

По умолчанию поиск по индексу включен на всех серверах шлюза. Поиск по индексу можно отключить или включить для каждого сервера шлюза в диалоговом окне **Изменить сервер** шлюза.

1. Откройте консоль администрирования Кибер Файлы.
2. Перейдите в раздел **Мобильный доступ** -> **Сервер шлюза** > **Изменить** > **Поиск**.
3. Установите:
   - флажок **Индексировать локальные источники данных для поиска файлов по именам**
   - флажок **Поддерживать поиск содержимого с помощью службы поиска Microsoft Windows, где это возможно** (необязательно)

5.5.0.3 Путь по умолчанию

По умолчанию на автономном сервере Кибер Файлы хранит файлы индексов в папке **Search Indexes**, вложенной в папку приложения сервера шлюза Кибер Файлы. Если файлы индекса должны находиться в другом расположении, введите путь к новой папке.

5.5.0.4 Поддерживать поиск содержимого с помощью службы поиска Microsoft Windows, где это возможно

Поддержка поиска по содержимому для общих папок включена по умолчанию, а с помощью этого параметра ее можно отключить или включить. Поиск по содержимому можно включить или отключить отдельно для каждого сервера шлюза.

Поиск Windows можно настроить на индексирование необходимых источников данных, щелкнув правой кнопкой мыши значок «Поиск Windows» на панели «Пуск» и выбрав **Параметры поиска Windows**. Поиск по содержимому Windows можно выполнять на транслируемых в общий доступ ресурсах Windows, однако удаленные машины должны содержаться в том же домене, что и сервер шлюза.

Примечание
Путь к тому источника данных должен включать имя узла или полное имя, иначе не будет работать поиск по содержимому на ресурсах трансляции общего доступа в Windows. IP-адреса не поддерживаются функцией поиска Windows.

Дополнительные настройки

Индексирование содержимого можно настроить для индексации содержимого файлов только определенных типов.

1. На сервере, на котором размещен сервер шлюза, откройте **Панель управления** -> **Параметры индексации**.
2. Выберите **Дополнительно** и откройте вкладку **Типы файлов**.
3. Найдите типы файлов, которые следует включить/исключить из поиска по содержимому (например, **doc**, **txt** и т. д.).
4. Выберите нужный тип файла и в разделе **Как должен быть индексирован этот файл** выберите **Свойства индекса и содержимое файла**, чтобы включить поиск содержимого для этого типа, или **Свойства индекса**, чтобы отключить его. Повторите этот шаг для всех нужных типов файлов.

5.5.1 SharePoint

Ввод этих учетных данных не обязателен для общей поддержки SharePoint, но необходим для перечисления семейств сайтов. Например, у вас два семейства веб-сайтов: http://sharepoint.example.com и http://sharepoint.example.com/SeparateCollection. Если без ввода учетных данных создать том, указывающий на http://sharepoint.example.com, то при перечислении тома не будет отображаться папка SeparateCollection. Учетной записи требуются полные права чтения для доступа к веб-приложению.

5.5.2 Регистрация новых серверов шлюза

За исключением автоматической регистрации сервера шлюза, работающего на той же машине, что и веб-приложение управления, регистрация серверов шлюза – это многоэтапный, выполняемый вручную процесс.

1. Перейдите к компьютеру, где установлена служба сервера шлюза.
2. В зависимости от ваших настроек в **средстве конфигурации**:
   a. Если выбрано **Все доступные адреса**, откройте **https://localhost:3000/gateway_admin**.
   b. Если выбран определенный IP-адрес, откройте **https://<указанный_ip_адрес>:3000/gateway_admin**.

Примечание
Порт 3000 используется по умолчанию. Если порт по умолчанию был изменен, добавьте его номер после localhost или IP-адреса.

3. Запишите **Ключ администрирования**.
4. Откройте веб-интерфейс Кибер Файлы.
5. Откройте вкладку **Мобильный доступ**.
6. Откройте страницу **Серверы шлюза**.
7. Нажмите кнопку **Добавить новый сервер шлюза**.
8. Введите отображаемое имя для сервера.
9. Введите DNS-имя или IP-адрес сервера шлюза.

Примечание
Если мобильные клиенты подключаются к шлюзу через обратный прокси-сервер или балансировщик нагрузки, то нужно включить функцию **Использовать альтернативный адрес для клиентских подключений** и ввести DNS-имя или IP-адрес обратного прокси-сервера (или балансировщика нагрузки).

10. Введите **Ключ администрирования**.
11. Если необходимо, разрешите подключения к этому шлюзу с самозаверенными сертификатами, установив флажок **Разрешить подключения от серверов Кибер Файлы с самозаверенными сертификатами**.
12. Нажмите кнопку **Сохранить**.

После регистрации сервера шлюза можно настроить пользовательское ограничение доступа для этого сервера шлюза. Дополнительные сведения об этом см. в разделе Изменение серверов шлюза.

5.5.3 Сведения о сервере

При открытии страницы **Сведения** сервера шлюза отображается большой объем полезной информации о выбранном сервере и его пользователях.

5.5.3.1 Состояние

В разделе «Состояние» выводятся данные о самом сервере шлюза. Они включают данные об операционной системе, типе лицензии, числе используемых лицензий, версии сервера шлюза и т. д.

5.5.3.2 Активные пользователи

Отображает таблицу пользователей, активных на этом сервере шлюза в настоящий момент.

- **Пользователь** – полное имя пользователя в Active Directory.
- **Местоположение** – IP-адрес устройства.
- **Устройство** – имя, присвоенное устройству пользователем.
- **Модель** – тип/модель устройства.
- **ОС** – операционная система устройства.
- **Версия клиента** – версия приложения Кибер Файлы, установленного на устройстве.
- **Политика** – политика, применяемая для используемой устройством учетной записи.
- **Время простоя** – время, проведенное пользователем при наличии подключения к шлюзу.

5.5.4 Настройки сервера шлюза

Чтобы изменить настройку сервера шлюза, необходимо перейти в меню настроек.

1. Перейдите на вкладку **Мобильный доступ** -> **Серверы шлюза**.
2. Щелкните стрелку рядом с пунктом **Сведения** для нужного сервера.
3. Нажмите кнопку **Изменить**.

5.5.4.1 Ведение журнала сервера шлюза

В разделе «Ведение журнала» можно указать, какие события от данного сервера шлюза будут отображаться в журнале аудита, а также включить ведение отладочного журнала сервера.

Включение журнала аудита для определенного сервера шлюза

1. Откройте веб-интерфейс.
2. Выполните вход от имени администратора.
3. Откройте вкладку **Мобильный доступ**.
4. Откройте вкладку **Серверы шлюзов**.
5. Найдите сервер, для которого нужно включить **Ведение журнала аудита.**
6. Нажмите кнопку **Сведения**.
7. В разделе **Ведение журнала** выберите **Ведение журнала аудита**.
8. Нажмите кнопку **Сохранить**.

Включение ведения журнала отладки для определенного сервера шлюза

Примечание
Расположение журналов отладки по умолчанию: C:\Program Files (x86)\Cyberprotect\Access\Gateway Server\Logs\AccessGateway

1. Откройте веб-интерфейс.
2. Выполните вход от имени администратора.

3. Откройте вкладку **Мобильный доступ**.
4. Откройте вкладку **Серверы шлюзов**.
5. Найдите сервер, для которого нужно включить **Ведение журнала отладки.**
6. Нажмите кнопку **Сведения**.
7. В разделе **Ведение журнала** выберите **Ведение журнала отладки**.
8. Нажмите кнопку **Сохранить**.

5.5.4.2 Параметры поиска сервера шлюза

Требования

Кибер Файлы использует **Поиск Windows**, чтобы разрешить поиск в сетевых источниках данных. **Поиск Windows** встроен в Windows Server, но по умолчанию не включен.

Чтобы включить его, выполните следующие действия.

- Добавьте/установите роль **Файловые службы** в диспетчере сервера.
- Убедитесь, что **служба поиска Windows** включена и запущена.

Примечание
Если эти требования не соблюдены, поиск в сетевых источниках данных будет невозможен.

Поиск также *не* поддерживается в следующих случаях:

- для файловых серверов NAS, хранилищ данных CMIS и SharePoint. Однако имеется поддержка файловых серверов SMB/CIFS.
- в корневом каталоге файловых серверов (//server); поиск будет работать только в фактических общих папках внутри (//server/share)
- если учетная запись службы на машине шлюза не имеет доступа (разрешений Windows) к компьютеру, на котором размещена общая папка. Чтобы это проверить, попробуйте запустить службу шлюза с учетной записью администратора.

Поле **Поиск** неактивно, если:

- по какой-либо причине невозможно выполнить поиск
- индексированный каталог пуст

Индексировать локальные источники данных для поиска файлов по именам

Поиск по сетевым источникам данных выполняется с помощью сервера шлюза Кибер Файлы и индекса службы поиска Windows. Если индексирование службы поиска Windows включено для нужного тома и он был проиндексирован, то на нем можно выполнять как глубокий поиск, так и поиск по содержимому.

По умолчанию поиск по индексу включен на всех серверах шлюза. Поиск по индексу можно отключить или включить для каждого сервера шлюза в диалоговом окне **Изменить сервер** шлюза.

1. Откройте консоль администрирования Кибер Файлы.
2. Перейдите в раздел **Мобильный доступ** -> **Сервер шлюза** > **Изменить** > **Поиск**.
3. Установите:
   - флажок **Индексировать локальные источники данных для поиска файлов по именам**
   - флажок **Поддерживать поиск содержимого с помощью службы поиска Microsoft Windows, где это возможно** (необязательно)

Путь по умолчанию

По умолчанию на автономном сервере Кибер Файлы хранит файлы индексов в папке **Search Indexes**, вложенной в папку приложения сервера шлюза Кибер Файлы. Если файлы индекса должны находиться в другом расположении, введите путь к новой папке.

Поддерживать поиск содержимого с помощью службы поиска Microsoft Windows, где это возможно

Поддержка поиска по содержимому для общих папок включена по умолчанию, а с помощью этого параметра ее можно отключить или включить. Поиск по содержимому можно включить или отключить отдельно для каждого сервера шлюза.

Поиск Windows можно настроить на индексирование необходимых источников данных, щелкнув правой кнопкой мыши значок «Поиск Windows» на панели «Пуск» и выбрав **Параметры поиска Windows**. Поиск по содержимому Windows можно выполнять на транслируемых в общий доступ ресурсах Windows, однако удаленные машины должны содержаться в том же домене, что и сервер шлюза.

Примечание
Путь к тому источника данных должен включать имя узла или полное имя, иначе не будет работать поиск по содержимому на ресурсах трансляции общего доступа в Windows. IP-адреса не поддерживаются функцией поиска Windows.

5.5.4.3 Дополнительные настройки

Индексирование содержимого можно настроить для индексации содержимого файлов только определенных типов.

1. На сервере, на котором размещен сервер шлюза, откройте **Панель управления** -> **Параметры индексации**.
2. Выберите **Дополнительно** и откройте вкладку **Типы файлов**.
3. Найдите типы файлов, которые следует включить/исключить из поиска по содержимому (например, **doc**, **txt** и т. д.).
4. Выберите нужный тип файла и в разделе **Как должен быть индексирован этот файл** выберите **Свойства индекса и содержимое файла**, чтобы включить поиск содержимого для этого типа, или **Свойства индекса**, чтобы отключить его. Повторите этот шаг для всех нужных типов файлов.

5.5.4.4 Параметры SharePoint

Ввод этих учетных данных не обязателен для общей поддержки SharePoint, но необходим для перечисления семейств сайтов. Например, у вас два семейства веб-сайтов:

- http://sharepoint.example.com и http://sharepoint.example.com/SeparateCollection.

Если без ввода учетных данных создать том, указывающий на **http://sharepoint.example.com**, то при перечислении тома не будет отображаться папка **SeparateCollection**. Учетной записи требуются **полные права на чтение** для доступа к веб-приложению.

5.5.4.5 Чтобы предоставить учетной записи полные права на чтение, выполните следующие действия (для SharePoint 2016 и SharePoint 2010).

1. Откройте **Центр администрирования SharePoint**.
2. Щелкните **Управление приложениями**.
3. В разделе **Веб-приложения** щелкните **Управление веб-приложениями**.
4. Выберите веб-приложение из списка и щелкните **Политика пользователя**.
5. Установите флажок для пользователя, которому необходимо предоставить разрешения, и щелкните **Изменить разрешения выбранных пользователей**. Если пользователя нет в списке, его или ее можно добавить, нажав кнопку **Добавить пользователей**.
6. В разделе **Уровни политики разрешений** установите флажок **Полное чтение – доступ на чтение любых элементов**.
7. Нажмите кнопку **Сохранить**.

5.5.4.6 Дополнительные параметры

Примечание
Рекомендуется менять эти настройки только по запросу представителя службы технической поддержки клиентов.

- **Скрыть недоступные элементы** – Если этот параметр включен,файлы и папки, на чтение которых у пользователя нет прав, не будут отображаться.
- **Скрыть недоступные элементы при повторном предоставлении общего доступа** – Если этот параметр включен,файлы и папки, размещенные в сетевом общем ресурсе, на чтение которых у пользователя нет прав, не будут отображаться.

  Примечание
  Включение этой функции может существенно снизить производительность при просмотре папок.

- **Скрыть недоступные узлы SharePoint** – Если этот параметр включен,сайты SharePoint, для которых у пользователя нет необходимых прав, не будут отображаться.
- **Минимальная версия клиента Android** – Если этот параметр включен,пользователям, подключающимся к этому шлюзу, потребуется эта или более поздняя версия клиентского приложения Кибер Файлы для Android.
- **Минимальная версия клиента iOS** – Если этот параметр включен,пользователям, подключающимся к этому шлюзу, потребуется эта или более поздняя версия клиентского приложения Кибер Файлы для iOS.
- **Использовать Kerberos для проверки подлинности SharePoint** – если сервер SharePoint требует проверку подлинности Kerberos, включите этот параметр. Потребуется также обновить объект компьютера Active Directory для серверов Windows, где работает программное обеспечение сервера шлюза. Серверу Windows с Кибер Файлы необходимо предоставить разрешение на передачу делегированных учетных данных серверу SharePoint от имени ваших пользователей. Включение делегирования Kerberos для сервера Кибер Файлы для Windows.
  1. В разделе **Пользователи и компьютеры Active Directory** найдите сервер или серверы Windows, на которых установлен сервер шлюза. Обычно они находятся в папке **Компьютеры** .
  2. Откройте окно **Свойства** для сервера Windows и выберите вкладку **Делегирование**.
  3. Установите флажок **Этот компьютер доверенный для делегирования указанных служб**.
  4. Выбрать **Использовать любой протокол проверки подлинности.** Это необходимо для согласования с сервером SharePoint.
  5. Теперь необходимо добавить серверы SharePoint, к которым у пользователей должен быть доступ, используя Кибер Файлы. Если среда SharePoint состоит из нескольких узлов с балансировкой нагрузки, то каждый узел SharePoint/Windows нужно будет добавить в этот список разрешенных компьютеров. Нажмите кнопку **Добавить...**, чтобы найти эти компьютеры Windows в AD и добавить их. Для каждого компьютера выберите только тип службы http.

Примечание
Подождите 15-20 минут, чтобы изменения вступили в силу в AD, прежде чем проверять подключение клиентов. Это произойдет не сразу.

- **Разрешить подключения к серверам SharePoint с использованием самозаверенных сертификатов** – Если этот параметр включен,разрешить подключения с этого шлюза к серверам SharePoint с использованием самозаверенных сертификатов.
- **Принимать самозаверенные сертификаты от этого сервера шлюза** – разрешает подключения от этого сервера Кибер Файлы к этому серверу шлюза, даже если сервер шлюза использует самозаверенный сертификат.
- **Разрешить подключения к серверам Кибер Файлы с использованием самозаверенных сертификатов** – разрешает подключения от этого сервера шлюза к серверам Кибер Файлы, даже если серверы Кибер Файлы используют самозаверенные сертификаты.

- **Показать скрытые общие ресурсы SMB** – Если этот параметр включен,показывает пользователям скрытые системные общие ресурсы SMB.
- **Время ожидания клиентского сеанса в минутах** – задает период, после которого пользователь отключается от сервера шлюза.
- **Использовать имя участника-пользователя (UPN) для проверки подлинности на серверах SharePoint.** Если этот параметр включен, пользователи будут проходить проверку подлинности на серверах SharePoint с помощью имени участника-пользователя (например, hristo@glilabs.com), в противном случае будет применяться домен/имя_пользователя (например, glilabs/hristo).
- **Выполнить проверку подлинности Negotiate/Kerberos в режиме пользователя**. Если этот параметр включен, то сервер шлюза будет выполнять проверку подлинности для доступа к источникам данных с использованием билета Kerberos пользователя, устанавливающего подключение. Используется только в конфигурациях, требующих проверки подлинности Kerberos (например, для единого входа (SSO), балансировки нагрузки и т. п.).

5.5.5 Пользовательское ограничение доступа

Можно изменить стандартные ограничения доступа, заданные в разделе Политики, либо настроить собственное ограничение доступа для каждого сервера шлюза.

Настройка пользовательского ограничения доступа для определенного сервера шлюза

1. Перейдите на вкладку **Мобильный доступ** -> **Серверы шлюза**.
2. Щелкните стрелку рядом с пунктом **Сведения** для нужного сервера.
3. Выберите **Ограничение доступа**.
4. Откройте вкладку **Использовать пользовательские настройки**.
5. Выберите ограничение доступа для этого сервера шлюза.
6. Нажмите кнопку **Применить**.

5.5.6 Кластерные группы

В Кибер Файлы вы можете создать кластерную группу серверов шлюза.

Кластерная группа – это коллекция серверов шлюза, совместно использующая одну и ту же конфигурацию. Это позволяет управлять всеми шлюзами в такой группе одновременно вместо того, чтобы задавать одни и те же настройки на каждом из шлюзов по отдельности. Как правило, эти серверы размещаются за балансировщиком нагрузки, чтобы обеспечить высокую доступность для мобильных клиентов и масштабируемость.

Для кластеризованного шлюза необходим балансировщик нагрузки, а также два или более шлюза и сервер Кибер Файлы. Все серверы шлюзов должны быть добавлены в кластерную группу в веб-интерфейсе Кибер Файлы и помещены за балансировщиком нагрузки. Сервер Кибер Файлы выступает в качестве сервера управления и сервера, на котором мобильные клиенты

регистрируются в системе управления. Он управляет всеми политиками, устройствами и настройками, роль шлюзов – предоставлять доступ к общим папкам.

5.5.6.1 Чтобы создать кластерную группу, выполните следующие действия.

Перед тем как продолжить, убедитесь, что вы уже настроили правильный **Адрес для администрирования** на каждом шлюзе. Это DNS-имя или IP-адрес сервера шлюза.

1. Откройте веб-интерфейс Кибер Файлы.
2. Откройте вкладку **Мобильный доступ**.
3. Откройте страницу **Серверы шлюза**.
4. Нажмите кнопку **Добавить кластерную группу**.
5. Введите отображаемое имя группы.
6. Введите DNS-имя или IP-адрес балансировщика нагрузки.
7. При необходимости выберите другой адрес для соединений Кибер Файлы, установив флажок и введя адрес.
8. Отметьте флажком каждый из шлюзов, которые требуется включить в группу.
9. Выберите шлюз, который будет управлять настройками группы. Все имеющиеся настройки этого шлюза (включая назначенные источники данных, за исключением адреса для администрирования) будут скопированы на каждый шлюз в группе.
10. Нажмите кнопку **Создать**.

5.5.6.2 Изменение кластерной группы.

Изменение кластерной группы не отличается от изменения настроек обычных шлюзов. Дополнительные сведения см. в статье Изменение сервера шлюза.

5.5.6.3 Добавление членов в существующую кластерную группу.

1. Откройте веб-интерфейс и перейдите в раздел **Мобильный доступ** -> **Серверы шлюза**.
2. Откройте меню действий для требуемой кластерной группы и среди доступных действий выберите **Добавить участников кластера**.
3. Выберите в списке требуемые серверы шлюза и нажмите кнопку **Добавить**.

5.5.6.4 Изменение основного сервера шлюза

1. Откройте веб-интерфейс и перейдите в раздел **Мобильный доступ** -> **Серверы шлюза**.
2. Разверните нужную кластерную группу.
3. Найдите сервер шлюза, который необходимо сделать основным.
4. Нажмите кнопку **Действия** и выберите **Сделать основным для группы**.

5.6 Управление источниками данных

Можно открыть общий доступ к каталогам NTFS, расположенным на сервере Windows, в системе CMIS или в удаленной общей папке SMB/CIFS, чтобы к ним могли обращаться пользователи Кибер Файлы. При подключении пользователей эти каталоги будут отображаться для них как тома общих папок.

5.6.1 Доступ к содержимому SharePoint 2007, 2010, 2013 и 2016

Кибер Файлы может предоставлять доступ к файлам, находящимся в библиотеках документов на серверах SharePoint 2007, 2010, 2013 и 2016. Источник данных Кибер Файлы SharePoint может указывать на весь сервер SharePoint, определенный узел или подузел SharePoint либо на конкретную библиотеку документов. Эти файлы можно открывать, комментировать, редактировать и синхронизировать так же, как файлы на традиционном файловом сервере или в хранилище NAS. Кибер Файлы также поддерживает **Извлечение** и **Возврат** файлов SharePoint.

Поддерживаемые методы проверки подлинности SharePoint

Кибер Файлы поддерживает серверы SharePoint, которые допускают проверку подлинности клиентов по алгоритмам NTLMv1, NTLMv2, протоколу Kerberos, а также проверку подлинности на основе утверждений. Если сервер SharePoint запрашивает проверку подлинности Kerberos, то потребуется внести обновления в объект компьютера в Active Directory, соответствующий серверу или серверам Windows, на которых работает ПО сервера Кибер Файлы. Серверу Windows с Кибер Файлы необходимо предоставить разрешение на передачу делегированных учетных данных серверу SharePoint от имени ваших пользователей.

5.6.2 Доступ к содержимому OneDrive для бизнеса

Кибер Файлы можно настроить так, чтобы разрешить пользователям доступ к личному содержимому OneDrive для бизнеса через источник данных SharePoint. Существуют некоторые ограничения и требования.

5.6.3 Изменение разрешений для общих файлов и папок

Кибер Файлы использует существующие учетные записи и пароли пользователей Windows. Поскольку Кибер Файлы применяет разрешения Windows NTFS, обычно для изменения разрешений на каталоги и файлы необходимо пользоваться встроенными средствами Windows. Стандартные средства Windows обеспечивают максимальную гибкость настройки политики безопасности.

К источникам данных Кибер Файлы, расположенным на других файловых серверах SMB/CIFS, доступ осуществляется с помощью подключения SMB/CIFS от сервера шлюза ко вторичному серверу или NAS. В этом случае доступ ко вторичному серверу осуществляется в контексте пользователя, выполнившего вход в один из клиентов Кибер Файлы. Чтобы у этого пользователя был доступ к файлам на вторичном сервере, необходимо предоставить его учетной записи

«Разрешения на общий доступ Windows» и соответствующие разрешения безопасности NTFS на доступ к этим файлам.

Разрешения для файлов, расположенных на серверах SharePoint, определяются в соответствии с разрешениями SharePoint, настроенными на сервере SharePoint. При доступе через Кибер Файлы пользователи получают те же разрешения, что и при доступе к библиотекам документов SharePoint через веб-браузер.

5.6.4 Папки

Папки можно назначить пользовательским политикам или политикам для групп Кибер Файлы. Такие папки автоматически отображаются у пользователей в приложении Кибер Файлы. Папки можно настроить так, чтобы они указывали на любую нужную папку, расположенную на сервере шлюза, в удаленной общей папке, на томе CMIS или в библиотеке SharePoint. Это позволяет открыть пользователям прямой доступ к любым важным папкам, при этом нет необходимости вручную переходить к нужной папке или точно знать сервер, имя общего тома и путь к этой папке.

Папки могут указывать на содержимое любого типа, к которому Кибер Файлы предоставляет доступ, если оно не расположено на съемном носителе. Они просто указывают на местоположения в серверах шлюза, которые уже настроены в средствах управления Кибер Файлы. Это может быть локальный том общей папки, том на другом файловом сервере или NAS, общая папка DFS, том CMIS или том SharePoint.

Примечание
При создании источника данных DFS нужно добавить полный путь к DFS следующим образом: **\\company.com\namespace\share**

Примечание
Если при «чистой» установке Кибер Файлы включен режим Sync & Share (синхронизации и общего доступа), а также имеется сервер шлюза, то будет автоматически создан источник данных Sync & Share. Он указывает на URL-адрес, заданный в разделе **Сервер** при начальной конфигурации. Эта папка позволяет мобильным пользователям получить доступ к вашим файлам и папкам Sync & Share.

5.6.4.1 Синхронизация папок

По желанию можно настроить синхронизацию папок с клиентским устройством. Параметры синхронизации папки Кибер Файлы включают:

Примечание
Этот параметр не действует для настольного клиента.

- **Нет** – папка отображается как сетевой ресурс в приложении Кибер Файлы. К ней можно получить доступ и работать точно так же, как с сервером шлюза.
- **Односторонняя** – папка отображается в приложении Кибер Файлы как локальная. Все ее содержимое будет синхронизировано и перенесено с сервера на устройство, а в дальнейшем

будет обновляться при добавлении, изменении и удалении файлов на сервере. Такая папка предназначается для предоставления локального (вне сети) доступа к расположенным на сервере файлам и отображается как доступная пользователю только на чтение.

- **Двусторонняя** – папка отображается в приложении Кибер Файлы как локальная. Все ее содержимое будет изначально синхронизировано и перенесено с сервера на устройство. В случае добавления, изменения или удаления файлов как на сервере, так и на устройстве соответствующие изменения синхронизируются (распространяются) и на устройство или на сервер соответственно.

5.6.4.2 Создание и изменение источника данных

Создание источника данных

1. Откройте веб-интерфейс Кибер Файлы.
2. Откройте вкладку **Мобильный доступ**.
3. Откройте вкладку **Источники данных**.
4. Перейдите в **Папки**.
5. Нажмите **Добавить новую папку**.
6. Введите отображаемое имя папки.
7. Выберите сервер шлюза, который будет предоставлять доступ к этой папке.
8. Выберите расположение данных. Они могут находиться на самом сервере шлюза, на другом сервере SMB, на узле или в библиотеке SharePoint или же на сервере синхронизации и общего доступа.

   Примечание
   Папку со съемного носителя нельзя использовать в качестве общей папки. Выберите папку в другом месте.

   Примечание
   При выборе Sync & Share обязательно введите полный путь к серверу с указанием номера порта, например https://mycompany.com:3000

9. В зависимости от выбранного расположения введите путь к папке, серверу, сайту или библиотеке.
10. Выберите тип **синхронизации** для этой папки.
11. Установите параметр **Показывать при просмотре сервера**, если этот источник данных должен отображаться при просмотре мобильными клиентами Кибер Файлы содержимого сервера шлюза.

Примечание
При создании источников данных SharePoint можно включить отображение отслеживаемых сайтов SharePoint.

12. Нажмите кнопку **Сохранить**.

Изменение источника данных

1. Откройте раздел **Источники данных** и найдите нужный источник.
2. Щелкните значок **Карандаш** напротив этого источника данных в правой части таблицы.
3. Измените нужные параметры и нажмите кнопку **Сохранить**.

5.6.4.3 Узлы и библиотеки SharePoint

К узлам и библиотекам SharePoint можно легко предоставить доступ пользователям мобильного приложения Кибер Файлы, создав источник данных. Существует два способа создания источников данных SharePoint (выбор зависит от конфигурации SharePoint).

Примечание
Каждый раз при указании URL-адреса убедитесь, что корневой сайт является семейством сайтов по умолчанию.

5.6.4.4 Создание источника данных для целый узел или подузел SharePoint

Создание источника данных для для узла или подузла SharePoint необходимо только заполнить поле **URL-адрес**. Укажите адрес узла или подузла SharePoint, например, https://sharepoint.mycompany.com:43222 или https://sharepoint.mycompany.com:43222/<имя_подузла>.

Отслеживаемые сайты SharePoint

Отслеживаемые сайты SharePoint можно включить при создании источника данных для вашего сайта. Для этого необходимо установить флажок «Показывать отслеживаемые сайты». Если этот параметр включен, у всех пользователей, отслеживающих сайты, в Кибер Файлы будет отображаться папка «Отслеживаемые сайты», содержащая ресурсы, к которым у пользователей есть доступ с этих сайтов.

Примечание
Отслеживаемые сайты SharePoint нельзя синхронизировать.

Создание источника данных для **Библиотека SharePoint**

Создание источника данных для для библиотеки SharePoint необходимо заполнить и поле **URL-адрес**, и поле **Название библиотеки документов**.В поле URL введите адрес своего узла или подузла SharePoint и в поле «Имя библиотеки документов» нужно ввести название для библиотеки.

Например, URL: https://sharepoint.mycompany.com:43222 и Document Library Name: My Library.

Создание источника данных для **конкретная папка в библиотеке SharePoint**

Создание источника данных для для конкретной папки в библиотеке SharePoint необходимо заполнить все поля.В поле URL введите адрес своего узла или подузла SharePoint, в поле «Имя библиотеки документов» нужно ввести название для библиотеки в поле «Вложенный путь» указывается имя нужной папки.

Например, URL: https://sharepoint.mycompany.com:43222, Document Library Name: Marketing Library и Subpath: Sales Report.

Примечание
При создании источника данных, указывающего на ресурс SharePoint по вложенному пути, нельзя включить параметр **Показать при просмотре сервера**.

Мобильное приложение Кибер Файлы поддерживает проверку подлинности NTLM, ограниченное делегирование Kerberos, проверку подлинности на основе утверждений и проверку подлинности SharePoint 365. В зависимости от настроек SharePoint может потребоваться внесение дополнительных изменений в конфигурацию сервера шлюза, используемого для подключения к таким источникам данных. Дополнительные сведения см. в статье Изменение сервера шлюза.

5.6.4.5 Тома CMIS (сервисов взаимодействия при управлении контентом)

Поддерживаются тома CMIS **Alfresco (CMIS)** и **Documentum (CMIS)**. Для решений CMIS других поставщиков, использующих протокол **AtomPub**, можно применить параметр **Общий CMIS (AtomPub)**. Этот параметр не поддерживается Cyberprotect и может не работать с решением конкретного поставщика.

Рекомендуется использовать на машине с томами CMIS сервер шлюза, чтобы уменьшить время ожидания в сетях с низкой пропускной способностью.

Примечание
Тома CMIS имеют ограничение, которое запрещает копирование папок.

5.6.4.6 OneDrive для бизнеса

Поскольку OneDrive для бизнеса работает на основе SharePoint, доступ к его содержимому можно настроить путем создания источника данных SharePoint в Кибер Файлы. Однако из-за этого имеются некоторые ограничения.

- Источник данных **должен** указывать на подстановочное значение для главной личной папки пользователя. Нельзя создать источники данных, указывающие на подпапки, но их можно открывать и просматривать из главной папки.
- Эти источники данных не будут работать, если сервер шлюза добавлен вручную в приложении. Они должны быть назначены через политику.

- Ваш каталог Active Directory должен либо использовать федеративные службы AD, либо являться Azure AD.
- Каждому пользователю будут видны только его собственные данные OneDrive без доступа к данным других пользователей, даже если они находятся в общем доступе и открываются через портал Microsoft.

Создание источника данных

1. Откройте веб-интерфейс Кибер Файлы.
2. Откройте вкладку **Мобильный доступ**.
3. Откройте вкладку **Источники данных**.
4. Перейдите в **Папки**.
5. Нажмите кнопку **Добавить новую папку**.
6. Введите отображаемое имя папки.
7. Выберите сервер шлюза, который будет предоставлять доступ к ресурсам.
8. В поле **Расположение данных** выберите вариант **SharePoint**. Появятся следующие поля:
   a. **URL** – введите расположение SharePoint сервера OneDrive for Business, узел или подузел, к которому вы хотите предоставить доступ, например:
   https://sharepoint.company.com/mysite/mysubsite/%USERNAME%
   Этот URL-адрес может указывать расположения только в пределах уровня (не указывайте default.aspx). В пути должна быть строка подстановки %USERNAME%, которая заменяется основной личной папкой пользователя.
   b. Оставьте поля **Название библиотеки документов** и **Вложенный путь** пустыми.
9. Нажмите кнопку **Сохранить**.

5.6.5 Назначенные источники

На этой странице можно произвести поиск пользователя или группы, чтобы определить, какие ресурсы им назначены. Ресурсы перечислены в двух таблицах: «Серверы» и «Папки».

- В таблице «Серверы» для сервера шлюза указываются отображаемое имя, DNS-имя или IP-адрес, а также политики, которым назначен этот сервер.
- В таблице «Папки» указываются отображаемое имя источника данных, сервер шлюза, тип синхронизации, путь и политики, которым назначен соответствующий источник данных.
- Нажав кнопку **Изменить назначенные ресурсы**, администратор может быстро изменить назначения для политики.

5.6.6 Серверы шлюза, видимые на клиентах

Серверы шлюза можно назначить политикам пользователей или групп, а также использовать в качестве источников данных. На этой странице показаны все серверы шлюза, которые отображаются в мобильном приложении Кибер Файлы пользователя, а также указано, назначены

ли эти серверы шлюзов определенной пользовательской или групповой политике. Здесь также можно изменить это назначение. Когда пользователи мобильного приложения Кибер Файлы просматривают содержимое сервера шлюза, они видят источники данных, для которых установлен параметр **Отображать при просмотре сервера шлюза**.

5.6.6.1 Чтобы изменить существующее назначение сервера, выполните следующие действия.

1. Нажмите кнопку **Изменить** для этого сервера.
   - Чтобы отменить назначение этого сервера пользователю, нажмите **X** для этого пользователя.
   - Чтобы назначить этому серверу нового пользователя или группу, найдите имя пользователя/группы и щелкните по нему.
2. Нажмите кнопку **Сохранить**.

Примечание
Если удалить сервер шлюза из консоли администрирования сервера Кибер Файлы, все пользовательские мобильные закладки для источников данных на этом сервере будут безвозвратно удалены. Их восстановление невозможно, даже если снова добавить этот сервер и источники данных.

5.7 Настройки

5.7.1 Параметры регистрации

- **Адрес регистрации мобильного клиента** – указывает адрес, который должен использоваться мобильными клиентами при регистрации для управления клиентами.

  Примечание
  Настоятельно рекомендуется использовать DNS-имя при указании адреса регистрации мобильного клиента. После успешной регистрации в управлении клиентами мобильное клиентское приложение Кибер Файлы сохраняет адрес сервера Кибер Файлы. Если это будет IP-адрес, то в случае изменения адреса сервер не будет доступен, отменить управление приложением будет невозможно, поэтому пользователю придется удалить все приложение и заново регистрироваться для управления.

- **Разрешить мобильным клиентам, восстановленным на новых устройствах, автоматически регистрироваться без PIN-кода**. Если этот параметр включен, то пользователи, управляемые более старыми версиями мобильного приложения Кибер Файлы, смогут зарегистрироваться на новом сервере без указания PIN-кода.
- **Использовать имя участника-пользователя (UPN) для проверки подлинности на серверах шлюза** – если этот параметр включен, то пользователи будут проходить проверку подлинности на серверах шлюза по имени UPN (в формате user@company.com). Если этот параметр

отключен, то пользователи будут проверять подлинность по имени домена и имени пользователя (в формате ДОМЕН/ПОЛЬЗОВАТЕЛЬ).

5.7.2 Для регистрации устройства потребуется следующее.

- **PIN-код + имя пользователя и пароль Active Directory** – для активации приложения Кибер Файлы и получения доступа к серверам Кибер Файлы пользователь должен ввести одноразовый PIN-код, имеющий ограниченный срок действия, а также действующие учетные данные в Active Directory. Эта процедура гарантирует, что пользователь может зарегистрировать только одно устройство и только после получения PIN-кода, выпущенного ИТ-администратором системы. Рекомендуется использовать этот параметр, когда требуется обеспечить повышенную безопасность за счет двухфакторной регистрации устройств.
- **Только имя пользователя и пароль Active Directory** – пользователь может активировать свой экземпляр приложения Кибер Файлы с помощью только имени пользователя и пароля Active Directory. Этот вариант позволяет пользователю зарегистрировать одно или несколько устройств в любой момент времени в будущем. При этом необходимо сообщить пользователям только имя сервера Кибер Файлы или URL-адрес, указывающий на сервер Кибер Файлы. Этот адрес можно разместить на веб-сайте или отправить по электронной почте, что упрощает регистрацию в Кибер Файлы для большого количества пользователей. Этот вариант предпочтительнее использовать в средах, где двухфакторная регистрация не требуется и множеству пользователей может потребоваться доступ к Кибер Файлы в любое время, например при развертывании среди студентов.

6 Синхронизация и общий доступ (Sync & Share)

Этот раздел веб-интерфейса доступен только в том случае, если включены функции Sync & Share. В противном случае будет отображаться кнопка **Включить поддержку синхронизации и обмена**.

6.1 Общие ограничения

Можно настроить базовые ограничения, такие как включение в список блокировки файлов определенного типа или размера.

Максимально разрешенный размер файла Позволяет установить максимальный размер файла для всех файлов Sync & Share.

Типы блокируемых файлов Позволяет заблокировать использование файлов определенных типов при работе с Sync & Share.

6.1.1 Чтобы настроить список блокировки для типов файлов, выполните следующие действия.

1. В веб-консоли разверните вкладку **Sync & Share** и откройте **Общие ограничения**.
2. В поле **Добавить** в разделе **Блокируемые типы файлов** введите через запятую все типы файлов, которые необходимо запретить.
3. Выберите **Сохранить**.

Примечание
Любые ранее отправленные файлы этих типов станут недоступны для перемещения и перестанут синхронизироваться. Их можно будет скачать или удалить только вручную.

6.1.2 Чтобы установить ограничение по максимальному размеру файла, выполните следующие действия.

1. В веб-консоли разверните вкладку **Sync & Share** и откройте **Общие ограничения**.
2. Установите флажок **Максимально разрешенный размер файла** и введите требуемый максимальный размер файла в поле ввода (в МБ).
3. Выберите **Сохранить**.

Примечание
Любые ранее отправленные файлы большего размера станут недоступны для перемещения и перестанут синхронизироваться. Их можно будет скачать или удалить только вручную.

6.2 Ограничения общего доступа

Разрешить участникам совместной работы приглашать других пользователей Если эта настройка отключена, то флажок **Разрешить пользователям приглашать других пользователей**

не будет отображаться при приглашении пользователей к папкам. Это не позволит приглашенным пользователям приглашать других пользователей.

6.2.1 Срок действия общего доступа к отдельным файлам

Включить общий доступ к одиночным файлам. Если этот режим включен, то будет разрешен общий доступ к ссылкам на отдельные файлы и можно будет управлять тем, как пользователи получают к ним доступ и в течение какого времени они доступны.

- **Разрешить общедоступные ссылки на скачивание**. Если этот режим включен, доступ к общему файлу при наличии ссылки предоставляется без ограничений.
- **Разрешить ссылки на скачивание «Для всех пользователей Кибер Файлы»**. Если этот режим включен, доступ к общему файлу могут получить только пользователи, обладающие учетными данными для Кибер Файлы.
  - **Разрешить скачивание только для внутренних пользователей (AD).** Если этот режим включен, доступ к общему файлу могут получить только пользователи с учетными данными Active Directory для Кибер Файлы.
- **Разрешить скачивание ссылок только пользователям, которым предоставлен доступ**. Если этот режим включен, то использование ссылок будет разрешено только пользователям, которым они предоставлены.
- **Ограничить срок действия ссылок на общие файлы.** Если этот параметр включен, то для файловых ссылок будет принудительно устанавливаться дата окончания срока действия.
  - **Максимальный срок действия.** Управляет максимальной продолжительностью (в сутках) до истечения срока действия файла.
- **Разрешить общий доступ только к одноразовым ссылкам для скачивания** Если параметр включен, пользователи могут отправлять только одноразовые ссылки. Эти ссылки будут отозваны после первого скачивания.

6.2.2 Предоставление общего доступа к папкам

Ограничить срок действия общих папок. Если этот параметр включен, то для всех папок, к которым предоставляется доступ, будет требоваться наличие даты окончания срока действия.

- **Максимальный срок действия.** Управляет максимальной продолжительностью (в сутках) до истечения срока действия папки.

6.2.3 Список разрешений

Если список разрешений включен, входить в систему могут только пользователи в настроенных группах LDAP или с доменами электронной почты (такими как example.com), указанными в списке. Для доменов можно использовать подстановочные знаки (например, *.example.com). Группы LDAP необходимо указывать по отличительным именам, например CN=mygroup, CN=Users, DC=mycompany, DC=com.

6.2.4 Список блокировки

Пользователи в настроенных группах LDAP или с доменами электронной почты (такими как example.com), указанными в списке блокировки, не могут входить в систему, даже если они находятся в списке разрешений. Для доменов можно использовать подстановочные знаки (например, *.example.com). Группы LDAP необходимо указывать по отличительным именам, например CN=mygroup, CN=Users, DC=mycompany, DC=com.

Примечание
Записи с подстановочными знаками могут содержать только одну звездочку, которая всегда должна располагаться в начале строки перед точкой (например, *.example.com, *.com).

6.3 Подготовка LDAP

Учетные записи для членов групп, перечисленных здесь, будут создаваться автоматически при первом входе в систему. Это упрощает процесс создания учетных записей, чтобы администратору не нужно было отправлять приглашение каждому пользователю.

6.3.1 Группа LDAP

Это список групп, выбранных в настоящий момент.

- **Обычное имя/отображаемое имя** – отображаемое имя, данное пользователю или группе.
- **Отличительное имя** – отличительное имя, данное пользователю или группе. Отличительное имя – это уникальное значение для записи в службе Directory Service.

6.4 Квоты

Администраторы могут задавать объем пространства, выделяемого каждому из пользователей в системе. Для внешних (эпизодических) и внутренних (Active Directory – LDAP) пользователей задаются раздельные настройки по умолчанию.
Администраторы могут назначать различные значения квоты для отдельных пользователей или по членству в группах Active Directory.

- **Включить квоты?** – при включении максимальный объем пространства пользователей ограничивается квотами.
  - **Стандартный интервал уведомления о квоте** – временной интервал в днях, задающий частоту получения пользователями уведомлений по электронной почте о приближающемся лимите квоты.
  - **Квота эпизодического пользователя** – задает квоту для эпизодических пользователей.
  - **Квота пользователя LDAP** – задает квоту для пользователей LDAP.
  - **Включить квоты для администратора?** – при включении к администраторам будет

применяться отдельная квота.

- **Квота администратора** – задает квоту для администраторов.

Примечание
Если пользователь входит в несколько групп, применяется наибольшая из квот.

Примечание
Квоты можно указывать для отдельных пользователей. Указание индивидуальной квоты переопределяет все прочие параметры квот. Чтобы добавить индивидуальные квоты для других пользователей, измените настройки пользователя на странице **Пользователи**.

Примечание
Можно задать размер квоты в мегабайтах, указав значение меньше 1 ГБ, **например 0.5**, **0.3**, **0.9** и т. д.

6.5 Политики очистки файлов

В Кибер Файлы документы, файлы и папки обычно сохраняются в системе до их явного удаления. Что позволяет пользователям восстанавливать удаленные файлы и сохранять предыдущие версии любого документа. В Кибер Файлы администраторы могут определять политики относительно сроков хранения удаленных файлов, максимального количества сохраняемых ревизий и времени удаления старых ревизий.

Кибер Файлы может автоматически очищать старые версии и удаленные файлы в файловом репозитории на основе описанных ниже политик. Это позволяет контролировать объем пространства, используемый Кибер Файлы. После очистки восстановление файлов невозможно.

Примечание
Самая новая неудаленная редакция каждого из файлов никогда не очищается вне зависимости от этих параметров.

- **Очищать удаленные файлы через** – при включении очищаются файлы, которые старше указанного значения.
- **Очищать предыдущие редакции старше** – при включении очищаются редакции файлов, которые старше указанного значения.
  - **Всегда сохранять не менее X редакций файла** – при включении минимальное число редакций файла сохраняется вне зависимости от их возраста.
- **Сохранять не более X версий файла** – при включении ограничивает максимальное число версий файла.
- **Разрешить пользователям окончательно удалять файлы и их версии** – при включении с этого момента файлы и их редакции будут полностью стираться без возможности восстановления.

Примечание
Используйте кнопку **Сохранить** для сохранения настроек. Используйте параметр **Нажмите здесь**, чтобы начать очистку немедленно (в дополнение к сохранению настроек), иначе регулярное сканирование выполняется каждые 60 минут.

6.6 Политики истечения срока действия пользователей

Можно задать прекращение действия приглашений и учетных записей пользователей после указанного периода неактивности.

- **Срок действия приглашений на общий доступ для внешних пользователей и запросов на сброс пароля истекает через X дн.** – при включении срок действия приглашений и запросов на сброс пароля для внешних пользователей будет заканчиваться через заданное количество дней.
- **Завершать срок действия приглашений, ожидающих обработки, через X дн.** – при включении срок действия всех ожидающих приглашений будет заканчиваться через заданное количество дней.
  - **Отправлять по электронной почте уведомление об истечении за X дней перед истечением срока действия приглашения** – при включении пользователям отправляется уведомление за заданное число дней до истечения срока действия их приглашений.
- **Удалять внешних пользователей, которые не входили в систему в течение X дн.** – при включении пользователи, не выполнявшие вход в течение заданного количества дней, удаляются.
  - **Отправлять по электронной почте уведомление за X дней до окончания срока действия пользователя** – при включении пользователям отправляется уведомление за заданное число дней до окончания срока действия учетной записи непостоянного пользователя.
- **Удалять доступ к синхронизации и общему доступу пользователей LDAP, которые не входили в систему X дней** – при включении удаляет доступ к синхронизации и общего доступа пользователей LDAP, которые не производили вход в течение указанного числа дней.
  - **Отправлять по электронной почте уведомление за X дней до окончания срока действия пользователя** – при включении пользователям отправляется уведомление за заданное число дней до окончания срока действия учетной записи данного пользователя.

6.6.1 Что происходит с контентом пользователя с истекшим сроком учетной записи?

Пользователи, у которых истек срок учетной записи, теряют доступ к контенту и право владения им, но сам контент сохраняется в системе.

Его нужно либо переназначить, либо окончательно удалить на странице Управление удаленными пользователями.

Внимание
До окончательного удаления контента пользователя с истекшим сроком учетной записи не будет освобождено пространство, занимаемое этим контентом. Очистка файлов удалит только контент, который был ранее удален пользователем с истекшим сроком учетной записи.

