STRONGPASS.

Руководство администратора.

2023

Содержание

1. О продукте

Strongpass это инструмент проактивной защиты от использования слабых паролей. Проверка пароля производится в момент, когда пользователь или администратор пытается установить пароль. Если пароль по результатам проверок признается небезопасным, то пользователь или администратор не сможет установить новый пароль.

За счет проактивных проверок Strongpass позволяет минимальными средствами резко повысить сложность атаки на инфраструктуру компании и минимизировать риски проникновения с использованием слабых паролей пользователей.

Все проверки производятся локально на сервере, где установлен Strongpass. Доступ в Интернет не требуется ни при каких условиях.

Strongpass не заменяет настройки групповых политик Windows или Linux, устанавливающие требования к сложности пароля, а дополняет их и предназначен для совместной работы с ними.

Основные результаты, которые достигаются при использовании Strongpass:

– для атакующего резко повышается время подбора пароля. Особенно сильно это будет проявляться при онлайн атаках подбора пароля и при наличии средств защиты ограничивающих количество запросов в единицу времени (rate limit). В зависимости от целей атакующего данный вектор может быть признан бесперспективным и атака будет прекращена по инициативе самого атакующего;
– за счет повышенного количества событий неудачных аутентификаций у службы ИБ появляется дополнительное время и данные для обнаружения и блокировки атакующего.

Возможности

Интеграция с Windows, Linux

Контролируются все возможные варианты смены пароля:

– через графический интерфейс;
– через командную строку;
– через web-интерфейс ADFS (https://domain/update/password) или OWA

Проверяются все попытки смены пароля вне зависимости от того выполняет смену пароля системный администратор или пользователь.

Результаты проверок записываются в журнал сообщений.

Собственный список запрещенных паролей или комбинаций символов. Собственный список запрещенных паролей требуется, если необходимо дополнительно усилить парольную политику в компании. Наиболее часто в качестве частей пароля используется:

– название компании, где работает сотрудник;
– последовательные символы на клавиатуре (например qaz, zxcv и т.д.)
– числа по возрастанию или убыванию (например: 123, 12345 и т.д.)

Использование собственного списка позволяет гибко настроить парольную политику и запретить использование отдельных слов, комбинаций символов или цифр.

Исключения. Можно исключить из проверок отдельных пользователей.

Простое управление. Продукт требует минимальных усилий по администрированию. После установки продукт сразу готов к работе и не требует предварительных настроек.

Все дополнительные настройки хранятся в текстовых файлах. Текстовый формат позволяет легко автоматизировать внесение изменений и управление. Изменения настроек не требуют перезагрузки сервера и начинают действовать немедленно.

2. Лицензирование

Продукт лицензируется по количеству защищаемых пользователей.

Для продажи лицензии Производитель необходимо предоставить:

- количество защищаемых пользователей в домене;
- имя домена;
- название компании;
- адрес электронной почты;
- имя сотрудника, ответственного за покупку лицензии.

После оплаты файл лицензии высылается на указанный в адрес электронной почты.

Лицензионный файл нужно сохранить на всех серверах, где установлен продукт.

Linux

Сохраните файл по пути:

```
/opt/strongpass/config/strongpass.lic
```

Перезапустите службу командой `systemctl restart strongpass`.

В случае, если лицензионный файл поврежден или срок действия лицензии закончился, сообщения об ошибках можно будет увидеть в журнале приложения (См. раздел «Журналирование»).

Windows

Сохраните файл по пути:

```
%System32%\strongpass\config\strongpass.lic
```

В случае, если у вас была временная демонстрационная лицензия, просто перезапишите существующий файл. Изменения вступят в силу в течение нескольких часов. Перезагружать сервер не требуется.

В случае, если лицензионный файл поврежден или срок действия лицензии закончился, сообщения об ошибках можно будет увидеть в Windows Event log (см. раздел «Журналирование) или журнале приложения (Linux).

3. Системные требования

Strongpass предназначен для установки на серверах, работающих в качестве контроллеров домена.

3.1. Аппаратные требования

- Процессор: не менее 2x1.8ГГц.
- ОЗУ: не менее 1.5 Гб виртуальной памяти.
- Дисковое пространство: 1.5 Гб.

3.2. Поддерживаемые операционные системы

Поддерживаются только 64-х битные операционные системы из списка ниже.

Linux:

- Astra Linux Special Edition 1.7 с установленной системой для централизованного управления и автоматизации ALD Pro или службой каталогов FreeIPA;
- Альт Сервер 10 с установленной службой каталогов FreeIPA;
- РЕД ОС 7.3 с установленной службой каталогов FreeIPA;

Windows:

- Windows Server 2022 с установленными доменными службами Active Directory;
- Windows Server 2019 с установленными доменными службами Active Directory;
- Windows Server 2016 с установленными доменными службами Active Directory.

Поддержка остальных операционных систем - по запросу.

4. Установка

4.1. Linux

4.1.1. Архитектура

Strongpass для Linux состоит из двух компонентов:

– модуля интеграции с FreeIPA, ALD Pro;
– сервиса проверки паролей;

Развертывание продукта можно произвести в двух вариантах:
– **Вариант 1.** Размещение всех компонентов на одном сервере. Оба компонента устанавливаются на все контроллеры домена.
– **Вариант 2.** Размещение сервиса проверки паролей на выделенном сервере. На все контроллеры домена необходимо установить только модуль интеграции.