6.7 Файловый репозиторий

Эти настройки определяют, где будут храниться файлы, отправленные для синхронизации и общего доступа. В конфигурации по умолчанию репозиторий файловой системы устанавливается на том же сервере, что и сервер Кибер Файлы. Файловый репозиторий используется для хранения файлов Sync & Share Кибер Файлы и предыдущих редакций. Кибер Файлы Средство конфигурации используется для указания адреса, порта и местоположения хранилища файлов репозитория. Настройка **Конечная точка репозитория хранения файлов** ниже должна соответствовать настройкам на вкладке «Файловый репозиторий» средства настройки. Чтобы просмотреть или изменить эти настройки, запустите файл Cyber Files Configuration Utility.exe, расположенный обычно в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\Configuration Utility.

- **Тип хранения файла** – выберите местоположение хранилища, которое будет использоваться для репозитория виртуальной файловой системы. Доступные варианты: **Файловая система**, **Swift S3**, **Ceph S3** и **Другое S3-совместимое хранилище**.

  Примечание
  Вариант **Другое S3-совместимое хранилище** можно использовать для поставщиков хранилищ S3, не указанных в списке, но правильная работа всех функций не гарантируется.

  Примечание
  Тип хранилища MinIO S3 поддерживается и может быть настроен как **Другое S3-совместимое хранилище**, однако мы не поддерживаем его использование через незащищенное подключение HTTP.

  Примечание
  В случае, когда сразу несколько пользователей загружают один и тот же файл, общее хранилище будет равно произведению количества этих пользователей и размера файла, т. е. используемое пространство пропорционально количеству пользователей и загрузок. Используемое хранилище будет равно общему объему всех файлов, загруженных всеми участвующими пользователями. Тем не менее, тот факт, что пользователи загружают один и тот же файл, а также тип используемого внутреннего хранилища, не повлияют на объем занимаемого хранилища.

- **Конечная точка репозитория хранения файлов** – задайте URL-адрес конечной точки репозитория файловой системы.

- **Уровень защиты** – укажите уровень защиты файлов, хранящихся в репозитории виртуальной файловой системы. Возможные варианты: **Нет**, **Низкий**, **Высокий**, **ГОСТ 28147-89**. Значение по умолчанию – **Высокий**.
- **Порог для предупреждения о заканчивающемся месте на диске хранения файлов** – когда свободное место на диске станет меньше этого порогового значения, администратор будет получать уведомления о нехватке свободного места.

6.8 Кибер Файлы - клиент

Эти настройки относятся к настольному клиенту.

- **Применять устаревший режим опроса** – заставляет клиенты опрашивать сервер вместо получения от сервера асинхронных уведомлений. Этот параметр следует включать только по инструкции службы поддержки пользователей Cyberprotect.
  - **Время опроса клиентского приложения** – задает временные интервалы, через которые клиент будет опрашивать сервер. Этот параметр доступен только при включенном параметре **Применять устаревший режим опроса**.
- **Минимальный интервал обновления клиентского приложения** – задает минимальное время (в секундах), в течение которого сервер будет ожидать перед повторным уведомлением клиента о доступности обновленного содержимого.
- **Предел частоты уведомления клиентского приложения** – задает максимальное количество уведомлений клиента об обновлении, которое сервер будет отправлять в минуту.
- **Показывать ссылку на скачивание клиентского приложения** – если этот параметр включен, то для веб-пользователей будет отображаться ссылка на скачивание настольного клиента.
- **Минимальная версия клиентского приложения** – задает минимальную версию клиента, которая может подключаться к серверу.
- **Не допускать подключение клиентских приложений** – если этот параметр включен, то настольные клиенты не смогут подключаться к серверу. Как правило, этот параметр следует включать только в целях администрирования. Она не препятствует подключениям к веб-интерфейсу.
- **Разрешить автоматическое обновление клиентского приложения до версии** – задает версию клиента для настольных ПК, которая будет развернута на всех клиентах для настольных ПК при автоматической проверке обновлений. Выберите параметр **Не разрешать обновления**, чтобы вообще запретить автоматическое обновление клиентов.

7 Пользователи и устройства

7.1 Управление устройствами

После того, как пользователи Кибер Файлы подключатся к веб-серверу Кибер Файлы, их устройства отображаются в списке **Устройства**.

Здесь можно просмотреть подробную информацию о статусе всех используемых устройств. Кроме того, можно очистить данные приложения Кибер Файлы или изменить его пароль.

- **Имя пользователя** – отображаемое имя Active Directory (AD) для пользователя LDAP или имя, выбранное эпизодическим пользователем.
- **Имя устройства** – заданное пользователем имя устройства.
- **Модель** – официальное название мобильного устройства пользователя.
- **ОС** – тип и версия мобильной или настольной операционной системы.
- **Версия** – версия приложения Кибер Файлы или используемого настольного клиента.
- **Статус** – статус приложения Кибер Файлы, который может принимать следующие значения:
  - Управляется;
  - Управляется, ожидание удаленной очистки данных;
  - Не управляется, выполнена удаленная очистка данных;
  - Не управляется, ожидание удаленной очистки данных;
  - Не управляется пользователем;
  - Данные очищены после неправильного ввода пароля.

Для настольного клиента единственным статусом будет Sync & Share.

- **Последний контакт** – дата и время последнего соединения между сервером управления и приложением или клиентом Кибер Файлы для ПК.
- **Политика** – имя и ссылка на политику управления, примененную к пользователю.
- **Действия**
  - **Дополнительная информация** – содержит дополнительные сведения об устройстве и редактируемое поле **Примечания**.
  - **Сброс пароля приложения** (только для мобильных устройств) – удаленный сброс пароля блокировки приложения Кибер Файлы на выбранном устройстве. Для этого необходимо сформировать код подтверждения, используя код сброса пароля, отображаемый на экране устройства пользователя.
  - **Удаленная очистка данных** (только для мобильных устройств) – если включить этот параметр, то все файлы в приложении Кибер Файлы, а также настройки приложения будут удалены при следующем подключении устройства к серверу управления. Другие приложения и данные ОС не затрагиваются.

- **Удалить из списка**– удаление настольного клиента из списка **Устройства**. Для мобильных устройств эта команда удаляет выбранное устройство из списка и отменяет управление им без очистки данных. Этот вариант обычно используется для удаления устройства, которое в дальнейшем не предполагается вновь подключать к серверу управления клиентами Кибер Файлы. Если включен параметр **Разрешать мобильным клиентам, восстановленным на новые устройства, автоматически регистрироваться без PIN-кода**, то такое новое устройство автоматически станет управляемым после подключения к серверу.

7.1.1 Экспорт сведений об устройствах

Сведения обо всех устройствах в этом списке можно экспортировать в файл TXT, CSV или XML.

Для этого нажмите кнопку **Экспорт** и выберите нужный формат файла.

Экспортированные данные включают следующее:

1. Имя пользователя
2. Имя используемого мобильного устройства или компьютера
3. Модель мобильного устройства
4. Тип и версия ОС на устройстве
5. Версия приложения или настольного клиента
6. Статус мобильного устройства или настольного клиента
7. Дата и время регистрации приложения Кибер Файлы на веб-сервере Кибер Файлы
8. Дата и время последнего контакта между приложением или настольным клиентом Кибер Файлыи веб-сервером Кибер Файлы
9. Имя примененной политики пользователей
10. Примечания

7.1.2 Выполнение удаленного сброса пароля приложения

Приложение Кибер Файлы можно защитить паролем блокировки, который необходимо вводить при запуске приложения. Если пользователь забудет пароль, то он не сможет получить доступ к Кибер Файлы. Пароль приложения не связан с паролем учетной записи пользователя в Active Directory.

Если пароль блокировки приложения потерян, единственные варианты – выполнить удаленный сброс пароля или позволить пользователю удалить Кибер Файлы с устройства и повторно установить его. В процессе удаления будут потеряны все имеющиеся данные и настройки. От этого не пострадает безопасность, однако пользователь, вероятно, утратит доступ к серверам Кибер Файлы, пока ему не поступит новое приглашение на регистрацию.

7.1.3 Выполнение удаленной очистки данных

Кибер Файлы позволяет удаленно выполнить очистку данных мобильного приложения. При этом будут удалены все файлы в локальном хранилище или кэше приложения Кибер Файлы. Все настройки приложений сбрасываются до ранее установленных по умолчанию, а любые настроенные в приложении серверы удаляются.

Для этого сделайте следующее.

1. Откройте Кибер Файлы веб-интерфейс.
2. Откройте вкладку **Пользователи и устройства** и перейдите в раздел **Устройства**.
3. Найдите устройство, для которого нужно выполнить удаленную очистку данных, и нажмите кнопку **Действия**.
4. Нажмите **Удаленная очистка данных...**
5. Подтвердите удаленную очистку данных, нажав **Очистить**.
6. Появится статус **Ожидание удаленной очистки данных** в столбце **Состояние** для соответствующего устройства.

   Примечание
   Администратор может отменить удаленную очистку данных, но только до подключения приложения к серверу управления. Этот пункт отображается в меню **Действия** после выдачи команды на удаленную очистку данных.

7. Удаленная очистка данных будет выполнена при следующем подключении устройства к серверу. На этом этапе очистку нельзя отменить.

Примечание
Требования к подключению Клиенты
Кибер Файлы должны иметь сетевой доступ к серверу Кибер Файлы, чтобы получать обновления профиля, команды на удаленный сброс пароля или удаленную очистку данных. Если для доступа к Кибер Файлы клиенту необходимо VPN-подключение, то это подключение необходимо и для приема команд управления.

7.2 Управление пользователями

Можно управлять всеми пользователями Sync & Share из раздела **Пользователи**.

Можно пригласить новых пользователей, нажав кнопку **Добавить пользователя**, либо изменить или удалить текущих пользователей, нажав кнопку **Действия**. При изменении пользователя можно предоставить ему права администратора (если у вас есть на это право), изменить адрес электронной почты, пароль либо отключить (включить) его учетную запись.

Если включены квоты, то можно установить для определенных пользователей особую квоту, но только при наличии у них доступа к Sync & Share.

7.2.1 Типы пользователей Sync & Share

Существует три типа пользователей Sync & Share.

Внешние (эпизодические) учетные записи пользователей

Эти учетные записи необходимо создавать вручную через приглашения по электронной почте, рассылаемые администратором, либо приглашения других пользователей на содержимое общего доступа (файл или папка).

Существует два подтипа внешних учетных записей: **Бесплатная** и **Лицензированная**.

По умолчанию каждая внешняя учетная запись, вновь создаваемая, является бесплатной. Только администратор Кибер Файлы может преобразовать бесплатную внешнюю учетную запись в лицензированную.

Пользователи с лицензированной учетной записью могут создавать, загружать, редактировать и удалять файлы и папки в собственном пространстве Sync & Share. Они также могут передавать свой контент другим пользователям.

Пользователи с бесплатной учетной записью не имеют пространства Sync & Share. Если им дать соответствующие права, бесплатные пользователи могут создавать новые файлы, загружать их из других источников, а также редактировать и удалять файлы только в папках, которые им предоставлены. Если они имеют права только для чтения, то они не могут создавать, загружать, изменять и удалять файлы, а могут только просматривать и скачивать файлы в папках, которые им предоставлены.

Пользователи с бесплатными учетными записями не могут приглашать новых пользователей в общий ресурс, даже если им были предоставлены такие права во время создания учетной записи.

Если файл предоставлен пользователю с бесплатной учетной записью, то он сможет только просмотреть или скачать его.

Пользователи с бесплатными учетными записями не могут использовать клиенты для ПК или мобильных устройств.

Примечание
Все вновь созданные внешние учетные записи должны активироваться вручную. Пользователь получит по электронной почте инструкции о том, как это сделать.

Внутренние (LDAP) учетные записи пользователей

Такие учетные записи работают на основе интеграции с Active Directory (AD). Они создаются вручную (как внешние), либо администратор может настроить настроенную группу LDAP и разрешить пользователям AD автоматически создавать учетные записи при первом входе в Кибер Файлы.

Внутренние учетные записи автоматически лицензируются в момент создания.

Пользователи с внутренней учетной записью могут создавать, загружать, редактировать и удалять файлы и папки в собственном пространстве Sync & Share. Они также могут передавать свой контент другим пользователям.

Они могут использовать клиент для ПК или мобильных устройств.

Учетные записи пользователей без доступа

Это административные учетные записи без доступа к Sync & Share. По умолчанию они не лицензируются. Пользователи с такими учетными записями не могут использовать клиенты Кибер Файлы для ПК или мобильных устройств.

Примечание
Администраторам без доступа кSync & Share не нужно задавать адрес электронной почты: они могут входить в систему со своими учетными данными LDAP. Такие учетные записи можно создавать, не настраивая SMTP для сервера Кибер Файлы. Дополнительные сведения см. на странице Администраторы и права доступа.

На вкладке **Пользователи** доступна следующая информация:

- **Имя** показывает имя пользователя (отображаемое имя Active Directory (AD) для пользователей LDAP либо имя, выбранное эпизодическим пользователем).
- **Имя пользователя** (необязательно). Показывает имя входа для пользователей LDAP.
- **UPN** (необязательно). Показывает универсальное имя участника для пользователей LDAP.
- **Домен** (необязательно). Показывает домен для пользователей LDAP.
- **Электронная почта** показывает адрес электронной почты пользователя.
- **Sync & Share**
  - **Статус** указывает тип используемой лицензии.
  - **Использование** показывает общий размер содержимого у пользователя.
- **Последний вход** – время и дата последнего входа.
- **Действия**
  - **Подробнее** отображает дополнительную информацию о пользователе.
  - **Показать устройства** отображает информацию об устройствах, используемых этим пользователем.
  - **Сброс пароля Sync & Share** отправляет письмо о сбросе пароля на электронную почту.
  - **Преобразовать в лицензированного** – преобразует бесплатного пользователя в лицензированного.
  - **Изменить пользователя** – позволяет изменить для пользователя адрес электронной почты, отключить или включить учетную запись, дать полные или отдельные административные права либо задать квоту для учетной записи. Для внешних пользователей можно изменить номер мобильного телефона, используемый для 2FA.
  - **Удалить** – удаляет пользователя.

7.2.1.1 Экспорт данных о пользователях

Данные обо всех зарегистрированных пользователях можно экспортировать в файл в формате TXT, CSV или XML.

Для этого нажмите кнопку **Экспорт** и выберите необходимый формат файла.

Экспортируются следующие данные:

1. Имя пользователя
2. Имя входа пользователя (для пользователей LDAP)
3. Универсальное имя участника (для пользователей LDAP)
4. Домен LDAP (для пользователей LDAP)
5. Адрес электронной почты
6. Имя политики
7. Ожидающий статус
8. Административные права доступа
9. Статус лицензирования пользователя
10. Статус отключения пользователя
11. Аутентификация LDAP
12. Количество папок, которые принадлежат пользователю
13. Количество файлов, которые принадлежат пользователю
14. Размер контента пользователя (в байтах)
15. Размер квоты пользователя (в байтах)
16. Дата и время последнего входа

7.2.2 Добавление внешнего пользователя (внеплановое)

Добавление внешнего пользователя (внеплановое)

1. Откройте веб-интерфейс Кибер Файлы.
2. Выполните вход с учетной записью администратора. Можно также использовать учетную запись с правами **управления пользователями**.
3. Откройте вкладку **Пользователи и устройства**.
4. Откройте вкладку **Пользователи**.
5. Нажмите кнопку **Добавить пользователя Sync & Share**.
6. Напишите письмо пользователю.
7. Выберите язык приглашения.
8. Нажмите кнопку **Добавить**.

Пользователь получит по электронной почте письмо со ссылкой. После перехода по ссылке ему будет предложено задать пароль. Затем пользователь получит письмо для подтверждения учетной записи. После открытия ссылки в письме учетная запись будет готова к использованию.

7.2.3 Добавление внутреннего пользователя (LDAP)

Добавление внутреннего пользователя (LDAP)

1. Откройте Кибер Файлы веб-интерфейс.
2. Выполните вход с учетной записью администратора. Можно также использовать учетную запись с правами **управления пользователями**.
3. Откройте вкладку **Пользователи и устройства**.
4. Откройте вкладку **Пользователи**.
5. Нажмите кнопку **Добавить пользователя Sync & Share**.
6. Напишите письмо пользователю.
7. Выберите язык приглашения.
8. Нажмите кнопку **Добавить**.

Пользователь теперь может выполнить вход со своими учетными данными LDAP. После входа пользователя выполняется регистрация его учетной записи.

Примечание
Если включено использование LDAP и имеется встроенная группа администраторов LDAP, то пользователи в этой группе смогут напрямую входить со своими учетными данными LDAP и иметь полные права администраторов.

7.2.4 Настройка специальной квоты

Можно задать специальную квоту для любого доступа с доступом к синхронизации и общему доступу.

Для этого выполните следующие действия.

1. В веб-интерфейсе откройте вкладку **Пользователи и устройства**.
2. Найдите нужного пользователя и нажмите кнопку **Действия**.
3. Выберите **Изменить пользователя** и включите параметр **Применять пользовательскую квоту?**.
4. Выберите нужный размер квоты и нажмите кнопку **Сохранить**.

Примечание
Флажок **Применять пользовательскую квоту?** доступен только в том случае, если предварительно включен параметр **Включить квоты?**.

7.2.5 Удаление пользователя и его контента

При удалении пользователя, у которого нет контента, учетная запись будет полностью удалена.

При удалении пользователя, у которого есть контент (включая пользователей с истекшим сроком), необходимо выбрать действия с контентом.

- **Сохранить и передать позже** – контент пользователя временно сохраняется в системе. Им можно управлять на вкладке **Передача контента удаленного пользователя**. Такой контент можно либо переназначить, либо удалить окончательно.

  Примечание
  Политики очистки по-прежнему действуют для этого контента так же, как и для контента активных пользователей.

- **Передать другому пользователю** – контент немедленно переназначается другому пользователю, в пространстве которого появляется папка **Контент унаследован от DeletedUserName <deletedusersemail>**. Выбранный пользователь становится владельцем унаследованного контента, включая папки, ранее опубликованные удаленным пользователем.
- **Удалить окончательно** – немедленно удаляет учетную запись и контент пользователя.

8 Руководства по клиентам

Сведения об использовании клиентов Кибер Файлы см. в Руководстве пользователя.

8.1 Клиент для Android

Приложение работает на смартфонах и планшетах с ОС Android 7.0 и новее. Устройства с архитектурой процессора x86 не поддерживаются.

Скачать клиент можно в веб-интерфейсе в меню профиля пользователя и на странице обновления продукта.

9 Администрирование сервера

9.1 Администрирование сервера

Если вы являетесь администратором, то при входе в веб-интерфейс можете переключаться между режимами **Администрирование** и **Пользователь**.

- Чтобы войти в режим **Администрирование**, щелкните значок пользователя и выберите **Консоль администрирования**.
- Чтобы войти в режим **Пользователь** , нажмите кнопку **Покинуть администрирование** в правом верхнем углу.

Примечание
Администраторы могут использовать документацию по API. Ссылку можно найти в нижнем колонтитуле веб-интерфейса в режиме администрирования.

9.2 Администраторы и права доступа

9.2.1 Ограничение доступа к странице администрирования

- **Доступ к страницам администрирования будет разрешен только для подключений из настроенных диапазонов IP-адресов** – позволяет администратору открыть доступ к веб-интерфейсу администрирования только для определенных IP-адресов.
  - **IP-адреса с доступом к страницам администрирования** – администратор вводит IP-адреса, которым разрешен доступ к странице **администрирования**. Это может быть список IP-адресов, подсетей или IP-диапазонов, перечисленных через запятую, **например** 10.1.2.3, 10.4.*, 10.10.1.1-10.10.1.99.

Примечание
Доступ администратора с локального хоста (localhost) не может быть ограничен.

Примечание
Эта функция не работает для серверов, использующих сервер шлюза как прокси для запросов к серверу Кибер Файлы.

9.2.2 Подготовленные группы администраторов LDAP

В этом разделе можно управлять группами администраторов. Пользователи в этих группах автоматически получат права администратора группы. Все права отображены в таблице. Включенные в данный момент отмечены зеленой галочкой.

С помощью кнопки **Действия** можно удалить или отредактировать группу. Можно также изменить административные права группы.

Чтобы добавить распределенную группу администраторов LDAP, выполните следующие действия.

1. Нажмите кнопку **Добавить распределенную группу**.
2. Укажите, должна ли группа иметь функциональность Sync & Share.
3. Отметьте все административные права, которые необходимо предоставить пользователям группы.
4. Найдите группу.
5. Щелкните на имя группы.
6. Выберите **Сохранить**.

9.2.3 Пользователи с правами администратора

В этом разделе приведены все пользователи с административными правами, тип проверки их подлинности (эпизодический или LDAP), наличие прав синхронизации и общего доступа (Sync & Share), а также состояние пользователей (отключено или включено).

Можно пригласить нового пользователя с полными или частичными правами администратора, нажав кнопку **Добавить администратора**. С помощью кнопки **Действия** пользователя можно удалить или изменить. Можно изменить административные права, статус, адрес электронной почты и пароль.

Приглашение одного администратора

1. Откройте веб-интерфейс Кибер Файлы.
2. Выполните вход с учетной записью администратора.
3. Разверните вкладку **Общие настройки** и откройте страницу **Администраторы**.
4. Нажмите кнопку **Добавить администратора** в разделе **Пользователи с правами администратора**.
5. Выберите вкладку **Active Directory/LDAP** или **Пригласить по электронной почте** в зависимости от типа приглашаемого пользователя и объекта, который он будет администрировать.
   a. **Чтобы пригласить пользователя через Active Directory/LDAP, сделайте следующее.**
      1. Выполните поиск пользователя, которого хотите добавить в Active Directory, и кликните на его общее имя.

      Примечание
      Поля **Пользователь LDAP** и **Эл. почта** будут заполнены автоматически.

      2. Включите или отключите функциональность Sync & Share.
      3. Выберите, какие административные права должны быть у пользователя.
      4. Нажмите кнопку **Добавить**.

b. **Чтобы отправить приглашение по электронной почте, выполните следующие действия.**

1. Введите адрес электронной почты пользователя, которого требуется добавить как администратора.

Примечание
Специальные пользователи, приглашенные по электронной почте, всегда смогут использовать функции Sync & Share.

2. Выберите, должен ли этот пользователь иметь лицензию.
3. Выберите, какие административные права должны быть у пользователя.
4. Выберите язык электронного приглашения.
5. Нажмите кнопку **Добавить**.

9.2.4 Права администратора

- **Полные права администратора** – предоставляет пользователю полные права администратора.
- **Может управлять пользователями** – предоставляет права для управления пользователями. Это включает права для приглашения новых пользователей, распределения групп LDAP, отправки приглашений для регистрации Кибер Файлы и управления подключенными мобильными устройствами.
- **Может управлять мобильными источниками данных** – предоставляет пользователю права для управления мобильными источниками данных. Это включает права для добавления новых серверов шлюза и источников данных, управления назначенными источниками, серверами шлюза, доступными для клиентов, и источниками данных предыдущих версий.
- **Может управлять мобильными политиками** – предоставляет пользователю права для управления мобильными политиками. Это включает права для управления политиками пользователей и групп, разрешенными приложениями и стандартными ограничениями доступа.
- **Может просматривать журнал аудита** – предоставляет пользователю права для просмотра журнала аудита.

Примечание
Новые пользователи, которые включены одновременно в распределенную группу администраторов LDAP и распределенную группу синхронизации и общего доступа (Sync & Share) LDAP, получают совмещенные разрешения.

Чтобы предоставить права администратора, выполните следующие действия.

1. Откройте вкладку **Sync & Share**.
2. Откройте вкладку **Пользователи**.
3. Нажмите кнопку **Действия** для пользователя, параметры которого требуется изменить.
4. Выберите **Изменить**.

5. Отметьте все права администратора, которые необходимо предоставить пользователю.
6. Выберите **Сохранить**.

Чтобы предоставить определенные права администратора, выполните следующие действия.

1. Нажмите кнопку **Действия** для пользователя, параметры которого требуется изменить.
2. Выберите **Изменить**.
3. Отметьте все права администратора, которые необходимо предоставить пользователю.
4. Выберите **Сохранить**.

9.3 Журнал аудита

9.3.1 Журнал

Здесь можно просмотреть сведения о недавних событиях, для которых была создана запись в журнале (период хранения может отличаться в зависимости от политики очистки).

Примечание
Чтобы настроить параметры и уровень ведения журнала сервера шлюза, см. раздел Ведение журнала сервера шлюза.

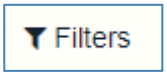
Список журналов

- **Временная метка** – показывает дату и время события.
- **Тип** – показывает уровень серьезности события.
- **Пользователь** – показывает учетную запись пользователя, ответственную за событие.
- **Сообщение** – показывает сведения о том, что произошло.

Если включено ведение журнала аудита на сервере шлюза, то будет также отображаться активность мобильных клиентов. Если настольным и веб-клиентам разрешен доступ к мобильным источникам данных, то они также будут отражены в журнале.

- **Имя устройства** – имя подключенного устройства.
- **IP-адрес устройства** – показывает IP-адрес подключенного устройства.
- **Сервер шлюза** – показывает имя сервера шлюза, к которому подключено устройство.
- **Путь сервера шлюза** – показывает путь к источнику данных на соответствующем сервере шлюза.

Фильтрация списка журналов

Можно отфильтровать записи, отображаемые в таблице журнала. Чтобы открыть или закрыть панель настроек фильтрации, нажмите значок 

наверху страницы.

- **Фильтровать по пользователю** – можно выбрать **Все**, **Без пользователя** или указать одного из доступных пользователей.
- **Фильтровать по общим проектам** – можно выбрать **Все**, **Без общего доступа** или указать один из доступных общих проектов.
- **Фильтровать по важности** – доступны категории **Все**, **Информация**, **Предупреждение**, **Ошибка** и **Критические**.
- **Фильтровать по серверу шлюза** – можно выбрать **Все**, **Без сервера** или указать один из ваших серверов шлюза.
- **Фильтровать по IP устройства** – можно выбрать **Все**, **Без IP устройства** или указать один из IP-адресов устройств, для которых была создана запись в журнале.
- **От/до** – фильтрация по дате и времени.
- **Поиск по тексту** – фильтрация по содержимому сообщений журналов.
- **Фильтровать по имени устройства** – можно выбрать **Все**, **Без имени устройства** или указать одно из имен устройств, для которых была создана запись в журнале.

9.3.2 Настройки

Кибер Файлы может автоматически очищать старые журналы и экспортировать их в файлы на основе определенных правил.

- **Автоматически очищать записи журнала старше X Y**. Если эта функция включена, журналы старше указанного количества дней/недель/месяцев будут автоматически очищаться.
  - **Экспортировать записи журнала в файл в виде X перед очисткой** – если эта функция включена, копия журналов перед очисткой будет экспортироваться в формате CSV, TXT или XML. Экспорт автоматически настроен на 03:00 по локальному времени сервера. Эту настройку нельзя изменить.
    - **Путь к экспортируемому файлу** – определяет папку, куда будут помещаться экспортированные журналы.

Внимание
Рекомендуется экспортировать журналы в папку за пределами папки установки Кибер Файлы, чтобы они не были утеряны при обновлении. Учетная запись пользователя, от имени которой работает служба Tomcat Кибер Файлы, должна иметь доступ на чтение и запись к выбранной папке. По умолчанию используется учетная запись локальной системы.

- **Показывать метки времени в экспортированных журналах аудита с использованием X** – этот параметр позволяет выбрать использование локального времени сервера или другого формата времени (UTC).

9.3.3 Параметры Syslog

Сервер Кибер Файлы позволяет передавать события из журнала аудита на сервер Syslog или любую SIEM-систему для централизованного мониторинга и обработки событий.

- **Передавать события аудита на сервер Syslog** – включает отправку событий из журнала аудита на указанный Syslog-сервер.

  Примечание
  События аудита, зарегистрированные до включения этой функции, не будут переданы на сервер Syslog.

  - **Сервер** – укажите IP- или URL-адрес сервера Syslog.
  - **Порт** – укажите порт подключения сервера Syslog. Значение порта по умолчанию: 514.
  - **Протокол** – выберите протокол передачи: TCP или UDP. Это значение должно совпадать с протоколом, используемым на сервере Syslog.

    Примечание
    UDP (User Datagram Protocol) – это более простой протокол подключений на основе сообщений. Он работает быстрее, однако имеет низкий уровень безопасности и устранения ошибок. При использовании протокола UDP размер сообщения не должен превышать 500 байт, в противном случае сообщение может не дойти (в зависимости от настроек оборудования).
    TCP (Transmission Control Protocol) предлагает "гарантированную доставку", в которой используется управление потоком для определения всех пакетов, успешно отправленных перед обработкой новых пакетов.

  - **Формат сообщения** – выберите формат отправки сообщения. Доступные варианты: CEF (RFC 3164) или Syslog (RFC 5424).

9.4 Сервер

9.4.1 Настройки сервера

- **Имя сервера** – косметическое имя сервера, используемое в качестве заголовка веб-сайта, а также для идентификации сервера в уведомлениях для администратора по электронной почте.
- **Веб-адрес** – обозначает корневое DNS-имя или IP-адрес, с помощью которых пользователь может войти на веб-сайт (начинается с http:// или https://). Не используйте в таких случаях имя localhost, поскольку этот адрес будет также использоваться в ссылках приглашений по электронной почте.
- **Язык журнала аудита** – выберите язык по умолчанию для журнала аудита.В настоящее время доступны: **английский, немецкий, французский, японский, итальянский, испанский, чешский, русский, польский, корейский, традиционный и упрощенный китайский**.Значение по умолчанию – **английский**.
- **Время ожидания сеанса в минутах** – задает продолжительность интервала времени, после которого будет произведен автоматический выход неактивных пользователей из системы. Если в течение указанного времени не выполнено никаких действий, пользователю будет предоставлено временное диалоговое окно с приглашением выполнить действие или быть

автоматически удаленным из системы.

Примечание
Если пользователь начал отправку или скачивание, которые не успеют завершиться до окончания времени ожидания сеанса, пользователь останется зарегистрированным, пока не завершится передача данных.

- **Включить поддержку Sync & Share** – с помощью этого флажка можно включить и отключить функции синхронизации и общего доступа.

9.4.2 Параметры уведомлений

- **Отправить администратору сводку ошибок по электронной почте?** – если этот параметр включен, то на указанные адреса электронной почты будет отправляться сводка по ошибкам.
  - **Адреса электронной почты** – один или несколько адресов электронной почты, на которые будет отправляться сводка по ошибкам.
  - **Частота уведомлений** – частота отправки сводок по ошибкам. Сообщения электронной почты отправляются только при наличии ошибок.

9.4.3 Двухфакторная проверка подлинности по SMS

Этот выпуск включает возможность двухфакторной проверки подлинности по SMS при входе через веб-клиент. Для этого используются номера мобильных телефонов из AD или номера, указанные пользователями. Двухфакторная проверка может требоваться при каждом входе, через заданные интервалы или только при входе из нового браузера.

Для отправки SMS-кодов необходимо создать учетную запись службы SMS-сообщений Twilio. Дополнительные сведения см. на странице https://www.twilio.com/sms. Дополнительные сведения по запуску пробной версии Twilio см. на странице бесплатной пробной версии Twilio.

Примечание
Для Twilio потребуется всего одна учетная запись, которая используется сервером Кибер Файлы, учетные записи для каждого пользователя не нужны.

Примечание
Обязательно выберите по крайней мере один из вариантов: **Требовать для внутренних или пользователей LDAP** или **Требовать для внешних пользователей**.

Требовать двухфакторной проверки подлинности веб-клиента по SMS

- **При первом входе в новых браузерах** – потребуется проверка подлинности по SMS, когда новый пользователь первый раз открывает веб-страницу сервера Кибер Файлы. После введения кода проверки и регистрации браузера больше не потребуется вводить SMS-код, пока используется тот же браузер и компьютер.
- **Через заданный интервал** – потребуется проверка подлинности по SMS через заданный интервал времени, независимо от количества попыток входа.

- **При каждом входе** – потребуется проверка подлинности по SMS при каждой попытке подключения пользователя.

Настройки Twilio

- **Идентификатор безопасности учетной записи Twilio** – идентификатор безопасности (SID) учетной записи Twilio вашей компании.
- **Маркер проверки подлинности Twilio** – маркер проверки подлинности Twilio вашей компании. Идентификатор и маркер можно найти в консоли Twilio на странице https://www.twilio.com/console.
- **SID службы сообщений Twilio** – идентификатор безопасности службы сообщений для двухфакторной проверки. Этот идентификатор находится на странице https://www.twilio.com/console/sms/dashboard. Если у вас несколько служб сообщений Twilio, используйте только SID службы, которая будет применяться для двухфакторной проверки. При создании службы сообщений Twilio оставьте поле **Сценарий использования** пустым или выберите двухфакторную проверку подлинности.

Примечание
В консоли Twilio необходимо выбрать страны, которые могут использовать эту службу сообщений. Установите флажки для нужных стран.

9.5 Пользовательская настройка веб-интерфейса

При желании можно настроить пользовательские эмблемы и цветовую схему сервера Кибер Файлы.

Примечание
Эти настройки также можно сделать через API Кибер Файлы. Дополнительные сведения см. в разделе Настройка веб-интерфейса через API.

9.5.1 Настройка пользовательских эмблем

1. Откройте веб-интерфейс Кибер Файлы и выполните вход от имени администратора.
2. Выберите **Общие настройки** > **Настройка веб-интерфейса**.
3. Установите флажок **Использовать пользовательский логотип**.
4. Укажите файлы эмблем, которые требуется изменить, и убедитесь, что они выбраны в раскрывающемся меню.

   Примечание
   Ограничения размеров изображения указываются в скобках **()**.

5. Выберите **Сохранить**.

9.5.2 Использование пользовательского приветствия

1. Откройте веб-интерфейс Кибер Файлы и выполните вход от имени администратора.
2. Выберите **Общие настройки** -> **Настройка веб-интерфейса**.
3. Установите флажок **Отображать пользовательское сообщение на веб-странице входа**.
4. Введите сообщение в текстовое поле и нажмите **Сохранить**.

9.5.3 Настройка цветовых схем

1. Откройте веб-интерфейс Кибер Файлы и выполните вход от имени администратора.
2. Выберите **Общие настройки** -> **Настройка веб-интерфейса**.
3. Щелкните раскрывающееся меню **Цветовая схема** и выберите нужную схему.
4. Выберите **Сохранить**.

9.6 Предпросмотр и редактирование в веб-браузере

Кибер Файлы предоставляет возможность предпросмотра и редактирования для распространенных типов документов и изображений внутри интерфейса веб-клиента без скачивания этих файлов.

- **Включить интеграцию с сервером онлайн-редактирования** – включает интегрированные функции онлайн-редактирования документов указанного сервера через WOPI. В текущей версии сервера Кибер Файлы подтверждена интеграция с Microsoft Office Online, «Р7-Офис. Сервер документов» и «МойОфис Сервер совместного редактирования (ССР)».
  - **URL-адрес сервера онлайн-редактирования документов** – введите URL-адрес обнаружения сервера онлайн-редактирования документов через WOPI.
  - **Использовать указанный сервер онлайн-редактирования документов для** – вариант **Изменение** позволяет редактировать файлы Microsoft Office DOCX, PPTX, XSLX, а вариант **Просмотр и изменение** позволяет редактировать упомянутые типы файлов, а также просматривать файлы DOC, XLS и PPT. Если этот параметр отключен, все файлы MS Office и PDF будут открываться встроенным средством предпросмотра Кибер Файлы.
  - **Включить службы Microsoft для проверки правописания и интеллектуального поиска Bing (только для Office Online)** – использует службы Microsoft Bing для проверки правописания при включенной интеграции с Microsoft Office Online.
  - **Разрешить подключение к указанному серверу онлайн-редактирования документов с помощью самозаверенных или недоверенных сертификатов.** Если этот параметр включен, то пользователи смогут подключаться к серверам онлайн-редактирования, использующим недоверенные сертификаты.
  - **Предпросмотр PDF-файлов с помощью указанного сервера онлайн-редактирования документов.** Если этот параметр включен, то пользователи смогут просматривать PDF-

файлы с помощью сервера онлайн-редактирования при условии, что данный сервер поддерживает такую функцию и для параметра **Использовать указанный сервер онлайн-редактирования документов для** установлено значение **Просмотр и изменение**. Во всех остальных случаях PDF-файлы будут открываться во встроенном средстве предпросмотра Кибер Файлы.

- **Включить встроенный предпросмотр документов в веб-клиенте** – включает функцию предпросмотра.

  Примечание
  Для файлов, защищенных паролем, недоступны эскизы и предварительный просмотр.

  - **Разрешить предпросмотр только для файлов, не требующих формирования на сервере (PDF, изображения, текстовые файлы)** – уменьшает нагрузку, вызываемую сетевыми операциями предпросмотра, разрешая предпросмотр только для файлов, не требующих дополнительного формирования. Такими файлами являются PDF-файлы, изображения и простые текстовые файлы.
  - **Максимальный размер кэша для последних сформированных предпросмотров** – задает максимальный размер кэша для хранения предварительно просмотренных файлов. Это значительно увеличивает скорость открытия предпросмотра файлов, если они уже недавно открывались.
  - **Максимум одновременных вызовов формирования** – задает максимальное число одновременных вызовов формирования предпросмотра.
  - **Разрешить подключение к веб-службам предпросмотра с помощью самозаверенных сертификатов** – разрешает обращаться к веб-службам предпросмотра, использующим самозаверенные сертификаты. Это другие службы Кибер Файлы Tomcat.
  - **Пользовательский URL-адрес для веб-службы предпросмотра** – включите, если у вас несколько серверов Кибер Файлы и необходимо указать, какой из них будет использоваться для предпросмотра.

- **Разрешить воспроизведение мультимедиа** – позволяет контролировать настройки воспроизведения мультимедиа, заданные по умолчанию, давая возможность просматривать видео в браузере, не скачивая файл целиком.
  - **Воспроизводить мультимедиа после скачивания** – запускает видео автоматически без нажатия кнопки **Воспроизвести**.
  - **Циклическое воспроизведение** – по окончании видео каждый раз начинает воспроизводиться сначала.
  - **Мультимедиа без звука по умолчанию** – указывает, будет ли вместе с видео воспроизводиться и аудио. Если задать этот параметр, видео будет воспроизводиться без звука.
  - **Включить элементы управления воспроизведением мультимедиа** – дает возможность пользоваться кнопками для управления воспроизведением видео: **Воспроизведение/пауза**, **Громкость +/-** и т. д.

9.7 SMTP

Сервер Кибер Файлы использует настроенный сервер SMTP для рассылки пользователям приглашений на доступ к общему ресурсу или на регистрацию мобильных устройств, а также для уведомления пользователей и администраторов о событиях на сервере.

- **Адрес сервера SMTP** – введите DNS-имя сервера SMTP, который будет использоваться для рассылки приглашений пользователям по электронной почте.
- **Порт сервера SMTP** – введите порт сервера SMTP. По умолчанию используется порт 587.
- **Использовать защищенное подключение?** – этот параметр позволяет использовать защищенное SSL-соединение с сервером SMTP. Параметр включен по умолчанию. Снимите флажок, чтобы отключить защищенный SMTP.
- **От (имя отправителя)** – это имя пользователя, которое отображается в строке «От:» в сообщениях электронной почты, отправляемых сервером.
- **От (адрес эл. почты)** – это адрес пользователя, который отображается в строке «От:» в сообщениях электронной почты, отправляемых сервером.
- **Использовать только этот адрес для всех уведомлений по электронной почте**. Если параметр включен, Кибер Файлы будет отправлять все уведомления только с этого адреса электронной почты.
- **Использовать проверку подлинности SMTP?**– установите этот параметр для подключения с использованием имени пользователя и пароля SMTP или удалите, чтобы подключаться без их использования.
  - **Имя пользователя SMTP** – введите имя пользователя для проверки подлинности SMTP.
  - **Пароль SMTP** – введите пароль для проверки подлинности SMTP.
  - **Подтверждение пароля SMTP** – введите повторно пароль SMTP для его подтверждения.
- **Отправить тестовое письмо** – отправляет тестовое сообщение электронной почты, чтобы проверить правильную работу всех настроек.

9.8 LDAP

С помощью службы Microsoft Active Directory можно предоставить пользователям вашей организации мобильный доступ, а также доступ к возможностям синхронизации и общего доступа. LDAP не требуется для неуправляемого мобильного доступа или поддержки синхронизации и общего доступа, однако он необходим для управляемого мобильного доступа.

- **Включить LDAP?** – если этот параметр включен, то можно настроить LDAP.
  - **Адрес сервера LDAP** – введите DNS-имя или IP-адрес сервера Active Directory, который нужно использовать для регулирования доступа.
  - **Порт сервера LDAP** – для Active Directory по умолчанию установлен порт 389. Вероятно, изменение этого параметра не потребуется.

Примечание
В случае поддержки нескольких доменов, скорее всего, понадобится использовать порт глобального каталога.

- **Использовать защищенное LDAP-подключение?** – по умолчанию этот параметр отключен. Установите флажок, чтобы подключаться к Active Directory по защищенному протоколу LDAP (также называемому LDAPS).

Примечание
При включении функции защищенного LDAP-подключения Кибер Файлы требует, чтобы полное доменное имя сервера LDAP присутствовало в сертификате как общее имя (CN) или альтернативное имя субъекта (SAN).

- **Отключить проверку SSL-сертификата LDAPS –** установите этот флажок, чтобы не проверять сертификат LDAPS при подключении к серверу LDAP. Это удобно, когда сертификат сервера LDAP не подписан публичным центром сертификации.
  Начиная с версии 8.7.0, для новых установок этот параметр отключен по умолчанию (сертификаты LDAPS будут проверяться). Однако, этот параметр включен по умолчанию при обновлении с версий ниже 8.7.0 (сертификаты LDAPS не будут проверяться). При обновлении с версий 8.7.0 и выше будет сохранена существующая настройка.

Примечание
Не отключайте этот параметр, если вы не знаете точный тип используемого сертификата или если ваши сертификаты LDAPS выпущены не публичным доверенным центром сертификации.

- **Имя пользователя или пароль LDAP** – эти учетные данные будут использоваться для всех запросов LDAP. Узнайте у администратора AD, назначены ли вам служебные учетные записи, которые нужно использовать.
- **База поиска LDAP** – введите корневой уровень, на котором должен начинаться поиск пользователей и групп. Если нужно выполнять поиск по всему домену, введите «dc=domainname, dc=domainsuffix».
- **Домены для проверки подлинности LDAP** – пользователи с адресами электронной почты, домены которых содержатся в этом списке, разделенном запятыми, должны выполнять проверку подлинности посредством LDAP. Пользователи в других доменах будут выполнять проверку подлинности по базе данных Кибер Файлы.

Примечание
Внутренние домены здесь не поддерживаются. Можно использовать только домены электронной почты с настроенным внешним именем.

  - **Требовать полного соответствия** – если эта функция включена, то только пользователи из доменов, введенных в **разделы для проверки подлинности LDAP**, будут считаться

пользователями LDAP. Пользователи в составе других доменов и поддоменов будут считаться специальными.

- **Интервал кэширования информации LDAP** задает интервал, с которым Кибер Файлы кэширует структуру Active Directory.
- **Заранее разрешать адреса электронной почты LDAP** – если включена эта настройка, Кибер Файлы будет искать в Active Directory пользователя с соответствующим адресом электронной почты по событиям входа и приглашения. Это позволяет пользователю выполнить вход со своим адресом электронной почты и получить немедленный отзыв по приглашениям, однако выполнение может оказаться медленным, если каталог LDAP очень большой. При обнаружении проблем с быстродействием или медленной реакции при проверке подлинности или приглашении снимите этот флажок.
- **Использовать поиск LDAP для рекомендаций для приглашений и ссылок на скачивание –** при выдаче рекомендаций LDAP будет выполняться поиск пользователей с совпадающими адресами электронной почты в LDAP. Такой поиск может оказаться медленным, если каталог LDAP имеет большой размер. Если при выдаче рекомендаций для поиска обнаружены проблемы с быстродействием, снимите этот флажок.
- **Разрешить вход из веб-клиента и настольного клиента с синхронизацией с использованием имеющихся учетных данных Windows/Mac.** Позволяет всем действительным пользователям LDAP входить в веб-интерфейс и клиент для ПК, не вводя своих учетных данных. См. Настройка единого входа.

Очистка кэша LDAP

Все недавние изменения LDAP распространяются на сервер LDAP. Однако существует небольшая задержка при обновлении кэша LDAP, хранящегося в памяти. Нажмите строку сообщения внизу страницы, чтобы очистить кэш LDAP, в результате чего изменения LDAP будут доступны мгновенно.

9.9 Проверка файлов

- **Включить интеграцию с Kaspersky Scan Engine**
  - **Адрес Kaspersky Scan Engine API** – Имя хоста или IP-адрес машины, на которой установлен Kaspersky Scan Engine (KSE).
  - **Разрешить подключение к Kaspesky Scan Engine API с помощью самозаверенных или недоверенных сертификатов** – разрешает обращаться к серверу Kaspersky Scan Engine, использующему самозаверенный сертификат.
  - **Токен API для авторизации (если авторизация включена)** – если в настройках Kaspersky Scan Engine включена авторизация по токену API, укажите его в этом поле.
  - **Прерывать загрузку файла на сервер при ошибках проверки** – включите, чтобы предотвратить отправку файлов на сервер, если KSE не удалось проверить файл.
  - **Путь к папке на сервере Кибер Файлы для проверки файлов** – укажите папку, в которой должны сохраняться проверяемые файлы, например, "C:\Program Files\Cyberprotect\Cyber Files\Access Server\Scanengine". Папка должна быть доступна для записи для сервера Кибер Файлы.

- **Scan Engine установлен на сервере, отличном от Кибер Файлы** – включите, если сервер Кибер Файлы и Kaspersky Scan Engine установлены на разных машинах.
  - **Общедоступный путь к папке на сервере Кибер Файлы для проверки файлов** – укажите сетевой путь к папке на сервере Кибер Файлы, в которой хранятся проверяемые файлы. Для этого потребуется открыть общий доступ к папке, которая указана в параметре **Путь к папке на сервере Кибер Файлы для проверки файлов**, например, "\\cyberfiles-server\scanengine". Папка должна быть доступна для чтения и записи для KSE.

9.10 Интеграция с DLP

Для централизованного мониторинга операций с файлами и папками сервер Кибер Файлы позволяет передавать соответствующую информацию на сервер Кибер Протего.

Доступны следующие настройки:

- **Включить интеграцию с Кибер Протего** – включает интеграцию с DLP-сервером Кибер Протего.
- **Адрес Кибер Протего API** – имя хоста или IP-адрес машины, на которой установлен и работает сервер Кибер Протего.
- **Разрешить подключение к Кибер Протего API с помощью самозаверенных или недоверенных сертификатов** – разрешает обращаться к Кибер Протего API, использующему самозаверенный сертификат.
- **Идентификатор** – идентификатор клиента API, сгенерированный на сервере Кибер Протего.
- **Секрет** – секрет, сгенерированный на сервере Кибер Протего для указанного клиента.

9.11 Шаблоны электронной почты

Кибер Файлы широко применяет электронную почту для рассылки пользователям и администраторам актуальной информации. С каждым событием связан шаблон в формате HTML и обычного текста. Чтобы выбрать событие и отредактировать оба шаблона, щелкните по раскрывающемуся меню «Шаблоны сообщений электронной почты».

Все сообщения, отправляемые сервером Кибер Файлы, можно настроить по своему усмотрению. Для каждого письма необходимо указать как HTML-шаблон, так и шаблон в текстовом формате. Тело шаблона должно быть написано на языке Liquid. Ознакомьтесь с установленными по умолчанию шаблонами, чтобы определить, каким образом их лучше всего адаптировать.

Примечание
Язык Liquid является языком разметки по умолчанию. Если у вас есть пользовательские шаблоны, написанные на ERB, то ERB будет языком разметки по умолчанию для вашего сервера даже после обновления.

Примечание
Если вы используете настраиваемые изображения в шаблонах электронной почты, они должны быть размещены на доступном ресурсе в Интернете.

При выполнении перехода с mobilEcho изменения, внесенные в шаблоны электронной почты, не переносятся, поэтому их настройку нужно провести повторно. Копии предыдущих шаблонов mobilEcho можно найти в папке **Устаревшие файлы mobilEcho**, по умолчанию расположенной здесь: C:\Program Files (x86)\Group Logic\Access Server\Legacy mobilEcho files. Эти файлы называются **invitation.html.erb** и **invitation.txt.erb**.

- **Выберите язык** – выберите язык по умолчанию для пригласительных сообщений.

  Примечание
  При отправке приглашения на регистрацию или на общий доступ к папкам или файлам можно выбрать другой язык в диалоговом окне приглашения.

- **Выберите шаблон письма** – выберите шаблон, который нужно просмотреть или изменить. Каждый шаблон используется для определенного события (например, регистрации пользователя для мобильного доступа или сброса пароля пользователя).

  Примечание
  Пользовательские шаблоны **не** обновляются автоматически при обновлении Кибер Файлы. Чтобы использовать обновления от Cyberprotect, необходимо вручную применить их к пользовательским шаблонам. Это нужно будет сделать для всех используемых языков.

- **Доступные параметры** – доступные параметры различаются для каждого шаблона и меняются в зависимости от выбранного шаблона.
- **Тема письма** – тема пригласительного электронного сообщения.
  По ссылке **Посмотреть стандартные значения** можно просмотреть стандартную тему для этого языка и шаблон сообщения.
- **Шаблон письма в формате HTML** – показывает шаблон письма в HTML-коде. Если введен допустимый HTML-код, то он будет отображен.
  По нажатию кнопки **Предварительный просмотр** будет отображен текущий шаблон.
- **Шаблон письма с обычным текстом** – отображает текстовый шаблон письма.
  По нажатию кнопки **Предварительный просмотр** будет отображен текущий шаблон.

Примечание
Не забывайте нажимать кнопку **Сохранить шаблоны** после внесения изменений.

Примечание
Редактирование шаблона на английском языке не отражается в вариантах на других языках. Шаблон на каждом из языков необходимо редактировать отдельно.

Обратите внимание, что с помощью параметров в шаблоны может включаться динамическая информация. При отправке сообщения эти параметры будут заменены соответствующими данными.

Для разных событий доступны разные параметры.

Примечание
При нажатии кнопки **Показать по умолчанию** отобразится установленный по умолчанию шаблон.

9.12 Лицензирование

Будет отображен список всех ваших лицензий.

- **Лицензия** – тип лицензии (пробная, на подписку и т. п.).
- **Использование лицензированных клиентов Sync & Share** – используемые в настоящее время лицензии Sync & Share пользователей LDAP.
- **Использование бесплатных клиентов Sync & Share** – используемые в настоящее время бесплатные лицензии Sync & Share внешних пользователей.
- **Использование мобильных клиентов** – используемые в настоящее время лицензии мобильного клиента.

9.12.1 Добавление новой лицензии

1. Скопируйте свой лицензионный ключ.
2. Вставьте его в поле **Добавить лицензионный ключ**.
3. Прочитайте и примите лицензионное соглашение, установив соответствующий флажок.
4. Нажмите кнопку **Добавить лицензию**.

Примечание
Если ваши лицензии имеют один и тот же уникальный идентификатор, то количество разрешенных пользователей будет просуммировано.

9.13 Ведение журнала отладки

Настройки на этой странице предназначены для включения расширенной информации журнала, которая может оказаться полезной при настройке и устранении неполадок в Кибер Файлы. Рекомендуется менять эти настройки только по запросу представителя службы технической поддержки клиентов. Дополнительное ведение журнала отладки может оказаться полезным при устранении проблем на сервере.

Примечание
Сведения о включении/отключении ведения журнала отладки для определенного сервера шлюза см. в разделе Изменение серверов шлюза.

Что касается версии 7.0 сервера Кибер Файлы, модуль **исключений** удален из списка доступных модулей и всегда включен по умолчанию. Пользователи, запустившие обновление предыдущей версии Кибер Файлы, все еще могут видеть модуль **исключений** в данном списке. После изменения параметров журнала и нажатия кнопки **Сохранить** он исчезнет.

Предупреждение
Эти настройки не следует использовать в обычных рабочих и производственных условиях.

- **Общий уровень ведения журнала отладки** – задает основной уровень сообщений, которые должны регистрироваться в журнале (информационные сообщения, предупреждения, неустранимые ошибки и т. д.)

  Примечание
  Включенные модули отладки всегда регистрируются в журнале на уровне отладки, независимо от установленного общего уровня ведения журнала отладки.

- **Доступные модули отладки** – показывает список доступных модулей.
- **Включенные модули отладки** – показывает активные модули.

Примечание
В случаях когда продукт был обновлен, а не установлен с нуля, файлы журнала будут располагаться в папке C:\Program Files (x86)\Group Logic\Common\apache-tomcat-7.0.42\logs.

Примечание
При чистой установке Кибер Файлы файлы журнала будут располагаться в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\apache-tomcat-7.0.42\logs

10 Задачи по обслуживанию

Примечание
Если требуется создать резервную копию всех элементов Кибер Файлы, прочтите статью Рекомендации по аварийному восстановлению (она также будет полезна для соответствия наилучшим практикам и при совершенствовании процедур резервного копирования).

10.1 Рекомендации по аварийному восстановлению

Высокая доступность и быстрое восстановление совершенно необходимы для критически важных приложений, таких как Кибер Файлы. В связи с ожидаемыми или непредвиденными обстоятельствами (от локальных отказов оборудования и нарушений работы сети до обслуживания по расписанию) может понадобиться подготовить средства восстановления Кибер Файлы до рабочего состояния в крайне сжатые сроки.

10.1.1 Введение.

Для критически важных приложений, таких как Кибер Файлы, крайне совершенно необходима высокая доступность. В связи с различными обстоятельствами (от локальных отказов оборудования и нарушений работы сети до обслуживания по расписанию) может понадобиться подготовить средства восстановления Кибер Файлы до рабочего состояния в крайне сжатые сроки.

Реализовать аварийное восстановление можно различными способами, включая резервное копирование с восстановлением, создание образов, виртуализацию и кластеризацию. Подход, включающий резервное копирование и восстановление, описан в следующих разделах.

10.1.2 Описание элементов Кибер Файлы.

Кибер Файлы – это решение, состоящее из нескольких отдельных, но при этом взаимосвязанных элементов:

Кибер Файлы Сервер шлюза

Примечание
Обычно располагается в папке: C:\Program Files (x86)\Cyberprotect\Cyber Files\Gateway Server

Кибер Файлы Сервер

Примечание
Обычно располагается в папке: C:\Program Files (x86)\Cyberprotect\Cyber Files\Access Server

Кибер Файлы Утилита конфигурации

Примечание
Обычно располагается в папке: C:\Program Files (x86)\Cyberprotect\Cyber Files\Configuration Utility

Хранилище файлов

Местоположение **хранилища файлов** задается в ходе установки при первом запуске **средства конфигурации**.

Примечание
В структуре хранилища файлов содержатся пользовательские файлы и папки в защищенном виде. Можно копировать эту структуру или создавать ее резервные копии с использованием любых стандартных средств копирования файлов (robocopy, xtree). Обычно данная структура должна находиться на сетевом томе с высокой доступностью или NAS, так что ее местоположение может отличаться от устанавливаемого по умолчанию.

База данных **PostGreSQL**. Это отдельный элемент, работающий как служба Windows, который устанавливается и используется программой Кибер Файлы. База данных Кибер Файлы является одним из важнейших элементов, так как в ней содержатся все конфигурации, взаимоотношения между пользователями и файлами, а также метаданные файлов.

Все эти компоненты необходимы для создания работающего экземпляра Кибер Файлы.

10.1.3 Ресурсы, необходимые для реализации процесса быстрого восстановления

Для реализации процесса аварийного восстановления необходимы следующие ресурсы.

- Соответствующее оборудование для размещения операционной системы, приложения и его данных. Оборудование должно соответствовать аппаратным и программным требованиям приложения.
- Процесс резервного копирования и восстановления, гарантирующий наличие и доступность ПО и элементов данных на момент, когда потребуется переключение.
- Подключение к сети, в том числе внутренние и наружные правила брандмауэра и маршрутизации, которые позволяют пользователям получить доступ к новому узлу с минимальными требуемыми изменениями параметров на стороне клиента или вообще без них.
- Сетевой доступ для Кибер Файлы для связи с контроллером домена Active Directory и SMTP-сервером.
- Возможность быстрого или автоматизированного переключения DNS для перенаправления входящего запроса на вторичный узел.

10.1.4 Процесс

Настройка резервного копирования

Рекомендуемый подход к обеспечению быстрого и надежного сценария восстановления можно изложить следующим образом.

1. Разверните установку Кибер Файлы, включая все элементы продукта, на вторичном (восстановленном) узле. Если это невозможно, хорошей альтернативой будет полная резервная копия или образ исходной машины. В виртуализированных средах эффективным и экономным средством показали себя периодические моментальные снимки.
2. Регулярно создавайте резервные копии пакета программного обеспечения Кибер Файлы (всех названных выше элементов, включая всю ветвь ПО Apache). Для этой задачи используйте любое стандартное решение резервного копирования корпоративного класса.
3. Как можно чаще создавайте резервные копии хранилища файлов (FileStore). Можно использовать стандартное решение резервного копирования, но хорошей, часто предпочтительной альтернативой будет автоматизированное средство дифференциального копирования (учитывая большой объем данных). Дифференциальное копирование минимизирует время выполнения операции, так как обрабатываются лишь различия между исходным и целевым файловыми хранилищами.
4. Как можно чаще создавайте резервные копии базы данных Кибер Файлы. Для них сценарий автоматизированной выгрузки базы данных, который запускается планировщиком задач Windows, создает дамп базы данных. После этого следует создать резервную копию дампа базы данных с помощью стандартного средства резервного копирования.

Восстановление

При том условии, что обеспечены и реализованы описанные выше в этом разделе условия, процесс перевода ресурсов резервного копирования в рабочий режим («в сети») относительно прост.

1. Запустите узел восстановления. При необходимости измените такие сетевые настройки, как IP-адрес и имя хоста. Проверьте подключение к Active Directory и доступ к SMTP.
2. При необходимости восстановите самую новую резервную копию пакета программного обеспечения Кибер Файлы.
3. Убедитесь, что Tomcat не запущен (панель управления Windows/«Службы»).
4. При необходимости восстановите хранилище FileStore. Убедитесь, что относительный путь к хранилищу FileStore такой же, как был на исходном компьютере. Если это не так, потребуется изменить местоположение с помощью средства конфигурации.
5. Убедитесь, что служба PostgreSQL не запущена (Панель управления Windows/«Службы»).
6. Восстановите базу данных Кибер Файлы.
7. Запустите службу Кибер Файлы Tomcat.
8. Перенесите DNS, чтобы запись указывала на новый узел.
9. Проверьте работу Active Directory и SMTP.

10.2 Рекомендации

10.2.1 1. Регулярно создавайте резервные копии базы данных

Плановое резервное копирование базы данных – один из важнейших аспектов управления Кибер Файлы. Процесс резервного копирования может быть полностью автоматизирован, что поможет поддерживать актуальность резервных копий.

Для развернутых систем с очень большими базами данных сервера Кибер Файлы может применяться другой метод резервного копирования и восстановления.

Установки с базами данных на несколько гигабайт и более могут потребовать дополнительной настройки во время **резервного копирования и восстановления**, чтобы ускорить или оптимизировать процесс.

10.2.2 2. В очень больших развертываниях рекомендуется выполнять чистку и анализ баз данных ежемесячно

Базам данных PostgreSQL требуется периодическое обслуживание, также называемое чисткой. Команда **VACUUM** должна регулярно обрабатывать каждую таблицу, чтобы:

- восстанавливать или повторно использовать дисковое пространство, занятое удаленными или обновленными строками;
- защищать от потери очень старых данных;
- обновлять статистику данных и ускорять сканирование индекса.

Команда **ANALYZE** собирает статистику по содержимому таблиц в базе данных и сохраняет результаты. Эту статистику впоследствии использует планировщик запросов для определения наиболее эффективных планов выполнения запросов.

Для чистки и анализа базы данных вручную выполните следующие действия.

1. Откройте программу Кибер Файлы PostgreSQL Administrator (также может называться PgAdmin). Оно находится в меню «Пуск» Windows в папке Кибер Файлы. Дважды щелкните **localhost** для подключения к серверу.
2. Щелкните правой кнопкой по базе данных cyberfiles_production и выберите **Обслуживание**.
3. Выберите **ЧИСТКА** и установите для параметра **АНАЛИЗ** значение «Да».

   Предупреждение
   Чистка может занять некоторое время. Этот процесс следует запускать в периоды низкой загрузки сервера.

4. Нажмите кнопку**OK**.

5. После завершения процесса **чистки** нажмите кнопку **Готово**.
6. Закройте средство PostgreSQL Administrator.

Чтобы настроить автоматическую чистку, прочитайте нашу статью: Автоматическая чистка базы данных

10.2.3 3. Для больших установок можно запустить настройку с балансировкой нагрузки или кластеризацию серверов шлюза.

10.3 Резервное копирование и восстановление Кибер Файлы

Если необходимо выполнить обновление, повышение версии или обслуживание сервера Кибер Файлы. В этой статье содержатся основные сведения о резервном копировании и восстановлении базы данных. Для конфигураций с балансировкой нагрузки процесс практически идентичен обычному резервному копированию и восстановлению. Все особенности будут добавлены на соответствующих этапах.

Примечание
Если база данных сервера Кибер Файлы слишком большая, на несколько гигабайтов, может потребоваться другой метод резервного копирования и восстановления. За помощью и инструкциями обратитесь в службу технической поддержки по адресу https://cyberprotect.ru/support.

Примечание
В отказоустойчивом кластере Microsoft некоторые пути могут различаться, но процесс резервного копирования будет одинаковым. Он должен выполняться на активном узле, и следует убедиться, что роль не выполнит отработки отказа и запуска во время резервного копирования.

Настоятельно рекомендуется сначала выполнить резервное копирование / восстановление в тестовой среде, а затем приступать к резервному копированию/восстановлению производственной среды.

10.3.1 Резервное копирование базы данных Кибер Файлы

1. Остановите службу Кибер Файлы Tomcat.

   Примечание
   Если применяется балансировка нагрузки для нескольких служб Cyber Files Tomcat, остановите их все.

2. Откройте Кибер Файлы PostgreSQL Administrator. Оно находится в меню «Пуск» Windows в папке Кибер Файлы. Подключитесь к серверу базы данных. Может потребоваться ввести пароль для пользователя postgres .
3. Разверните раздел **Базы данных** и щелкните правой кнопкой базу данных cyberfiles_production.
4. Выберите **Обслуживание**.
5. Выберите **ЧИСТКА** и установите для параметра **АНАЛИЗ** значение «Да».
6. Нажмите кнопку **OK**.
7. Разверните базу данных, раздел **Схемы** и раздел **Общедоступные**. Обратите внимание на число в разделе **Таблицы** . Это может помочь удостовериться в успешности восстановления базы данных.
8. Закройте средство PostgreSQL Administrator и откройте командную строку с повышенными привилегиями.
9. В командной строке перейдите в каталог PostgreSQL, **например,**"C:\Program Files(x86)\Cyberprotect\Cyber Files\Common\PostgreSQL\<version>\bin"

   Примечание
   Необходимо будет изменить путь, чтобы он указывал на папку PostgreSQL, если это старая или выборочная установка (например, C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\PostgreSQL\9.4\bin\).

10. Введите следующую команду: pg_dumpall --host localhost --port 5432 --username postgres --file alldbs.sql
    - alldbs.sql будет именем файла резервной копии, сохраненной в каталоге bin PostgreSQL. Вы можете использовать путь в приведенной выше команде, если хотите сохранить его в другом месте, например, измените последнюю часть приведенной выше команды следующим образом: --file D:\Backups\alldbs.sql
    - Если используется порт, отличный от порта по умолчанию, замените 5432 на нужный номер порта.
    - Если вы по умолчанию не используете учетную запись администратора PSQL postgres, то в приведенной выше команде измените postgres на имя вашей учетной записи администратора.
    - В процессе этого вам потребуется несколько раз ввести пароль пользователя postgres . При каждом запросе вводите пароль и нажимайте клавишу «Ввод».

    Примечание
    Ввод пароля никак не отражается в окне командной строки.

11. Скопируйте файл резервной копии в надежное место.
12. Перейдите к файлу postgresql.conf и скопируйте его в безопасное место, так как он может содержать важные настройки. Он по умолчанию находится в базовой папке PostgreSQL C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\PostgreSQL\<version>\Data.

10.3.2 Резервное копирование базы данных сервера шлюза

1. Остановите службу шлюза Кибер Файлы.
2. Перейдите в папку базы данных сервера шлюза, по умолчанию расположенную в C:\Program Files (x86)\Cyberprotect\Cyber Files\Gateway Server\database
3. Скопируйте файл mobilEcho.sqlite3 в надежное место.
4. Если у вас несколько серверов шлюза, повторите этот процесс для каждого и проследите, чтобы файлы баз данных не перепутались.

10.3.3 Дополнительные файлы для резервного копирования

Если вы вносили изменения в любые из этих файлов, рекомендуется создать резервные копии, чтобы перенести ваши настройки при восстановлении или переносе программы Кибер Файлы.

Файл postgresql.conf, так как он может содержать важные настройки для базы данных. Как правило, он находится в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\PostgreSQL\<version>\Data.

- Файл web.xm по умолчанию расположен в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Access Server\Web Application\WEB-INF\. Содержит настройки единого входа.
- Файл server.xml по умолчанию расположен в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\apache-tomcat-<version>\conf. Содержит настройки Tomcat.
- Файл krb5.conf по умолчанию расположен в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\apache-tomcat-<version>\conf. Содержит настройки единого входа.
- Файл login.conf по умолчанию расположен в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\apache-tomcat-<version>\conf.
- Ваши сертификаты и ключи, используемые для Кибер Файлы.
- Файл cyberfilessrv.cfg по умолчанию расположен в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Access Server.
- Пользовательские цветовые схемы по умолчанию расположены в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Access Server\Web Application\customizations\.
- Файл pg_hba.conf по умолчанию расположен в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\PostgreSQL\<version>\Data.

10.3.4 Восстановление базы данных Кибер Файлы

1. Откройте на панели управления оснастку **Службы** и остановите службу Кибер Файлы Tomcat.

Примечание
Для конфигураций с балансировкой нагрузки остановите все службы Кибер Файлы Tomcat.

2. Откройте приложение Кибер Файлы PostgreSQL Administrator, подключитесь к локальному серверу базы данных, выберите **Базы данных** и проверьте наличие базы с именем cyberfiles_production.
3. Щелкните базу данных правой кнопкой и выберите **Обновить**.
4. Разверните ее, разверните раздел **Схемы**, затем раздел **Общедоступные** и убедитесь, что раздел **Таблицы** содержит ноль (0) элементов.
   - Если база данных содержит таблицы, щелкните по ней правой кнопкой и переименуйте в oldcyberfiles_production. Затем перейдите в **Базы данных**, щелкните правой кнопкой и создайте новую базу данных с именем cyberfiles_production.
5. Закройте PostgreSQL Administrator и откройте командную строку с повышенными привилегиями.
6. В командной строке перейдите в папку bin PostgreSQL.
   например, cd "C:\Program Files\Cyberprotect\Cyber Files\Common\PostgreSQL\<version>\bin"
7. Скопируйте файл резервной копии базы данных alldbs.sql (или с другим именем, выбранным вами) в папку **bin**.
8. В командной строке введите следующую команду: psql -U postgres -f alldbs.sql
9. Введите пароль postgres в ответ на запрос.

   Примечание
   Восстановление может занять много времени в зависимости от размера базы данных.

10. После завершения восстановления закройте окно командной строки.
11. Снова откройте приложение Кибер Файлы PostgreSQL Administrator и подключитесь к локальному серверу базы данных.
12. Выберите **Базы данных**.
13. Разверните базу данных cyberfiles_production, раздел **Схемы** и раздел **Общедоступные**. Убедитесь, что **Таблицы** содержат такое же число элементов, как на шаге 5 раздела «Создайте резервную копию базы данных сервера Кибер Файлы».

Примечание
Если версия сервера Кибер Файлы, на который восстанавливается база данных, новее версии из резервной копии базы данных и служба Кибер Файлы Tomcat уже запущена, то количество таблиц в новой базе данных сервера Кибер Файлы может быть больше, чем во время создания резервной копии.

10.3.5 Восстановление базы данных сервера шлюза

1. Остановите службу шлюза Кибер Файлы.
2. Скопируйте файл резервной копии базы данных сервера шлюза mobliEcho.sqlite3 в новую папку базы данных (по умолчанию C:\Program Files (x86)\Cyberprotect\Cyber Files\Gateway

Server\database), заменив существующий файл.

3. Повторите эту процедуру для всех серверов шлюза.

10.3.6 Восстановление дополнительных файлов и настроек

Не забудьте скопировать все изменения, сделанные в файлах конфигурации Кибер Файлы (web.xml, server.xml, krb5.conf, сертификаты, пользовательские цветовые схемы, шаблоны электронной почты, pg_hba.conf или newrelic.yml), и перенести их в новые файлы.

10.3.7 Тестирование восстановленного сервера Кибер Файлы

Успешно выполнив резервное копирование/восстановление или перенос данных на другую машину, нужно возобновить работу Кибер Файлы и проверить, что все параметры правильные.

10.3.7.1 Возобновление работы обычной установки

1. Запустите средство конфигурации Кибер Файлы и проверьте правильность всех указанных там настроек.
2. Нажмите кнопку «OK», чтобы запустить все службы.
3. Это должно возобновить работу всех служб одновременно и восстановить все функциональные возможности Кибер Файлы.
4. Если какие-либо компоненты находятся на другой машине, перейдите на эту машину и запустите их. В этом случае служба PostgreSQL должна работать, чтобы служба Кибер Файлы Tomcat запустилась без ошибок.

10.3.7.2 Возобновление работы установки с балансировкой нагрузки

1. Выберите один из серверов Кибер Файлы в качестве основного. Он будет основным только в том смысле, что будет подключен первым.
2. Если служба PostgreSQL расположена на другой машине, сначала запустите ее, поскольку это повлияет на сервер Кибер Файлы.
3. Перейдите на машину основного сервера Кибер Файлы и запустите средство конфигурации Кибер Файлы.
4. Убедитесь, что все параметры правильные. Если все в порядке, нажмите кнопку «OK», чтобы запустить все службы.
5. Откройте веб-консоль Кибер Файлы и выполните вход от имени администратора. Проверьте, что все параметры правильные.
6. Проверив параметры, перейдите к каждой машине с установленным компонентом Кибер Файлы и запустите его через средство конфигурации.

10.4 Управление журналом Tomcat в Windows

В рамках нормальной работы Tomcat создает ряд файлов журналов и записывает в них данные.

Если их не очищать периодически, такие файлы накапливаются и занимают ценное дисковое пространство. В ИТ-сообществе считается общепринятым, что со временем информационная ценность этих журналов быстро падает. Если не вступают в силу другие факторы, такие как нормативное требование или выполнение определенных политик, то самым разумным будет сохранять эти файлы журналов в системе в течение некоторого числа дней.

10.4.1 Введение

В рамках нормальной работы Tomcat создает ряд файлов журналов и записывает в них данные. В Windows эти файлы обычно находятся в следующем каталоге:

“C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\apache-tomcat-7.0.34\logs»
Кибер Файлы сохраняет собственные журналы в том же каталоге, что и отдельные файлы.

Примечание
Файлы журнала Кибер Файлыполучают имена вида **cyberfiles_date**.

Существует много средств, способных автоматизировать задачу удаления ненужных файлов журнала. Например, можно воспользоваться встроенной в Windows командой ForFiles.

Примечание
Сведения о ForFiles, синтаксис команды и примеры использования см. в статье http://technet.microsoft.com/en-us/library/cc753551(v=ws.10).aspx

10.4.2 Пример процесса

Описанный ниже пример процесса автоматизирует очистку файлов журнала, которые старше некоторого числа дней. В образце пакетного файла это число определено как параметр, чтобы его можно было изменять в соответствии с различными политиками сохранения данных.

Примечание
Образец сценария (пакетного файла) предназначен для работы в Windows 2008. Щелкните здесь, чтобы загрузить сценарий.
Также можно скопировать код сценария, вставить его в пустой текстовый документ и сохранить под именем AASTomcatLogPurge.bat.

Полный код пакетного сценария:

```
ECHO OFF

REM Script: aETomcatLogsPurge.bat

REM 2012-05-12: Version: 1.0: MEA: Created

ECHO Этот сценарий удаляет из указанного каталога файлы, созданные раньше заданного количества дней назад

ECHO Он запускается из командной строки или из планировщика

ECHO У этого процесса должны быть разрешения на удаление файлов в целевой папке
```

```
REM ===== КОНФИГУРАЦИЯ ==================================================

REM Примечание. Все пути, в которых есть пробелы, должны быть заключены в двойные кавычки

REM Измените этот файл и задайте значения LogPath и NumDays ниже

REM Путь к папке, в которой находятся все журналы Tomcat

set LogPath="C:\Program Files (x86)\Group Logic\Common\apache-tomcat-7.0.34\logs"

REM NumDays – файлы журнала старше NumDays будут обрабатываться

set NumDays=14

REM ===== КОНЕЦ КОНФИГУРАЦИИ
==========================================================

ECHO

ECHO ===== НАЧАЛО ============

REM Параметры ForFiles:

REM "/p": путь к папке, в которой требуется удалять файлы.

REM "/s": просматривать все папки, вложенные в папку, указанную в пути пакетного файла

REM "/d": удалять файлы, которые старше текущей даты минус это число дней. Например, "/d -7" означает старше 7 дней назад

REM "/c": команда, выполняемая для фактического удаления файлов: "cmd /c del @file".

forfiles /p %LogPath% /s /d -%NumDays% /c "cmd /c del @FILE"

:End

ECHO ===== ПАКЕТНЫЙ ФАЙЛ ЗАВЕРШЕН
============================================
```

Предупреждение

Этот пример предоставляется как общая рекомендация, чтобы вы могли спланировать и реализовать собственный процесс, учитывающий специфику вашего развертывания. Пример не предназначен для использования во всех ситуациях и средах, не тестировался в них, поэтому использовать его следует только в качестве основы. Вы используете пример на собственный страх и риск. **Не используйте его в рабочих средах, не проведя сначала всестороннее испытание в автономном режиме.**

10.4.3 Шаги

1. Скопируйте этот сценарий на компьютер, на котором выполняется Кибер Файлы (Tomcat), и откройте его в Блокноте или другом подходящем редакторе обычных текстовых файлов.

2. Найдите раздел, показанный на рисунке ниже, и измените переменные LogPath и NumDays, указав конкретные путь и настройки сохранения:

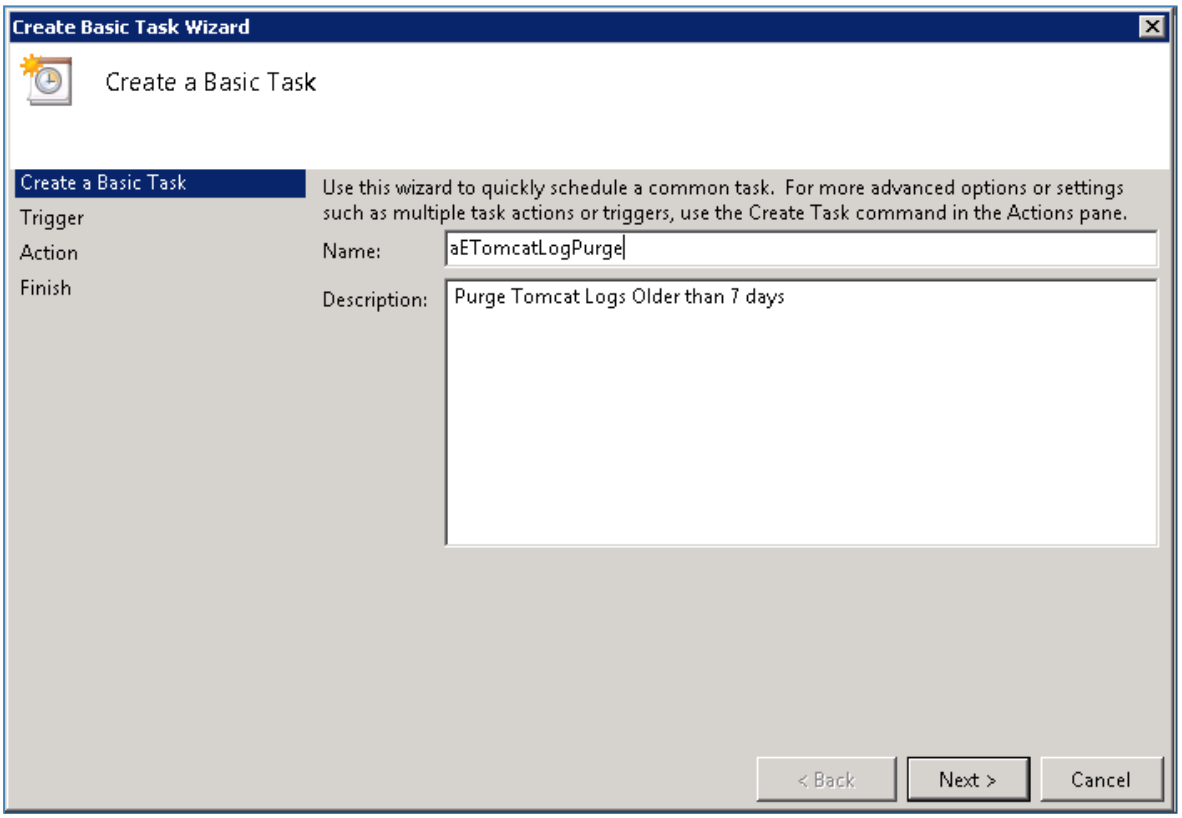
```
REM ===== CONFIGURATIONS ================================================
REM Note: all paths containing spaces must be enclosed in double quotes
 REM Edit this file and set LogPath and NumDays below
REM Path to the folder where all Tomcat logs are
 set LogPath="C:\Program Files (x86)\Group Logic\Common\apache-tomcat-7.0.34\logs"

REM NumDays - Log files older than NumDays will be processed
 set NumDays=14
REM ===== END OF CONFIGURATIONS ======================
ECHO
ECHO ===== START ============
```

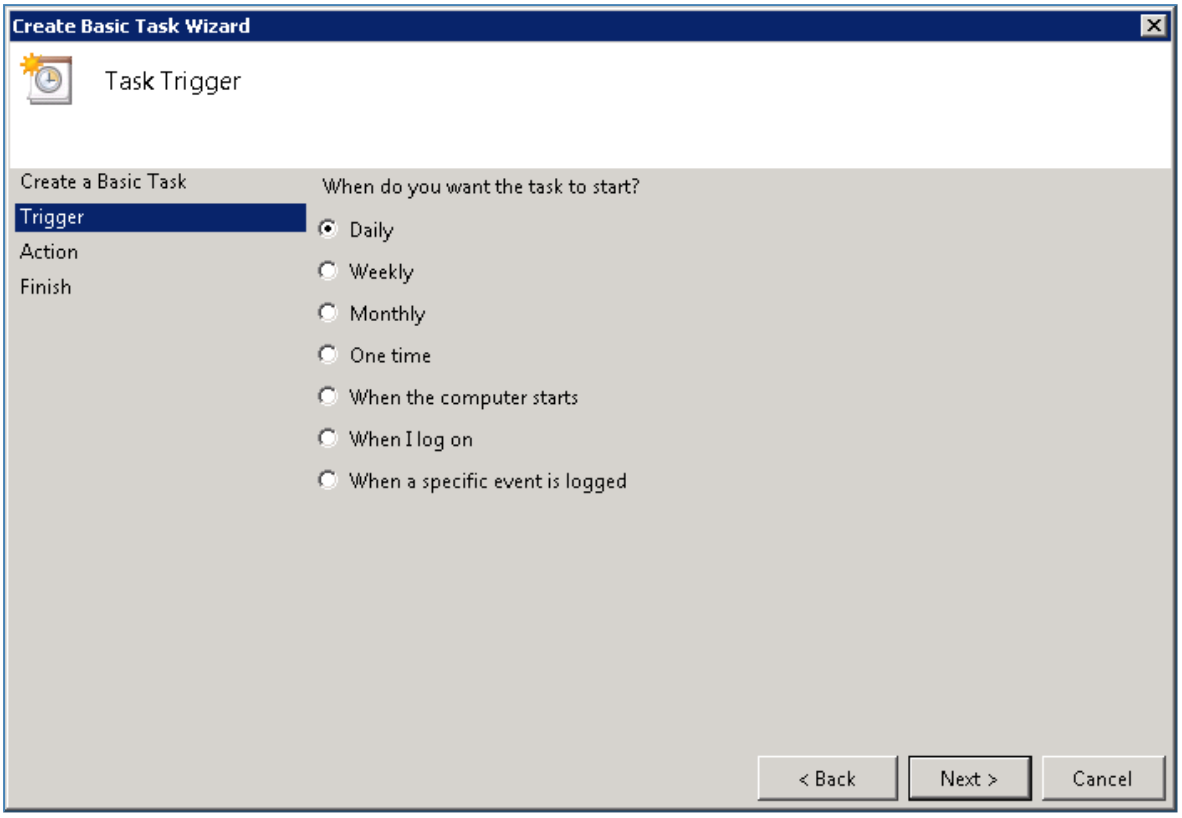
Примечание

В Кибер Файлы файлы журналов хранятся в той же папке, что и файлы журналов Tomcat. (C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\apache-tomcat-7.0.34\logs)

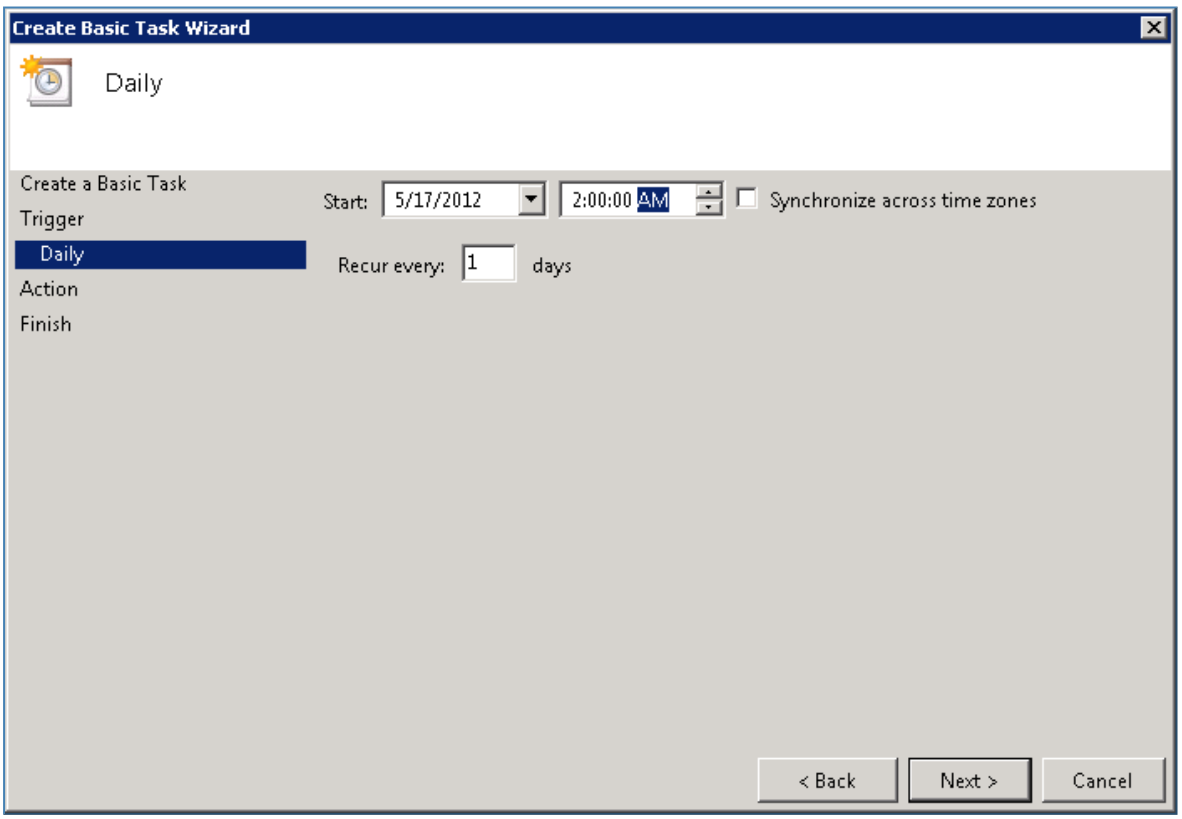
3. Сохраните файл.
4. Чтобы автоматизировать процесс, откройте **планировщик задач** и создайте новую задачу. Определите имя и описание задачи.



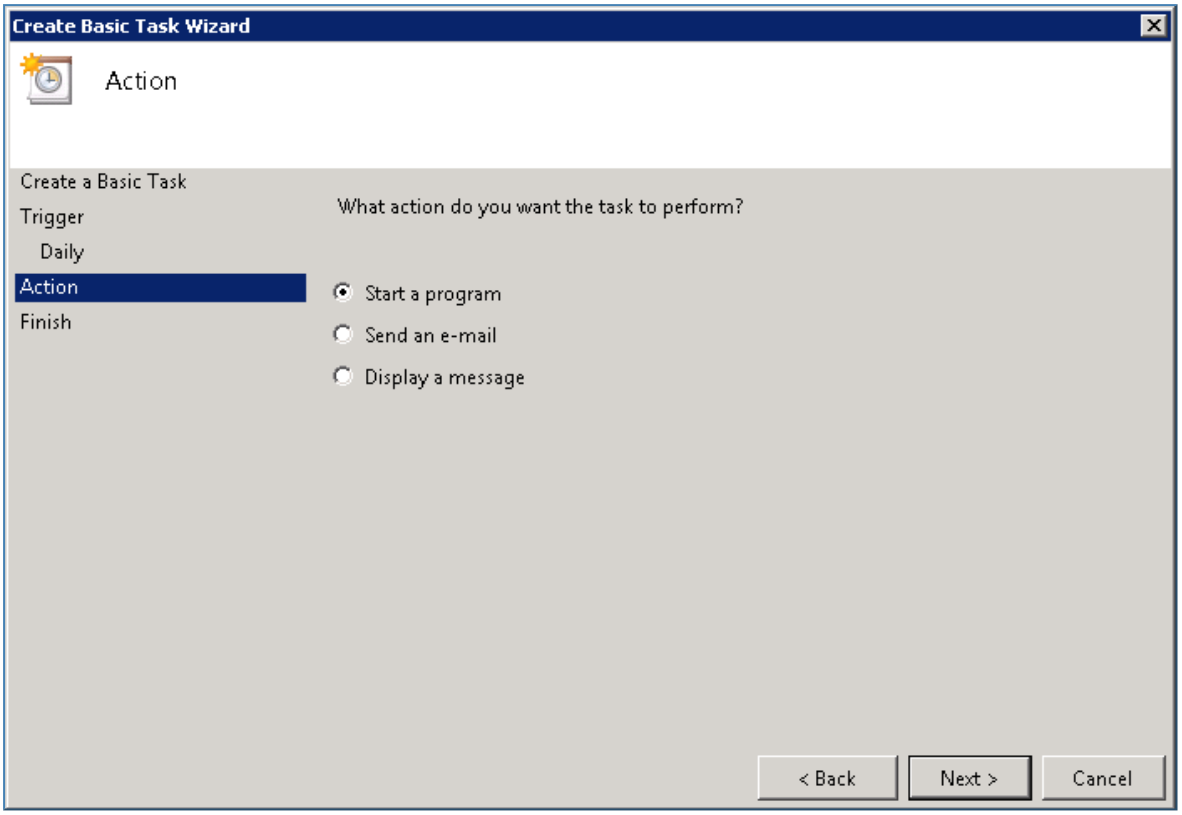
5. Настройте задачу на ежедневное выполнение.



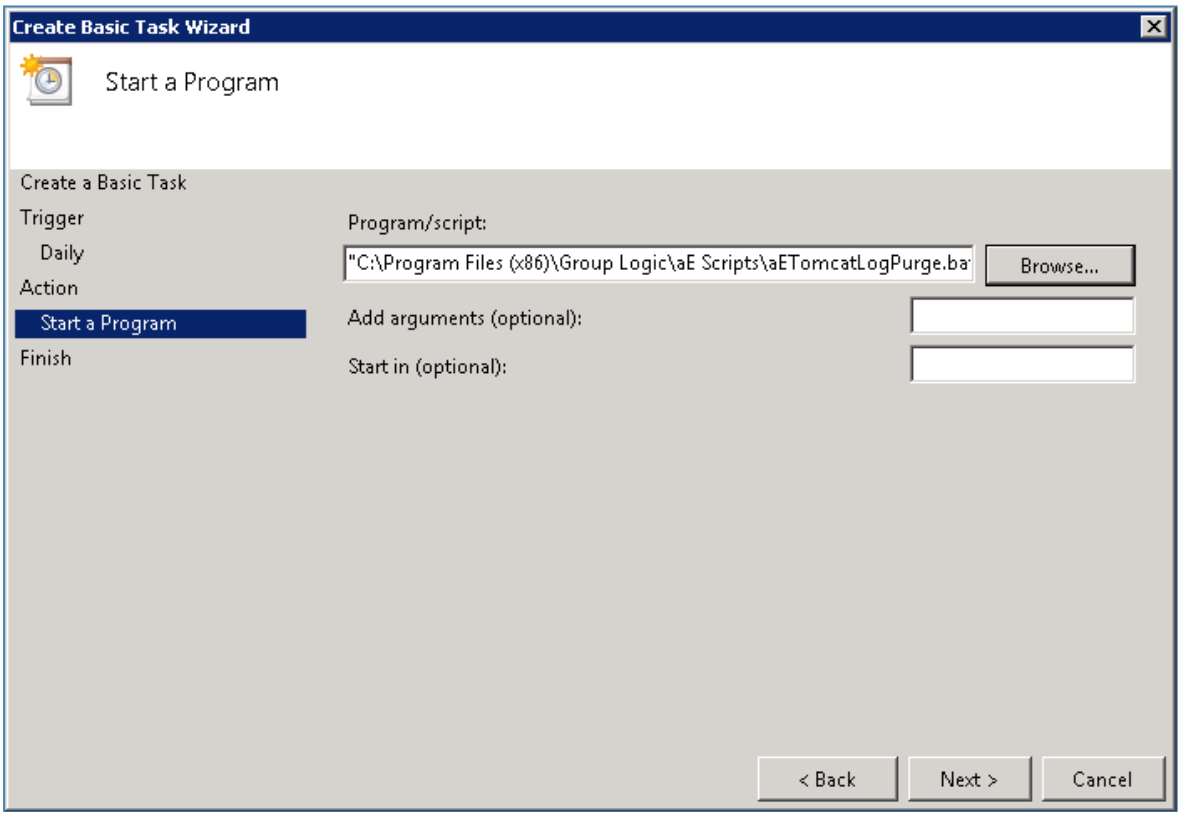
6. Определите, в какое время должна запускаться задача. Рекомендуется запускать процесс в то время, когда система не испытывает значительной нагрузки и не выполняются другие процессы по обслуживанию.



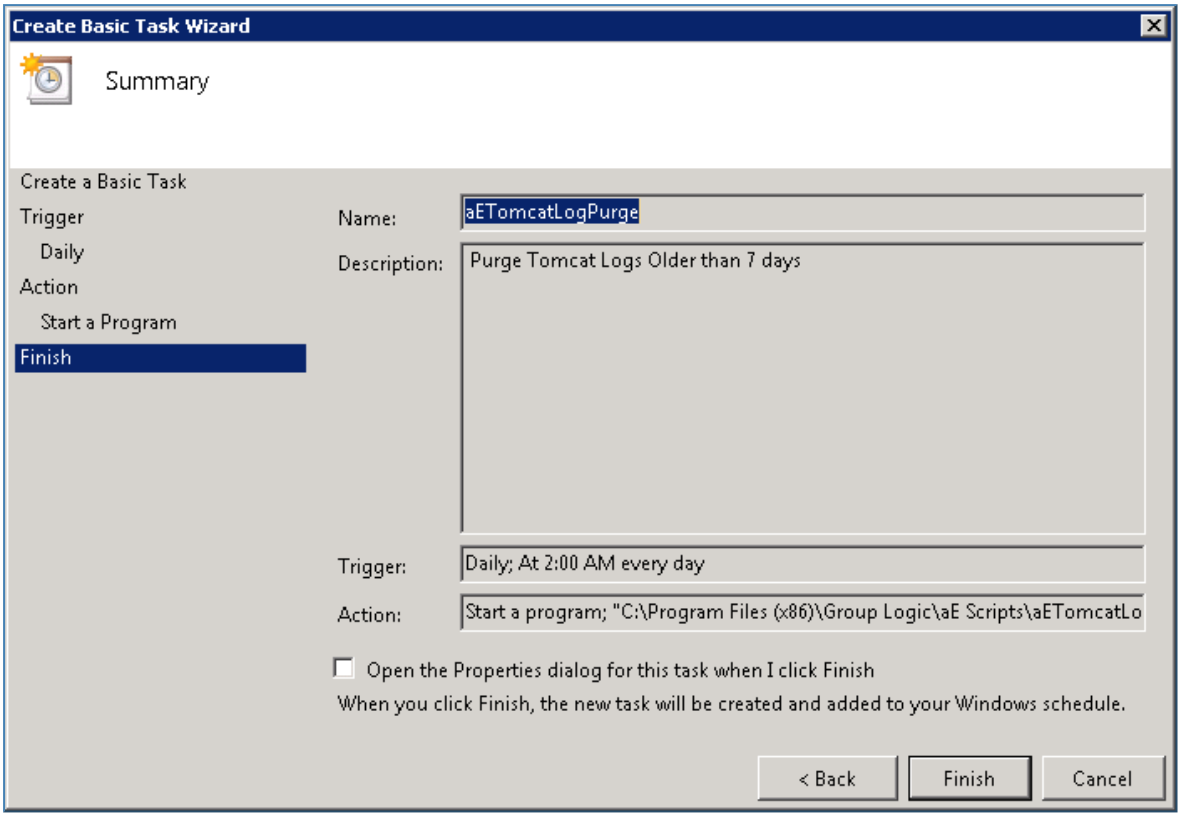
7. Установите тип действия «**Запуск программы**».



8. Нажмите кнопку **Обзор**, перейдите к файлу сценария (пакетному файлу) и выберите его.



9. Затем нажмите кнопку **Готово**.



10. В списке задач можно щелкнуть по задаче правой кнопкой мыши, выбрать пункт «Свойства» и проверить, будет ли задача выполняться и при вошедшем в систему пользователе, и без него (для автоматической работы без участия пользователя).
11. Можно проверить правильность настройки и выполнения задачи, выбрав задачу, щелкнув по ней правой кнопкой мыши и выбрав «Запуск». В журнале планировщика должны регистрироваться запуск, останов и любые возможные ошибки.

10.5 Автоматическое резервное копирование базы данных

С помощью планировщика задач Windows можно легко настроить график автоматического резервного копирования базы данных Кибер Файлы.

10.5.1 Создание сценария резервного копирования базы данных

1. Откройте **Блокнот** (или другой текстовый редактор) и введите следующее:

```
@echo off
```

```
for /f "tokens=1-4 delims=/ " %%i in ("%date%") do (
```

```
set dow=%%i
set month=%%j
set day=%%k
set year=%%l
)
set datestr=%month%_%day%_%year%
echo datestr is %datestr%
set BACKUP_FILE=AAS_%datestr%_DB_Backup.sql
echo backup file name is %BACKUP_FILE%
SET PGPASSWORD=password
echo on
bin\pg_dumpall -U postgres -f %BACKUP_FILE%
move "%BACKUP_FILE%" "C:\destination folder"
```

2. Замените «**password**» паролем пользователя **postgres** , заданным вами при установке Кибер Файлы.
3. Замените **C:\destination folder** на путь к папке, где следует сохранять резервные копии.
4. Сохраните файл как **DatabaseBackup.bat** (расширение должно быть таким, это важно) и выберите **Все файлы** в качестве типа файла.
5. Переместите файл в папку установки PostgreSQL, расположенную в каталоге с номером версии (например, \9.3\).

10.5.2 Создание запланированной задачи

1. Войдите на **панель управления** и выберите **Администрирование**.
2. Откройте **Планировщик заданий**.
3. Щелкните **Действие** и выберите **Создать задачу**.

На вкладке Общие:

1. Введите название и описание задачи (например, AAS Database Backup).
2. Установите флажок **Выполнять для всех пользователей**.

На вкладке Триггеры:

1. Нажмите **Создать**.
2. Выберите **По расписанию** в поле «Начать задачу».
3. Выберите вариант «Ежедневно» и укажите время запуска сценария и количество повторных запусков (как часто следует делать резервную копию базы данных).
4. Выберите **Включено** в разделе **Дополнительные параметры** и нажмите кнопку **OK**.

На вкладке Действия:

1. Нажмите **Создать**.
2. Выберите **Запуск программы** в поле **Действие**.
3. Рядом с полем **Программа или сценарий** нажмите кнопку **Обзор**, после чего найдите и выберите файл **DatabaseBackup.bat**.
4. В поле **«Рабочая папка (не обязательно)»** введите путь к папке, в которой находится сценарий. Например, если путь к сценарию – C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\PostgreSQL\9.3\PSQL.bat, то введите C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\PostgreSQL\9.3\
5. Нажмите кнопку**OK**.
6. Настройте по необходимости дополнительные параметры на других вкладках и нажмите кнопку **OK**.
7. Вам будет предложено указать учетные данные для текущей учетной записи.

10.6 Автоматическая чистка базы данных

Это руководство поможет создать задание, которое будет запускаться и чистить базу данных PostgreSQL по расписанию. Чистка – важный процесс, особенно в установках с большими базами данных (несколько гигабайт).

Примечание
Автоматическая чистка PostgreSQL задана в файле конфигурации. В установках с высокой загрузкой автоматическая чистка может никогда не выполняться, поскольку она не запускается при высокой загрузке сервера. В таких случаях рекомендуется создать запланированное задание для запуска чистки как минимум раз в месяц.

10.6.1 Настройка PostgreSQL и создание сценария

Проверка возможности запуска задания

Убедитесь, что пароль пользователя postgres сохранен в файл pgpass, иначе сценарий не запустится. Проще всего это сделать с помощью средства Кибер Файлы PostgreSQL Administrator.

1. Откройте Кибер Файлы PostgreSQL Administrator. Оно находится в меню «Пуск» Windows в папке Кибер Файлы.
2. Подключитесь к базе данных, в диалоговом окне ввода пароля установите флажок **Сохранить пароль** и нажмите кнопку **OK**. Таким образом пароль пользователя postgres будет сохранен в файл pgpass. Этот файл будет создан в папке C:\Users\<currentUser>\AppData\Roaming\postgresql.

   Примечание
   Может отобразиться диалоговое окно с информацией о сохранении паролей – это нормальное поведение программы. Нажмите кнопку**OK**.

   - Либо можно вручную создать файл с именем **pgpass.conf** и ввести в него следующий текст: localhost:5432:*:postgres:yourpassword
   - Обязательно введите **действующий** пароль пользователя postgres и правильный порт. Сохраните файл.
3. В этом примере мы скопируем файл **pgpass.conf** и поместим копию в папку **D:\Backup**. У пользователя, запускающего запланированное задание, должен быть доступ для чтения файла.

Создание сценария

В приведенном здесь примере путь к каталогу PostgreSQL задан как C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\PostgreSQL\<VERSION>\bin\.

Примечание
Примечание. Необходимо будет изменить путь, чтобы он указывал на папку PostgreSQL , если это старая или выборочная установка (например, C:\Program Files (x86)\Cyberprotect\Access\Common\PostgreSQL\9.4\bin\).

1. Создайте папку для хранения файлов журнала и предоставьте пользователю, запускающему задание, разрешения на чтение, запись и выполнение для этой папки. Рекомендуем выбрать учетную запись администратора этой машины. В нашем примере журналы будут храниться в папке D:\Backup\.
2. Откройте любой текстовый редактор (например, Блокнот) и вставьте следующий образец сценария.

   ```
   SET PGPASSFILE=D:\Backup\pgpass.conf
   "C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\PostgreSQL\9.4\bin\psql.exe" --
   ```

host=localhost --port 5432 --username=postgres -d cyberfiles_production -c "VACUUM VERBOSE ANALYZE" >"D:\Backup\vacuum_report_%date:/=.%.log" 2>&1

3. Измените сценарий в соответствии со своей установкой.
   - Измените путь к файлу psql.exe на фактический путь к нему.
   - Измените параметр --port на нужный номер порта, если вы меняли значение по умолчанию.
   - Если вы выбрали другого пользователя PostgreSQL, измените параметр --username=, поменяв postgres на имя нужного пользователя.
   - Измените часть пути к папке журналов D:\Backup\ на путь к нужной папке.
   - Измените часть пути к папке журналов D:\Backup\ на фактический путь к файлу pgpass.conf.
4. Сохраните файл как **vacuum.bat**. Не забудьте выбрать **Все типы** в поле **Тип файла** при сохранении.

Примечание
С некоторыми форматами даты может возникать ошибка при создании файла **.log**. Чтобы узнать формат даты, можно открыть командную строку и выполнить команду: echo %date%. Если в дате используются недопустимые символы, такие как косая черта, их необходимо преобразовать. В приведенном выше примере дополнительная часть :/=. выполняет преобразование. При возникновении проблем обратитесь в службу поддержки пользователей Cyberprotect.

10.6.2 Настройка планировщика заданий

1. Откройте **Планировщик заданий** из раздела **Панель управления** -> **Администрирование** - > **Планировщик заданий**.
2. Щелкните правой кнопкой мыши **Планировщик заданий (локальный)** и выберите **Создать задачу**.
3. На вкладке **Общие**.
   - Введите **Имя** и **Описание**.
   - Выберите **Выполнять для всех пользователей**.
   - Задайте **учетную запись пользователя**, от имени которого будет запускаться задание. Рекомендуется использовать учетную запись NETWORK SERVICE этой машины.
4. На вкладке **Триггеры**:
   - Нажмите кнопку **Создать** и задайте расписание для запуска чистки. Это должен быть период низкой загрузки сервера. Рекомендуется выполнять чистку как минимум раз в месяц.
5. На вкладке **Действия** :
   - Нажмите кнопку **Создать** и в разделе **Действие** выберите **Запуск программы**.
   - В поле **Программа или сценарий** введите cmd.exe
   - В поле **Добавить аргументы** введите: /c "C:\Scripts\vacuum.bat"

Примечание
Не забудьте изменить путь в этой команде на фактический путь к файлу vacuum.bat.

- На вкладках **Условия** и **Параметры** оставьте настройки по умолчанию.
- Нажмите кнопку **OK** , чтобы сохранить новое задание. Может появиться запрос на ввод пароля администратора.

Убедитесь, что задание работает нормально

1. Запустите чистку вручную из планировщика заданий, чтобы протестировать задание и убедиться, что файл журнала записывается в нужную папку.
2. Убедитесь, что запланированное задание запускается в указанное время.

10.7 Миграция Кибер Файлы на тот же сервер

Это руководство поможет перенести экземпляр Кибер Файлы на текущие машины.

Внимание
Перед переносом рабочих серверов настоятельно рекомендуется выполнить эти шаги в тестовой среде. Тестовое развертывание должно иметь ту же архитектуру, что и рабочие серверы, а также пару тестовых пользовательских компьютеров и мобильных клиентов, чтобы обеспечить совместимость в рабочей среде.

10.7.1 Перед началом миграции на тот же сервер

Предупреждение
Настоятельно рекомендуется выполнить тестовое резервное копирование/восстановление вне рабочей среды.

Выполните следующее:

- Обратите внимание расположены ли веб-сервер Кибер Файлы, PostgreSQL, шлюз и репозиторий файлов на одном компьютере.
- Запишите DNS, IP-адрес и порт веб-сервера Кибер Файлы.
- Запишите DNS, IP-адрес и порт сервера шлюза.
- Запишите адрес и порт файлового репозитория.
- Запишите местоположение хранилища файлов.
- Запишите номер версии PostgreSQL текущего сервера.
  Простейший способ сделать это – посмотреть на имя папки внутри главного каталога PostgreSQL (по умолчанию это каталог C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\PostgreSQL), имя внутренней папки содержит старший номер версии PostgreSQL (например, **9.2**; **9.3**; **9.4**).

Примечание
Большую часть этой информации можно найти в программе настройки.

Базовые этапы процесса миграции на тот же сервер

Перед началом переноса убедитесь, что все готово к выполнению этих шагов.

1. Создайте резервную копию PostgreSQL.
2. Создайте резервную копию базы данных сервера шлюза.
3. Создайте резервную копию нескольких дополнительных файлов.
4. Удалите Киберпротект Кибер Файлы.
5. Удалите каталог данных PostgreSQL.
6. [Необязательно] Удалите Java.
7. Установите Кибер Файлы с помощью установщика той же версии, которая была удалена.
8. Восстановите базу данных сервера шлюза.
9. Настройте сервер.
10. Проверьте административные настройки Кибер Файлы.
11. Проведите тестирование новой конфигурации.

10.7.2 Перенос Кибер Файлы

Как перенести Кибер Файлы

1. ***Создайте резервную копию PostgreSQL***
   a. Откройте на панели управления оснастку **Службы** и остановите службу Кибер Файлы Tomcat.
   b. Откройте средство Кибер Файлы PostgreSQL Administrator. Оно находится в меню «Пуск» Windows в папке Кибер Файлы. Подключитесь к серверу базы данных. Может потребоваться ввести пароль для пользователя postgres .
   c. Разверните раздел **Базы данных** и щелкните правой кнопкой базу данных cyberfiles_ production.
   d. Выберите **Обслуживание**.
   e. Выберите **ЧИСТКА** и установите для параметра **АНАЛИЗ** значение «Да».
   f. Нажмите кнопку**OK**.
   g. Разверните базу данных, раздел **Схемы** и раздел **Общедоступные**. Обратите внимание на число в разделе **Таблицы** . Это может помочь удостовериться в успешности восстановления базы данных.
   h. Закройте средство PostgreSQL Administrator и откройте командную строку с повышенными привилегиями.

i. В командной строке перейдите в папку bin PostgreSQL.

например, cd "C:\Program Files(x86)\Cyberprotect\Cyber Files\Common\PostgreSQL\<version>\bin"

Примечание

Примечание. Необходимо будет изменить путь, чтобы он указывал на папку PostgreSQL, если это старая или выборочная установка (например, C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\PostgreSQL\9.4\bin\).

j. Введите следующую команду: pg_dumpall --host localhost --port 5432 --username postgres --file alldbs.sql

- alldbs.sql будет именем файла резервной копии, сохраненной в каталоге bin PostgreSQL. Вы можете использовать путь в приведенной выше команде, если хотите сохранить его в другом месте, например, измените последнюю часть приведенной выше команды следующим образом: --file D:\Backups\alldbs.sql
- Если используется порт, отличный от порта по умолчанию, замените 5432 на нужный номер порта.
- Если вы по умолчанию не используете учетную запись администратора PSQL postgres, то в приведенной выше команде измените postgres на имя вашей учетной записи администратора.
- В процессе потребуется несколько раз ввести пароль пользователя postgres. При каждом запросе вводите пароль и нажимайте клавишу **Ввод**.

Примечание

Ввод пароля никак не отражается в окне командной строки.

2. *Создайте резервную копию базы данных сервера шлюза*
   a. Остановите службу **Кибер Файлы Gateway**.
   b. Перейдите в папку базы данных сервера шлюза, по умолчанию расположенную в C:\Program Files (x86)\Cyberprotect\Cyber Files\Gateway Server\database
   c. Создайте резервную копию файла mobilEcho.sqlite3.
3. ***Дополнительные файлы для резервного копирования***

   Если вы вносили изменения в любые из этих файлов, рекомендуется создать резервные копии, чтобы перенести ваши настройки при восстановлении или переносе программы Кибер Файлы.

   - Файл postgresql.conf, так как он может содержать важные настройки для базы данных. Как правило, он находится в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\PostgreSQL\<version>\Data.
   - Файл web.xm по умолчанию расположен в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Access Server\Web Application\WEB-INF\. Содержит настройки единого входа.
   - Файл server.xml по умолчанию расположен в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\apache-tomcat-<version>\conf. Содержит настройки Tomcat.

- Файл krb5.conf по умолчанию расположен в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\apache-tomcat-<version>\conf. Содержит настройки единого входа.
- Файл login.conf по умолчанию расположен в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\apache-tomcat-<version>\conf.
- Ваши сертификаты и ключи, используемые для Кибер Файлы.
- Файл cyberfilessrv.cfg по умолчанию расположен в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Access Server.
- Пользовательские цветовые схемы по умолчанию расположены в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Access Server\Web Application\customizations\.
- Файл pg_hba.conf по умолчанию расположен в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\PostgreSQL\<version>\Data.

4. ***Удалите Киберпротект Кибер Файлы***
   a. Откройте установщик Кибер Файлы.
   b. Примите условия лицензионного соглашения и нажмите **Удалить**.
   c. Выберите все компоненты и нажмите **Удалить**.
5. ***Удалите каталог данных PostgreSQL***

   При удалении сервера PostgreSQL его папка **Data** не удаляется автоматически. Удалите вручную всю папку PostgreSQL, по умолчанию расположенную здесь: C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\PostgreSQL\

   Примечание
   Если вы пользуетесь более старой или пользовательской установкой (например, C:\Program Files\Cyberprotect\Access\Common\PostgreSQL\), вам следует изменить путь к файлам.

6. ***[Необязательно] Удалите Java***

   При желании можно удалить версию Java, установленную для веб-сервера Кибер Файлы. Java также можно удалить через панель управления.
7. ***Переустановите** Киберпротект Кибер Файлы*
   a. Запустите новый установщик Кибер Файлы и нажмите **Далее**.
   b. Прочитайте и примите лицензионное соглашение.
   c. Выберите **Установить** и следуйте инструкциям программы установки.

      Примечание
      Если веб-сервер Кибер Файлы, PostgreSQL и шлюз устанавливаются на отдельные машины, выберите **Пользовательская** и укажите нужные компоненты.

   d. В окне настройки PostgreSQL введите пароль суперпользователя PostgreSQL, который использовался изначально.
   e. Нажмите кнопку **Далее**.
   f. Проверьте выбранные компоненты и нажмите **Установить**.

g. После завершения установки нажмите кнопку **Выйти**. Появится диалоговое окно с сообщением о запуске средства конфигурации.
h. После запуска средства конфигурации оставьте его открытым, не нажимая **OK** или **Применить**.
i. Откройте на панели управления оснастку **Службы** и остановите службу Кибер Файлы Tomcat.

Примечание
Для конфигураций с балансировкой нагрузки остановите все службы Кибер Файлы Tomcat.

j. Откройте приложение Кибер Файлы PostgreSQL Administrator, подключитесь к локальному серверу базы данных, выберите **Базы данных** и убедитесь в наличии базы данных с именем cyberfiles_production.
k. Щелкните базу данных правой кнопкой и выберите **Обновить**.
l. Разверните ее, разверните раздел **Схемы**, затем раздел **Общедоступные** и убедитесь, что раздел **Таблицы** содержит ноль (0) элементов.
   - Если база данных содержит таблицы, щелкните по ней правой кнопкой и переименуйте в oldcyberfiles_production.
   - Затем перейдите в **Базы данных**, щелкните правой кнопкой и создайте новую базу данных с именем cyberfiles_production.
m. Закройте PostgreSQL Administrator и откройте командную строку с повышенными привилегиями.
n. В командной строке перейдите в папку bin PostgreSQL.
   Например, cd "C:\Program Files\Cyberprotect\Cyber Files\Common\PostgreSQL\<version>\bin"
o. Скопируйте файл резервной копии базы данных alldbs.sql (или с другим именем, выбранным вами) в папку **bin**.
p. В командной строке введите следующую команду: psql -U postgres -f alldbs.sql
q. Введите пароль postgreSQL при появлении запроса.

Примечание
Восстановление может занять много времени в зависимости от размера базы данных.

r. После завершения восстановления закройте окно командной строки.
s. Снова откройте **PostgreSQL Administrator** и подключитесь к локальному серверу базы данных.
t. Выберите **Базы данных**.
u. Разверните базу данных cyberfiles_production , раздел **Схемы** и **Общедоступные**.
   Убедитесь, что количество **таблиц** такое же, как было изначально.

8. ***Восстановите базу данных сервера шлюза***

Скопируйте созданный вами файл резервной копии базы данных сервера шлюза mobilEcho.sqlite3 в папку базы данных нового сервера шлюза (по умолчанию C:\Program Files (x86)\Cyberprotect\Cyber Files\Gateway Server\database), заменив существующий файл.

9. ***Настройте сервер***

   Примечание
   Настоятельно рекомендуется не менять DNS-имена, используемые в Кибер Файлы, а только IP-адреса, на которые они указывают. В следующих инструкциях предполагается, что вы повторно используете DNS-имена предыдущего экземпляра Кибер Файлы.

   a. Вернитесь к открытому средству конфигурации Кибер Файлы и задайте параметры для сервера шлюза, веб-сервера Кибер Файлы и репозитория файлов.
   b. Нажмите кнопку **Применить**, а затем **OK**.
   c. В следующем диалоговом окне нажмите **OK**.Откроется браузер с веб-интерфейсом Кибер Файлы.
   d. Выполните вход на сервер.
   e. Щелкните **Администрирование**.
   f. Перейдите на страницу **Мобильный доступ** -> **Серверы шлюза**.
   g. В списке серверов шлюза должен отображаться ваш сервер шлюза.
   h. Если адресом для сервера шлюза является DNS-запись, вносить изменения в параметры сервера не потребуется при условии, что DNS-запись указывает на машину сервера. Если адресом для шлюза является IP-адрес, убедитесь, что это IP-адрес сервера шлюза.

10. ***Проверьте административные настройки Кибер Файлы***

    Когда восстановление базы данных будет завершено, прежде чем продолжить, настоятельно рекомендуется выполнить вход в веб-интерфейс и убедиться, что настройки успешно восстановлены и по-прежнему актуальны. Примеры важных элементов, которые необходимо проверить:

    - Ведение журнала аудита – убедитесь, что у новой папки журналов Кибер Файлы имеются все необходимые права для записи журналов.
    - Параметры администрирования – проверьте правильность всех параметров LDAP, SMTP и общих параметров администрирования.
    - Серверы шлюза и источники данных – убедитесь, что все серверы шлюза доступны по правильным адресам, и проверьте правильность путей ко всем источникам данных.

10.7.3 Проведите тестирование новой конфигурации

После завершения миграции убедитесь, что все работает, выполнив следующие простые действия.

- Просмотрите разделы веб-интерфейса и проверьте, что все работает правильно. Убедитесь, что ваши настройки на месте и не были изменены.
- Передайте файл через веб-интерфейс в раздел Sync & Share. Сделайте то же самое для всех настроенных вами сетевых узлов (если есть).

- Скачайте любой файл Sync & Share, который существовал до миграции, чтобы убедиться, что подключение к существующему хранилищу файлов по-прежнему работает.
- Подключитесь к новой конфигурации с помощью клиента для ПК и/или мобильного клиента.
- Передайте и скачайте несколько файлов через клиент для ПК и/или мобильный клиент.

10.8 Перенос Кибер Файлы на другой сервер

Это руководство поможет вам перенести существующую установку Киберпротект Кибер Файлы на новые машины.

Внимание
Перед переносом рабочего сервера настоятельно рекомендуется выполнить эти шаги в тестовой среде. Тестовое развертывание должно иметь ту же архитектуру, что и рабочие серверы, а также пару тестовых пользовательских компьютеров и мобильных клиентов, чтобы обеспечить совместимость в рабочей среде.

10.8.1 Перед началом работы

Предупреждение
Настоятельно рекомендуется выполнить тестовое резервное копирование/восстановление вне рабочей среды.

Выполните следующее:

- Обратите внимание расположены ли веб-сервер Кибер Файлы, PostgreSQL, шлюз и репозиторий файлов на одном компьютере.
- Запишите DNS, IP-адрес и порт веб-сервера Кибер Файлы.
- Запишите DNS, IP-адрес и порт сервера шлюза.
- Запишите адрес и порт файлового репозитория.
- Запишите местоположение хранилища файлов.
- Запишите номер версии PostgreSQL текущего сервера.
  Простейший способ сделать это – посмотреть на имя папки внутри главного каталога PostgreSQL (по умолчанию это каталог C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\PostgreSQL), имя внутренней папки содержит старший номер версии PostgreSQL (например, **9.2**; **9.3**; **9.4**).

Примечание
Большую часть этой информации можно найти в программе настройки.

Базовые этапы процесса переноса:

Перед началом переноса убедитесь, что все готово к выполнению этих шагов.

1. Измените DNS-записи, чтобы они указывали на новую машину сервера.
2. Сделайте резервную копию текущих файлов базы данных и сертификатов.
3. Переместите файлы базы данных и сертификаты на новую машину.
4. Перенесите хранилище файлов.
5. Установите на новой машине веб-сервер Кибер Файлы.
6. Переместите сертификаты на новую машину.
7. Поместите файлы базы данных в новое расположение веб-сервера Кибер Файлы.
8. Используйте программу настройки для запуска нового веб-сервера Кибер Файлы.
9. Проверьте правильность адреса мобильного шлюза Кибер Файлы.
10. Проведите тестирование новой конфигурации.

10.8.2 Перенос баз данных веб-сервера и шлюза Кибер Файлы

На исходном сервере, где работают Tomcat/Gateway/PostgreSQL

Примечание
Если база данных веб-сервера Кибер Файлы слишком большая (несколько гигабайтов), может потребоваться другой метод резервного копирования и восстановления.

1. Остановите службу Кибер Файлы Tomcat.
   i. Откройте средство Кибер Файлы PostgreSQL Administrator. Оно находится в меню «Пуск» Windows в папке Кибер Файлы. Подключитесь к серверу базы данных. Может потребоваться ввести пароль для пользователя postgres.
   ii. Разверните раздел **Базы данных** и щелкните правой кнопкой базу данных cyberfiles_ production.
   iii. Выберите **Обслуживание**.
   iv. Выберите **ЧИСТКА** и установите для параметра **АНАЛИЗ** значение «Да».
   v. Нажмите кнопку**OK**.
   vi. Разверните базу данных, раздел **Схемы** и раздел **Общедоступные**. Обратите внимание на число в разделе **Таблицы** . Это может помочь удостовериться в успешности восстановления базы данных.
   vii. Закройте средство PostgreSQL Administrator и откройте командную строку с повышенными привилегиями.
   viii. В командной строке перейдите в папку bin PostgreSQL.
   например, cd "C:\Program Files(x86)\Cyberprotect\Cyber Files\Common\PostgreSQL\<version>\bin"

Примечание
Примечание. Необходимо будет изменить путь, чтобы он указывал на папку PostgreSQL, если это старая или выборочная установка (например, C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\PostgreSQL\9.4\bin\).

ix. Введите следующую команду: pg_dumpall --host localhost --port 5432 --username postgres --file alldbs.sql
   - alldbs.sql будет именем файла резервной копии, сохраненной в каталоге bin PostgreSQL. Вы можете использовать путь в приведенной выше команде, если хотите сохранить его в другом месте, например, измените последнюю часть приведенной выше команды следующим образом: --file D:\Backups\alldbs.sql
   - Если используется порт, отличный от порта по умолчанию, замените 5432 на нужный номер порта.
   - Если вы по умолчанию не используете учетную запись администратора PSQL postgres, то в приведенной выше команде измените postgres на имя вашей учетной записи администратора.
   - В процессе этого вам потребуется несколько раз ввести пароль пользователя postgres . При каждом запросе вводите пароль и нажимайте клавишу «Ввод».

Примечание
Ввод пароля никак не отражается в окне командной строки.

2. ***Создайте резервную копию базы данных сервера шлюза***
   a. Остановите службу **Кибер Файлы Gateway**.
   b. Перейдите в папку базы данных сервера шлюза, по умолчанию расположенную в C:\Program Files (x86)\Cyberprotect\Cyber Files\Gateway Server\database
3. Скопируйте файл mobilEcho.sqlite3 на новую машину, где будет установлен сервер шлюза.

10.8.3 Дополнительные файлы для резервного копирования

Если вы вносили изменения в любые из этих файлов, рекомендуется создать резервные копии, чтобы перенести ваши настройки при восстановлении или переносе программы Кибер Файлы.

Файл postgresql.conf, так как он может содержать важные настройки для базы данных. Как правило, он находится в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\PostgreSQL\<version>\Data.

- Файл web.xm по умолчанию расположен в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Access Server\Web Application\WEB-INF\. Содержит настройки единого входа.
- Файл server.xml по умолчанию расположен в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\apache-tomcat-<version>\conf. Содержит настройки Tomcat.
- Файл krb5.conf по умолчанию расположен в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\apache-tomcat-<version>\conf. Содержит настройки единого входа.

- Файл login.conf по умолчанию расположен в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\apache-tomcat-<version>\conf.
- Ваши сертификаты и ключи, используемые для Кибер Файлы.
- Файл cyberfilessrv.cfg по умолчанию расположен в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Access Server.
- Пользовательские цветовые схемы по умолчанию расположены в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Access Server\Web Application\customizations\.
- Файл pg_hba.conf по умолчанию расположен в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\PostgreSQL\<version>\Data.

10.8.3.1 На новом сервере, где будет размещен Кибер Файлы Server

Установка Кибер Файлы

1. Запустите программу установки Кибер Файлы и нажмите кнопку **Далее**. Прочитайте и примите лицензионное соглашение.
2. Выберите **Установить** и следуйте инструкциям программы установки.

   Примечание
   Если веб-сервер Кибер Файлы, PostgreSQL и шлюзы устанавливаются на отдельные машины, выберите **Пользовательская** и укажите нужные компоненты.

3. В окне настройки PostgreSQL введите пароль суперпользователя PostgreSQL, который использовался на исходном сервере. Нажмите кнопку **Далее**.
4. Проверьте выбранные компоненты и нажмите кнопку **Установить**.
5. После завершения установки нажмите кнопку **Выйти**. Появится диалоговое окно с сообщением о запуске программы настройки.
6. После запуска программы настройки оставьте ее открытой, не нажимая кнопки **OK** или **Применить**.
7. Откройте на панели управления оснастку **Службы** и остановите службу Кибер Файлы Tomcat.

   Примечание
   Для конфигураций с балансировкой нагрузки остановите все службы Кибер Файлы Tomcat.

8. Откройте приложение Кибер Файлы PostgreSQL Administrator, подключитесь к локальному серверу базы данных, выберите **Базы данных** и проверьте наличие базы с именем cyberfiles_production.
9. Щелкните базу данных правой кнопкой и выберите **Обновить**.
10. Разверните ее, разверните раздел **Схемы**, затем раздел **Общедоступные** и убедитесь, что раздел **Таблицы** содержит ноль (0) элементов.
    - Если база данных содержит таблицы, щелкните по ней правой кнопкой и переименуйте в oldcyberfiles_production. Затем перейдите в **Базы данных**, щелкните правой кнопкой и

создайте новую базу данных с именем cyberfiles_production.

11. Закройте PostgreSQL Administrator и откройте командную строку с повышенными привилегиями.
12. В командной строке перейдите в папку bin PostgreSQL.
    Например, cd "C:\Program Files\Cyberprotect\Cyber Files\Common\PostgreSQL\<version>\bin"
13. Скопируйте файл резервной копии базы данных alldbs.sql (или с другим именем, выбранным вами) в папку **bin**.
14. В командной строке введите следующую команду: psql -U postgres -f alldbs.sql
15. Введите пароль postgres в ответ на запрос.

    Примечание
    Восстановление может занять много времени в зависимости от размера базы данных.

16. После завершения восстановления закройте окно командной строки.
17. Снова откройте **PostgreSQL Administrator** и подключитесь к локальному серверу базы данных.
18. Выберите **Базы данных**.
19. Разверните базу данных cyberfiles_production , **Schemas** и **Public**. Убедитесь, что количество **таблиц** такое же, как на исходном сервере.

    Примечание
    Если версия веб-сервера Кибер Файлы, на который восстанавливается база данных, новее версии веб-сервера Кибер Файлы из резервной копии базы данных и служба Кибер Файлы Tomcat уже запущена, то количество таблиц в новой базе данных веб-сервера Кибер Файлы может быть больше, чем во время создания резервной копии.

Восстановите базу данных сервера шлюза

Скопируйте базу данных сервера шлюза mobliEcho.sqlite3, полученную со старого сервера, в папку базы данных нового сервера шлюза (по умолчанию в папке:C:\Program Files (x86)\Cyberprotect\Cyber Files\Gateway Server\database), заменив существующий файл.

Настройте новый сервер

Примечание
Настоятельно рекомендуется не изменять DNS-имена, используемые программой Кибер Файлы, а только IP-адреса, на которые они указывают. Следующие инструкции предполагают использование DNS-имен предыдущего экземпляра Кибер Файлы.

1. Вернитесь к открытому средству конфигурации Кибер Файлы и задайте параметры для сервера шлюза, веб-сервера Кибер Файлы и репозитория файлов.
2. Нажмите кнопку **Применить**, а затем **OK**. В следующем диалоговом окне нажмите кнопку **OK**, после чего в браузере откроется веб-интерфейс Кибер Файлы.
3. Выполните вход на сервер.

4. Щелкните **Администрирование**. Перейдите на страницу **Мобильный доступ** -> **Серверы шлюза**.
5. В списке серверов шлюза должен отображаться ваш сервер шлюза.
6. Если адресом для сервера шлюза является DNS-запись, вносить изменения в параметры сервера не потребуется, если DNS-запись указывает на новую машину сервера. Если адресом для шлюза является IP-адрес, необходимо будет изменить сервер шлюза.

Проверьте административные настройки Кибер Файлы

Когда восстановление базы данных будет успешно завершено, перед тем как продолжить, настоятельно рекомендуется выполнить вход в веб-интерфейс и убедиться, что параметры перенесены и по-прежнему актуальны. Примеры важных элементов, которые необходимо проверить:

- Ведение журнала аудита – убедитесь, что у новой папки журналов Кибер Файлы имеются все необходимые права для записи журналов.
- New Relic – если вы используете New Relic, скопируйте файл newrelic.yml со старой машины на эту и убедитесь, что путь в веб-интерфейсе Кибер Файлы указывает на этот файл.
- Параметры администрирования – проверьте правильность всех параметров LDAP, SMTP и общих параметров администрирования.
- Серверы шлюза и источники данных – убедитесь, что все серверы шлюза доступны по правильным адресам, и проверьте правильность путей ко всем источникам данных.

10.8.4 Проведите тестирование новой конфигурации

После завершения настройки нового сервера убедитесь, что все работает, выполнив пару простых действий.

- Просмотрите разделы веб-интерфейса и проверьте, что все работает правильно. Убедитесь, что параметры на месте и не были изменены.
- Загрузите файл через веб-интерфейс в раздел синхронизации и общего доступа и сделайте то же самое для всех настроенных сетевых узлов (если есть).
- Подключитесь к новому серверу с помощью клиента для ПК и/или мобильного клиента.
- Загрузите и скачайте несколько файлов через клиент для ПК и/или мобильный клиент.

10.8.5 Очистка исходного сервера

Если вы убедились, что новый сервер работает правильно, и не планируете снова использовать старый сервер, рекомендуется удалить Кибер Файлы со старой машины.

Откройте программу установки Кибер Файлы, примите лицензионное соглашение и щелкните «Удалить». Выберите все компоненты и нажмите кнопку «Удалить». Все компоненты Кибер Файлы будут удалены с машины.

Примечание
Если у вас нет установщика Кибер Файлы, откройте панель управления, удалите сервер PostgreSQL, сервер шлюза и сервер репозитория файлов, веб-сервер, программу сбора конфигураций, утилиту настройки Кибер Файлы, а также LibreOffice.

- При удалении сервера PostgreSQL его папка **Data** не удаляется автоматически. Удалите вручную всю папку PostgreSQL, по умолчанию расположенную здесь: C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\PostgreSQL\

  Примечание
  Если вы пользуетесь более старой или пользовательской установкой (например, C:\Program Files\Cyberprotect\Access\Common\PostgreSQL\), вам следует изменить путь к файлам.

- При желании можно удалить версию Java, установленную для веб-сервера Кибер Файлы. Java также можно удалить через панель управления.

10.9 Обновление PostgreSQL до новой основной версии

В основных выпусках PostgreSQL часто добавляются новые функции, которые меняют некоторые методы внутренней работы PostgreSQL.

Для установок с одним сервером можно использовать полную процедуру миграции на тот же сервер.

Внимание
Киберпротект Кибер Файлы поддерживает обновление PostgreSQL только с помощью установщика Кибер Файлы. Официальные дистрибутивы PostgreSQL не поддерживаются. Никакие другие версии, кроме поставляемой с программой, не поддерживаются.

Примечание
Обновление PostgreSQL может занимать много времени.

Внимание
Настоятельно рекомендуется выполнить тестовое обновление вне рабочей среды.

11 Дополнительные материалы

11.1 Конфликтующее программное обеспечение

Есть некоторые программные продукты, которые могут привести к проблемам в работе Кибер Файлы. Известные на данный момент конфликты перечислены ниже.

- **VMware View™ Persona Management** – это приложение вызывает проблемы в процессе синхронизации настольного клиента Кибер Файлы и при удалении файлов. Размещение синхронизируемой папки Кибер Файлы вне **профиля пользователя Persona Management** должно разрешить известные конфликты.
- **Антивирусное ПО** не должно сканировать синхронизируемые папки, поскольку могут возникнуть конфликты с процессом синхронизации. Рекомендуется добавить папку файлового хранилища Кибер Файлы в разрешенный или игнорируемый список антивирусной программы. Если защита файлов не была отключена, все элементы в папке файлового хранилища будут защищены и антивирусная программа не сможет ничего обнаружить, но может вызвать проблемы с некоторыми элементами.

11.2 Для сервера Кибер Файлы

11.2.1 Балансировка нагрузки Кибер Файлы

Существует два основных метода балансировки нагрузки Кибер Файлы.

Балансировка нагрузки только на шлюзах мобильного доступа Кибер Файлы

Эта конфигурация обеспечивает балансировку компонентов Кибер Файлы, на которые приходится наибольшая нагрузка, на серверы мобильных шлюзов, при этом мобильные клиенты всегда будут иметь к ним доступ. Сервер Кибер Файлы не помещается за балансировщик нагрузки, так как этот сервер не нужен для подключения к мобильным шлюзам Кибер Файлы при неуправляемом доступе. Дополнительные сведения см. в статье Кластерные группы.

Балансировка нагрузки всех компонентов Кибер Файлы

В этой конфигурации выполняется балансировка нагрузки всех компонентов Кибер Файлы, что обеспечивает высокую доступность для всех пользователей. Для тестирования подобной конфигурации потребуются как минимум две отдельные машины. Многие из настроек, касающиеся балансировки нагрузки, для разного программного обеспечения и оборудования различаются, поэтому в данном руководстве они рассматриваться не будут.

В примере конфигурации будут использоваться три разные машины. Одна из них будет действовать как файловый репозиторий и база данных, а две другие – одновременно как веб-серверы Кибер Файлы и мобильные шлюзы Кибер Файлы. Ниже приведены инструкции по настройке данной конфигурации.

В этом руководстве содержится подробное описание правильной балансировки нагрузки продукта Кибер Файлы в вашей рабочей среде.

11.2.1.1 На сервере, где будут размещаться база данных PostgreSQL и файловый репозиторий, выполните следующие действия.

1. Запустите программу установки Кибер Файлы и нажмите кнопку **Далее**. Прочитайте и примите лицензионное соглашение.
2. В программе установки Кибер Файлы выберите вариант **Настроить**, затем выберите **Репозиторий файлов Кибер Файлы** и **Сервер баз данных PostgreSQL**, затем нажмите **Далее**.
3. Выберите место установки файлового репозитория и средства конфигурации.
4. Выберите место установки PostgreSQL и введите пароль для суперпользователя **postgres**.
5. Откройте TCP-порт 5432. Он будет использоваться для доступа к базе данных PostgreSQL с удаленных машин.
6. Завершив установку, перейдите в средство конфигурации.
   a. Появится запрос на открытие программы настройки. Нажмите кнопку **OK**.
   b. Выберите адрес и порт, по которым будет доступен файловый репозиторий.

   Примечание
   Нужно будет задать такие же адрес и порт в веб-интерфейсе Кибер Файлы. Дополнительные сведения см. в статьях Использование средства конфигурации и Файловый репозиторий.

   c. Выберите путь к хранилищу файлов. Это будет место размещения фактических файлов.
   d. Нажмите кнопку **OK**, чтобы применить изменения, и закройте **средство конфигурации**.
7. Перейдите в каталог установки PostgreSQL (например, C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\PostgreSQL\<VERSION>\data\) и откройте файл **pg_hba.conf** в текстовом редакторе.
8. Включите записи с узлами для каждого из ваших серверов Кибер Файлы с использованием их внутренних адресов и сохраните файл. Файл **pg_hba.conf** (HBA расшифровывается как host-based authentication, проверка подлинности на основе хоста) контролирует аутентификацию клиентов и хранится в каталоге данных кластера базы данных. В нем указываются серверы, которым разрешено соединение, и их права, например
   # TYPE DATABASE USER ADDRESS METHOD
   # First Кибер Файлы & Gateway server
   host all all 10.27.81.3/32 md5
   # Second Кибер Файлы & Gateway server
   host all all 10.27.81.4/32 md5
   В этих примерах все пользователи, подключающиеся с первого сервера Кибер Файлы (10.27.81.3/32) и второго сервера Кибер Файлы (10.27.81.4/32), могут получить доступ к базе данных с полными привилегиями (кроме привилегии репликации) через зашифрованное md5 соединение.

9. Чтобы включить удаленный доступ к этому экземпляру PostgreSQL, необходимо изменить файл **postgresql.conf**. Выполните следующие действия.
   a. Найдите и откройте файл **postgresql.conf**. По умолчанию это путь C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\PostgreSQL\<VERSION>\Data\postgresql.conf
   b. Найдите строку #listen_addresses = 'localhost'
   c. Включите эту команду, удалив символ **#** в начале строки.
   d. Замените localhost на ***** для прослушивания всех доступных адресов. Чтобы настроить PostgreSQL на прослушивание только определенного адреса, введите нужный IP-адрес вместо *****.
      - **Например,** listen_addresses = '*' означает, что PostgreSQL будет прослушивать все доступные адреса.
      - **Например,** listen_addresses = '192.168.1.1' означает, что PostgreSQL будет прослушивать указанный адрес.
   e. Сохраните изменения, сделанные в файле **postgresql.conf**.
   f. Перезапустите службу сервера PostgreSQL Кибер Файлы.
10. Откройте средство **Кибер Файлы PostgreSQL Administrator t** (также может называться PgAdmin). Оно находится в меню «Пуск» Windows в папке Кибер Файлы. Подключитесь к своему локальному серверу, выберите **Базы данных** и создайте новую базу данных, щелкнув правой кнопкой мыши или выбрав команду **Новая база данных** в меню **Правка** -> **Новый объект**. Дайте ей имя **cyberfiles_production**.

Примечание
По умолчанию PostgreSQL использует порт 5432. Убедитесь, что этот порт открыт в брандмауэре или программе маршрутизации.

11.2.1.2 На двух серверах, которые будут одновременно выступать как серверы доступа Кибер Файлы и серверы Кибер Файлы шлюза, выполните следующие действия.

1. Запустите программу установки Кибер Файлы и нажмите кнопку **Далее**. Прочитайте и примите лицензионное соглашение.
2. В программе установки Кибер Файлы выберите вариант **Настроить** и выберите только **Кибер ФайлыВеб-сервер** и **Кибер Файлы Мобильный шлюз** , затем продолжите процесс установки.
3. Завершив установку, перейдите в средство конфигурации.
   a. Появится запрос на открытие программы настройки. Нажмите кнопку **OK**.
   b. **На вкладке Кибер ФайлыВеб-сервер:**
      - Введите адрес и порт для обращения к серверу управления Кибер Файлы (например, 10.27.81.3 и 10.27.81.4).
      - Выберите сертификат. Это должен быть тот же SSL-сертификат, что привязан к DNS-адресу балансировщика нагрузки.

- Нажмите кнопку **Применить**.

Примечание
Если у вас нет сертификата, то Кибер Файлы создаст самозаверенный сертификат. Этот сертификат НЕ должен использоваться в производственных средах.

c. **На вкладке Кибер ФайлыМобильный шлюз**:
   - Введите адрес и порт для обращения к серверу шлюза (например, 10.27.81.10 и 10.27.81.11).
   - Выберите сертификат. Это должен быть тот же SSL-сертификат, что привязан к DNS-адресу балансировщика нагрузки.
   - Нажмите кнопку **Применить**.

Примечание
Если у вас нет сертификата, то Кибер Файлы создаст самозаверенный сертификат. Этот сертификат НЕ должен использоваться в производственных средах.

4. Перейдите в каталог установки Кибер Файлы (например, C:\Program Files (x86)\Cyberprotect\Cyber Files\Access Server\) и откройте файл **cyberfilessrv.cfg** в текстовом редакторе.
5. Задайте имя пользователя, пароль и внутренний адрес для сервера, на котором будет выполняться база данных, и сохраните файл. Это настроит сервер Кибер Файлы для доступа к вашей удаленной базе данных PostgreSQL, например
   DB_DATABASE =cyberfiles_production
   DB_USERNAME =postgres
   DB_PASSWORD =password123
   DB_HOSTNAME =10.27.81.2
   DB_PORT =5432
6. Откройте Services.msc и перезапустите службы Кибер Файлы.

11.2.1.3 На одном из веб-серверов Кибер Файлы и мобильных шлюзов Кибер Файлы выполните следующие действия.

Это сервер, который вы настроите первым, и его параметры будут продублированы на все другие серверы. После репликации параметров все серверы будут идентичны. Нет разницы, какой сервер выбрать.

1. Откройте Services.msc и перезапустите службы **Кибер Файлы Tomcat** . Это заполнит созданную вами базу данных.
2. Откройте адрес https://myaccess (например, https://10.27.81.3 или https://10.27.81.4) в веб-браузере и завершите Мастер настройки.
   a. **На вкладке «Лицензирование»:**
      - Введите свой лицензионный ключ, установите флажок и нажмите кнопку **Продолжить**.

b. **На вкладке «Общие настройки»:**
   - Введите имя сервера.
   - В качестве веб-адреса следует указать внешний адрес вашего балансировщика нагрузки (например, mylb.company.com). Если вы используете порт, отличный от 443, нужно будет указать номер порта.
   - Адрес регистрации клиентов должен быть внешним адресом вашего балансировщика нагрузки (например, mylb.company.com).
   - Выберите цветовую схему.
   - Выберите язык для сообщений журнала аудита.

c. **На вкладке SMTP:**
   - Введите DNS-имя или IP-адрес сервера SMTP.
   - Введите порт сервера SMTP.
   - Если для сервера SMTP не используются сертификаты, снимите флажок **Использовать защищенное подключение?**.
   - Введите имя, которое будет отображаться в поле «От» сообщений электронной почты, отправляемых сервером.
   - Введите адрес, на который сервер будет отправлять сообщения.
   - Если на сервере SMTP используется проверка подлинности по имени пользователя и паролю, установите флажок «Использовать аутентификацию SMTP?» и введите нужные учетные данные.
   - Выберите **Сохранить**.

d. **На вкладке LDAP:**
   - Установите флажок **Включить LDAP**.
   - Введите DNS-имя или IP-адрес сервера LDAP.
   - Введите порт сервера LDAP.
   - Если для подключений к серверу LDAP используется сертификат, установите флажок «Использовать защищенное LDAP-подключение».
   - Введите свои учетные данные LDAP с доменом (например, mycompany\myname).
   - Введите базу поиска LDAP.
   - Введите требуемый домен или домены для проверки подлинности LDAP (чтобы включить аутентификацию LDAP, например, для учетной записи с адресом joe@glilabs.com, следует ввести glilabs.com).
   - Выберите **Сохранить**.

e. **На вкладке Локальный шлюз:**

> **Примечание**
> Если мобильный шлюз и веб-сервер Кибер Файлы устанавливаются на одном компьютере, то веб-сервер Кибер Файлы автоматически обнаружит шлюз и будет управлять им.

- Задайте DNS-имя или IP-адрес для локального сервера шлюза. Это внутренний адрес за балансировщиком нагрузки (например, 10.27.81.10).
- Выберите **Сохранить**.

f. **На вкладке Хранилище файлов:**

- Адрес файлового репозитория должен быть внутренним адресом сервера, созданного для этой роли (например, 10.27.81.2).

3. После завершения мастера настройки нажмите кнопку **Завершить** и перейдите в раздел **Мобильный доступ** > **Серверы шлюза**.
4. Пора зарегистрировать второй сервер шлюза.
   a. Введите **отображаемое имя** для второго шлюза.
   b. Адрес **для администрирования** должен быть внутренним адресом за балансировщиком нагрузки (например, 10.27.81.11).
   c. Введите **Ключ администрирования**. Вы можете получить его, перейдя на машину, куда устанавливается добавляемый шлюз, https://mygateway:443 (например, https://10.27.81.10 или https://10.27.81.11), там будет показан ключ. Дополнительные сведения см. в статье «Регистрация новых серверов шлюза».
   d. Выберите **Сохранить**.
5. Создайте кластерную группу и добавьте в нее все серверы шлюза. Основным сервером должен быть назначен один из серверов, с которым вы работали в мастере настройки. Дополнительные сведения см. в статье «Кластерные группы».

Примечание
Перед тем как продолжить, убедитесь, что вы уже настроили правильный адрес для администрирования на каждом шлюзе. Это DNS-имя или IP-адрес сервера шлюза.

   a. Разверните вкладку **Мобильный доступ**.
   b. Откройте страницу **Серверы шлюза**.
   c. Нажмите кнопку **Добавить кластерную группу**.
   d. Введите отображаемое имя группы.
   e. Введите внутреннее DNS-имя или IP-адрес балансировщика нагрузки (например, 10.27.81.1).
   f. Отметьте флажком каждый из шлюзов, которые требуется включить в группу.
   g. Выберите шлюз, который будет управлять настройками группы. Это должен быть шлюз, который вы настроили первым. Все имеющиеся настройки этого шлюза (включая назначенные источники данных, за исключением адреса для администрирования) будут скопированы на каждый шлюз в группе.

11.2.1.4 На балансировщике нагрузки:

1. Включите функцию поддержания сеанса на основе длительности (или ее аналог) в своем балансировщике нагрузки и задайте бессрочные сеансы.

2. Если требуется проверка работоспособности (проверка на получение HTTP-статуса 200), это можно сделать отправкой команды на адрес https://INTERNALSERVERNAME:MANAGEMENTPORT/signin (например, https://myaccessserver1.company.com/signin и https://myaccessserver2.company.com/signin).

Откройте в браузере адрес https://mylb.company.com, чтобы проверить работу созданной конфигурации.

11.2.2 Установка Кибер Файлы с балансировкой нагрузки

В этом руководстве содержится общий обзор требований к установке с балансировкой нагрузки и процессов, вовлеченных в развертывание Кибер Файлы в среде с балансировкой нагрузки. Ваша установка может отличаться от нашего примера, однако способ взаимодействия компонентов аналогичен.

Рекомендуемая конфигурация – разделение всех частей сервера Кибер Файлы на отдельные компьютеры под контролем балансировщиков нагрузки. Файловый репозиторий и хранилище файлов могут размещаться на одном компьютере.

Настоятельно рекомендуется выполнить эти действия в тестовой среде. Тестовое развертывание должно иметь ту же архитектуру, что и запланированная рабочая установка, а также пару тестовых пользовательских компьютеров и мобильных клиентов, чтобы обеспечить совместимость в вашей среде.

11.2.2.1 Системные требования

Требования к оборудованию

В рабочей среде рекомендуется использовать минимум три (3) сервера Кибер Файлы Tomcat и три (3) сервера шлюза, чтобы в случае сбоя одного сервера нагрузка распределялась между двумя активными серверами.

Примечание
Предложенная установка предполагает, что эти серверы будут размещены на сервере виртуальной машины. При использовании нескольких серверов рекомендуется использовать внутреннее соединение с низким значением задержки между гостевыми виртуальными машинами.

- 1 средство балансировки нагрузки для веб-серверов Кибер Файлы.
- 1 средство балансировки нагрузки для серверов шлюза Кибер Файлы.
- 3 сервера Кибер Файлы Tomcat, каждый с 32 ГБ ОЗУ и 16-ядерным ЦП.
- 3 сервера шлюза Кибер Файлы, каждый с 8 ГБ ОЗУ и 4-ядерным ЦП.

Примечание
Для сервера шлюза важнее скорости диска и сети, чем ЦП или памяти.

- 1 сервер PostgreSQL с 32 ГБ ОЗУ и 16-ядерным ЦП.
- 1 служба файлового репозитория + хранилище файлов. Параметры этого сервера не настолько важны.

Сетевые подключения

- Средство балансировки нагрузки для серверов Кибер Файлы Tomcat необходимо настроить для использования DNS-адреса текущего сервера Кибер Файлы.
- Средство балансировки нагрузки для серверов шлюза необходимо настроить для использования DNS-адреса текущего сервера шлюза.
- Сервер Tomcat должен подключаться к средству балансировки нагрузки шлюза для синхронизации сетевых узлов на настольном ПК и обзора сетевых узлов в веб-интерфейсе. В этой кластерной установке на страницах администрирования веб-интерфейса Кибер Файлы и серверов шлюза параметр **Адрес для клиентских подключений** является внешним адресом средства балансировки нагрузки. Для серверов шлюза также используется параметр **Использовать альтернативный адрес для подключений сервера Кибер Файлы**, а в параметре **Адрес для подключений веб-сервера Кибер Файлы** указан внутренний адрес балансировщика нагрузки шлюза.
- Сервер шлюза должен подключаться к средству балансировки нагрузки Tomcat для подключений мобильных клиентов.

Примечание
Для источника данных синхронизации и общего доступа необходимо изменить адрес на адрес средства балансировки нагрузки Tomcat.

11.2.2.2 Установка и настройка PostgreSQL

Установка компонента сервера PostgreSQL

1. Запустите программу установки Кибер Файлы и нажмите кнопку **Далее**. Прочитайте и примите лицензионное соглашение.
2. Нажмите **Пользовательская** и выберите только сервер базы данных PostgreSQL. Нажмите кнопку **Далее**.
3. Выберите место установки PostgreSQL, введите пароль для суперпользователя postgres и нажмите «Далее».
4. Выберите пункт **Открыть порт 5432 в брандмауэре**. Этот порт будет использоваться для удаленного доступа к базе данных PostgreSQL.
5. Завершите установку.

Разрешение подключений для серверов Tomcat

1. После завершения установки перейдите в папку **данных** PostgreSQL (по умолчанию в C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\PostgreSQL\<version>\Data) и откройте файл pg_hba.conf в текстовом редакторе.

2. Добавьте записи хостов для каждого из серверов Кибер Файлы Tomcat, использующих внутренние адреса, и сохраните файл.

   Файл pg_hba.conf (HBA означает Host-based authentication – проверка подлинности на основе хоста) контролирует проверку подлинности клиентов и хранится в каталоге данных кластера базы данных. В нем указываются серверы, которым разрешено соединение, и их права, например

   # TYPE DATABASE USER ADDRESS METHOD

   # Loadbalancer1 (First Кибер Файлы & Gateway server)

   host cyberfiles_production postgres 10.144.70.247/32 md5

   Примечание

   В этом примере учетная запись пользователя с именем postgres может подключаться с сервера по адресу 10.144.70.247 и получать доступ к базе данных cyberfiles_production со всеми правами (кроме права на **репликацию**) посредством подключения с хешированием MD5.

Настройка требуемого количества подключений

1. Найдите и измените значение max_connections на 510.
2. Удалите первый символ # из следующей строки: #listen_addresses = 'localhost'. Замените localhost символом *. Строка должна иметь следующий вид: listen_addresses = '*'
3. Удалите первый символ # из следующей строки: #effective_cache_size = 128MB и замените **128MB** на **12GB**. Строка должна иметь следующий вид: effective_cache_size = 12GB
4. Добавьте следующее примечание: - #ПРИМЕЧАНИЕ. Этот параметр настройки предполагает, что PostgreSQL самостоятельно работает на #ВМ с оперативной памятью не менее 16 ГБ. Подробная информация на #https://wiki.postgresql.org/wiki/Tuning_Your_PostgreSQL_Server
5. Сохраните внесенные изменения и закройте файл **postgresql.conf**.
6. Перезапустите службу сервера PostgreSQL Кибер Файлы.

11.2.2.3 Установка серверов Кибер Файлы

Установка только веб-сервера Кибер Файлы

1. Запустите программу установки Кибер Файлы и примите условия лицензионного соглашения.
2. Выберите **Настраиваемый**, а затем ТОЛЬКО веб-сервер Кибер Файлы.

   Примечание

   Если щелкнуть сервер Tomcat, будет автоматически выбран сервер PostgreSQL, но его можно отключить щелчком мыши.

3. Завершите установку и убедитесь, что служба Кибер Файлы Tomcat остановлена.

Конфигурация сервера

Все настройки, измененные на одном веб-сервере Кибер Файлы, необходимо таким же образом изменить на всех других веб-серверах Кибер Файлы.

Примечание
Обязательно добавьте запись в файле pg_hba.conf для каждого веб-сервера Кибер Файлы!

Настройка сервера для подключения к требуемой базе данных

1. Перейдите в папку веб-сервера Кибер Файлы (по умолчанию C:\Program Files (x86)\Cyberprotect\Cyber Files\Access Server) и откройте файл cyberfilessrv.cfg . Этот файл сообщает серверу, где расположена служба базы данных PostgreSQL.
2. Задайте следующие значения:
   DB_HOSTNAME =10.144.70.248
   DB_PORT =5432
   DB_POOLSIZE =250

   Примечание
   DB_HOSTNAME – это IP-адрес, на котором сейчас запущена служба PostgreSQL. В данном примере это 10.144.70.248.

   Примечание
   Рекомендуется настройка DB_POOLSIZE со значением минимум 250.
3. Сохраните файл.

Настройка максимального числа потоков

В установке Tomcat с балансировкой нагрузки важно, чтобы общее число всех потоков, которые могут создавать экземпляры Tomcat, не превышало максимального числа подключений, настроенных для приема в базе данных PostgreSQL.

Это определяется 3 важными настройками:

- В файле cyberfilessrv.cfg: DB_POOLSIZE = 200. Рекомендуется установить значение минимум 250.
- В файле Tomcat server.xml: maxThreads = 150. Рекомендуется оставить значение 150 по умолчанию.
- В файле postgresql.conf задайте значение max_connections. Этот параметр должен быть настроен на предыдущих этапах. Однако его значение не должно быть меньше суммы всех значений DB_POOLSIZE в Tomcat, заданных для каждого сервера Кибер Файлы, плюс 10. Например, 510 для 2 серверов Tomcat, 760 для 3 серверов Tomcat и т. д.

Примечание
Для изменений, внесенных в эти файлы, требуется перезагрузка соответствующих служб.

Настройка правильного входа в систему

В конфигурации с балансировкой нагрузки служба Tomcat Кибер Файлы не указывает правильные IP-адреса в журналах. Чтобы убедиться, что каждое подключение зарегистрировано правильно, внесите изменения, описанные ниже.

1. В файле server.xml найдите строку <Valve className=”org.apache.catalina.valves.AccessLogValve” directory=”logs” prefix=”localhost_access_log.” suffix=”.txt” pattern=”%h %l %u %t "%r" %s %b”/>.
2. Добавьте requestAttributesEnabled=”true” в конце строки.
3. Под ней добавьте следующее:
   <Valve className="org.apache.catalina.valves.RemoteIpValve" remoteIpHeader="X-Forwarded-For" protocolHeader="X-Forwarded-Proto"/>
4. Сохраните файл и перезапустите службу Кибер Файлы Tomcat.

11.2.2.4 Установка серверов шлюза

Установка нового сервера шлюза

1. На новом компьютере запустите программу установки Кибер Файлы и примите условия лицензионного соглашения.
2. Выберите пункт **Пользовательская** и установите только компонент сервера шлюза. Завершите установку.
3. В инструменте конфигурации задайте адрес, порт и сертификат шлюза. Это должен быть тот же SSL-сертификат, что привязан к DNS-адресу балансировщика нагрузки шлюза.

11.2.2.5 Параметры хранилища и файлового репозитория

Если планируется использовать хранилище S3, службу файлового репозитория устанавливать не нужно, так как хранилище файлов будет располагаться в хранилище S3 по вашему выбору.

Установка службы файлового репозитория

1. Скопируйте программу установки Кибер Файлы на компьютер, где будут располагаться репозиторий и хранилище файлов.
2. Запустите программу установки, примите условия лицензионного соглашения и выберите пункт «Пользовательская».
3. Выберите только параметр «Файловый репозиторий» и нажмите кнопку «Далее».
4. Выберите нужные пути установки и нажмите «Далее».
5. Следуйте инструкциям до завершения установки.

6. Запустится средство конфигурации. Выберите адрес и порт, по которым будет доступна служба файлового репозитория.
7. Выберите целевое расположение хранилища файлов. Расположение по умолчанию: C:\ProgramData\Cyberprotect\Cyber Files\FileStore.

Примечание
Если хранилище файлов расположено в удаленной сетевой папке, то компьютер или учетная запись пользователя, в которых запущена служба репозитория файлов, должен иметь полный доступ к папке файлового хранилища в сетевой папке.

Примечание
Учетная запись также должна иметь права на чтение и запись в локальной папке репозитория (например, C:\Program Files (x86)\Cyberprotect\Cyber Files\File Repository\Repository), чтобы иметь возможность записи в файл журнала.

8. Запустите службу файлового репозитория Кибер Файлы.

Кибер Файлы – настройки

1. Откройте веб-интерфейс Кибер Файлы и войдите в него как администратор.
2. Перейдите по пути **Sync & Share** -> **Файловый репозиторий** и убедитесь, что адрес конечной точки для репозитория и хранилища файлов идентичен тому, который вы выбрали в средстве конфигурации.

11.2.2.6 Настройки, характерные для средств балансировки нагрузки

1. Откройте в браузере адрес https://mylb.company.com, чтобы проверить работу созданной конфигурации.
2. Включите функцию поддержания сеанса на основе длительности (или ее аналог) в своем балансировщике нагрузки и задайте бессрочные сеансы.
3. Если требуется проверка работоспособности (проверка на получение HTTP-статуса 200), это можно сделать отправкой команды на адрес https://INTERNALSERVERNAME:MANAGEMENTPORT/api/v1/server_version (то есть https://myaccessserver.company.com/signin и https://myaccessserver.company.com/api/v1/server_version).
4. Чтобы обеспечить правильную регистрацию IP-адресов и подключений в установке с балансировкой нагрузки, необходимо настроить средство балансировки нагрузки с помощью следующих заголовков:
   - Поле X-Forwarded-For – определение реально используемых IP-адресов подключаемых клиентов вместо IP-адресов средства балансировки нагрузки для каждого подключения.
   - Поле X-Forwarded-Proto – определение реально используемого протокола.

11.2.3 Миграция на конфигурацию с балансировкой нагрузки

В этом руководстве содержится общий обзор требований к установке с балансировкой нагрузки и процессов, вовлеченных в миграцию для развертывания с балансировкой нагрузки. Ваша установка может отличаться от нашего примера, однако способ взаимодействия компонентов и их настроек аналогичен.

Рекомендуемая конфигурация – разделение всех частей сервера Кибер Файлы на отдельные компьютеры под контролем балансировщиков нагрузки. Файловый репозиторий и хранилище файлов могут размещаться на одном компьютере.

Перед переносом рабочего сервера настоятельно рекомендуется выполнить эти шаги в тестовой среде. Тестовое развертывание должно иметь ту же архитектуру, что и рабочие серверы, а также пару тестовых пользовательских компьютеров и мобильных клиентов, чтобы обеспечить совместимость в вашей среде.

В этом руководстве приведен пример установки Кибер Файлы в стандартном развертывании, где все компоненты установлены на одном компьютере.

Примечание
В этом примере мы сохраним работу оригинальной службы Кибер Файлы Tomcat и подключим ее к новой конфигурации. Это действие не является обязательным.

Прежде чем продолжить внесение изменений в развернутую систему, ознакомьтесь с нашими статьями о средстве Backup & Recovery.

11.2.3.1 Системные требования

Требования к оборудованию

В рабочей среде рекомендуется использовать минимум три (3) сервера Кибер Файлы Tomcat и три (3) сервера шлюза, чтобы в случае сбоя одного сервера нагрузка распределялась между двумя активными серверами.

Примечание
Предложенная установка предполагает, что эти серверы будут размещены на сервере виртуальной машины. При использовании нескольких серверов рекомендуется использовать внутреннее соединение с низким значением задержки между гостевыми виртуальными машинами.

- 1 средство балансировки нагрузки для веб-серверов Кибер Файлы.
- 1 средство балансировки нагрузки для серверов шлюза Кибер Файлы.
- 3 сервера Кибер Файлы Tomcat, каждый с 32 ГБ ОЗУ и 16-ядерным ЦП.
- 3 сервера шлюза Кибер Файлы, каждый с 8 ГБ ОЗУ и 4-ядерным ЦП.

Примечание
Для сервера шлюза важнее скорости диска и сети, чем ЦП или памяти.

- 1 сервер PostgreSQL с 32 ГБ ОЗУ и 16-ядерным ЦП.
- 1 служба файлового репозитория + хранилище файлов. Параметры этого сервера не настолько важны.

Сетевые подключения

- Средство балансировки нагрузки для серверов Кибер Файлы Tomcat необходимо настроить для использования DNS-адреса текущего сервера Кибер Файлы.
- Средство балансировки нагрузки для серверов шлюза необходимо настроить для использования DNS-адреса текущего сервера шлюза.
- Сервер Tomcat должен подключаться к средству балансировки нагрузки шлюза для синхронизации сетевых узлов на настольном ПК и обзора сетевых узлов в веб-интерфейсе. В этой кластерной установке на страницах администрирования веб-интерфейса Кибер Файлы и серверов шлюза параметр **Адрес для клиентских подключений** является внешним адресом средства балансировки нагрузки. Для серверов шлюза также используется параметр **Использовать альтернативный адрес для подключений сервера Кибер Файлы**, а в параметре **Адрес для подключений веб-сервера Кибер Файлы** указан внутренний адрес балансировщика нагрузки шлюза.
- Сервер шлюза должен подключаться к средству балансировки нагрузки Tomcat для подключений мобильных клиентов.

Примечание
Для источника данных синхронизации и общего доступа необходимо изменить адрес на адрес средства балансировки нагрузки Tomcat.

11.2.3.2 Миграция сервера PostgreSQL

Ваша база данных – наиболее важный компонент, который должен мигрировать в первую очередь.

Конфигурация на имеющемся сервере PostgreSQL

1. Откройте панель управления **Службы** (services.msc) и остановите службу **Кибер Файлы Tomcat** .
2. Откройте приложение **Кибер ФайлыАдминистратор PostgreSQL** и подключитесь к серверу базы данных. Щелкните знак «плюс» (**+**) рядом с разделом **Базы данных**.
3. Щелкните правой кнопкой по базе данных cyberfiles_production.
4. Выберите **Обслуживание**.
5. Выберите **ЧИСТКА** и установите для параметра **АНАЛИЗ** значение «Да».
6. Нажмите кнопку**OK**.

7. Откройте командную строку с повышенными привилегиями и перейдите в папку **bin** Postgres с помощью команды **cd**. (по умолчанию в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\PostgreSQL\<version>\bin).
8. Если текущей папкой в командной строке является папка **bin**, введите следующую команду:
   pg_dumpall --host localhost --port 5432 --username postgres --file alldbs.sql

   Примечание
   alldbs.sql – сгенерированный файл резервной копии, сохраняемый в папке **bin** . Он может содержать полный путь, если вы хотите сохранять файлы в любом другом месте, например **D:\Backups\alldbs.sql.**

   Примечание
   Если используются другой порт и/или пользователь, измените команду соответствующим образом.

9. По завершении резервного копирования остановите и отключите службу **Кибер Файлы PostgreSQL Server**.
10. Скопируйте и переместите файл резервной копии на новую машину, на которой будет размещен PostgreSQL.

Конфигурации на новом сервере PostgreSQL

1. Запустите программу установки Кибер Файлы и нажмите кнопку **Далее**. Прочитайте и примите лицензионное соглашение.
2. Нажмите **Пользовательская** и выберите только сервер базы данных PostgreSQL. Нажмите кнопку **Далее**.
3. Выберите место установки PostgreSQL и введите пароль для суперпользователя postgres.

   Примечание
   Это местоположение должно быть доступно для остальных серверов, а пароль должен совпадать с используемым ранее паролем на оригинальном сервере PostgreSQL.

4. Выберите пункт **Открыть порт 5432 в брандмауэре** и продолжите установку. Этот порт будет использоваться для удаленного доступа к базе данных PostgreSQL.

Настройка доступа к базе данных PostgreSQL

1. После завершения установки перейдите в папку **данных** PostgreSQL (по умолчанию в C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\PostgreSQL\<version>\Data) и откройте файл pg_hba.conf в текстовом редакторе.
2. Добавьте записи хостов для каждого из серверов Tomcat Access, использующих внутренние адреса, и сохраните файл. Если вам известны не все адреса серверов, позже можно вернуться к редактированию файла, но до этого момента серверы не смогут подключаться к базе данных.
   Файл pg_hba.conf (HBA означает Host-based authentication – проверка подлинности на основе хоста) контролирует проверку подлинности клиентов и хранится в каталоге данных кластера

базы данных. В нем указываются серверы, которым разрешено соединение, и их права, например

TYPE DATABASE USER ADDRESS METHOD

Loadbalancer1 (First Кибер Файлы & Gateway server)

host cyberfiles_production postgres 10.144.70.247/32 md5

Примечание

В этом примере учетная запись пользователя с именем postgres может подключаться с сервера по адресу 10.144.70.247 и получать доступ к базе данных cyberfiles_production со всеми правами (кроме права на **репликацию**) посредством подключения с хешированием MD5.

Откройте файл postgresql.conf и внесите изменения, описанные ниже.

1. Удалите первый символ # из следующей строки: #listen_addresses = 'localhost'. Замените localhost символом *. Строка должна иметь следующий вид: listen_addresses = '*'
2. Удалите первый символ # из следующей строки: #effective_cache_size = 128MB и замените **128MB** на **12GB**. Строка должна иметь следующий вид: effective_cache_size = 12GB
3. Добавьте следующее примечание: - #ПРИМЕЧАНИЕ. Этот параметр настройки предполагает, что PostgreSQL самостоятельно работает на #ВМ с оперативной памятью не менее 16 ГБ. Подробная информация на #https://wiki.postgresql.org/wiki/Tuning_Your_PostgreSQL_Server
4. Найдите параметр max_connections и замените его значение нужным значением. Оно не должно быть меньше суммы всех параметров DB_POOLSIZE Tomcat, заданных для каждого узла сервера Access, плюс 10. Рекомендуется задать для параметра DB_POOLSIZE значение 250.

   В этом примере мы задали значение DB_POOLSIZE до 250 и у нас два сервера Tomcat Access, поэтому для параметра max_connections должно быть установлено значение 510. Для трех серверов Tomcat Access значение будет равно 760.
5. Сохраните внесенные изменения и закройте файл **postgresql.conf**.
6. Перезапустите службу сервера PostgreSQL Кибер Файлы.

Импорт базы данных

На новом сервере PostgreSQL

1. Откройте приложение Кибер Файлы «Администратор PostgreSQL», подключитесь к локальному серверу базы данных, выберите **Базы данных** и проверьте наличие базы с именем cyberfiles_production.
2. Скопируйте резервный файл **alldbs.sql** базы данных в папку **bin** своей установки PostgreSQL (по умолчанию C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\PostgreSQL\<version>\bin)
3. Откройте командную строку с повышенными привилегиями и перейдите в папку **bin** PostgreSQL с помощью команды **cd**.
4. Введите следующую команду: psql -U postgres -f alldbs.sql

5. При появлении соответствующего запроса введите пароль для пользователя postgres . Таким образом, база данных на старом сервере PostgreSQL будет восстановлена на новый сервер PostgreSQL.

11.2.3.3 Конфигурация сервера Кибер Файлы

Подключение дополнительных серверов Кибер Файлы

Установка только веб-сервера Кибер Файлы

1. Запустите программу установки Кибер Файлы и примите условия лицензионного соглашения.
2. Выберите **Настраиваемый**, а затем ТОЛЬКО веб-сервер Кибер Файлы.

   Примечание
   При выборе веб-сервера Кибер Файлы также автоматически выбирается и сервер PostgreSQL, но его можно отключить щелчком мыши.

3. Завершите установку и убедитесь, что служба Кибер Файлы Tomcat остановлена.

Конфигурация сервера

Все настройки, измененные на одном веб-сервере Кибер Файлы, необходимо таким же образом изменить на всех других веб-серверах Кибер Файлы.

Примечание
Обязательно добавьте запись в файле pg_hba.conf для каждого веб-сервера Кибер Файлы!

11.2.4 Настройка сервера для подключения к требуемой базе данных

1. Перейдите в папку веб-сервера Кибер Файлы (по умолчанию C:\Program Files (x86)\Cyberprotect\Cyber Files\Access Server) и откройте файл cyberfilessrv.cfg . Этот файл сообщает серверу, где расположена служба базы данных PostgreSQL.
2. Задайте следующие значения:
   DB_HOSTNAME =10.144.70.248
   DB_PORT =5432
   DB_POOLSIZE =250

   Примечание
   DB_HOSTNAME – это IP-адрес, на котором сейчас запущена служба PostgreSQL. В данном примере это 10.144.70.248.

   Примечание

Рекомендуется настройка DB_POOLSIZE со значением минимум 250.

3. Сохраните файл.

11.2.5 Настройка максимального числа потоков

В установке Tomcat с балансировкой нагрузки важно, чтобы общее число всех потоков, которые могут создавать экземпляры Tomcat, не превышало максимального числа подключений, настроенных для приема в базе данных PostgreSQL.

Это определяется 3 важными настройками:

- В файле cyberfilessrv.cfg: DB_POOLSIZE = 200. Рекомендуется установить значение минимум 250.
- В файле Tomcat server.xml: maxThreads = 150. Рекомендуется оставить значение 150 по умолчанию.
- В файле postgresql.conf задайте значение max_connections. Этот параметр должен быть настроен на предыдущих этапах. Однако его значение не должно быть меньше суммы всех значений DB_POOLSIZE в Tomcat, заданных для каждого сервера Кибер Файлы, плюс 10. Например, 510 для 2 серверов Tomcat, 760 для 3 серверов Tomcat и т. д.

Примечание
Для изменений, внесенных в эти файлы, требуется перезагрузка соответствующих служб.

11.2.6 Настройка правильного входа в систему

В конфигурации с балансировкой нагрузки служба Tomcat Кибер Файлы не указывает правильные IP-адреса в журналах. Чтобы убедиться, что каждое подключение зарегистрировано правильно, внесите изменения, описанные ниже.

1. В файле server.xml найдите строку <Valve className=”org.apache.catalina.valves.AccessLogValve” directory=”logs” prefix=”localhost_access_log.” suffix=”.txt” pattern=”%h %l %u %t "%r" %s %b”/>.
2. Добавьте requestAttributesEnabled=”true” в конце строки.
3. Под ней добавьте следующее:
   <Valve className="org.apache.catalina.valves.RemoteIpValve" remoteIpHeader="X-Forwarded-For" protocolHeader="X-Forwarded-Proto"/>

Предупреждение
Если также используется функция ограничения IP-адресов, избегайте установки заголовка XFF, так как это может оказать влияние на безопасность пользователя, связанную с этой функцией. Вместо этого рекомендуется настроить балансировку нагрузки для доверия адресам XFF, добавляемым прокси-сервером. В таком случае заголовок XFF из запросов

также будет копироваться (даже если это уже так).

4. Сохраните файл и перезапустите службу Кибер Файлы Tomcat.

Соединение со старым сервером Кибер Файлы

При желании вы можете и дальше использовать имеющийся сервер Кибер Файлы, однако его необходимо подключить к новой базе данных.

Подключение Кибер Файлы к удаленной базе данных

1. Перейдите в папку веб-сервера Кибер Файлы (по умолчанию C:\Program Files (x86)\Cyberprotect\Cyber Files\Access Server) и откройте файл cyberfilessrv.cfg . Этот файл сообщает серверу, где расположена служба базы данных PostgreSQL.
2. Задайте следующие значения:

   DB_HOSTNAME =10.144.70.248

   DB_PORT =5432

   DB_POOLSIZE = 250

   Примечание
   DB_HOSTNAME задает IP-адрес, на котором располагается база данных PostgreSQL. В данном примере это 10.144.70.248.

3. Сохраните файл и запустите службу **Кибер Файлы Tomcat** на панели управления **Службы** (services.msc).
4. Все неиспользуемые компоненты Кибер Файлы можно удалить.

11.2.6.1 Миграция хранилища и файлового репозитория

Ознакомьтесь с нашим руководством Перенос хранилища и файлового репозитория. Необходимо проверить только одну дополнительную настройку: убедиться, что у компонентов Кибер Файлы есть доступ к компьютеру, на котором размещаются репозиторий и хранилище файлов.

Если планируется использовать хранилище S3, службу файлового репозитория устанавливать не нужно, так как хранилище файлов будет располагаться в хранилище S3 по вашему выбору.

Если планируется оставить репозиторий и хранилище файлов в месте первоначального их расположения, убедитесь только, что новые серверы Кибер Файлы указывают на соответствующую конечную точку репозитория.

11.2.6.2 Миграция сервера шлюза

Установка нового сервера шлюза

1. На новом компьютере запустите программу установки Кибер Файлы и примите условия лицензионного соглашения.

2. Выберите пункт **Пользовательская** и установите только компонент сервера шлюза. Завершите установку.
3. В инструменте конфигурации задайте адрес, порт и сертификат шлюза. Это должен быть тот же SSL-сертификат, что привязан к DNS-адресу балансировщика нагрузки шлюза.

Миграция всех настроек с предыдущего сервера шлюза

1. На старом компьютере с установленными шлюзом и службой Tomcat откройте веб-интерфейс сервера Кибер Файлы и страницу серверов шлюза. Отобразится запись, обозначающая старый шлюз.
2. Добавьте новый шлюз, нажав **Добавить сервер шлюза**, и введите все актуальные данные.
3. Нажмите **Добавить кластерную группу**.
   - Введите отображаемое имя.
   - Введите **Адрес для клиентских подключений**. В этом кластере «**Адрес для клиентских подключений**» – это адрес внешнего балансировщика нагрузки. Затем нажмите «**Использовать альтернативный адрес для... подключения к серверу**», а в поле «**Адрес для подключения к серверу Кибер Файлы** » введите внутренний адрес балансировщика нагрузки шлюза.
4. В строке **Серверы шлюза, доступные для кластеризации** установите флажок **Включить** для обоих серверов шлюза.
5. В строке **Сервер шлюза, настройки которого будут ведущими** выберите старый сервер шлюза.
6. Нажмите кнопку **Добавить**, и на странице сервера шлюза отобразится новый кластер. Раскройте его, нажав знак «плюс» (+).
7. Теперь в новом шлюзе должны оказаться все перенесенные настройки. Назначьте новый шлюз главным для кластера, открыв раскрывающееся меню **Действия** и выбрав пункт **Сделать основным для группы**.
8. Можно оставить старый шлюз как есть, убрать его из группы кластеров или убрать и удалить его. Рекомендуется оставить его как часть кластера до момента полной настройки и правильной работы.

11.2.6.3 Управление журналами и их очистка

После установки дополнительных серверов Кибер Файлы необходимо перейти к папке, где хранятся журналы Кибер Файлы Tomcat, и задать нужные права в этих файлах, чтобы журналы можно было записывать и очищать.

11.2.6.4 Настройки, характерные для средств балансировки нагрузки

1. Откройте в браузере адрес https://mylb.company.com, чтобы проверить работу созданной конфигурации.
2. Включите функцию поддержания сеанса на основе длительности (или ее аналог) в своем балансировщике нагрузки и задайте бессрочные сеансы.

3. Если требуется проверка работоспособности (проверка на получение HTTP-статуса 200), это можно сделать отправкой команды на адрес https://INTERNALSERVERNAME:MANAGEMENTPORT/api/v1/server_version (то есть https://myaccessserver.company.com/signin и https://myaccessserver.company.com/api/v1/server_version).
4. Чтобы обеспечить правильную регистрацию IP-адресов и подключений в установке с балансировкой нагрузки, необходимо настроить средство балансировки нагрузки с помощью следующих заголовков:
   - Поле X-Forwarded-For – определение реально используемых IP-адресов подключаемых клиентов вместо IP-адресов средства балансировки нагрузки для каждого подключения.
   - Поле X-Forwarded-Proto – определение реально используемого протокола.

11.2.6.5 Очистка исходных серверов

Если вы продолжаете использовать Tomcat Кибер Файлы, который находится на исходном рабочем сервере, рекомендуется удалить элементы Кибер Файлы, которые больше там не используются.

На панели управления можно удалить сервер PostgreSQL, сервер шлюза и сервер файлового репозитория Кибер Файлы (при наличии).

11.2.7 Настройка веб-интерфейса через API

С помощью API можно легко обновить цветовую схему веб-интерфейса без перезапуска служб и простоя систем. Некоторые из этих настроек можно выполнить через веб-интерфейс Кибер Файлы .

Установка CURL

1. Чтобы использовать команды API, потребуется установить Curl.
   a. Скачайте Curl с официального сайта по адресу https://curl.haxx.se/download.html

   Примечание
   Убедитесь, что скачиваете версию с поддержкой SSL!

   b. Следуйте инструкциям программы установки Curl до завершения процесса или просто распакуйте архив Curl.

11.2.7.1 Создание особой цветовой схемы

1. Откройте командную строку с повышенными привилегиями и введите следующую команду:
   curl -X PUT -F customization_settings[color_scheme_administration_css_file]=@<path_to_file> -F customization_settings[color_scheme_client_scss_file]=@<path_to_file> -u <user>:<password> https://<your_site>/api/v1/settings/customization -v

Примечание
В именах файлов необходимо использовать определенный синтаксис именования! color_scheme_<**name_of_scheme>**.css для консоли администрирования и web_client_<**name_of_scheme>**.scss для консоли веб-клиента. <**name_of_scheme>** – имя новой схемы, которое будет отображаться в интерфейсе Кибер Файлы и должно быть одинаковым для обоих файлов.

Приведенная выше команда:

- Выберет **.css**-файл для консоли администрирования.
- Выберет **.scss**-файл для консоли веб-клиента.
- Создаст новую тему, которую можно будет выбрать из раскрывающегося списка **Цветовая схема** в веб-интерфейсе.

Примечание
Если нужно изменить лишь часть цветовой схемы, то при вводе приведенной выше команды необходимо использовать новую .css-схему для изменившейся части и существующую .css-схему для части, которую не требуется изменять.

2. Ниже приводится пример команд для отправки схемы для административной части интерфейса и схемы для веб-клиента, которые обнаружены.
3. В данном примере оба файла находятся в D:\WebUI и мы выбираем **NewColor** в качестве имени цветовой схемы, видимой в веб-интерфейсе:
   curl -X PUT -F customization_settings[color_scheme_administration_css_file]=@D:\WebUI\color_scheme_NewColor.css -F customization_settings[color_scheme_client_scss_file]=@D:\WebUI\web_client_NewColor.scss -u administrator:123456 https://myCompany.com/api/v1/settings/customization
4. Можно также использовать команду -F customization_settings[color_scheme]=<name_of_scheme> для переключения текущей темы на новую, ту, которую вы добавляете. Добавление этой команды к остальным выглядит следующим образом:
   curl -X PUT -F customization_settings[color_scheme_administration_css_file]=@D:\WebUI\color_scheme_NewColor.css -F customization_settings[color_scheme_client_scss_file]=@D:\WebUI\web_client_NewColor.scss -F customization_settings[color_scheme]=NewColor -u administrator:123456 https://myCompany.com/api/v1/settings/customization -v

Устранение неполадок

- Команда выполнена, но в интерфейсе не отображается новая тема
  Убедитесь, что имена файлов соответствуют синтаксису, определенному в **color_scheme_<name_of_scheme>.css** и **web_client_<name_of_scheme>.scss**
- Получена ошибка **Протокол https не поддерживается или отключен в libcurl**
  Удалите все одинарные кавычки (') вокруг вашего адреса. Если необходимо использовать кавычки, используйте двойные кавычки (""), например "https://myCompany.com/api/v1/settings/customization"
- Получена ошибка сертификата

Если вы используете самозаверенные сертификаты или выполняете команды с использованием IP-адреса, необходимо добавить флаг **-k** в конце команды, чтобы игнорировать ошибки сертификатов.

11.2.8 Автоматическая настройка клиента для ПК

Функции управления групповыми политиками Майкрософт дают возможность легко установить и настроить клиента для ПК Кибер Файлы на нескольких компьютерах удаленно. Конечному пользователю потребуется только запустить клиент, а затем ввести пароль. Функции управления групповыми политиками также гарантируют, что пользователи случайно не изменят правильные настройки. В этом случае они просто выйдут из системы, а после входа верные настройки будут применены снова.

Создание и настройка объекта управления групповой политикой:

1. На контроллере домена откройте консоль **управления групповыми политиками**.
2. Щелкните правой кнопкой нужный домен и выберите команду **Создать объект GPO в этом домене и связать его...**
3. Введите имя и нажмите кнопку **OK**.
4. Разверните раздел **Объекты групповой политики** и выберите новую политику.
5. На вкладке **Область** выберите требуемые сайты, домены, подразделения, группы, пользователей и компьютеры.

11.2.8.1 Автоматическая установка клиента

Этот раздел поможет установить клиента для ПК Кибер Файлы в автоматическом режиме при входе пользователя на всех необходимых компьютерах.

Создание точки распространения программы установки

Все компьютеры, на которых будет установлен клиент, должны иметь доступ к программе установки. Это можно сделать, создав папку, предоставив к ней доступ необходимым пользователям и поместив в эту папку программу установки.

1. Щелкните правой кнопкой мыши папку с программой установки и выберите **Свойства**.
2. Откройте вкладку **Общий доступ** и нажмите кнопку **Общий доступ**.
3. Введите группу домена, организационную единицу или пользователей, которым будет установлен клиент. Это должна быть та же группа (или другой объект), что и в поле **Объект групповой политики**.
4. Нажмите кнопку **OK/Готово** и закройте все остальные диалоговые окна.

Примечание
Программа установки должна быть доступна для необходимых компьютеров по своему сетевому адресу (например, \\WIN2008\Software\AAClientInstaller.msi)

Получение программы установки на компьютере пользователя

1. На контроллере домена разверните раздел **Объекты групповой политики** и щелкните правой кнопкой новый объект политики.
2. Выберите команду **Изменить** и разверните узел **Конфигурация пользователя** -> **Настройки** -> **Параметры Windows** -> **Файлы**.
3. Щелкните правой кнопкой «Файлы» и выберите «Создать» -> «Файл».
4. Выберите **Создать** в поле **Действие**.
5. В поле **Исходные файлы** либо нажмите кнопку обзора и перейдите к программе установки клиента, либо введите полный путь к ней (например, \\WIN2008\Software\AAClientInstalelr.msi).
6. В поле **Файл назначения** введите папку назначения и имя файла назначения. Программа установки клиента будет скопирована из сетевой общей папки и помещена в папку назначения на компьютере пользователя при входе в систему.

   Примечание
   если ввести **C:\Folder\ThisFile.msi**, то программа установки клиента будет помещена на пользовательский диск **C** в папку Folder и получит имя **ThisFile.msi**.

7. Нажмите кнопку **OK**.

Установка клиентской части

Создание сценария установки

1. Создайте пустой текстовый файл и вставьте в него следующий сценарий:

   msiexec /i "C:\AAC.msi" /quiet

   sleep 180

   DEL /F /S /Q /A "C:\AAC.msi"

   Этот сценарий откроет командную строку, установит клиент, ничего при этом не отображая, и удалит программу установки через 3 минуты.
2. Замените путь C:\AAC.msi в обоих местах путем, который был введен в поле **Файл назначения**, а затем выберите **Файл** -> **Сохранить как...**
3. Введите имя для сценария и убедитесь, что оно имеет расширение **.bat**. В поле **Тип файла:** выберите **Все файлы**. Убедитесь, что файл либо находится на контроллере домена, либо доступен с него. Этот файл важен и его нельзя изменять или удалять, поэтому его нужно поместить в определенное место, которое не изменится.

Использование сценария при входе пользователя

1. Откройте **Управление групповыми политиками**, разверните раздел **Объекты групповой политики** и щелкните правой кнопкой мыши новый **Объект политики**.
2. Выберите команду **Изменить** и разверните узел **Конфигурация пользователя** -> **Политики** -> **Параметры Windows** -> **Сценарии (вход/выход)**.
3. Дважды щелкните **Вход** и нажмите **Добавить**.

4. В диалоговом окне **Добавление сценария** нажмите **Обзор (...)** и перейдите в папку, где был сохранен сценарий.
5. Выберите сценарий и нажмите **Открыть**.
6. Нажмите **OK**, затем еще раз нажмите **OK** в следующем диалоговом окне.
7. Готово. Всем пользователям в указанной группе или подразделении теперь будет установлен клиент Кибер Файлы при входе в систему.

11.2.8.2 Создание папки и записей реестра

В этом примере мы создадим записи для полей «Имя пользователя», «Папка синхронизации», «URL-адрес сервера», флажка «Автоматическое обновление» и укажем, следует ли клиенту подключаться к серверам с самозаверенными сертификатами.

1. Разверните раздел **Объекты групповой политики** и щелкните правой кнопкой по новому объекту политики.
2. Выберите команду **Изменить** и разверните узел **Конфигурация пользователя** -> **Настройки** -> **Параметры Windows**.

Создание синхронизируемой папки:

1. Щелкните правой кнопкой **Папки** и выберите **Создать** -> **Папка**.
2. Выберите для параметра **Действие** значение **Создать**.
3. Для пути введите следующий токен: %USERPROFILE%\Desktop\AAS Data Folder

Создание реестра:

1. Щелкните правой кнопкой **Реестр** и выберите **Создать** -> **Элемент реестра**.
2. Выберите для параметра **Действие** значение **Создать**.
3. Для параметра **Куст** выберите **HKEY_CURRENT_USER**.
4. Введите следующий путь: Software\Group Logic, Inc.\activEcho Client\
5. Теперь выполните следующие действия с необходимыми записями.
6. Для имени пользователя:
   a. В поле **Имя значения** введите **Username**.
   b. В поле **Тип значения** выберите **REG_SZ**.
   c. В поле **Значение данных** введите следующий токен: %USERNAME%@%USERDOMAIN%

Примечание
Если необходимо использовать **Единый вход**, то **не следует** настраивать токен «Имя пользователя». Вместо этого выполните следующие действия.

- **Для SSO**:
- В поле **Имя значения** введите **AuthenticateViaSSO**.

- В поле **Тип значения** выберите **REG_SZ**.
- В поле **Значение данных** введите **1**.

7. Для URL-адреса сервера:
   a. В поле **Имя значения** введите **Server URL**.
   b. В поле **Тип значения** выберите **REG_SZ**.
   c. В поле **Значение данных** введите адрес сервера Кибер Файлы, например **https://myaccess.com**
8. Для синхронизируемой папки:
   a. В поле **Имя значения** введите **activEcho Folder**.
   b. В поле **Тип значения** выберите **REG_SZ**.
   c. В поле **Значение данных** введите следующий токен и путь: %USERPROFILE%\Desktop\AAS Data Folder
9. Для автоматического обновления:
   a. В поле **Имя значения** введите **AutoCheckForUpdates**.
   b. В поле **Тип значения** выберите **DWORD**.
   c. В поле **Значение данных** введите **00000001**. Значение **1** включает этот параметр, после чего клиент будет автоматически проверять наличие обновлений. Если задать значение **0**, параметр будет отключен.
10. Для сертификатов:
    a. В поле **Имя значения** введите **AllowInvalidCertificates**.
    b. В поле **Тип значения** выберите **DWORD**.
    c. В поле **Значение данных** введите **00000000**. Значение **0** отключает этот параметр, и клиент не сможет подключиться к серверам Кибер Файлы с использованием недействительных сертификатов. Если задать значение **1**, параметр будет включен.

11.2.9 Настройка единого входа

В этом руководстве описываются расширенные настройки функции единого входа при работе с Кибер Файлы.

Примечание
Единый вход может использоваться только при рабочем домене.

Примечание
Единый вход не работает, если для Кибер Файлы используется конфигурация с одним портом, когда сервер шлюза перенаправляет запросы на сервер Кибер Файлы.

Единый вход не работает, если программа Кибер Файлы установлена на контроллере домена. Кроме того, независимо от ограничений SSO, в целях повышения производительности настоятельно не рекомендуется устанавливать сервер Кибер Файлы на контроллере домена.

Функция единого входа позволяет всем действительным пользователям LDAP входить в веб-интерфейс и клиент для ПК, не вводя своих учетных данных. Пользователь должен иметь учетную запись Кибер Файлы, либо на сервере должно быть включено распределение ресурсов LDAP.

- Кибер Файлы отображает на странице входа ссылку, по которой пользователь может войти с учетной записью, которая использовалась для входа на этот компьютер.

  Примечание
  Чтобы обеспечить единый вход, необходимо открыть интерфейс Кибер Файлы по его полному доменному имени (например, https://access.company.com). Единый вход не работает, если вы открываете интерфейс через IP-адрес. Имена пользователей должны находиться в том же домене, что и основная настройка единого входа, чтобы пользователи могли получить доступ к своей папке "Sync & Share" через KCD из мобильных приложений.

- В настольном клиенте предусмотрен новый переключатель, который включает единый вход. Пользователю достаточно ввести URL-адрес сервера Кибер Файлы. После этого он автоматически войдет в систему с учетной записью, использованной для входа в компьютер.

  Примечание
  Но это применимо только для клиентов Windows. Поддержка Mac будет предусмотрена в следующем выпуске.

  Примечание
  SSO с настольного клиента требует доступа к корпоративной сети. Это означает, что пользователь SSO должен иметь также доступ к собственной сети.

11.2.9.1 Веб-сервер Кибер Файлы и шлюз на одной машине

Это самая распространенная конфигурация, которая состоит из одного веб-сервера Кибер Файлы и одного сервера шлюза Кибер Файлы, расположенных на одной и той же машине. Это вариант установки по умолчанию.

В домене

Это выполняемое однократно действие, которое должно быть выполнено для регистрации веб-сервера Кибер Файлы на сервере Kerberos в данном домене. Мы будем использовать setspn.exe для указания того, к какой учетной записи LDAP будет сделан запрос для проверки подлинности единого входа.

Примечание
Если вы хотите использовать **мобильные клиенты с проверкой подлинности по сертификатам**, то DNS-записи для веб-сервера Кибер Файлы и сервера шлюза **не должны совпадать** с именем компьютера. Если SPN веб-сервера Кибер Файлы представляет собой имя компьютера, сервер шлюза будет воспринимать сервер Кибер Файлы как расположенный «на моем компьютере» и не будет выполнять проверку подлинности Kerberos.
Например, computerAccess.domain.com/computer.domain.com и computerAccess.domain.com/computerGW.domain.com будут работать, а computer.domain.com/computerGW.domain.com не будет.

Настройка учетной записи LDAP для осуществления единого входа

Примечание
Если требуется использование источников данных SMB или SharePoint, то необходимо настроить учетную запись Active Directory таким образом, чтобы разрешить делегирование Kerberos для каждого из источников данных SMB и SharePoint. Дополнительные сведения см. в статье Дополнительная настройка делегирования.

1. Откройте командную строку.

   Примечание
   Необходимо войти в систему от имени учетной записи домена с правами на использование **setspn**.

2. Введите команду setspn -s HTTP/**computername.domain.com account name**

   Пример. Если ваш веб-сервер Кибер Файлы установлен на ahsoka.acme.com и вы хотите использовать john@acme.com в качестве учетной записи LDAP с предварительной проверкой подлинности для получения билетов Kerberos, то команда будет выглядеть так:
   setspn -s HTTP/ahsoka.acme.com john

   Примечание
   Имя учетной записи LDAP, используемое в приведенной выше команде, **ДОЛЖНО** соответствовать учетной записи, которую вы укажете в свойстве spnego.preauth.username в файле web.xml.

   Примечание
   Как правило, эта учетная запись совпадает с учетной записью LDAP, указываемой администратором в веб-интерфейсе Кибер Файлы в меню **Общие настройки**-> **LDAP** -> **Имя пользователя LDAP**/ **Пароль LDAP**, но это не обязательно.

3. Если веб-сервер Кибер Файлы работает на порте, отличном от порта по умолчанию (то есть любой порт, кроме 443), следует также зарегистрировать SPN с указанием этого номера порта.

   Например, Если сервер работает на порту 444, команда принимает вид:

setspn -s HTTP/ahsoka.acme.com:444 john

Примечание
Значение **HTTP** в приведенных выше командах относится к классу службы **HTTP**, а не к протоколу **HTTP**. Класс службы **HTTP** обрабатывает запросы и **HTTP** и **HTTPS** . Не требуется и **НЕ СЛЕДУЕТ** создавать SPN с использованием **HTTPS** в качестве имени класса службы.

4. Перейдите на контроллер домена и откройте **Пользователи и компьютеры Active Directory**.
5. Найдите пользователя, который использовался в приведенных выше командах (в данном случае **john**).
6. Откройте вкладку **Делегирование** и выберите **Доверять этому пользователю делегирование любой службы (только Kerberos)**.
7. Нажмите кнопку **OK**.

Настройка SPN для сервера шлюза

Чтобы сервер Kerberos в роли KDC (Центр распределения ключей) мог проверять подлинность пользователи на сервере шлюза, необходимо зарегистрировать службу шлюза на сервере KDC. Выполните команду setspn, указав в командной строке имя узла сервера, на котором она работает как user.

Для работы в такой конфигурации потребуется внести дополнительную DNS-запись для используемого сервера шлюза.

1. На своем сервере DNS откройте **Зоны опережающего просмотра** для используемого домена, щелкнув правой кнопкой мыши и создав новую запись **узла** (запись A) для сервера шлюза.
2. Введите наименование. Оно будет адресом DNS, который будет использоваться для доступа к серверу шлюза.
   Например, ahsoka-gw.acme.com
3. Введите IP-адрес сервера шлюза (без порта). Если серверы шлюза и Кибер Файлы находятся на одном и том же IP-адресе, введите этот IP-адрес.
4. Выберите **Создать связанную запись указателя (PTR)** и нажмите **Добавить узел**.
5. Вернитесь к компьютеру с Кибер Файлы.
6. Откройте командную строку.
7. Введите следующую команду **setspn**: setspn -s HTTP/**gatewaydns.domain.com computername**
   Например, если используемый сервер шлюза работает на узле ahsoka в домене и используется DNS-запись ahsoka-gw.acme.com, выполните следующую команду:
   setspn -s HTTP/ahsoka-gw.acme.com ahsoka
8. Если сервер шлюза работает на порту, отличном от заданного по умолчанию (то есть на любом, кроме 443), необходимо также зарегистрировать имя участника-службы, указав номер порта; например, если сервер шлюза работает на порту 444:
   setspn -s HTTP/ahsoka-gw.acme.com:444 ahsoka

9. Измените параметры **Адрес для администрирования** и **Адрес для клиентских подключений** нужного вам сервера шлюза, указав в них новую запись DNS сервера шлюза, которая была создана на шаге 4.

Примечание
Оба адреса должны быть одинаковыми. В них необходимо указать правильную запись DNS.

На сервере Кибер Файлы

11.2.9.2 Установка учетной записи домена для проверки подлинности единого входа

1. Перейдите в папку C:\Program Files (x86)\Cyberprotect\Cyber Files\Access Server\Web Application\WEB-INF\
2. Найдите и откройте файл web.xml. В этом файле необходимо задать логин и пароль домена, в котором будет работать служба единого входа. Эта учетная запись **должна** совпадать с учетной записью, которую вы использовали для регистрации службы HTTP в Kerberos в разделе **В домене**.
3. В файле web.xml требуется задать два параметра: имя пользователя домена и пароль, с которыми будет работать служба единого входа. Найдите следующие строки:

```
<init-param>
<param-name>spnego.preauth.username</param-name>
<param-value>yourusername</param-value>
</init-param>
<init-param>
<param-name>spnego.preauth.password</param-name>
<param-value>yourpassword</param-value>
</init-param>
```

4. Замените **yourusername** на требуемое имя пользователя LDAP.
5. Замените **yourpassword** на пароль LDAP для указанной выше учетной записи LDAP. Если ваш пароль содержит один из следующих пяти специальных символов: **&**, **>**, **"**, **'** или **<**, их необходимо будет экранировать в XML-документе. Для этого замените символы следующим образом:
   - **<** на **<**
   - **>** на **>**
   - **"** на **"**
   - **'** на **'**
   - **&** на **&**

   например, если ваш пароль – <my&best'password", его необходимо записать в файле web.xml как <my&best'password"

11.2.9.3 Настройка поиска доменов Kerberos

1. Перейдите в папку C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\apache-tomcat-7.0.59\conf
2. Найдите и откройте файл krb5.conf
3. В файле krb5.conf администратору необходимо задать только два параметра:
   a. Доменное имя для единого входа (например, ACME.COM). Обратите внимание, что это должно быть имя вашего домена, а **не** DNS-имя сервера.

   Примечание
   Доменное имя в файле krb5.conf следует указывать в **ВЕРХНЕМ РЕГИСТРЕ**, иначе поиск билетов Kerberos может завершиться неудачно.

   b. Адрес центра распределения ключей Kerberos (обычно соответствует адресу контроллера основного домена, например acmedc.ACME.COM)
4. Файл krb5.conf в нашем случае выглядит следующим образом:

```
[libdefaults]
  default_realm = ACME.COM
  default_tkt_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
  default_tgs_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
  permitted_enctypes  = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
  [realms]
  ACME.COM = {
  kdc = acmedc.ACME.COM
  default_domain = ACME.COM
  [domain_realm]
  .ACME.COM = ACME.COM
```

5. Замените все вхождения ACME.COM именем своего домена (**в верхнем регистре!**). Обратите внимание, что это должно быть имя вашего домена, а **не** DNS-имя сервера.
6. Замените значение «kdc =» на имя вашего контроллера домена. Имя домена должно быть записано прописными буквами, например kdc = yourdc.YOURDOMAIN.COM
7. После обновления файлов конфигурации следует перезапустить сервер Кибер Файлы (службу Tomcat для Кибер Файлы), чтобы изменения вступили в силу.

11.2.9.4 Включение единого входа в веб-интерфейсе

1. Откройте веб-интерфейс Кибер Файлы и войдите в него как администратор.
2. Перейдите на вкладку **Общие настройки** и откройте страницу **LDAP**.
3. В нижней части страницы установите флажок **Разрешить вход из веб-клиента и клиента для настольных ПК с синхронизацией с использованием имеющихся учетных данных**

Windows/Mac.

4. Выберите **Сохранить**.

Добавление других серверов шлюза

Примечание
Эти шаги работают, только если машины, на которых устанавливаются серверы шлюзов, расположены в одном домене с веб-сервером Кибер Файлы.

Чтобы сервер Kerberos в роли KDC (Центра распределения ключей) мог проверять подлинность пользователей на сервере шлюза, необходимо зарегистрировать службу шлюза на сервере KDC. Выполните команду setspn, указав в командной строке имя узла сервера, на котором работает служба, как user.

11.2.9.5 Для любого сервера шлюза, расположенного не на той же машине, что веб-сервер Кибер Файлы

1. Откройте командную строку.
2. Введите следующую команду **setspn**: setspn -s HTTP/**computername.domain.com computername**
   Например, если сервер шлюза работает на узле cody в этом домене, выполните следующую команду:
   setspn -s HTTP/cody.acme.com cody
3. Если сервер шлюза работает на порту, отличном от заданного по умолчанию (то есть на любом, кроме 443), необходимо также зарегистрировать имя участника-службы, указав номер порта; например, если сервер шлюза работает на порту 444:
   setspn -s HTTP/cody.acme.com:444 cody
4. Повторите эту процедуру для каждого дополнительного сервера шлюза.

Разовая конфигурация для леса доменов

Есть небольшая разовая настройка, которую необходимо выполнить для включения поддержки единого входа в браузере.

Внимание
Это следует сделать для каждого пользователя на каждой машине.

Примечание
В инструкциях к конфигурации в качестве примера используется *acme.com*. Если ваши службы находятся в разных доменах, повторите шаги, в которых указывается *acme.com*, для всех ваших доменов. (**Например,** добавьте **.acme.com* и **.another.com* и **.yetanother.com*).

11.2.9.6 Сервер Кибер Файлы и сервер шлюза на разных машинах

В домене

Это выполняемое однократно действие, которое должно быть выполнено для регистрации сервера Кибер Файлы на сервере Kerberos в данном домене. Мы будем использовать setspn.exe для указания того, к какой учетной записи LDAP будет сделан запрос для проверки подлинности единого входа.

Примечание
Если вы хотите использовать **мобильные клиенты с проверкой подлинности по сертификатам**, то DNS-записи для веб-сервера Кибер Файлы и сервера шлюза **НЕ** должны являться именем данного компьютера. Если SPN сервера Кибер Файлы представляет собой имя машины, сервер шлюза будет воспринимать сервер Кибер Файлы как расположенный «на моей машине» и не будет выполнять проверку подлинности Kerberos.
Например,
computerAccess.domain.com / computer.domain.com и computerAccess.domain.com / computerGW.domain.com сработает, а computer.domain.com / computerGW.domain.com – НЕТ.

Настройка учетной записи LDAP для осуществления единого входа

Примечание
Если требуется использование источников данных SMB или SharePoint, то необходимо настроить учетную запись Active Directory таким образом, чтобы разрешить делегирование Kerberos для каждого из источников данных SMB и SharePoint. Дополнительные сведения см. в статье Дополнительная настройка делегирования.

1. Откройте командную строку.

   Примечание
   Необходимо войти в систему от имени учетной записи домена с правами на использование **setspn**.

2. Введите команду setspn -s HTTP/**computername.domain.com account name**

   Пример. Если ваш сервер Кибер Файлы установлен на ahsoka.acme.com и вы хотите использовать john@acme.com в качестве учетной записи LDAP с предварительной проверкой подлинности для получения билетов Kerberos, то команда будет выглядеть так:
   setspn -s HTTP/ahsoka.acme.com john

   Примечание
   Имя учетной записи LDAP, используемое в приведенной выше команде, **ДОЛЖНО** соответствовать учетной записи, которую вы укажете в свойстве spnego.preauth.username в файле web.xml.

Примечание
Как правило, эта учетная запись совпадает с учетной записью LDAP, указываемой администратором в веб-интерфейсе Кибер Файлы в меню **Общие настройки**-> **LDAP** -> **Имя пользователя LDAP**/ **Пароль LDAP**, но это не обязательно.

3. Если сервер Кибер Файлы работает на порте, отличном от порта по умолчанию (то есть любой порт, кроме 443), следует также зарегистрировать SPN с указанием номера порта.
   Например, Если сервер работает на порту 444, команда принимает вид:
   setspn -s HTTP/ahsoka.acme.com:444 john

Примечание
Значение **HTTP** в приведенных выше командах относится к классу службы **HTTP**, а не к протоколу **HTTP**. Класс службы **HTTP** обрабатывает запросы и **HTTP** и **HTTPS** . Не требуется и **НЕ СЛЕДУЕТ** создавать SPN с использованием **HTTPS** в качестве имени класса службы.

4. Перейдите на контроллер домена и откройте **Пользователи и компьютеры Active Directory**.
5. Найдите пользователя, который использовался в приведенных выше командах (в данном случае **john**).
6. Откройте вкладку **Делегирование** и выберите **Доверять этому пользователю делегирование любой службы (только Kerberos)**.
7. Нажмите кнопку **OK**.

Настройка SPN для сервера шлюза

Чтобы сервер Kerberos в роли KDC (Центр распределения ключей) мог проверять подлинность пользователи на сервере шлюза, необходимо зарегистрировать службу шлюза на сервере KDC. Выполните команду setspn, указав в командной строке имя узла сервера, на котором она работает как user.

11.2.9.7 Для любого сервера шлюза, расположенного не на той же машине, что сервер Кибер Файлы

1. Откройте командную строку.
2. Введите следующую команду **setspn**: setspn -s HTTP/**computername.domain.com computername**
   Например, если сервер шлюза работает на узле 'cody' в этом домене, выполните следующую команду:
   setspn -s HTTP/cody.acme.com cody
3. Если сервер шлюза работает на порту, отличном от заданного по умолчанию (то есть на любом, кроме 443), необходимо также зарегистрировать имя участника-службы, указав номер порта; например, если сервер шлюза работает на порту 444:
   setspn -s HTTP/cody.acme.com:444 cody
4. Повторите эту процедуру для каждого сервера шлюза.

11.2.9.8 Если на машине с сервером Кибер Файлы установлен сервер шлюза

Этот пункт необходим, только если сервер шлюза установлен на одной с сервером Кибер Файлы. Если нет, пропустите этот раздел. Для работы в такой конфигурации потребуется внести дополнительную DNS-запись для используемого сервера шлюза.

1. На своем сервере DNS откройте **Зоны опережающего просмотра** для используемого домена, щелкнув правой кнопкой мыши и создав новую запись **узла** (запись A) для сервера шлюза.
2. Введите наименование. Оно будет адресом DNS, который будет использоваться для доступа к серверу шлюза.

   Например, codygw.acme.com
3. Введите IP-адрес сервера шлюза (без порта). Если серверы шлюза и Кибер Файлы находятся на одном и том же IP-адресе, введите этот IP-адрес.
4. Выберите **Создать связанную запись указателя (PTR)** и нажмите **Добавить узел**.
5. Вернитесь к компьютеру с Кибер Файлы.
6. Откройте командную строку.
7. Введите следующую команду **setspn**: setspn -s HTTP/**gatewaydns.domain.com computername**

   Например, если используемый сервер шлюза работает на узле 'cody' в домене и используется DNS-запись codygw.acme.com, выполните следующую команду:

   setspn -s HTTP/codygw.acme.com cody
8. Если сервер шлюза работает на порту, отличном от заданного по умолчанию (то есть на любом, кроме 443), необходимо также зарегистрировать имя участника-службы, указав номер порта; например, если сервер шлюза работает на порту 444:

   setspn -s HTTP/codygw.acme.com:444 cody
9. Если это еще не сделано, необходимо изменить соответствующий **адрес администрирования** сервера шлюза таким образом, чтобы он совпадал с DNS-записью сервера шлюза, созданной на шаге 4.

На сервере Кибер Файлы

11.2.9.9 Отредактируйте файл web.xml:

1. Перейдите в папку C:\Program Files (x86)\Cyberprotect\Cyber Files\Access server\Web Application\WEB-INF\
2. Найдите и откройте файл web.xml. В этом файле необходимо задать логин и пароль домена, в котором будет работать служба единого входа. Эта учетная запись **должна** совпадать с учетной записью, которую вы использовали для регистрации службы HTTP в Kerberos в разделе **В домене**.
3. В файле web.xml требуется задать два параметра: имя пользователя домена и пароль, с которыми будет работать служба единого входа. Найдите следующие строки:

<init-param>
<param-name>spnego.preauth.username</param-name>
<param-value>yourusername</param-value>
</init-param>
<init-param>
<param-name>spnego.preauth.password</param-name>
<param-value>yourpassword</param-value>
</init-param>

4. Замените **yourusername** на требуемое имя пользователя LDAP.
5. Замените **yourpassword** на пароль LDAP для указанной выше учетной записи LDAP. Если ваш пароль содержит один из следующих пяти специальных символов: **&**, **>**, **"**, **'** или **<**, их необходимо будет экранировать в XML-документе. Для этого замените символы следующим образом:
   - **<** на **<**
   - **>** на **>**
   - **"** на **"**
   - **'** на **'**
   - **&** на **&**

   например, если ваш пароль – <my&best'password", его необходимо записать в файле web.xml как <my&best'password"

11.2.9.10 Отредактируйте файл krb5.conf:

1. Перейдите в папку C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\apache-tomcat-7.0.59\conf
2. Найдите и откройте файл krb5.conf
3. В файле krb5.conf администратору необходимо задать только два параметра:
   a. Доменное имя для единого входа (например, ACME.COM)

   Примечание
   Доменное имя в файле krb5.conf следует указывать в **ВЕРХНЕМ РЕГИСТРЕ**, иначе поиск билетов Kerberos может завершиться неудачно.

   b. Адрес центра распределения ключей Kerberos (обычно соответствует адресу контроллера основного домена, например acmedc.ACME.COM)
4. Файл krb5.conf в нашем случае выглядит следующим образом:

[libdefaults]
default_realm = ACME.COM
default_tkt_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
default_tgs_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
permitted_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc

[realms]

ACME.COM = {

kdc = acmedc.ACME.COM

default_domain = ACME.COM

[domain_realm]

.ACME.COM = ACME.COM

5. Замените все вхождения ACME.COM именем своего домена (**в верхнем регистре!**).
6. Замените значение «kdc =» на имя вашего контроллера домена. Имя домена должно быть записано прописными буквами, например kdc = yourdc.YOURDOMAIN.COM
7. После обновления файлов конфигурации следует перезапустить сервер Кибер Файлы (службу Tomcat для Кибер Файлы), чтобы изменения вступили в силу.

11.2.9.11 Включение единого входа в веб-интерфейсе

1. Откройте веб-интерфейс Кибер Файлы и войдите в него как администратор.
2. Перейдите на вкладку **Общие настройки** и откройте страницу **LDAP**.
3. В нижней части страницы установите флажок **Разрешить вход из веб-клиента и клиента для настольных ПК с синхронизацией с использованием имеющихся учетных данных Windows/Mac**.
4. Выберите **Сохранить**.

Разовая конфигурация для леса доменов

Есть небольшая разовая настройка, которую необходимо выполнить для включения поддержки единого входа в браузере.

Внимание

Это следует сделать для каждого пользователя на каждой машине.

Примечание

В инструкциях к конфигурации в качестве примера используется *acme.com*. Если ваши службы находятся в разных доменах, повторите шаги, в которых указывается *acme.com*, для всех ваших доменов. (**Например,** добавьте **.acme.com* и **.another.com* и **.yetanother.com*).

11.2.9.12 Кибер Файлы в лесу доменов

Начиная с версии Microsoft Windows Server 2012, было добавлено **ограниченное делегирование Kerberos на основе ресурсов**, которое позволяет выполнять ограниченное делегирование по лесу доменов. Таким образом в развертываниях может использоваться единый вход даже при наличии ресурсов, расположенных в разных доменах (одного леса), без необходимости устанавливать сервер шлюза на ресурсы.

Примечание
Для использования этой функции все домены леса должны находиться в **режиме работы домена 2012** или выше.

В этой статье содержатся инструкции по следующим настройкам.

- Настройка сервера Кибер Файлы для использования SSO.
- Все конфигурации в домене для работы ограниченного делегирования по лесу.
- Настройка, выполняемая пользователями для входа через SSO.

Требования

Это руководство предназначено для конфигурации с несколькими доменами в одном лесу. Таким образом, подразумевается, что параметры LDAP правильно настроены, пользователи домена могут без проблем выполнять вход и что подключение между доменами внутри леса также правильно настроено.

- Этот тип ограниченного делегирования доступен только в контроллерах домена, находящихся в **режиме работы домена 2012** или выше. Windows Server 2012 – первая система, которая разрешает ограниченное делегирование Kerberos на основе ресурсов.
- **Глобальный каталог** должен быть включен и запущен.

Разовая конфигурация для леса доменов

Есть небольшая разовая настройка, которую необходимо выполнить для включения поддержки единого входа в браузере.

Внимание
Это следует сделать для каждого пользователя на каждой машине.

Примечание
В инструкциях к конфигурации в качестве примера используется *acme.com*. Если ваши службы находятся в разных доменах, повторите шаги, в которых указывается *acme.com*, для всех ваших доменов. (**Например,** добавьте **.acme.com* и **.another.com* и **.yetanother.com*).

Разовая конфигурация для Windows

11.2.10 Для Microsoft Edge и Google Chrome

Конфигурация для Microsoft Edge и Google Chrome выполняется через свойства обозревателя Microsoft Windows.

Настройка свойств обозревателя Windows

1. Откройте **Панель управления** Windows.
2. Выберите **Свойства обозревателя**.
3. На вкладке **Безопасность** выберите **Местная интрасеть**.
4. Нажмите **Узлы**, затем **Дополнительно**.
5. Добавьте адрес вашего сервера Киберпротект Кибер Файлы (например, https://ahsoka.acme.com или просто *.acme.com).
6. Нажмите кнопку**OK**.
7. Перезапустите браузер.

Как разрешить делегирование учетных данных в Chrome

Внимание
Делегирование учетных данных необходимо для просмотра сетевых узлов из веб-интерфейса. В Microsoft Edge этот параметр включен по умолчанию. Чтобы включить делегирование учетных данных в Chrome, необходимо настроить разрешение в браузере.

1. Откройте редактор реестра (**regedit32.exe**)
2. Перейдите к пункту HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome
3. Создайте разделы Google\Chrome, если они отсутствуют.
   a. Щелкните папку Policies правой кнопкой мыши и выберите **Создать** -> **Раздел**.
   b. Ведите **Google** в качестве имени папки.
   c. Щелкните папку **Google** правой кнопкой мыши и выберите **Создать** -> **Раздел**.
   d. Введите **Chrome** в качестве имени папки.
   e. Щелкните папку Chrome, затем на белой панели справа щелкните правой кнопкой мыши и выберите **Создать** -> **Строковый параметр**.
   f. Введите имя раздела: AuthNegotiateDelegateAllowlist.
4. Укажите имя домена (например, ahsoka.acme.com или *.acme.com) в качестве значения для раздела реестра AuthNegotiateDelegateAllowlist.
5. Перезапустите Chrome.

11.2.11 Для Firefox

1. Введите about:config в адресной строке и нажмите Enter.
2. Нажмите и измените настройку network.negotiate-auth.trusted-uris, добавив https://ahsoka.acme.com или just .acme.com (элементы в списке разделяются запятой).

   Примечание
   При добавлении поддоменов используйте формат .example.com (**НЕ** *.example.com)

3. Чтобы включить поддержку сетевых **источников данных**, необходимо также внести изменения в настройку network.negotiate-auth.delegation-uris, добавив ahsoka.acme.com или просто имя домена – acme.com.
4. Перезапустите **Firefox**.

Разовая конфигурация для Mac

Примечание
Следующие действия необходимо выполнить для каждого пользователя на каждой машине.

11.2.12 Для Safari

Все будет работать без дополнительной настройки.

11.2.13 Для Firefox

1. Введите about:config в адресной строке и нажмите Enter.
2. Нажмите и измените настройку network.negotiate-auth.trusted-uris, добавив https://ahsoka.acme.com или just .acme.com (элементы в списке разделяются запятой).

   Примечание
   При добавлении поддоменов используйте формат .example.com (**НЕ** *.example.com)

3. Чтобы включить поддержку сетевых **источников данных**, необходимо также внести изменения в настройку network.negotiate-auth.delegation-uris, добавив ahsoka.acme.com или просто имя домена – acme.com.
4. Перезапустите **Firefox**.

11.2.14 Для Chrome

1. С помощью приложения **Ticket Viewer** (**/System/Library/CoreServices/Ticket Viewer**) можно проверить наличие билета Kerberos и создать его, если он не был создан автоматически.

   Примечание
   Можно также создать билет в программе **Терминал**, введя kinit, а затем свой пароль.

2. Чтобы настроить список разрешений Chrome для обеспечения проверки подлинности в любых используемых доменах, откройте **Терминал** и выполните следующие команды.
   $ defaults write com.google.Chrome AuthServerAllowlist “*.acme.com”
   $ defaults write com.google.Chrome AuthNegotiateDelegateAllowlist “*.acme.com”
3. Перезапустите браузер Chrome.

Для сервера Кибер Файлы

Настройка учетной записи домена для проверки подлинности единого входа

1. Перейдите в папку C:\Program Files (x86)\Cyberprotect\Cyber Files\Access Server\Web Application\WEB-INF\
2. Найдите и откройте файл web.xml. В этом файле необходимо задать логин и пароль домена, в котором будет работать служба единого входа.

   Эта учетная запись **должна** совпадать с учетной записью, которую вы будете использовать для регистрации службы **HTTP** в Kerberos в следующих разделах, поэтому рекомендуем ее записать.
3. В файле web.xml требуется задать два параметра: имя пользователя домена и пароль, с которыми будет работать служба единого входа. Найдите следующие строки:

   ```
   <init-param>
   <param-name>spnego.preauth.username</param-name>
   <param-value>yourusername</param-value>
   </init-param>
   <init-param>
   <param-name>spnego.preauth.password</param-name>
   <param-value>yourpassword</param-value>
   </init-param>
   ```
4. Замените **yourusername** на требуемое имя пользователя LDAP.
5. Замените **yourpassword** на пароль LDAP для указанной выше учетной записи LDAP. Если ваш пароль содержит один из следующих пяти специальных символов: **&**, **>**, **"**, **'** или **<**, их необходимо будет правильно закодировать в XML-документе. Для этого замените символы следующим образом:
   - **<** на **<**
   - **>** на **>**
   - **"** на **"**
   - **'** на **'**
   - **&** на **&**

   Пример. Если ваш пароль – <my&best'password", его необходимо записать в файле web.xml как <my&best'password"

Настройка поиска доменов Kerberos

1. Перейдите в папку C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\apache-tomcat-7.0.59\conf
2. Найдите и откройте файл krb5.conf
3. В файле krb5.conf администратору необходимо задать только два параметра:

a. Доменное имя для единого входа (например, ACME.COM).
   - Это должен быть домен, в котором расположены веб-сервер Кибер Файлы и серверы шлюза.
   - Обратите внимание, что это должно быть имя вашего домена, а **не** DNS-имя сервера.

Примечание
Доменное имя в файле krb5.conf следует указывать в **ВЕРХНЕМ РЕГИСТРЕ**, иначе поиск билетов Kerberos может завершиться неудачно.

b. Адрес центра распределения ключей Kerberos (обычно соответствует **DNS**-адресу контроллера основного домена, например acmedc.ACME.COM). Это адрес контроллера домена, в котором расположены сервер Кибер Файлы и его компоненты.

4. Файл krb5.conf в нашем случае выглядит следующим образом:

```
[libdefaults]
      default_realm = ACME.COM
      default_tkt_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
      default_tgs_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
      permitted_enctypes   = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
   [realms]
      ACME.COM = {
         kdc = acmedc.ACME.COM
         default_domain = ACME.COM
   [domain_realm]
      .ACME.COM = ACME.COM
```

5. Замените все вхождения ACME.COM именем своего домена (**в верхнем регистре!**). Обратите внимание, что это должно быть имя вашего домена, а **не** DNS-имя сервера.
6. Замените значение «kdc =» именем DNS вашего контроллера домена. Имя домена должно быть записано прописными буквами, например kdc = yourdc.YOURDOMAIN.COM
7. После обновления файлов конфигурации следует перезапустить сервер Кибер Файлы (службу Tomcat для Кибер Файлы), чтобы изменения вступили в силу.

Включение единого входа в веб-интерфейсе

1. Откройте веб-интерфейс Кибер Файлы и войдите в него как администратор.
2. Перейдите на вкладку **Общие настройки** и откройте страницу **LDAP**.
3. В нижней части страницы установите флажок **Разрешить вход из веб-клиента и клиента для настольных ПК с синхронизацией с использованием имеющихся учетных данных Windows/Mac**.
4. Нажмите кнопку **Сохранить**.

11.2.15 Настройка дополнительной DNS-записи для вашего Кибер Файлы веб-сервера

Если на этом компьютере установлен сервер шлюза, то необходима отдельная DNS-запись для веб-сервера Кибер Файлы.

1. На своем DNS-сервере откройте **Зоны опережающего просмотра** для используемого домена, щелкните правой кнопкой мыши и создайте новый **Узел** (в записи) для веб-сервера Кибер Файлы.
2. Введите наименование. Это будет адресом DNS, который будет использоваться для доступа к веб-серверу Кибер Файлы.
   Например, ahsokaccess.acme.com
3. Введите IP-адрес веб-сервера Кибер Файлы (без порта). Если вы используете шлюз и веб-серверы Кибер Файлы на одном IP-адресе, введите его.
4. Выберите **Создать связанную запись указателя (PTR)** и нажмите **Добавить узел**.

11.2.16 Настройка SPN для веб-сервера Кибер Файлы

1. На машине, где работает Кибер Файлы, откройте утилиту командной строки.

   Примечание
   Необходимо войти в систему от имени учетной записи домена с правами на использование **setspn**.

2. Введите команду setspn -s HTTP/**access_DNS_name.domain.com account name**

   Примечание
   Имя учетной записи LDAP в приведенной выше команде **ДОЛЖНО** соответствовать учетной записи, которую вы указали в файле web.xml .

   - например, если ваш веб-сервер Кибер Файлы установлен в домене ahsoka.acme.com и вы хотите использовать john@acme.com в качестве учетной записи LDAP с предварительной аутентификацией для предоставления билетов Kerberos, команда будет выглядеть следующим образом:
     setspn -s HTTP/ahsokaaccess.acme.com john
   - например, если ваш веб-сервер Кибер Файлы установлен на ahsoka.acme.com и вы хотите использовать jane@tree.com в качестве учетной записи LDAP с предварительной аутентификацией для предоставления временных данных (билетов) Kerberos, команда будет выглядеть следующим образом:
     setspn -s HTTP/ahsokaaccess.acme.com tree\jane

Примечание
Как правило, эта учетная запись обычно совпадает с учетной записью LDAP, указанной администратором в веб-интерфейсе Кибер Файлы в **настройках LDAP**, но это необязательно.

3. Если веб-сервер Кибер Файлы работает через порт, отличный от порта по умолчанию (то есть любой порт, кроме 443), следует также зарегистрировать SPN с указанием номера порта.
Например,Если ваш сервер работает на порту 444, команда будет следующей:
setspn -s HTTP/ahsokaaccess.acme.com:444 john ИЛИ
setspn -s HTTP/ahsokaaccess.acme.com:444 tree\jane

Примечание
Значение **HTTP** в приведенных выше командах относится к классу службы **HTTP**, а не к протоколу **HTTP**. Класс службы **HTTP** обрабатывает запросы и **HTTP** и **HTTPS** . Не требуется и **НЕ СЛЕДУЕТ** создавать SPN с использованием **HTTPS** в качестве имени класса службы.

4. Перейдите на контроллер домена, к которому относятся пользователи, и откройте **Пользователи и компьютеры Active Directory**. Если у вас несколько доменов с пользователями, откройте тот, к которому принадлежит учетная запись, использованная на предыдущих этапах.
5. Найдите пользователя, который указывался в приведенных выше командах (в данном случае **john** или **jane**).
6. Откройте вкладку **Делегирование** и выберите **Доверять этому пользователю делегирование любой службы (только Kerberos)**. Включение этого параметра позволяет объекту LDAP делегировать проверку подлинности любой службе. В данном случае это служба сервера шлюза.
7. Нажмите кнопку**OK**.

11.2.17 Проверка входа в Кибер Файлы

1. Перейдите на машину, которая не является контроллером домена или веб-сервером Кибер Файлы.
2. Откройте веб-консоль Кибер Файлы и воспользуйтесь ссылкой под полем для ввода пароля на странице входа.

Примечание
Необходимо войти в систему на машине как пользователь домена, который приглашен в Кибер Файлы, уже выполнил вход или является участником распределенной группы LDAP.

Примечание
Чтобы браузер принимал запросы SSO, необходимо выполнить все действия в разделе На машине любого пользователя.

Для сервера шлюза

Настройка SPN для сервера шлюза

Чтобы сервер Kerberos KDC (Центр распространения ключей) мог выполнять проверку подлинности пользователей для сервера шлюза, необходимо зарегистрировать службу шлюза на сервере KDC. Для этого выполните команду **setspn**, указав в командной строке имя узла сервера, на котором служба запускается от имени пользователя, указанного в команде **setspn**.

11.2.18 Настройка дополнительной DNS-записи для сервера шлюза

Чтобы эта конфигурация работала, также необходима отдельная DNS-запись для сервера шлюза.

1. На своем DNS-сервере откройте **Зоны опережающего просмотра** для используемого домена, щелкните правой кнопкой мыши и создайте новую запись **узла** (в записи) для сервера шлюза.
2. Введите наименование. Оно будет адресом DNS, который будет использоваться для доступа к серверу шлюза.

   Например, codygw.acme.com
3. Введите IP-адрес сервера шлюза (без порта). Если вы используете шлюз и серверы Кибер Файлы на одном IP-адресе, введите его.
4. Выберите **Создать связанную запись указателя (PTR)** и нажмите **Добавить узел**.

11.2.19 Настройка SPN для локального сервера шлюза

1. Перейдите на машину с Кибер Файлы.
2. Откройте командную строку.
3. Установка SPN для сервера шлюза
   a. Если сервер шлюза работает под учетной записью локальной системы, команда принимает следующий вид:
   b. setspn -s HTTP/**gatewaydns.domain.com computername**

   Например, если используемый сервер шлюза работает на узле 'cody' в данном домене и используется DNS-запись codygw.acme.com, выполните следующую команду:
   setspn -s HTTP/codygw.acme.com cody
   c. Если сервер шлюза работает на порте, отличном от заданного по умолчанию (то есть на любом, кроме 443), необходимо также зарегистрировать SPN, указав номер порта, например в случае, если сервер шлюза работает на порте 444:
   setspn -s HTTP/codygw.acme.com:444 cody
4. Если это еще не сделано, необходимо изменить соответствующий **адрес администрирования** сервера шлюза таким образом, чтобы он совпадал с созданной DNS-записью сервера шлюза (т. е. codygw.acme.com).

11.2.19.1 Проверка правильности SPN-имен, заданных для шлюза

1. Если у вас есть локальный том для локального сервера шлюза, вы можете проверить работу SPN и делегирования, выполнив вход через SSO. Это следует сделать на машине, которая не является сервером Кибер Файлы и контроллером домена, иначе SSO не будет работать.
2. Просмотрите том локального сервера шлюза. Если просмотр работает, можно продолжать, в противном случае проверьте, что успешно настроены правильные SPN-имена для нужных объектов.

Примечание
Если выполнить попытку с томом на удаленном файловом сервере, должна появиться ошибка «Доступ запрещен».

Настройка ограниченного делегирования на основе ресурсов

Примечание
Этот тип ограниченного делегирования доступен только в контроллерах домена, находящихся в режиме работы домена 2012R2 или выше. Windows Server 2012 – первая система, которая разрешает ограниченное делегирование Kerberos по домену.

Можно использовать ограниченное делегирование на основе ресурсов, чтобы предоставить пользователям доступ к файловым серверам и прочим сетевым ресурсам, расположенным в другом домене.

1. Перейдите на контроллер домена, в котором расположен файловый сервер, и откройте **PowerShell**.
2. Если сервер шлюза работает под учетной записью **LocalSystem**:
   a. $computer1 = Get-ADComputer -Identity <gateway_server_computer> -server <domain_controller_for_this_domain>
   например, $computer1 = Get-ADComputer -Identity cody -server dc.acme.com
   Эта команда получает объект «компьютер» для сервера шлюза, указывает экземпляр доменных служб AD для подключения и сохраняет эту информацию в переменной $computer1.
   b. Set-ADComputer <file_server_computer> -PrincipalsAllowedToDelegateToAccount $computer1
   например, Set-ADComputer cody -PrincipalsAllowedToDelegateToAccount $computer1
   Эта команда задает свойство объекта «компьютер» файлового сервера **Principals Allowed To Delegate To Account** для объекта «компьютер» сервера шлюза. Это позволяет серверу шлюза выполнять делегирование на компьютер файлового сервера.
3. Если сервер шлюза работает под **учетной записью пользователя**:
   a. $user1 = Get-ADUser -Identity <logon_user_of_the_gateway_service> -server <domain_controller_for_this_domain>
   например, $user1 = Get-ADUser -Identity jane -server dc.acme.com
   Эта команда получает объект «пользователь» для сервера шлюза, указывает экземпляр

доменных служб AD для подключения и сохраняет эту информацию в переменной $user1.

b. Set-ADComputer <file_server_computer> -PrincipalsAllowedToDelegateToAccount $user1
например, Set-ADComputer cody -PrincipalsAllowedToDelegateToAccount $user1
Эта команда задает свойство объекта «компьютер» файлового сервера **Principals Allowed To Delegate To Account** для объекта «компьютер» сервера шлюза. Это позволяет выбранному пользователю выполнять делегирование на компьютер файлового сервера.

4. Чтобы проверить, что для учетной записи пользователя сервера шлюза было разрешено делегирование учетных данных, можно выполнить следующую команду:
Get-ADComputer <file_server_machine> -Properties PrincipalsAllowedToDelegateToAccount
Например, Get-ADComputer omega -Properties PrincipalsAllowedToDelegateToAccount
5. Повторите эти шаги для всех файловых серверов.

Прежде чем делегирование распространится, пройдет некоторое время – от 10 до 15 минут в небольших развертываниях LDAP и еще дольше в крупных структурах.

Добавление других серверов шлюза

Примечание
Эти шаги работают, только если машины, на которых устанавливаются серверы шлюзов, расположены в одном домене с веб-сервером Кибер Файлы.

Чтобы сервер Kerberos в роли KDC (Центра распределения ключей) мог проверять подлинность пользователей на сервере шлюза, необходимо зарегистрировать службу шлюза на сервере KDC. Выполните команду setspn, указав в командной строке имя узла сервера, на котором работает служба, как user.

11.2.19.2 Для любого сервера шлюза, расположенного не на той же машине, что веб-сервер Кибер Файлы

1. Откройте командную строку.
2. Введите следующую команду **setspn**: setspn -s HTTP/**computername.domain.com computername**
Например, если сервер шлюза работает на узле cody в этом домене, выполните следующую команду:
setspn -s HTTP/cody.acme.com cody
3. Если сервер шлюза работает на порту, отличном от заданного по умолчанию (то есть на любом, кроме 443), необходимо также зарегистрировать имя участника-службы, указав номер порта; например, если сервер шлюза работает на порту 444:
setspn -s HTTP/cody.acme.com:444 cody
4. Повторите эту процедуру для каждого дополнительного сервера шлюза.

Настройка сервера шлюза в другом домене

Если **ограниченное делегирование Kerberos на основе ресурсов** недоступно, есть другой способ настроить SSO для удаленных общих папок и ресурсов, расположенных в другом домене. Для

этого на машине в другом домене устанавливается сервер шлюза. Это позволяет использовать обычное ограниченное делегирование Kerberos и **применимо для доменов в режиме работы 2008**.

11.3 Установка сервера шлюза на машине в нужном домене

1. Скачайте установщик Кибер Файлы и перенесите его на вашу машину.
2. Запустите программу установки Кибер Файлы, примите условия лицензионного соглашения и нажмите кнопку **Далее**.
3. Выберите **Настроить...** и установите только флажок сервера шлюза.
4. Нажмите кнопку **Установить**. После завершения установки закройте программу.
5. В **программе настройки** укажите IP-адрес шлюза и порт.

11.4 Запуск службы шлюза под учетной записью пользователя

1. Откройте **Панель управления** и выберите **Администрирование** -> **Службы**.
2. Найдите службу сервера шлюза Кибер Файлы, щелкните по ней правой кнопкой мыши и выберите **Свойства**.
3. Выберите вкладку **Вход** и установите переключатель **Эта учетная запись**.
4. Выберите пользователя, от имени которого будет работать служба, нажав кнопку **Обзор** и выполнив поиск, либо просто введите имя пользователя и пароль. Этот пользователь **должен** принадлежать домену, в котором установлен Кибер Файлы. Рекомендуется использовать выделенную учетную запись, а не ту, которая использовалась для настройки SPN сервера Кибер Файлы.
5. Нажмите кнопку **OK**, после чего можно закрыть панель управления **Службы**. Пока не перезапускайте службу, поскольку она не запустится без необходимых разрешений для учетной записи пользователя.

11.4.1 Предоставление выбранному пользователю необходимых прав

1. Чтобы служба работала от имени пользователя, необходимо предоставить этому пользователю право **Работа в режиме операционной системы** и включить его в группу «Локальные администраторы».
2. Откройте оснастку **Локальная политика безопасности** и перейдите в раздел **Локальные политики** -> **Назначение прав пользователя**. Может потребоваться внести это изменение в **диспетчере групповых политик** в зависимости от системы развертывания.

3. Откройте объект **Работа в режиме операционной системы** и нажмите кнопку **Добавить пользователя или группу**.
4. Выберите пользователя, выделенного для службы шлюза.
5. Закройте все открытые диалоговые окна и перейдите в раздел **Панель управления** -> **Учетные записи пользователей** -> **Управление учетными записями**.
6. Нажмите кнопку **Добавить** и введите домен и имя пользователя выделенной учетной записи.
7. Теперь можно перезапустить службу шлюза Кибер Файлы на панели управления **Службы** .

11.5 Настройка SPN для удаленного сервера шлюза

1. Перейдите на любую машину в домене, где расположен сервер Кибер Файлы.
2. Откройте командную строку.
3. Для настройки SPN используется следующая команда: **setspn -s HTTP/gatewaydns.domain.com useraccountfor_gw**

   Пример. Если сервер шлюза работает на узле "magpie" в домене **tree.com** под учетной записью пользователя peter из домена **acme.com**, выполните следующую команду:

   setspn -s HTTP/magpie.tree.com peter

   Если сервер шлюза работает на порте, отличном от заданного по умолчанию (то есть на любом, кроме 443), необходимо также зарегистрировать SPN, указав номер порта, например в случае, если сервер шлюза работает на порте 444:
   setspn -s HTTP/magpie.tree.com:444 peter
4. Если это еще не сделано, необходимо изменить соответствующий **адрес администрирования** сервера шлюза таким образом, чтобы он совпадал с созданной DNS-записью сервера шлюза (то есть magpie.tree.com).
5. Убедитесь, что на сервере шлюза включен параметр Выполнить проверку подлинности Negotiate/Kerberos в режиме пользователя. После включения этого параметра необходимо перезапустить службу шлюза Кибер Файлы.
6. При создании **источников данных** для ресурсов во втором домене используйте расположенный в нем сервер шлюза.

   Например, Чтобы предоставить пользователям доступ к файлам на сервере repository.tree.com, необходимо выбрать сервер шлюза, расположенный в домене tree.com (например, magpie.tree.com)

11.5.0.1 Проверка правильности SPN-имен, заданных для шлюза

1. Если у вас есть локальный том для локального сервера шлюза, вы можете проверить работу SPN и делегирования, выполнив вход через SSO.
2. Просмотрите том локального сервера шлюза. Если просмотр не работает, проверьте, что успешно настроены правильные SPN-имена для нужных объектов.
3. Распространение изменений в делегировании может занять некоторое время (10-15 минут в небольших развертываниях LDAP и еще дольше в крупных).

11.5.0.2 Убедитесь, что имя SPN зарегистрировано

Как проверить, зарегистрировано ли имя SPN должным образом

1. Откройте командную строку с повышенными привилегиями.
2. Введите команду setspn -Q HTTP/**computername.domain.com**.
   например setspn -Q HTTP/ahsoka.acme.com
3. Чтобы запросить имена SPN, зарегистрированные на определенного пользователя домена, используйте параметр -l (L в нижнем регистре);
   например setspn -l john
4. После регистрации SPN и перед проверкой подлинности с использованием единого входа необходимо либо перезагрузить клиентскую машину, либо выполнить следующую команду на клиентской машине:
   klist purge

11.5.0.3 Использование источников данных SMB или SharePoint

Если требуется использование источников данных SMB или SharePoint, то необходимо настроить учетную запись Active Directory таким образом, чтобы разрешить делегирование Kerberos для каждого из источников данных SMB и SharePoint.

Для сетевых папок и серверов SharePoint выполните следующие действия.

Выполнив эти инструкции, вы включите делегирование с сервера шлюза на целевые серверы.

1. Откройте раздел **Пользователи и компьютеры Active Directory**.
2. Найдите объект-компьютер, соответствующий серверу шлюза.

   Примечание
   Если сервер шлюза работает под учетной записью **пользователя**, выберите объект этого **пользователя**.

3. Щелкните по пользователю правой кнопкой мыши и выберите «Свойства».
4. Откройте вкладку **Делегирование**.
5. Установите флажок **Доверять этому компьютеру делегирование только указанных служб**.
6. Здесь выберите **Использовать любой протокол проверки подлинности**.
7. Нажмите кнопку **Добавить**.
8. Нажмите **Пользователи или компьютеры**.
9. Выполните поиск объекта сервера для общей папки SMB или сервера SharePoint и нажмите кнопку **OK**.

- Для общих папок SMB выберите службу **cifs**.
- Для SharePoint выберите службу **http**.

10. Повторите эти действия для каждого сервера, к которому нужен доступ сервера шлюза Кибер Файлы.
11. Повторите эту процедуру для каждого сервера шлюза.

Изменения делегирования вступят в силу в течение нескольких минут в зависимости от размера леса домена. Возможно, для вступления изменений в силу придется подождать 15 минут или больше. Если изменения не работают через 15 минут, попробуйте перезапустить службу шлюзов Кибер Файлы.

11.5.0.4 Использование мобильных клиентов с проверкой подлинности по сертификатам клиента

Это дополнительный шаг, который следует выполнить. Необходимо настроить делегирование от сервера шлюза к серверу Кибер Файлы, независимо от того, работают они на одной машине или на разных.

Ограниченное делегирование Kerberos

Этот тип делегирования работает, если сервер Кибер Файлы и сервер шлюза находятся в одном домене.

1. Для этого откройте Active Directory на контроллере домена.
2. Найдите и измените объект компьютера сервера шлюза и перейдите на вкладку делегирования.
3. Выберите **Доверять этому компьютеру для делегирования только указанным службам** и **Использовать любой протокол проверки подлинности**.
4. Чтобы выбрать SPN сервера Кибер Файлы, щелкните «Добавить» и введите имя пользователя учетной записи, связанной с **HTTP** SPN сервера Кибер Файлы.

   Примечание
   Не ищите компьютер, на котором работает сервер Кибер Файлы, – необходимо выполнить поиск по имени пользователя.

   Примечание
   Проверка подлинности Kerberos для доступа к серверу Кибер Файлы несовместима с режимом одного порта.

5. Выполнив поиск пользователя, вы должны увидеть службы **HTTP** и выбрать их (может быть две службы, если имя SPN зарегистрировано дважды: один раз с портом и один раз без него).
6. Нажмите кнопку **Применить** и закройте все диалоговые окна.

Ограниченное делегирование Kerberos на основе ресурсов

Этот тип делегирования будет работать, даже если сервер Кибер Файлы и сервер шлюза находятся в разных доменах одного леса.

Примечание
Для использования этой функции все домены, к которым будет обращаться Кибер Файлы, должны находиться в **режиме работы домена 2012** или выше.

1. Еще раз убедитесь, что DNS-запись, которая была выделена для сервера Кибер Файлы и для которой вы задали имя SPN, действительно установлена в качестве адреса тома S&S на странице «Источники данных».
2. Настройте делегирование между сервером Кибер Файлы и сервером шлюза. На этот раз делегирование будет выполняться от сервера шлюза к серверу Кибер Файлы.
3. Выполните следующие команды для указанных пользователей:
   $pc1 = Get-ADComputer -Identity <имя_машины_шлюза>
   Set-ADUser <учетная_запись_SSO_пользователя_Access> -PrincipalsAllowedToDelegateToAccount $pc1
   Например, $pc1 = Get-ADComputer -Identity ahsoka
   Set-ADUser john -PrincipalsAllowedToDelegateToAccount $pc1
4. Если шлюз работает как учетная запись пользователя, необходимо будет настроить делегирование между двумя учетными записями с помощью следующих команд:
   $user1 = Get-ADUser -Identity <Учетная_запись_шлюза>
   Set-ADUser <учетная_запись_SSO_пользователя_Access> -PrincipalsAllowedToDelegateToAccount $user1
   Например, $user1 = Get-ADUser -Identity gwuser
   Set-ADUser john -PrincipalsAllowedToDelegateToAccount $user1

Прежде чем делегирование распространится, пройдет некоторое время – от 10 до 15 минут в небольших развертываниях LDAP и еще дольше в крупных структурах.

11.5.0.5 Для сред с балансировкой нагрузки

Сервер шлюза может выполнять всю проверку подлинности по протоколу HTTP в режиме пользователя вместо проверки подлинности Kerberos/Negotiate со стороны веб-сервера. Это необходимо, чтобы обеспечить работу SSO для шлюзов, размещенных за балансировщиком нагрузки.

Чтобы включить эту функцию, откройте веб-интерфейс, выберите **Мобильный доступ** -> **Серверы шлюза**, щелкните пункт **Изменить** в кластерной группе, выберите **Дополнительно** и установите флажок **Выполнить проверку подлинности Negotiate/Kerberos в режиме пользователя**.

Включение сетевых узлов

Для доступа к сетевым узлам в Интернете при использовании SSO необходимо внести несколько изменений. Поскольку серверы шлюза работают за балансировщиком нагрузки, при регистрации в Kerberos должна использоваться учетная запись пользователя, а не имя компьютера.

Для этого службы шлюза должны работать под учетной записью пользователя. Можно либо использовать того же пользователя LDAP, от имени которого зарегистрирован сервер Кибер Файлы, либо выбрать нового специально для служб шлюза.

В любом случае выбранному пользователю нужно предоставить право действовать как часть операционной системы на машинах с установленными серверами шлюза.

Выбор пользователя для действий в качестве части операционной системы

1. На машине с сервером шлюза щелкните **Пуск** -> **Выполнить**.
2. Введите **gpedit.msc** и нажмите кнопку **OK**.
3. Разверните пункт **Параметры Windows**, а затем **Параметры безопасности**.
4. Разверните пункт **Локальные политики** и щелкните **Назначение прав пользователя**.
5. Щелкните правой кнопкой **Действовать как часть операционной системы** в списке и выберите **Свойства**.
6. В этом окне можно добавлять и удалять пользователей и группы. Введите нужное имя пользователя и нажмите кнопку «OK».
7. Закройте все окна и перезапустите сервер, чтобы изменение вступило в силу.

Запуск службы сервера шлюза под выбранной учетной записью пользователя

Добавив пользователя, от имени которого будет работать служба, необходимо настроить службу шлюза на использование этой учетной записи. Для этого выполните следующие действия.

1. На машине с установленным сервером шлюза щелкните **Пуск** и выберите **Выполнить**.
2. Введите **services.msc** и нажмите кнопку **OK**. Либо откройте **Панель управления** и выберите **Администрирование** -> **Службы**.
3. Щелкните правой кнопкой **Кибер Файлы Шлюз** в этом списке и выберите **Свойства**.
4. Откройте вкладку **Вход**.
5. Установите переключатель **Эта учетная запись:** и введите учетные данные пользователя, которому были предоставлены права операционной системы.
6. Нажмите кнопку **OK** и закройте все окна.

Настройка имен SPN для кластера шлюза

Чтобы сервер Kerberos KDC (центр распределения ключей) мог выполнять проверку подлинности пользователей для кластера шлюза, каждый сервер шлюза и балансировщик нагрузки необходимо

зарегистрировать на сервере KDC, выполнив команду **setspn** и указав имя учетной записи, под которой будет работать служба.

1. Откройте командную строку.
2. Введите следующую команду:

   setspn -s HTTP/computername.domain.com username

   Например, если служба шлюза запускается от имени пользователя **john**, то команда будет выглядеть так:

   setspn -s HTTP/gatewayserver1.acme.com john
3. Если сервер шлюза работает на порту, отличном от заданного по умолчанию (то есть на любом, кроме 443), необходимо также зарегистрировать имя участника-службы, указав номер порта; например, если сервер шлюза работает на порту 444:

   setspn -s HTTP/gatewayserver1.acme.com:444 john
4. Повторите эти шаги для каждого сервера шлюза и для балансировщика нагрузки. Имя SPN для балансировщика нагрузки должно выглядеть следующим образом:

   setspn -s HTTP/gwloadbalancerdns.acme.com john

Примечание
Если у вас есть балансировщик нагрузки, который делит трафик между двумя шлюзами (в данном случае gwloadbalancerdns.acme.com), не регистрируйте его, так как в половине случаев запросы не достигнут правильного шлюза (локального). Если сервер балансировщика нагрузки направит запрос на неправильный шлюз, выполнить вход не удастся. Имена DNS не могут указывать на другую службу после запуска.

Если вам потребуется дополнительная помощь, обращайтесь в службу поддержки.

11.5.0.6 Устранение неполадок единого входа

- Пользователи клиента для ПК или веб-клиента должны работать на компьютере, отличном от того, на котором запущен сервер Кибер Файлы (но в том же домене), иначе SSO не будет работать.
- Использование SSO с клиента для настольных ПК требует доступа к корпоративной сети. Это означает, что пользователь SSO должен иметь также доступ к собственной сети.
- Доступ к серверу необходимо осуществлять по тому же полному доменному имени, которое использует SPN, например https://ahsoka.acme.com. Нельзя использовать другие имена DNS или IP-адреса, например https://localhost или https://10.20.56.33.
- Убедитесь в возможности входа на сервер Кибер Файлы без использования SSO, введя точно такие же учетные данные LDAP, которые используются вашим клиентским компьютером под управлением Windows. Это позволит убедиться, что учетные данные действительны для Кибер Файлы, независимо от настроек SSO.
- Убедитесь, что у вас есть доступ ко всем источникам данных без использования SSO с учетными данными пользователя LDAP.

- Если войти через SSO не удается, еще раз убедитесь в том, что веб-браузер настроен для единого входа по полному доменному имени, к которому вы подключаетесь, и что выполнен вход на клиентском компьютере с использованием учетной записи домена.
- Единый вход не будет работать, если сервер Кибер Файлы работает на контроллере домена.
- Кибер Файлы не будет работать с SSO, если вы пытаетесь выполнить вход с машины, являющейся контроллером домена.

Примечание
В связи с особенностями работы Kerberos вы не можете пройти проверку подлинности через SSO из клиентского приложения или веб-браузера, запущенного на контроллере домена или сервере Кибер Файлы.

Примечание
Кроме того, сервер Кибер Файлы не может пройти проверку подлинности на контроллере домена, если сервер Кибер Файлы работает на контроллере домена.

- Если при попытке входа с использованием SSO возникает **ошибка 401**, проверьте имя пользователя и пароль в файле **web.xml** и убедитесь, что все специальные символы правильно экранированы. К специальным символам относятся: **&**, **>**, **"**, **'** или **<**. Сведения о том, как их экранировать, см. на **шаге 5** раздела **Редактирование файла web.xml**.

11.5.1 Использование доверенных сертификатов сервера с Кибер Файлы

В этом разделе описано, как настроить Кибер Файлы для работы с доверенными сертификатами сервера.

По умолчанию в Кибер Файлы предусмотрены самогенерируемые SSL-сертификаты, предназначенные для тестирования. С использованием сертификата, подписанного доверенным центром сертификации, создается удостоверение сервера, которое позволит клиентам подключаться к нему без ошибок.

Примечание
Веб-браузеры отображают предупреждающие сообщения при использовании самозаверенных сертификатов. Можно пропустить эти сообщения и приступить к использованию системы для тестирования.

Использование самозаверенных сертификатов в рабочей системе не поддерживается. В производственных развертываниях необходимо использовать сертификаты ЦС.

11.5.1.1 Создание запроса на сертификат

Примечание
Решение Кибер Файлы не предназначено для создания сертификатов. Данный запрос сертификата не обязателен для работы Кибер Файлы, но его требуют поставщики сертификатов.

Примечание
Если поставщик запрашивает тип сервера, выберите **IIS**. Сертификаты должны быть установлены в хранилище сертификатов Windows, прежде чем Кибер Файлы сможет их использовать.

11.5.1.2 Создание запроса сертификата с помощью служб IIS

Дополнительные сведения об этой процедуре см. в следующей статье базы знаний Майкрософт: http://technet.microsoft.com/en-us/library/cc732906(v=ws.10).aspx

11.5.1.3 Создание запроса на сертификат с помощью OpenSSL

Примечание
Для выполнения данных инструкций необходимо установить OpenSSL.

Примечание
Дополнительные сведения об этой процедуре или поддержку можно получить у своего поставщика сертификатов.

Создание пары закрытого ключа и запроса на открытый сертификат подписи (CSR) для веб-сервера AAServer

1. Откройте командную строку с повышенными привилегиями и введите следующую команду:

   ```
   openssl req -new -nodes -keyout myserver.key -out AAServer.csr -newkey rsa:2048
   ```

2. При этом будут созданы два файла. Файл **myserver.key** содержит закрытый ключ. Не передавайте этот файл другим пользователям. Создайте резервную копию закрытого ключа, так как его невозможно будет восстановить, если он будет утерян. Закрытый ключ используется как входной аргумент команды создания **запроса подписи сертификата (CSR)**.

   Примечание
   Если возникает ошибка **ПРЕДУПРЕЖДЕНИЕ. Не удается открыть файл конфигурации /usr/local/ssl/openssl.cnf**, выполните следующую команду: **set OPENSSL_CONF=C:\OpenSSL-Win64\bin\openssl.cfg**. Замените путь тем, куда был установлен OpenSSL. После завершения этой процедуры еще раз выполните шаг 1.

3. Потребуется ввести данные для запроса CSR. В качестве имени веб-сервера указывайте **Общее имя (CN)**. Если имя домена – **mydomain.com**, добавьте домен к имени узла (используйте полное доменное имя).

4. Поля адреса электронной почты, имени компании и пароля вызова можно оставить пустыми для сертификата веб-сервера.
5. После этого запрос CSR будет создан. Откройте файл **server.csr** в текстовом редакторе, скопируйте и вставьте его содержимое в веб-форму регистрации.

11.5.1.4 Установка сертификата в хранилище сертификатов Windows

Требования

Используемый сертификат должен содержать свой закрытый ключ. Файл сертификата должен быть представлен в формате **.PFX** или **.P12**.
Какой именно сертификат, значения не имеет, поскольку они являются взаимозаменяемыми.

Примечание
Если поставщик сертификатов выдал вам сертификат и ключ в виде двух отдельных файлов, их можно объединить в один **PFX**-файл с помощью следующей команды.

openssl pkcs12 -export -in <yourcertificate.extension> -inkey <yourkey.extension> -out <newfile.pfx>

Например, openssl pkcs12 -export -in acmecert.crt -inkey acmecertkey.key -out acmecombined.pfx

Для выполнения этой команды необходимо установить OpenSSL.

Установка сертификата в хранилище сертификатов Windows

Примечание
Если сервер Кибер Файлы и сервер шлюза используют разные сертификаты, повторите эти шаги для обоих серверов.

---

1. На сервере откройте меню **Пуск** и выберите **Выполнить**.
2. В поле **Открыть** введите **mmc** и нажмите **OK**.
3. В меню **Файл** выберите **Добавить или удалить оснастку-в**.
4. В диалоговом окне **Добавить или удалить оснастку** нажмите кнопку **Добавить**.
5. В диалоговом окне **Добавить изолированную оснастку** щелкните **Сертификаты** и нажмите кнопку **Добавить**.
6. В диалоговом окне **Оснастка диспетчера сертификатов** щелкните **Учетная запись компьютера** (этот параметр не выбран по умолчанию) и нажмите кнопку **Далее**.
7. В диалоговом окне **Выбор компьютера** щелкните **Локальный компьютер** (компьютер, на котором запущена консоль) и нажмите кнопку **Готово**.
8. В диалоговом окне **Добавить изолированную оснастку** нажмите кнопку **Закрыть**.
9. В диалоговом окне **Добавить или удалить оснастку** нажмите кнопку **OK**.
10. В левой области консоли дважды щелкните **Сертификаты** (**Локальный компьютер**).
11. Щелкните правой кнопкой **Личные**, выберите пункт **Все задачи** и нажмите кнопку **Импорт**.
12. На странице **Мастер импорта сертификатов** нажмите кнопку **Далее**.

13. На странице **Импортируемый файл** нажмите кнопку **Обзор**, найдите файл сертификата и нажмите кнопку **Далее**.

    Примечание
    Если импортируется PFX-файл, то, чтобы отобразить его, потребуется изменить фильтр файлов на **Personal Information Exchange (*.pfx, *.p12)**.

14. Если для сертификата задан пароль, введите его на странице **Пароль** и нажмите кнопку **Далее**.
15. Установите следующие флажки:
    a. **Пометить этот ключ как экспортируемый**
    b. **Включить все расширенные свойства**
16. На странице **Хранилище сертификатов** щелкните **Поместить все сертификаты в следующее хранилище** и нажмите кнопку **Далее**.
17. Нажмите **Готово**, а затем **OK**, чтобы подтвердить успешный импорт.

Все сертификаты, успешно установленные в хранилище сертификатов Windows, будут доступны при использовании утилиты конфигурации Кибер Файлы.

11.5.1.5 Настройте Кибер Файлы на использование вашего сертификата

После успешной установки сертификата в хранилище сертификатов Windows необходимо настроить Кибер Файлы на его использование.

1. Запустите программу настройки Кибер Файлы. Можно использовать ярлык в меню «Пуск» Windows.

   Примечание
   По умолчанию программа настройки находится в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\Configuration Utility.

2. На вкладке **Веб-сервер** нажмите кнопку **[...]** и выберите свой сертификат из списка.
3. На вкладке **Мобильный шлюз** нажмите кнопку **[...]** и выберите свой сертификат из списка.
4. Нажмите кнопку **Применить**. Веб-службы перезапустятся и через минуту возобновят работу с использованием указанного сертификата. Вы можете проверить, что используются нужные сертификаты.

11.5.1.6 Использование промежуточных сертификатов

Если центр сертификации выдал вам промежуточный сертификат наряду с вашим сертификатом, его необходимо также добавить на Кибер Файлы Server с помощью средства конфигурации.

Примечание
Средство конфигурации выполняет поиск только в хранилище **Промежуточные сертификаты**. Если ваш сертификат установлен в другом хранилище, откройте утилиту **certmgr.msc** и переместите свой промежуточный сертификат из текущего хранилища в хранилище **Промежуточные центры сертификации** -> **Сертификаты**.

1. Запустите программу настройки Кибер Файлы. Можно использовать ярлык в меню «Пуск» Windows.

   Примечание
   По умолчанию программа настройки находится в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\Configuration Utility.

2. На вкладке **Веб-сервер** нажмите кнопку **[...]** и выберите свой сертификат из списка.
3. Нажмите кнопку «плюс» (**+**) рядом с полем **Сертификат цепочки** и выберите нужный **промежуточный сертификат** из списка. Если нужного сертификата нет в списке, проверьте, правильно ли он установлен и в каком хранилище.
4. На вкладке **Мобильный шлюз** нажмите кнопку **[...]** и выберите свой сертификат из списка. Дополнительные шаги для промежуточных сертификатов не требуются.
5. Нажмите кнопку **Применить**. Служба будет перезапущена, и после включения вы сможете проверить, что используются выбранные сертификаты.

11.5.2 Поддержка различных версий настольного клиента

Если требуется использовать не самую последнюю версию настольного клиента, Кибер Файлы выполните следующие действия.

1. Скачайте нужную версию настольного клиента. Убедитесь в наличии следующих 4 файлов:
   - ACFClientMac.zip
   - ACFClientInstaller.msi
   - CyberprotectCyberFilesInstaller.dmg
   - CyberprotectCyberFilesClientInstaller.exe
2. Скопируйте эти файлы.
3. На этом сервере откройте папку настольных клиентов Кибер Файлы (C:\Program Files (x86)\Cyberprotect\Cyber Files\Access Server\Web Application\clients).
4. Создайте вложенную папку для данной версии клиента. Ее имя должно совпадать с **номером версии клиента** (например, **8.7.0x664**, **8.7.0x632**).
5. Вставьте упомянутые выше 4 файла во вновь созданную вложенную папку.
6. Затем откройте **Веб-интерфейс пользователя** сервера Кибер Файлы.
7. Выполните вход от имени **администратора**, перейдите на вкладку **Sync & Share** и откройте страницу **Клиент Кибер Файлы**.

8. Найдите параметр **Разрешить автоматическое обновление клиентского приложения до версии**.
9. Выберите требуемую версию в раскрывающемся меню.

11.5.3 Перемещение файлового хранилища FileStore в другое местоположение.

11.5.3.1 Служба работает с учетной записью локальной системы

1. Перейдите на компьютер, где установлен Кибер Файлы.
2. Остановите службы **Сервер репозитория файлов Кибер Файлы** и **Кибер Файлы Tomcat**.
3. Текущее хранилище **FileStore** находится в папке, выбранной в **программе настройки**. Расположение по умолчанию – C:\ProgramData\Cyberprotect\Cyber Files\FileStore.
4. Скопируйте или переместите папку **FileStore** вместе со всем содержимым в нужное местоположение.
   Например, D:\MyCustom Folder\FileStore

Примечание
Если **файловое хранилище** расположено в удаленной сетевой папке, то компьютер, на котором запущена служба **файлового репозитория**, должен иметь полный доступ к папке **файлового хранилища** в сетевой папке.

---

5. Откройте **средство конфигурации**.
6. На вкладке **Файловый репозиторий** измените путь к хранилищу **FileStore** на тот, куда была перенесена папка **FileStore**.
7. Запустите службу **Сервер репозитория файлов Кибер Файлы**.
8. Запустите службу **Кибер Файлы Tomcat** и закройте оснастку **Службы**.

11.5.3.2 Служба работает под учетной записью пользователя

1. Перейдите на компьютер, где установлен Кибер Файлы.
2. Остановите службы **Сервер репозитория файлов Кибер Файлы** и **Кибер Файлы Tomcat**.
3. Текущее хранилище **FileStore** находится в папке, выбранной в **программе настройки**. Расположение по умолчанию – C:\ProgramData\Cyberprotect\Cyber Files\FileStore.
4. Скопируйте или переместите папку **FileStore** вместе со всем содержимым в нужное местоположение.
   Например, D:\MyCustom Folder\FileStore
5. Откройте **средство конфигурации**.
6. На вкладке **Файловый репозиторий** измените путь к хранилищу **FileStore** на тот, куда была перенесена папка **FileStore**.

7. Если **файловое хранилище** расположено в удаленной сетевой папке, то пользователь, от имени которого запущена служба **Файлового репозитория**, должен иметь полный доступ к папке **файлового хранилища** в сетевой папке.
8. Учетная запись также должна иметь права на чтение и запись в локальной папке **Repository** (например, C:\Program Files (x86)\Cyberprotect\Cyber Files\File Repository\Repository), чтобы иметь возможность записи в файл журнала.
9. Запустите службу **Сервер репозитория файлов Кибер Файлы**.
10. Запустите службу **Кибер Файлы Tomcat** и закройте оснастку **Службы**.

11.5.4 Выполнение Кибер Файлы Tomcat на нескольких портах

Хотя программа настройки поддерживает установку только одного порта для службы Tomcat, саму службу Tomcat можно настроить для работы на нескольких портах. Это можно сделать, добавив дополнительные коннекторы с нужными портами в XML-файл сервера Tomcat. Обновление и перезапуск службы Tomcat с использованием программы настройки не повлияет на новые коннекторы.

Примечание
Рекомендуется настраивать эту конфигурацию после того, как программа настройки уже выполнялась и служба Tomcat была успешно запущена.

11.5.4.1 Настройка дополнительного коннектора Tomcat

1. Остановите службу Кибер Файлы Tomcat, если она запущена.
2. Найдите и откройте файл server.xml. По умолчанию он расположен в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\apache-tomcat-7.0.59\conf.

   Примечание
   Число в имени папки (7.0.59) может быть другим в зависимости от версии Tomcat.

3. Найдите в файле раздел **Connector**, который выглядит так:

   <Connector maxHttpHeaderSize="65536" maxThreads="150" enableLookups="false" disableUploadTimeout="true" acceptCount="100" scheme="https" secure="true" SSLEnabled="true" SSLProtocol="TLSv1.2" SSLCertificateFile="${catalina.base}/conf/AAServer_LocalHost.crt" SSLCertificateKeyFile="${catalina.base}/conf/AAServer_LocalHost.key" SSLHonorCipherOrder="true" SSLCipherSuite="ECDH+AESGCM:ECDH+AES256:ECDH+AES128:RSA+AESGCM:RSA+AES:!aNULL:!eNULL:!LOW:!3DES:!RC4:!MD5:!EXP:!PSK:!SRP:!DSS" connectionTimeout="-1" URIEncoding="UTF-8" address="0.0.0.0" port="**443**"/>

Примечание
В зависимости от текстового редактора при открытии файла **server.xml** вышеприведенный код, скорее всего, будет отображаться в одну строку.

Примечание
Если вы выбрали не порт **443** в **программе настройки**, то в примере выше этот порт будет указан в разделе **Connector**.

4. Скопируйте весь раздел **Connector** и вставьте копию сразу после оригинала. Оба раздела должны иметь одинаковый отступ.
5. Замените **443** (или порт, выбранный в **программе установки**) на нужный второй порт, на котором будет работать Tomcat, например
   <Connector maxHttpHeaderSize="65536" maxThreads="150" enableLookups="false" disableUploadTimeout="true" acceptCount="100" scheme="https" secure="true" SSLEnabled="true" SSLProtocol="TLSv1.2" SSLCertificateFile="$
   {catalina.base}/conf/AAServer_LocalHost.crt" SSLCertificateKeyFile="${catalina.base}
   /conf/AAServer_LocalHost.key" SSLHonorCipherOrder="true"
   SSLCipherSuite="ECDH+AESGCM:ECDH+AES256:ECDH+AES128:RSA+AESGCM:RSA+AES:!aN
   ULL:!eNULL:!LOW:!3DES:!RC4:!MD5:!EXP:!PSK:!SRP:!DSS" connectionTimeout="-1"
   URIEncoding="UTF-8" address="0.0.0.0" port="**4430**"/>

   Примечание
   Убедитесь, что код для нового **коннектора** записан так же, как старый, то есть, если старый код записан в одну строку, новый должен быть тоже.
6. Откройте веб-интерфейс Кибер Файлы и перейдите в раздел **Общие настройки** -> **Параметры сервера**.
7. Убедитесь, что адрес, указанный в поле **Веб-адрес**, использует один из портов для коннекторов. Этот адрес пользователи будут видеть в приглашениях по электронной почте. Для него можно выбрать только один порт.

11.5.5 Подключение серверов Кибер Файлы к нескольким сетям

Подключение шлюза и сервера Кибер Файлы к нескольким сетям – простая задача, выполняемая с помощью программы настройки.

Единственным требованием является наличие двух отдельных сетевых интерфейсов и IP-адресов.

Настройка подключения к нескольким сетям

1. Откройте средство конфигурации Кибер Файлы.
2. Откройте вкладку **Веб-сервер** и введите первый IP-адрес и порт 443.

3. Откройте вкладку **Сервер шлюза** и введите второй IP-адрес и порт 443.
4. Нажмите кнопку**OK**.

Примечание
Работа стека TCP/IP в Microsoft Windows Server 2008 полностью изменена. Один транспорт IP теперь поддерживает несколько уровней, и «основного» IP-адреса больше нет. Поэтому, если одному интерфейсу назначены несколько IP-адресов, все эти адреса обрабатываются одинаково и все они регистрируются в DNS. То есть это не является ошибкой, а предусмотрено разработчиками. Но это приводит к проблемам, поскольку, если с ним ничего не делать, используемый IP-адрес будет циклично перебираться (системой DNS).

Эту ситуацию можно обойти, отключив динамическую регистрацию DNS на сетевой интерфейсной плате и затем создав DNS-запись хоста вручную. Еще более простой способ обхода – установить оперативное исправление по ссылке **KB975808:** http://support.microsoft.com/?kbid=975808. После установки этого оперативного управления можно будет использовать флаг netsh skipassource. С его помощью при добавлении новых адресов можно указать стеку, что новый адрес не используется для исходящих пакетов. Поэтому такие IP-адреса не будут регистрироваться на серверах DNS. Например:

```
netsh int ipv4 add address "Local Area Connection" 192.168.1.2 skipassource=true
```

11.5.6 Развертывание отдельных сервлетов для предпросмотра в веб-браузере

Функция предпросмотра в веб-браузере Кибер Файлы позволяет просматривать содержимое файла без необходимости скачивания. При большом количестве пользователей это может снизить производительность развертывания. Чтобы компенсировать нагрузку на основные серверы Кибер Файлы, можно установить дополнительные серверы Tomcat с сервлетами для предпросмотра в веб-браузере.

Перед серией серверов Tomcat можно поместить балансировщик нагрузки, чтобы дополнительно оптимизировать нагрузку для сервлетов предпросмотра. Для запросов на предпросмотр не требуется состояние, поэтому дополнительно настраивать балансировщик нагрузки не нужно.

Примечание
Для файлов, защищенных паролем, недоступны эскизы и предварительный просмотр.

11.5.6.1 Установка и настройка сервлета

Установка Tomcat

Сервер Apache Tomcat 9.0.54 можно установить из ZIP-файла или с помощью исполняемого файла установки. Рекомендуется использовать установщик, но подойдет и ZIP-архив. Единственным различием будет способ настройки сервера Apache Tomcat 9.0.54.

Требования для обоих сценариев

1. Убедитесь, что установлена 64-битная версия среды выполнения Java (JRE). Также подойдет 64-битная версия комплекта разработчика Java (JDK). Версия Java должна быть не ниже 8.
2. Скачайте 64-битную версию Apache Tomcat 9.0.54. Устанавливаемая версия не должна быть новее версии, поддерживаемой программой Кибер Файлы. Версия, используемая программой Кибер Файлы, указана в начале истории выпусков.

Использование исполняемого файла установки

1. Скачайте файл установки для 64-битной версии Apache Tomcat 9.0.54. Список версий можно найти на сайте Apache Tomcat. Щелкните нужную версию, затем откройте папку bin и скачайте EXE-файл (например, **apache-tomcat-9.0.54.exe**).
2. Запустите установщик и следуйте инструкциям мастера установки. Можно оставить все параметры по умолчанию. При необходимости измените порт прослушивания, по умолчанию используется 8080.

   Примечание
   Установщик найдет папку установки Java автоматически.

3. После завершения установки на машине с Кибер Файлы перейдите в папку установки Кибер Файлы (по умолчанию C:\Program Files (x86)\Cyberprotect\Cyber Files\Access Server\).
4. Скопируйте папку **AccessPreviewServlet** на новую машину с установленным Apache Tomcat и вставьте в папку **webapps** сервера Tomcat (по умолчанию C:\Program Files\Apache Software Foundation\Tomcat 9.0.54\webapps)
5. Перейдите в папку **conf** установки Apache Tomcat (по умолчанию C:\Program Files\Apache Software Foundation\Tomcat 9.0.54\conf) и создайте резервную копию файла **server.xml**.
6. Затем откройте файл, найдите строки <Host name="localhost" appBase="webapps"unpackWARs="true" autoDeploy="true"> и поместите непосредственно под ними следующие строки:

   ```
   <!-- for Access Web preview -->
   ```

   ```
   <Context path="/AccessPreviewServlet" docBase="C:\Program Files\Apache Software Foundation\Tomcat 9.0.54\webapps\AccessPreviewServlet">
   ```

   ```
   </Context>
   ```

   Примечание
   Если вы установили Apache Tomcat не в стандартное местоположение, необходимо будет изменить путь **docBase=""** в соответствии с фактическим путем к папке установки.

7. Сохраните и закройте файл.

8. Чтобы запустить службу Tomcat, откройте **Панель управления** -> **Администрирование** -> **Службы** и запустите службу Apache Tomcat.

Использование архива с установкой Apache Tomcat

1. Скачайте **ZIP-файл** с 64-битной версией Apache Tomcat 9.0.54. Список версий можно найти на сайте Apache Tomcat. Щелкните нужную версию, затем откройте папку bin и скачайте основной ZIP-файл (например, **apache-tomcat-9.0.54.zip**).
2. Извлеките содержимое архива в выбранную папку, например **C:\Program Files\Apache Tomcat**.
3. Перейдите в папку **C:\Program Files\Apache Tomcat\apache-tomcat-<version>** и откройте папку **bin**.

   Примечание
   Имя извлеченной папки содержит номер версии, замените **<version>** на номер вашей версии Tomcat, например **C:\Program Files\Apache Tomcat\apache-tomcat-9.0.54**.

4. Откройте **startup.bat** в текстовом редакторе и найдите строку **setlocal**.
5. Добавьте под ней следующие строки:
   set "CATALINA_HOME=Your Tomcat Folder"
   например, set"CATALINA_HOME=C:\Program Files\Apache Tomcat\apache-tomcat-9.0.54"

   Примечание
   Это задает папку Tomcat по умолчанию для всех параметров. Используйте фактический путь к папке Apache Tomcat.

   set "JRE_HOME=Java main folder location"
   например, set "JRE_HOME=C:\Program Files\Java\jre1.8.0_112"

   Примечание
   Это задает папку JRE по умолчанию для всех параметров. Используйте фактический путь к папке Java.

   Примечание
   Если вы используете JDK, нужна команда **JAVA_HOME** вместо **JRE_HOME**.

6. Сохраните изменения, сделанные в файле.
7. После этого на машине с Кибер Файлы перейдите в папку установки Кибер Файлы (по умолчанию C:\Program Files (x86)\Cyberprotect\Cyber Files\Access Server\).
8. Скопируйте папку **AccessPreviewServlet** на новую машину с Apache Tomcat и вставьте в папку **webapps** сервера Tomcat (по умолчанию C:\Program Files\Apache Tomcat\apache-tomcat-9.0.54\webapps).
9. Перейдите в папку **conf** установки Apache Tomcat (например, **C:\Program Files\Apache Tomcat\apache-tomcat-9.0.54\conf)** и создайте резервную копию файла **server.xml**.

10. Затем откройте файл, найдите строки <Host name="localhost" appBase="webapps" unpackWARs="true" autoDeploy="true"> и поместите непосредственно под ними следующие строки:

```
<!-- for Access Web preview -->
```

```
<Context path="/AccessPreviewServlet" docBase="C:\Program Files\Apache Tomcat\apache-tomcat-9.0.54\webapps\AccessPreviewServlet">
```

```
</Context>
```

11. Измените путь docBase="" в соответствии с фактическим путем к папке установки. Сохраните и закройте файл.

Примечание

Если не менять порт прослушивания по умолчанию, то сервлет будет прослушивать порт **8080**. Чтобы изменить порт, найдите в файле **server.xml** следующие строки:

<Connector port="**8080**" protocol="HTTP/1.1"

connectionTimeout="20000"

redirectPort="8443" />

Замените **8080** на нужный номер порта.

12. Чтобы запустить службу Tomcat, перейдите в папку bin и дважды щелкните файл **startup.bat**. Черное окно DOS должно оставаться открытым во время работы Tomcat.

11.5.6.2 Конфигурация сервера Кибер Файлы

1. Откройте веб-интерфейс Кибер Файлы и выберите **Общие настройки**-> **Предпросмотр в веб-браузере**.
2. Включите **Пользовательский URL-адрес для веб-службы предпросмотра** и введите адрес нового сервлета предпросмотра. (**Например,**http://accesswp.company.com:8080. Указываемый вами URL-адрес должен содержать этот номер порта. Если используется кластерная установка или балансировка нагрузки, то URL-адресом будет адрес балансировщика нагрузки.
3. В зависимости от количества серверов, настроенных для работы сервлета предпросмотра, может потребоваться увеличить **Максимум одновременных вызовов формирования** в настройках сервера Кибер Файлы.
4. Найдите параметр **Максимум одновременных вызовов формирования** и задайте нужное значение.

   Значение по умолчанию – 2. Для формирования документа может использоваться большая часть одного ядра процессора. Число потоков формирования не должно превышать 50 % доступных ядер процессора. Превышение рекомендуемого значения может привести к снижению производительности других служб сервера.

11.5.6.3 Балансировка нагрузки для сервлетов предпросмотра в веб-браузере

Сервлеты для **предпросмотра в веб-браузере** должны располагаться за балансировщиком нагрузки.

1. Включите функцию поддержания сеанса на основе длительности (или ее аналог) в своем балансировщике нагрузки и задайте бессрочные сеансы.
2. Если требуется проверка работоспособности (проверка на получение HTTP-статуса 200), достаточно отправить команду ping на адрес **http://servername.yourdomain.com:port/AccessPreviewServlet/generate_preview/**. Например, адрес:https://servlet1.acme.com/AccessPreviewServlet/generate_preview и https://servlet2.acme.com/AccessPreviewServlet/generate_preview
3. Откройте в браузере адрес балансировщика нагрузки, чтобы проверить работу конфигурации. Например, адрес: https://loadbalancer.yourdomain.com

11.5.7 Потоковая репликация PostgreSQL

В этом документе предоставляется пошаговая инструкция по настройке потоковой репликации между двумя серверами PostgreSQL. Потоковая репликация – это лишь один из множества методов поддержки оперативного режима базы данных PostgreSQL, но другие методы в этом документе не рассматриваются.

Примечание
В этом документе не описывается процесс установки PostgreSQL или Кибер Файлы, а только настройка потоковой репликации.

11.5.7.1 Потоковая репликация

Процесс потоковой репликации основан на сегменте журнала опережающей записи (WAL). WAL является стандартным методом обеспечения целостности данных. Основной принцип WAL состоит в том, что изменения в файлах данных (где расположены таблицы и индексы) применяются только после фиксации этих изменений в журнале, т. е. после того, как записи журнала, описывающие изменения, сбрасываются в постоянное хранилище. Если следовать этой процедуре, то не потребуется сбрасывать страницы данных на диск после каждой фиксации транзакции, поскольку в случае аварии можно будет восстановить базу данных с помощью журнала, т. е. все изменения, не примененные к страницам данных, можно будет сделать на основе записей журнала.

Использование WAL значительно сокращает количество операций записи на диск, поскольку для гарантированной фиксации транзакций на диск достаточно сбрасывать только журнал, а не каждый измененный транзакцией файл данных. Файл журнала записывается последовательно, поэтому стоимость синхронизации журнала намного меньше стоимости сохранения страниц данных на диск.

WAL также обеспечивает поддержку резервного копирования в онлайн-хранилище, восстановления на определенный момент времени и репликации. Потоковая репликация представляет собой непрерывную отправку записей WAL через соединение TCP/IP между основным и резервным серверами по протоколу walsender через подключения репликации. Хотя потоковая репликация может быть синхронной, учитывая ресурсы, необходимые для синхронного процесса и его влияние на производительность, мы решили рассматривать в качестве действенного сценария только асинхронную потоковую репликацию.

11.5.7.2 Требования

- Два сервера PotsgreSQL: в этой процедуре активный сервер будет называться основным сервером, а пассивный сервер – резервным.

  Примечание
  Для подключений Кибер Файлы можно использовать только основной сервер. Резервный сервер можно использовать только в случае выполнения отработки отказа, когда он становится основным.

- PostgreSQL 11,6: Мы будем внедрять такие функции, как «слот репликации», требующие PostgreSQL 11,6. Эта версия входит в состав Кибер Файлы 8.7 или выше и используется только при новой установке (не применяется при обновлении).
- Один виртуальный IP-адрес (необязательно): этот виртуальный IP-адрес будет использоваться всеми интерфейсными серверами с ролью Кибер Файлы Server и всегда должен принадлежать активному хосту (основному серверу).
- Мы рекомендуем заранее установить Кибер Файлы и инициализировать базу данных основного сервера.

11.5.7.3 На основном сервере

Создание пользователя репликации

Эта учетная запись будет использоваться процессом репликации для отправки WAL с основного сервера на резервный. В целях безопасности рекомендуется создать выделенную учетную запись с разрешениями на репликацию вместо использования учетной записи суперпользователя по умолчанию (т. е. **postgres**).

1. На основном сервере выполните следующую команду:
   psql -c "CREATE USER replicator REPLICATION LOGIN ENCRYPTED PASSWORD 'XXXXX';" -U postgres
   Эту команду также можно выполнить удаленно с помощью следующих параметров:
   psql -c "CREATE USER replicator REPLICATION LOGIN ENCRYPTED PASSWORD 'XXXXX';" -h <IP_OF_PRIMARY_SERVER> -U postgres

Примечание
PSQL находится в подпапке **bin** в папке установки PostgreSQL. В зависимости от переменной среды PATH может потребоваться указать путь для команды или перейти в нужную папку перед выполнением команды. Это примечание также относится к последующим командам в этой процедуре.

Настройка доступа

Измените управление доступом на основном сервере, чтобы разрешить подключение от резервного сервера.

1. Для этого измените файл **pg_hba.conf** (расположенный в подпапке **data**), добавив следующую строку:
   host replication replicator <**IP_OF_STANDBY_SERVER**>/32 trust
2. Если нужна повышенная безопасность при связи между серверами баз данных, то проверка подлинности может затребовать у клиента пароль с хешированием MD5 с возможностью также требовать использование протокола SSL (**hostssl**), например
   host replication replicator <**IP_OF_STANDBY_SERVER**>/32 md5
   hostssl replication replicator <**IP_OF_STANDBY_SERVER**>/32 md5

Настройка потоковой репликации

1. Перейдите в папку установки PostgreSQL. Расположение по умолчанию:

   C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\PostgreSQL\<version>
2. В папке Data откройте файл postgresql.conf для внесения изменений. Найдите и измените следующие строки:

   Примечание
   Убедитесь, что в начале этих строк не стоит символ **#**. С этим символом команды рассматриваются как комментарии и не будут работать.

   listen_addresses = '**IP_OF_PRIMARY_SERVER**, 127.0.0.1'
3. После внесения вышеуказанных изменений перезапустите службу PostgreSQL.

Создание слота репликации

1. На основном сервере выполните следующую команду:
   psql -U postgres -c "SELECT * FROM pg_create_physical_replication_slot('access_slot');"
2. Проверьте, что слот создан, с помощью следующей команды:
   psql -U postgres -c "SELECT * FROM pg_replication_slots;"

11.5.7.4 На резервном сервере

Убедитесь, что у всех нужных серверов есть доступ друг к другу.

В случае отказа основного сервера резервный сервер станет основным и будет отвечать на все запросы серверов Кибер Файлы.

Рекомендуется настроить доступ к резервному серверу для всех серверов Кибер Файлы сейчас, чтобы не потребовалось перезапускать службу PostgreSQL на резервном сервере в процессе перехода.

Примечание
Когда резервный сервер находится в режиме ожидания, база данных доступна только для чтения («горячий резерв»). Таким образом, невозможно настроить и использовать резервный сервер в качестве рабочей базы данных по ошибке.

1. Измените управление доступом на резервном сервере, чтобы разрешить подключение от всех серверов Кибер Файлы.
2. Для этого перейдите в папку установки PostgreSQL и измените файл **pg_hba.conf** (расположенный в подпапке data), добавив следующую строку для каждого сервера:
   host all all <IP_OF_CYBER_FILES_SERVER_1>/32 md5
   host all all <IP_OF_CYBER_FILES_SERVER_1>/32 md5

Настройка потоковой репликации

1. Перейдите в папку установки PostgreSQL. Расположение по умолчанию:

   C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\PostgreSQL\<version>
2. В папке Data откройте файл postgresql.conf для внесения изменений. Найдите и измените следующие строки:

   Примечание
   Убедитесь, что в начале этих строк не стоит символ **#**. С этим символом команды рассматриваются как комментарии и не будут работать.

   - listen_addresses = '**IP_OF_STANDBY_SERVER**, 127.0.0.1'
   - hot_standby = on

   Параметр hot_standby определяет, можно ли подключаться и делать запросы во время потоковой репликации. Если параметр включен, база данных будет принимать запросы на чтение, поэтому можно будет проверить, работает ли процесс репликации, просмотрев содержимое таблиц базы данных.

Примечание
Для параметра listen_addressesвозможно дублирование строк в файле postgresql.conf, где первая (закомментированная) строка существует как часть шаблона файла по умолчанию, а вторая (раскомментированная) строка добавляется программой установки продукта. Изменять следует только первую строку, при этом не следует раскомментировать любые другие строки (при их наличии).

Примечание
Если строка max_connections в файле postgresql.conf была изменена на основном сервере с присвоением значения, отличающегося от значения, заданного по умолчанию, ее необходимо будет изменить и на резервном сервере.

Примечание
При использовании md5 или password в качестве метода проверки подлинности, указанного в файле pg_hba.conf, для этого подключения потребуется пароль. Для того чтобы ввести этот пароль, в файл recovery.conf на резервном сервере необходимо добавить следующую команду: primary_conninfo = 'host=<IP_ADDRESS_OF_PRIMARY_SERVER> port=<PORT_OF_PRIMARY_SERVER> user=<USERNAME> password=<PASSWORD_FOR_USERNAME>'
. Например, вот как это будет выглядеть для службы Postgres, работающей по IP-адресу 10.0.0.1, порт 5432, для пользователя replicator с паролем 1234: primary_conninfo = 'host=10.0.0.1 port=5432 user=replicator password=1234'

3. **Остановите службу PostgreSQL на резервном сервере, чтобы выполнить начальное сохранение базы данных и запустить процесс потоковой репликации.**

Резервное копирование файлов конфигурации

Сделайте резервную копию всех файлов конфигурации **.conf**, включая **pg_hba.conf**, **postgresql.conf**, **pg_ident.conf**. Эти файлы будут перезаписаны в процессе начального сохранения, и их необходимо будет восстановить после этого шага.

Очистка папки data

Удалите (или переименуйте) подпапку **data**. Переименование папки – хороший способ сохранить копию предыдущей конфигурации, чтобы можно было вернуть базу данных резервного сервера в согласованное состояние в случае возникновения проблем при начальном сохранении или при запуске базы данных.

Начальное сохранение

Начальное сохранение выполняется путем резервного копирования основной базы данных в папку на резервном сервере.

1. Убедитесь, что основной сервер не используется активно. Самый простой способ – это остановить службу Tomcat для Кибер Файлы и снова запустить ее после завершения

сохранения.

2. Чтобы запустить начальное сохранение на уровне резервного сервера, используйте следующую команду:

   pg_basebackup.exe -h <IP_OF_PRIMARY_SERVER> -D <PATH_TO_NEW_DATA_DIR> -U replicator -v -P --slot=access_slot

   Примечание
   Путь <PATH_TO_NEW_DATA_DIR> должен вести к папке Данные, например C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\PostgreSQL\11.6\Data

Восстановление файлов конфигурации

Скопируйте все файлы конфигурации **.conf** (включая **pg_hba.conf**, **postgresql.conf**, **pg_ident.conf**) из резервной папки в новую папку Data, перезаписав все существующие файлы.

Создание слота репликации

1. На резервном сервере выполните следующую команду:

   psql -U postgres -c "SELECT * FROM pg_create_physical_replication_slot('access_slot');"

2. Проверьте, что слот создан, с помощью следующей команды:

   psql -U postgres -c "SELECT * FROM pg_replication_slots;"

Средства управления потоковой репликацией

1. Откройте папку Data и создайте (или измените) файл recovery.conf.
2. Добавьте следующие строки, если они отсутствуют:
   - standby_mode = 'on'
   - primary_conninfo = 'host=<**IP_OF_PRIMARY_SERVER**> port=5432 user=replicator password= <**PASSWORD_USED_FOR_REPLICATOR_USER**>'
   - primary_slot_name = 'access_slot'
   - trigger_file = '<**PATH_TO_TRIGGER_FILE**>' # As an example 'failover.trigger'
   - recovery_min_apply_delay = 5min
3. После сохранения вышеуказанных изменений запустите службу PostgreSQL на резервном сервере.

   Примечание
   В случае перехода на резервный сервер файл recovery.conf будет переименован в recovery.done.

Дополнительная информация

- Параметр standby_mode задает запуск сервера PostgreSQL в качестве резервного. В этом случае сервер не остановит восстановление, достигнув конца архива WAL, а попытается продолжить восстановление путем извлечения новых сегментов WAL, подключаясь к основному

серверу, как указано в параметре primary_conninfo (который определяет строку подключения для соединения резервного сервера с основным).

- Мы используем слот репликации, созданный на предыдущих шагах на основном сервере, с помощью параметра primary_slot_name.
- Параметр trigger_file определяет файл-триггер, присутствие которого заканчивает восстановление на резервном сервере и делает сервер основным. Это будет использоваться в процессе перехода на резервный сервер.
- При необходимости можно задать параметр recovery_min_apply_delay. По умолчанию резервный сервер восстанавливает записи WAL с основного сервера как можно быстрее. Может быть полезно копировать данные с временной задержкой, что даст возможность исправить ошибки потери данных. Этот параметр позволяет отложить восстановление на фиксированный промежуток времени в миллисекундах, если не указаны другие единицы.

  Например, если установить для параметра значение 5 min, то резервный сервер будет воспроизводить каждую фиксацию транзакции, только когда системное время на резервном сервере будет как минимум на пять минут больше времени фиксации, переданного основным сервером.

  Задержка репликации между серверами может превышать значение этого параметра, в этом случае временная задержка не добавляется. Обратите внимание, что задержка рассчитывается между временной меткой WAL, записанной на основном сервере, и текущим временем на резервном сервере. Задержки при передаче данных из-за запаздывания в сети или конфигураций каскадной репликации могут значительно сократить фактическое время ожидания. Если системные часы на основном и резервном серверах не синхронизированы, применение записей при восстановлении может происходить раньше ожидаемого; но это не является серьезной проблемой, поскольку полезные значения этого параметра намного больше обычных расхождений времени между серверами.

11.5.7.5 Тестирование перехода на резервный сервер

Мы рекомендуем протестировать приведенные выше настройки и убедиться, что переход на резервный сервер выполняется правильно, перед внедрением в рабочую установку.

Если основной сервер работает, сначала нужно его остановить, а затем передавать его роль резервному серверу. Это необходимо для того, чтобы основной сервер не обрабатывал дальнейшие запросы и не возникали проблемы.

Резервный сервер можно сделать основным, создав файл триггера, указанный в файле **recovery.conf**. Теперь, когда резервный сервер взял на себя роль основного, убедитесь, что ваши серверы Кибер Файлы настроены на его использование.

Примечание
После того как будет инициирован и успешно завершится переход на резервный сервер, файл recovery.conf будет переименован в recovery.done. Файл триггера будет удален.

Сделать это можно, перейдя в папку C:\Program Files (x86)\Cyberprotect\Cyber Files\Access Server и внеся изменения в файл cyberfilessrv.cfg. Убедитесь, что DB_HOSTNAME и DB_PORT указывают

на адрес и порт того сервера PostgreSQL, который сейчас является основным. При внесении любых изменений потребуется перезапустить службу Кибер Файлы Tomcat.

11.5.7.6 Перенос экземпляров

1. Для этого обновления необходимо выделить некоторое время на простой, остановив Кибер Файлы.
2. Кроме того, необходимо также остановить основной и резервный серверы PostgreSQL.
3. Обновите основной сервер, следуя инструкциям из " Обновление PostgreSQL до новой основной версии" (стр. 147).
4. Установите основную версию PostgreSQL на резервный сервер.
5. Следуйте инструкциям по потоковой репликации, доступным как для основного так и для резервногосерверов.

11.5.8 Настройка PostgreSQL для удаленного доступа

Удаленный доступ может помочь, если вы управляете несколькими экземплярами PostgreSQL или просто предпочитаете управлять базой данных удаленно.

11.5.8.1 Чтобы включить удаленный доступ к этому экземпляру PostgreSQL, выполните следующие действия.

1. Перейдите в каталог установки PostgreSQL: C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\PostgreSQL\9.4\Data\
2. Откройте файл **pg_hba.conf** в текстовом редакторе.
3. Добавьте записи хостов для каждого компьютера, который будет иметь удаленный доступ с использованием своего внутреннего адреса, и сохраните файл. Файл **pg_hba.conf** (HBA означает Host-based authentication – проверка подлинности на основе хоста) контролирует проверку подлинности клиентов и хранится в каталоге данных кластера базы данных. В нем указываются серверы, которым разрешено соединение, и их права, например
   # TYPE DATABASE USER ADDRESS METHOD
   # First Кибер Файлы & Gateway server
   host all all 10.27.81.3/32 md5
   # Second Кибер Файлы & Gateway server
   host all all 10.27.81.4/32 md5
   В этих примерах все пользователи, подключающиеся с первого компьютера (10.27.81.3/32) и второго компьютера (10.27.81.4/32), могут получить доступ к базе данных с полными привилегиями (кроме привилегии репликации) через зашифрованное md5 соединение.
4. Найдите и откройте файл **postgresql.conf**. По умолчанию это путь C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\PostgreSQL\9.4\Data\

a. Найдите строку #listen_addresses = 'localhost'

b. Включите эту команду, удалив символ **#** в начале строки.

c. Замените localhost на ***** для прослушивания всех доступных адресов. Чтобы настроить PostgreSQL на прослушивание только определенного адреса, введите нужный IP-адрес вместо *****.

- **Например,** listen_addresses = '*' означает, что PostgreSQL будет прослушивать все доступные адреса.
- **Например,** listen_addresses = '192.168.1.1' означает, что PostgreSQL будет прослушивать указанный адрес.

5. Сохраните изменения, сделанные в файле **postgresql.conf**.
6. Перезапустите службу сервера PostgreSQL Кибер Файлы.

Примечание
По умолчанию PostgreSQL использует порт 5432. Убедитесь, что этот порт открыт в брандмауэре или программе маршрутизации.

11.5.9 Запуск Кибер Файлы в режиме HTTP

Эти настройки предоставляются для ситуаций, когда требуется использовать обмен данными по HTTP между Кибер Файлы и внутренними сервисами, например службами балансировки нагрузки или решениями прокси. Серверы Кибер Файлы, обменивающиеся информацией по незащищенным локальным сетям или через Интернет, должны всегда работать в режиме HTTPS. При внутренней работе в режиме HTTP сетевой трафик Кибер Файлы становится видимым всем участникам, у которых есть доступ ко внутренней сети.

Чтобы переключиться с HTTPS на HTTP, необходимо изменить некоторые настройки в следующих файлах.

- Файл Tomcat server.xml , расположенный в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\apache-tomcat-7.0.75\conf

  Примечание
  Номер версии Tomcat может отличаться в зависимости от версии используемого Кибер Файлы.

- Файл cyberfilessrv.cfg, расположенный в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Access Server.

11.5.9.1 Редактирование файла «server.xml»

В этом файле необходимо установить соответствующий коннектор HTTP, а коннекторы HTTPS следует отключить.

1. Откройте файл в текстовом редакторе и найдите имеющийся коннектор HTTPS. Строка должна иметь следующий вид:

<Connector maxHttpHeaderSize="65536" maxThreads="150" enableLookups="false" disableUploadTimeout="true" acceptCount="100" scheme="https" secure="true" SSLEnabled="true" SSLProtocol="TLSv1.2" SSLCertificateFile="${catalina.base}/conf/AAServer_LocalHost.crt" SSLCertificateKeyFile="${catalina.base}/conf/AAServer_LocalHost.key" SSLHonorCipherOrder="true" SSLCipherSuite="ECDH+AESGCM:ECDH+AES256:ECDH+AES128:RSA+AESGCM:RSA+AES:!aNULL:!eNULL:!LOW:!3DES:!RC4:!MD5:!EXP:!PSK:!SRP:!DSS" connectionTimeout="-1" URIEncoding="UTF-8" bindOnInit="false" port="443" address="0.0.0.0"/>

2. Отключите коннектор HTTPS, заключив его в <!-- и -->. Другими словами, нужно ввести <!-- перед <Connector maxHttp.... и --> после ... address="0.0.0.0"/>
3. Создайте новый коннектор HTTP, который будет выглядеть следующим образом:
   <Connector maxHttpHeaderSize="65536" maxThreads="150" enableLookups="false" disableUploadTimeout="true" acceptCount="100" scheme="http" secure="true" connectionTimeout="-1" URIEncoding="UTF-8" port="80" address="0.0.0.0"/>
4. Можно выбрать другой порт (кроме порта по умолчанию) и ограничить адреса для подключения к определенному адресу, чтобы служба не использовала все доступные.
5. Убедитесь, что порт, который следует использовать, открыт в вашем брандмауэре.
6. Проверьте, имеется ли этот коннектор перенаправления в файле server.xml:
   <!-- <Connector port="80" connectionTimeout="20000" protocol="HTTP/1.1" redirectPort="443"/> -->
7. Если такая запись есть и следует использовать порт 80, отключите коннектор, проставив символы <!- и ->, как показано выше.
8. Сохраните файл после внесения необходимых изменений.

11.5.9.2 Редактирование файла «cyberfilessrv.cfg»

Здесь необходимо только задать для параметра REQUIRE_SSL значение **true** вместо **false**, чтобы он выглядел следующим образом:

REQUIRE_SSL = false

1. Сохраните файл после внесения необходимых изменений.
2. Перезапустите службу Кибер Файлы Tomcat для применения изменений.

11.5.9.3 Ограничения режима HTTP

- В режиме HTTP связь с сервером шлюза не поддерживается, так как для работы шлюза требуется HTTPS. Доступ к сетевому узлу через веб-интерфейс или мобильные клиенты не поддерживается.
- Единый вход не работает.
- При использовании настольных клиентов необходимо вручную указать **HTTP** в поле адреса сервера, иначе подключение будет невозможно, например http://myaccess.com:3000

11.5.10 Запуск Кибер Файлы Tomcat с помощью незащищенных версий TLS

Примечание
Работа развертываний, использующих старые версии TLS, может быть нарушена из-за изменений, внесенных в этот выпуск. Ниже описан способ обхода этой проблемы, хотя больше не поддерживает такие конфигурации.

Начиная с Кибер Файлы 8.7.0, все новые установки и обновления будут поддерживать только TLSv1.2.

Эти действия не поддерживаются и предоставляются «как есть», чтобы можно было использовать TLSv1 и TLSv1.1, если имеется необходимость применять эти незащищенные версии TLS.

Управление конфигурациями TLS при обновлении Tomcat 9

Примечание
Обновление конфигурации коннектора выполняется так же, как это описано в разделах Выполнение Кибер Файлы в режиме HTTP и Выполнение Кибер Файлы Tomcat на нескольких портах.

Примечание
Перед тем как включать TLSv1 и TLSv1.1, удостоверьтесь в том, что это действительно необходимо. В большинстве веб-браузеров TLSv1 и TLSv1.1 больше не используются, а по умолчанию задействована версия TLSv1.2. Некоторые другие сервисы, которые интегрируются с Кибер Файлы, нужно просто обновить, чтобы они могли работать с TLSv1.2. Например, для Office Online требуется исправление KB5001973)

1. Остановите службу Кибер Файлы Tomcat.
2. Перейдите к файлу server.xml. По умолчанию он расположен в папке C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\apache-tomcat-9.0.54\conf

   Примечание
   Путь может отличаться, если вы перешли на более новую версию Кибер Файлы или выполнили пользовательскую установку. Можно воспользоваться записью Кибер Файлы Tomcat в службах Windows, чтобы найти путь к папке Apache Tomcat, в котором должна быть папка conf.

3. Сделайте копию исходного, неизмененного файла server.xml, сохранив его под другим именем, на случай, если нужно будет вернуться к поддерживаемой версии.
4. В разделе Connector исходного файла найдите приведенное далее содержимое:

```
<Connector maxHttpHeaderSize="65536" maxThreads="150" enableLookups="false"
disableUploadTimeout="true" acceptCount="100" scheme="https" secure="true"
```

```
SSLEnabled="true" SSLProtocol="TLSv1.2"
SSLCertificateFile="${catalina.base}/conf/AACert.cer"
SSLCertificateKeyFile="${catalina.base}/conf/AACert.key" SSLHonorCipherOrder="true"
SSLCipherSuite="ECDH+AESGCM:ECDH+AES256:ECDH+AES128:RSA+AESGCM:RSA+AE
S:!aNULL:!eNULL:!LOW:!3DES:!RC4:!MD5:!EXP:!PSK:!SRP:!DSS" connectionTimeout="-1"
URIEncoding="UTF-8" bindOnInit="false" relaxedQueryChars="[,]" port="443"
address="0.0.0.0"/>
```

5. Внесите в текст следующие изменения:

   Строка

   ```
   SSLProtocol="TLSv1.2"
   ```

   Новая строка

   ```
   SSLProtocol=”TLSv1+TLSv1.1+TLSv1.2"
   ```

6. Внеся изменения, сохраните файл.
7. Запустите службу Кибер Файлы Tomcat.

11.5.11 Обновление Кибер Файлы в отказоустойчивом кластере Microsoft

Следующие шаги позволяют обновить кластер серверов Кибер Файлы до более новой версии Кибер Файлы.

Примечание
Перед обновлением просмотрите наши статьи по резервному копированию и сохраните копию конфигурации.

1. Перейдите к активному узлу.
2. Откройте **Администратор кластера**/**Диспетчер отказоустойчивого кластера**.
3. Остановите все службы Кибер Файлы (в том числе **postgres-some-version**). Общий диск должен оставаться подключенным к сети.
4. Отключите все антивирусное ПО на компьютере, иначе оно может прервать процедуру установки.
5. Дважды щелкните по исполняемому файлу программы установки.
6. Нажмите **Далее**, чтобы начать установку.
7. Прочитайте и примите лицензионное соглашение.
8. Нажмите **Обновить**.
9. Просмотрите список компонентов, которые будут установлены, и нажмите кнопку **Установить**.
10. Введите пароль суперпользователя **postgres** и нажмите кнопку **Далее**.

11. После завершения установки нажмите кнопку **Выйти**, чтобы закрыть программу установки.

Предупреждение
Не переводите кластерную группу в режим «в сети»!

12. Перенесите кластерную группу на второй узел.
13. Повторите ту же процедуру установки на втором узле.
14. Верните все службы Кибер Файлы в режим «в сети».

11.5.12 УстановкаКибер Файлы в отказоустойчивом кластере Microsoft

Приведенные ниже руководства помогут установить Кибер Файлы в кластере.

11.5.12.1 Установка Кибер Файлы в отказоустойчивом кластере Microsoft Windows 2012 (R2)

Установка Кибер Файлы

Перед установкой Кибер Файлы необходимо выполнить вход от имени администратора домена.

1. Скачайте установщик Кибер Файлы.
2. Отключите все антивирусное ПО на компьютере, иначе оно может прервать процедуру установки.
3. Дважды щелкните по исполняемому файлу программы установки.
4. Нажмите **Далее**, чтобы начать установку.
   Прочитайте и примите лицензионное соглашение.
5. Нажмите **Установить**.

Примечание
Если развертывается несколько серверов Кибер Файлы или устанавливается нестандартная конфигурация, то можно указать устанавливаемые компоненты, нажав кнопку **Выборочная установка**.

6. Оставьте путь по умолчанию или выберите новый путь для главной папки Кибер Файлы и нажмите **OK**.
7. Задайте пароль для пользователя Postgres и запишите его. Этот пароль понадобится для резервного копирования и восстановления базы данных.
8. Выберите на общем диске расположение для папки **Postgres Data** и нажмите **Далее**.
9. Откроется окно с отображением всех компонентов, которые будут установлены. Нажмите **OK**, чтобы продолжить.

10. После завершения установки Кибер Файлы нажмите **Выйти**

Создание роли

1. Откройте **Диспетчер отказоустойчивого кластера** и щелкните правой кнопкой мыши **Роли**.
2. Выберите **Создать пустую роль**. Присвойте роли подходящее имя (например, Кибер Файлы, кластер AAS)

Настройки активного узла

1. Настройте расположение базы данных сервера шлюза на общем диске.
   a. Перейдите в папку C:\Program Files (x86)\Cyber Files\Gateway Server\
   b. Найдите файл **database.yml** и откройте его в текстовом редакторе.
   c. Найдите строку database_path: './database/' и замените **./database/** путем, который используется у вас (например, database_path: 'S:/access_cluster/database/').

   Примечание
   Используйте косую черту (/) в качестве разделителя пути.

   Примечание
   Можно скопировать настроенный файл database.yml с первого узла на второй.

Добавление всех независимых служб к роли Кибер Файлы

Выполните следующую процедуру для каждой из следующих служб: шлюз Кибер Файлы, Кибер Файлы PostgreSQL (они могут различаться в зависимости от версии Кибер Файлы), репозиторий Кибер Файлы и Кибер Файлы Tomcat

1. Щелкните по роли Кибер Файлы правой кнопкой мыши и выберите **Добавить ресурс**.
2. Выберите **Универсальная служба**.
3. Выберите нужную службу и нажмите **Далее**.
4. В окне подтверждения нажмите **Далее**.
5. В окне сводки нажмите **Готово**.

Задание точки доступа

1. Щелкните по роли Кибер Файлы правой кнопкой мыши и выберите **Добавить ресурс**.
2. Выберите **Клиентская точка доступа**.
3. Введите имя точки доступа.
4. Выберите сеть.
5. Введите IP-адрес и нажмите **Далее**.

6. В окне подтверждения нажмите **Далее**.
7. В окне сводки нажмите **Готово**.

Добавление общего диска

1. Щелкните по роли Кибер Файлы правой кнопкой мыши и выберите **Добавить хранилище**.
2. Выберите нужный общий диск.

Настройка зависимостей

1. Выберите роль Кибер Файлы и откройте вкладку **Ресурсы**.

Для служб PostgreSQL и «Репозиторий файлов Кибер Файлы» выполните следующие действия.

1. Щелкните по службе правой кнопкой и выберите **Свойства**.
2. Откройте вкладку **Зависимости**.
3. Щелкните **Ресурс** и выберите добавленный общий диск.
4. Нажмите кнопку **Применить** и закройте окно.

Для службы «Сервер шлюза Кибер Файлы» выполните следующие действия.

1. Щелкните по службе правой кнопкой и выберите **Свойства**.
2. Откройте вкладку **Зависимости**.
3. Щелкните **Ресурс** и выберите добавленный общий диск и **Сетевое имя** (это название точки доступа для клиентов).
4. Нажмите кнопку **Применить** и закройте окно.

Для службы « Кибер Файлы Tomcat» выполните следующие действия.

1. Щелкните по службе правой кнопкой и выберите **Свойства**.
2. Откройте вкладку **Зависимости**.
3. Щелкните **Ресурс** и выберите службы PostgreSQL и «Сервер шлюза Кибер Файлы» в качестве зависимостей. Нажмите кнопку **Применить** и закройте окно.

Примечание
Если сервер шлюза и сервер Кибер Файлы должны запускаться на разных IP-адресах, добавьте второй адрес в качестве ресурса к роли Кибер Файлы и определите его как зависимость для сетевого имени.

Запуск роли и использование программы настройки

1. Щелкните по роли Кибер Файлы правой кнопкой мыши и выберите **Запустить роль**.

2. Запустите программу настройки. На новой установке она обычно находится в каталоге C:\Program Files (x86)\Cyber Files\Common\Configuration Utility
3. Настройте службу «Сервер шлюза Кибер Файлы» для прослушивания IP-адресов для группы «Служба Кибер Файлы».
4. Настройте службу «Сервер Кибер Файлы» для прослушивания IP-адресов для группы «Служба Кибер Файлы».

   Примечание
   Если установлен флажок **Перенаправлять запросы с порта 80**,

5. Настройте репозиторий файлов Кибер Файлы для прослушивания на localhost и измените путь хранения файлов на общий диск. Этот путь должен быть одинаковым для обоих узлов.
6. Нажмите кнопку **OK**, чтобы завершить настройку и перезапустить службы.

Установка и конфигурация на втором узле

1. Отключите все антивирусное ПО на компьютере, иначе оно может прервать процедуру установки.
2. Установите Кибер Файлы на второй узел, но на этот раз указывайте стандартное расположение папки **Данные Postgres** и тот же пароль пользователя postgres, что и для первого узла.
3. Выполните установку.
4. Настройте расположение базы данных сервера шлюза на общем диске.
   a. Перейдите в папку C:\Program Files (x86)\Cyber Files\Gateway Server\
   b. Найдите файл **database.yml** и откройте его в текстовом редакторе.
   c. Найдите строку database_path: './database/' и замените **./database/** путем, который используется у вас (например, database_path: 'S:/access_cluster/database/').

      Примечание
      Используйте косую черту (/) в качестве разделителя пути.

      Примечание
      Можно скопировать настроенный файл database.yml с первого узла на второй.
      Этот путь должен соответствовать пути на первом узле.

Для PostgreSQL выполните следующие действия.

1. Откройте **Диспетчер отказоустойчивого кластера**.
2. Найдите и выберите ресурс PostgreSQL Generic Service.
3. Щелкните по ней правой кнопкой и выберите **Свойства**.

4. Откройте вкладку **Репликация реестра**.
5. Нажмите кнопку **Добавить** и введите следующий текст: SYSTEM\CurrentControlSet\Services\CyberAccessPostgreSQL\(для старых версий службы Кибер Файлы может отличаться, например **postgresql-x64-9.2**)
6. Перенесите роль Кибер Файлы на второй узел.

Использование программы настройки на втором узле

1. Щелкните по роли Кибер Файлы правой кнопкой мыши и выберите **Запустить роль**.
2. Запустите программу настройки. На новой установке она обычно находится в каталоге C:\Program Files (x86)\Cyber Files\Common\Configuration Utility
3. Настройте службу «Сервер шлюза Кибер Файлы» для прослушивания IP-адресов для группы «Служба Кибер Файлы».
4. Настройте службу «Сервер Кибер Файлы» для прослушивания IP-адресов для группы «Служба Кибер Файлы».

   Примечание
   Если установлен флажок **Перенаправлять запросы с порта 80**,

5. Настройте репозиторий файлов Кибер Файлы для прослушивания на localhost и измените путь хранения файлов на общий диск. Этот путь должен быть одинаковым для обоих узлов.
6. Нажмите кнопку **OK**, чтобы завершить настройку и перезапустить службы.

11.5.13 Настройка IPv6

Перед началом работы — известные ограничения

В настоящее время средство конфигурации не поддерживает IPv6 автоматически. После внесения вручную изменений в файл server.xml и привязки SSL вы больше не сможете использовать средство конфигурации, поскольку оно удаляет все изменения, которые не поддерживаются его интерфейсом. Все перезапуски службы и изменения конфигурации сервера нужно будет выполнять вручную, пока средство конфигурации не будет поддерживать IPv6.

Необходимые изменения, вручную внесенные в файлы server.xml и web.xml, не сохранятся при обновлении версии. Не забудьте создать резервную копию этих файлов в любом месте за пределами папки установки Кибер Файлы. После обновления необходимо будет сравнить отредактированный вручную файл с новым установленным файлом и перенести все необходимые изменения.

Все адреса, которые разрешаются в формат IPv6, должны быть указаны как DNS-адреса в веб-интерфейсе.

Примечание
Страница администрирования – функция ограничения доступа к странице администрирования требует диапазона IP-адресов, которым разрешен доступ к страницам администрирования. Текущий формат интерфейса поддерживает только IPv4.

Выполнение настройки IPv6

Для включения поддержки IPv6 необходимо выполнить три шага.

11.5.13.1 Шаг 1. Настройка шлюза для поддержки IPv6

Чтобы шлюз работал с IPv6, необходимо создать привязку SSL, а затем добавить нужные адреса в список iplisten.

Примечание
Для выполнения этого шага потребуется значение certhash отпечатка сертификата Киберпротект, нужный IP-адрес IPv6 и порт, который будет прослушивать шлюз. Как получить значение certhash см. в разделе Получение отпечатка сертификата Киберпротект.

Создайте привязку SSL

Можно создать привязку для всех адресов IPv6 или для определенного адреса IPv6.

Привязка ко всем адресам IPv6.

Команда должна иметь следующий вид:

netsh http add sslcert ipport=[::]:**YourPortNumber** certhash=**YourCerthashValue** appid={72876ec6-d443-48ef-add3-fa7a0cbc4762} certstorename=MY clientcertnegotiation=enable dsmapperusage=enable

Внимание
Необходимо ввести порт, который будет прослушивать шлюз, и заменить значение certhash значением из вашего сертификата.

Примечание
Чтобы создать привязку к *определенному* адресу IPv6, замените «**::**» нужным адресом.

Примечание
Если требуется удалить привязку SSL, используйте следующую команду, заменив адрес и порт теми, которые следует удалить:
netsh http delete sslcert ipport=[**AddressToRemove**]:**PortToRemove**

Добавьте нужный адрес IPv6 в список iplisten.

В список iplisten можно добавить либо все IP-адреса, либо определенный IP-адрес.

Добавление всех IP-адресов IPv6 в список iplisten.

1. Используйте следующую команду: netsh http add iplisten ipaddress=::

   Примечание
   Чтобы добавить *определенный* IP-адрес IPv6 в список iplisten, замените «**::**» нужным IP-адресом IPv6,
   например netsh http add iplisten ipaddress=fd59:ffdf:9580::3

2. Перезапустите службу шлюза из приложения «Службы» Windows.

Примечание
Теперь шлюз должен быть доступен как через локальный хост (::1), так и через любой IP-адрес. Если вы задали определенный IP-адрес IPv6, у вас не будет доступа к шлюзу через локальный хост, а только по указанному адресу.

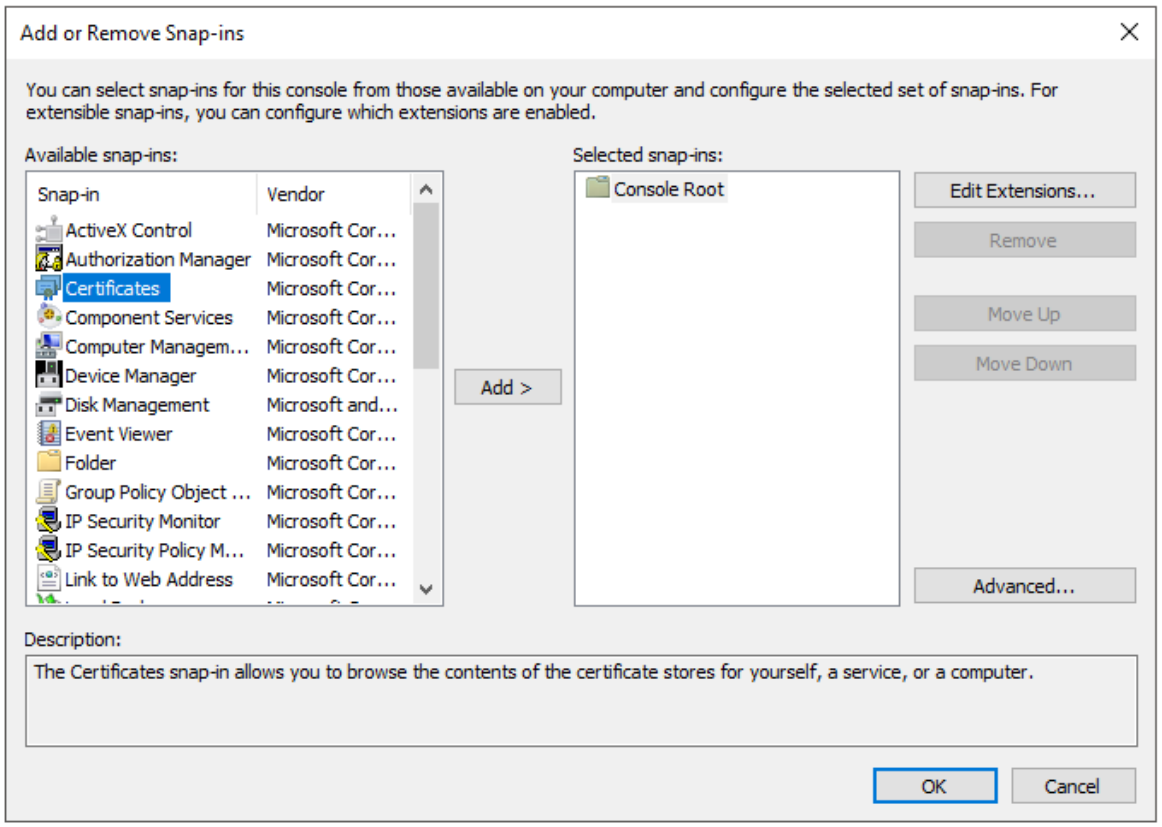
Предупреждение
Если вы хотите иметь доступ к шлюзу через локальный хост после настройки определенного IP-адреса, необходимо удалить этот адрес из списка iplisten с помощью следующей команды, а затем перезапустить службу шлюза из приложения «Службы» Windows.
Например: netsh http delete iplisten ipaddress=fd59:ffdf:9580::3

Как получить отпечаток сертификата Кибер Файлы

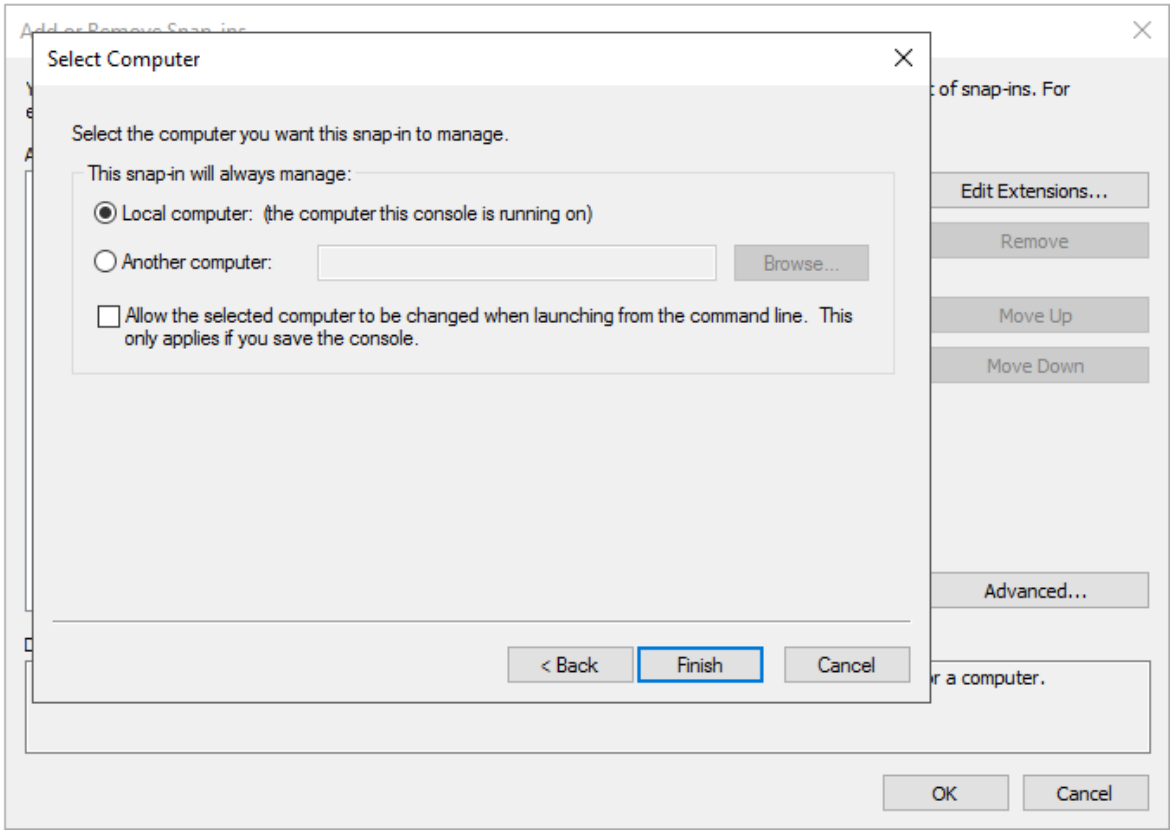
Есть два способа получить отпечаток сертификата Киберпротект. Первый способ – на вкладке сведений о сертификате в оснастке сертификатов. Второй – через командную строку с помощью уже настроенной привязки SSL.

Получение отпечатка сертификата из оснастки сертификатов

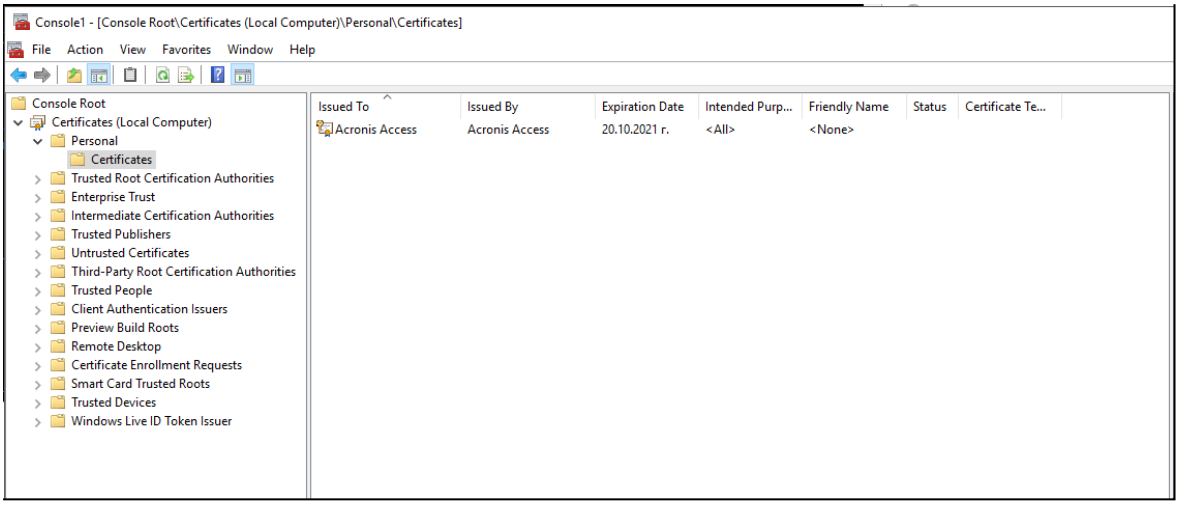
1. Откройте диалоговое окно **Выполнить** и введите mmc.exe, чтобы открыть **Консоль управления (MMC)**.
2. Нажмите **Файл -> Добавить или удалить оснастку...**
3. Выберите **Сертификаты**.



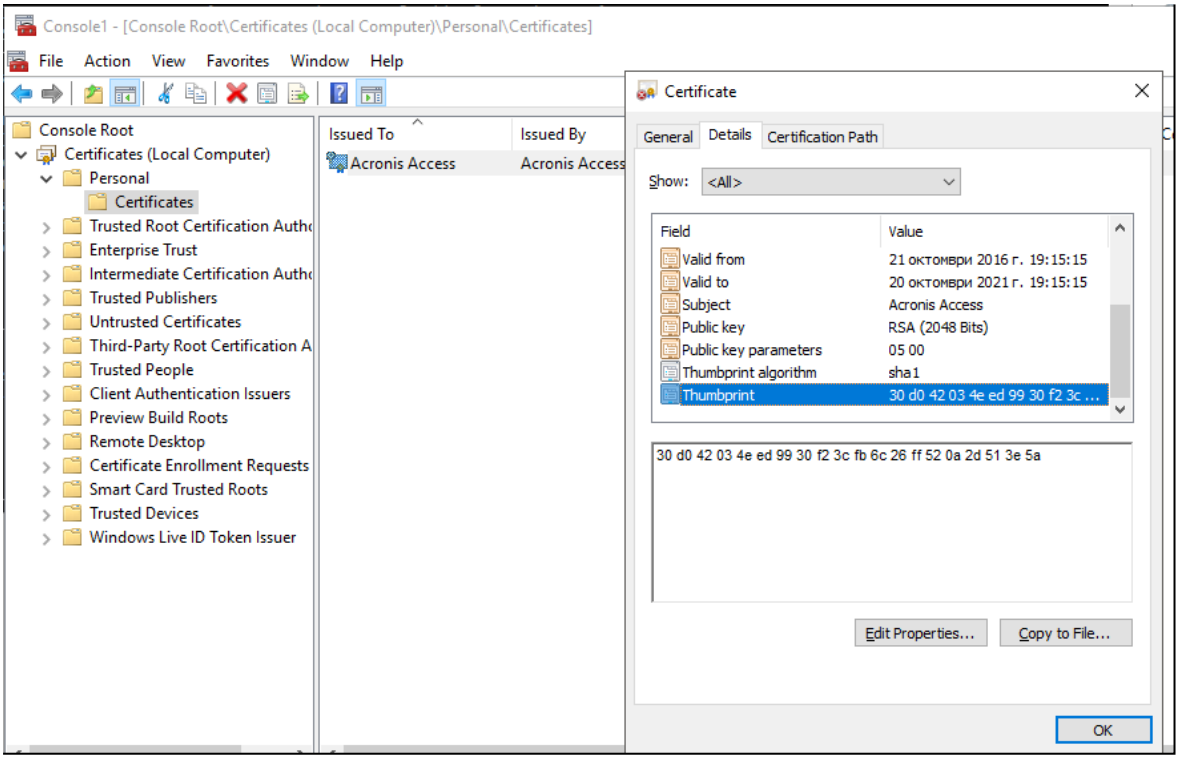
4. Нажмите **Добавить** в диалоговом окне.



5. Выберите **учетную запись компьютера**, нажмите «Далее», выберите локальный компьютер и нажмите «Готово»:
6. В диалоговом окне добавления и удаления оснасток нажмите **OK**.



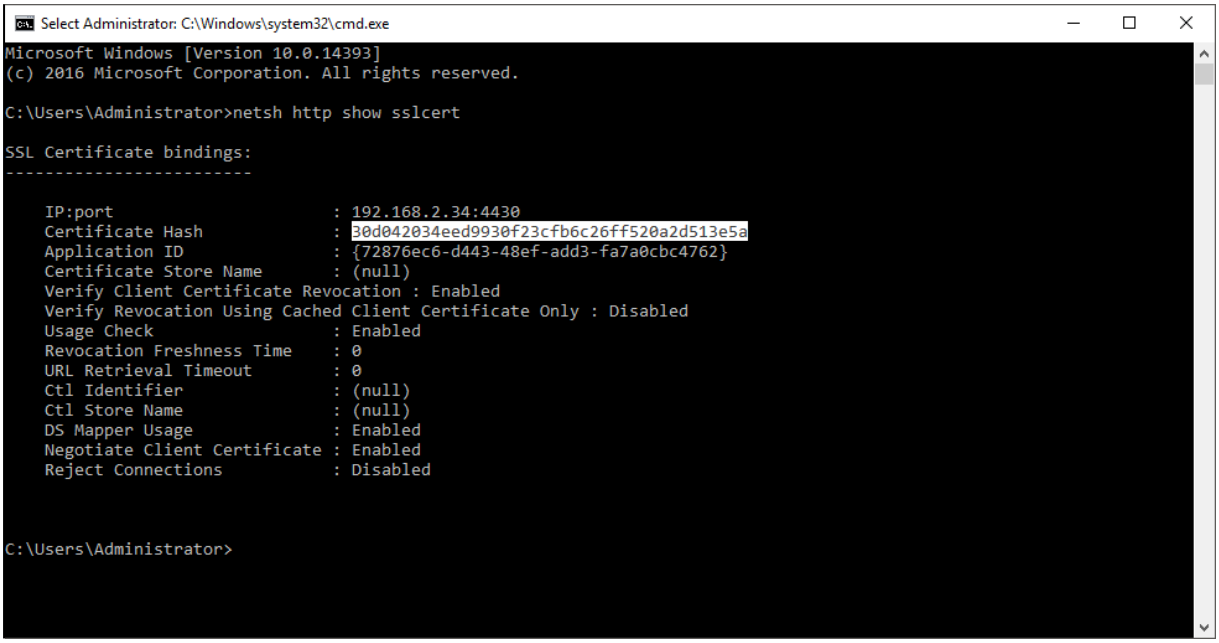
7. Разверните пункт «Сертификаты» слева, выберите «Личное -> Сертификаты», где должен отобразиться сертификат Киберпротект.



8. Дважды щелкните по сертификату, выберите вкладку **Состав** и прокрутите список до отпечатка.
9. Скопируйте его куда-нибудь и удалите пробелы. Для команды, создающей привязку SSL, потребуется значение без пробелов.

Получение отпечатка сертификата с помощью уже настроенной привязки SSL

1. Откройте командную строку.
2. Введите: netsh http show sslcert
3. Если привязка SSL существует, она отобразится.



.

Примечание
Выделенная строка – это нужный вам хеш сертификата.

11.5.13.2 Шаг 2. Настройка сервера Кибер Файлы для поддержки IPv6

Включение на сервере локального прослушивания всех адресов IPv6.

Внимание
Чтобы создать привязку к определенному адресу IPv6, см. примечание к шагу 4.

1. Найдите файл **server.xml**.

   Примечание
   По умолчанию этот файл находится в папке **C:\Program Files (x86)\Cyberprotect\Cyber Files\Common\apache-tomcat-9.0.54\conf**
   Число в имени папки (7.0.70) может быть другим в зависимости от версии Tomcat, и путь может отличаться, если вы обновляли версию или меняли параметры установки. Можно использовать запись **Киберпротект Кибер Файлы Tomcat** в приложении **Службы** Windows, чтобы определить путь к программной папке Tomcat, в которой содержится папка **conf** .

2. Сделайте резервную копию файла **server.xml**.
3. Откройте исходный файл **server.xml** в текстовом редакторе.

4. Добавьте дополнительный коннектор с адресом «::» для поддержки всех адресов IPv6.
   i. Найдите в файле **server.xml** часть, которая выглядит следующим образом:
   <Connector maxHttpHeaderSize="65536" maxThreads="150" enableLookups="false" disableUploadTimeout="true" acceptCount="100" scheme="https" secure="true" SSLEnabled="true" SSLProtocol="TLSv1+TLSv1.1+TLSv1.2" SSLCertificateFile="${catalina.base}/conf/AAServer_LocalHost.crt" SSLCertificateKeyFile="${catalina.base}/conf/AAServer_LocalHost.key" SSLHonorCipherOrder="true" SSLCipherSuite="ECDH+AESGCM:ECDH+AES256:ECDH+AES128:RSA+AESGCM:RSA+AES:!aNULL:!eNULL:!LOW:!3DES:!RC4:!MD5:!EXP:!PSK:!SRP:!DSS" connectionTimeout="-1" URIEncoding="UTF-8" bindOnInit="false" relaxedQueryChars="[,]" address="0.0.0.0" port="443"/>
   ii. Затем с новой строки рядом с существующим коннектором добавьте этот дополнительный коннектор с адресом «::»
   <Connector maxHttpHeaderSize="65536" maxThreads="150" enableLookups="false" disableUploadTimeout="true" acceptCount="100" scheme="https" secure="true" SSLEnabled="true" SSLProtocol="TLSv1+TLSv1.1+TLSv1.2" SSLCertificateFile="${catalina.base}/conf/AAServer_LocalHost.crt" SSLCertificateKeyFile="${catalina.base}/conf/AAServer_LocalHost.key" SSLHonorCipherOrder="true" SSLCipherSuite="ECDH+AESGCM:ECDH+AES256:ECDH+AES128:RSA+AESGCM:RSA+AES:!aNULL:!eNULL:!LOW:!3DES:!RC4:!MD5:!EXP:!PSK:!SRP:!DSS" connectionTimeout="-1" URIEncoding="UTF-8" bindOnInit="false" relaxedQueryChars="[,]" address="**::**" port="443"/>

   Примечание
   Вместо добавления всех адресов IPv6 (**::**) можно задать определенный адрес IPv6, заменив «**::**» нужным адресом в блоке коннекторов.
   Например:
   <Connector maxHttpHeaderSize="65536" maxThreads="150" enableLookups="false" disableUploadTimeout="true" acceptCount="100" scheme="https" secure="true" SSLEnabled="true" SSLProtocol="TLSv1+TLSv1.1+TLSv1.2" SSLCertificateFile="${catalina.base}/conf/AAServer_LocalHost.crt" SSLCertificateKeyFile="${catalina.base}/conf/AAServer_LocalHost.key" SSLHonorCipherOrder="true" SSLCipherSuite="ECDH+AESGCM:ECDH+AES256:ECDH+AES128:RSA+AESGCM:RSA+AES:!aNULL:!eNULL:!LOW:!3DES:!RC4:!MD5:!EXP:!PSK:!SRP:!DSS" connectionTimeout="-1" URIEncoding="UTF-8" bindOnInit="false" relaxedQueryChars="[,]" address="**fd59:ffdf:9580::3**" port="443"/>

5. Сохраните изменения и перезапустите службу Киберпротект Кибер Файлы Tomcat из оснастки «Службы» Windows.

Внимание
При любых изменениях файла **server.xml** требуется перезапуск службы Киберпротект Кибер Файлы Tomcat.

Предупреждение
Эти изменения, сделанные вручную, НЕ сохранятся при обновлении версии. Не забудьте создать резервную копию этих файлов в любом месте за пределами папки установки Киберпротект Кибер Файлы Server. После обновления необходимо будет вручную объединить различия между отредактированным и новым установленным файлом и перенести все необходимые изменения в файл **server.xml**.

11.5.13.3 Шаг 3. Настройка Strict Transport Security (HSTS) для поддержки IPv6

1. Найдите файл **web.xml**.

   Примечание
   По умолчанию файл **web.xml** расположен в папке **C:\Program Files (x86)\Cyberprotect\Cyber Files\Access Server\Web Application\WEB-INF**

2. Сделайте резервную копию файла **web.xml**.
3. Откройте исходный файл **web.xml** в текстовом редакторе и добавьте следующий блок.

```
<filter>
    <filter-name>httpHeaderSecurity</filter-name>
    <filter-class>org.apache.catalina.filters.HttpHeaderSecurityFilter</filter-class>
   <init-param>
      <param-name>hstsMaxAgeSeconds</param-name>
      <param-value>31536000</param-value>
   </init-param>
   <init-param>
      <param-name>hstsIncludeSubDomains</param-name>
      <param-value>true</param-value>
   </init-param>
</filter>
<filter-mapping>
   <filter-name>httpHeaderSecurity</filter-name>
   <url-pattern>/*</url-pattern>
   <dispatcher>REQUEST</dispatcher>
   <dispatcher>FORWARD</dispatcher>
</filter-mapping>
```

4. Сохраните изменения.
5. Перезапустите службу Киберпротект Кибер Файлы Tomcat из оснастки «Службы» Windows.

Примечание

Используя инструменты разработчика в браузере, вы должны видеть заголовок Strict-Transport-Security для всех запросов.

Предупреждение

Эти изменения, сделанные вручную, НЕ сохранятся при обновлении версии. Не забудьте создать резервную копию этого файла в любом месте за пределами папки установки Киберпротект Кибер Файлы Server. После обновления необходимо будет сравнить отредактированный вручную файл с новым установленным файлом и перенести все необходимые изменения в новый файл **web.xml**.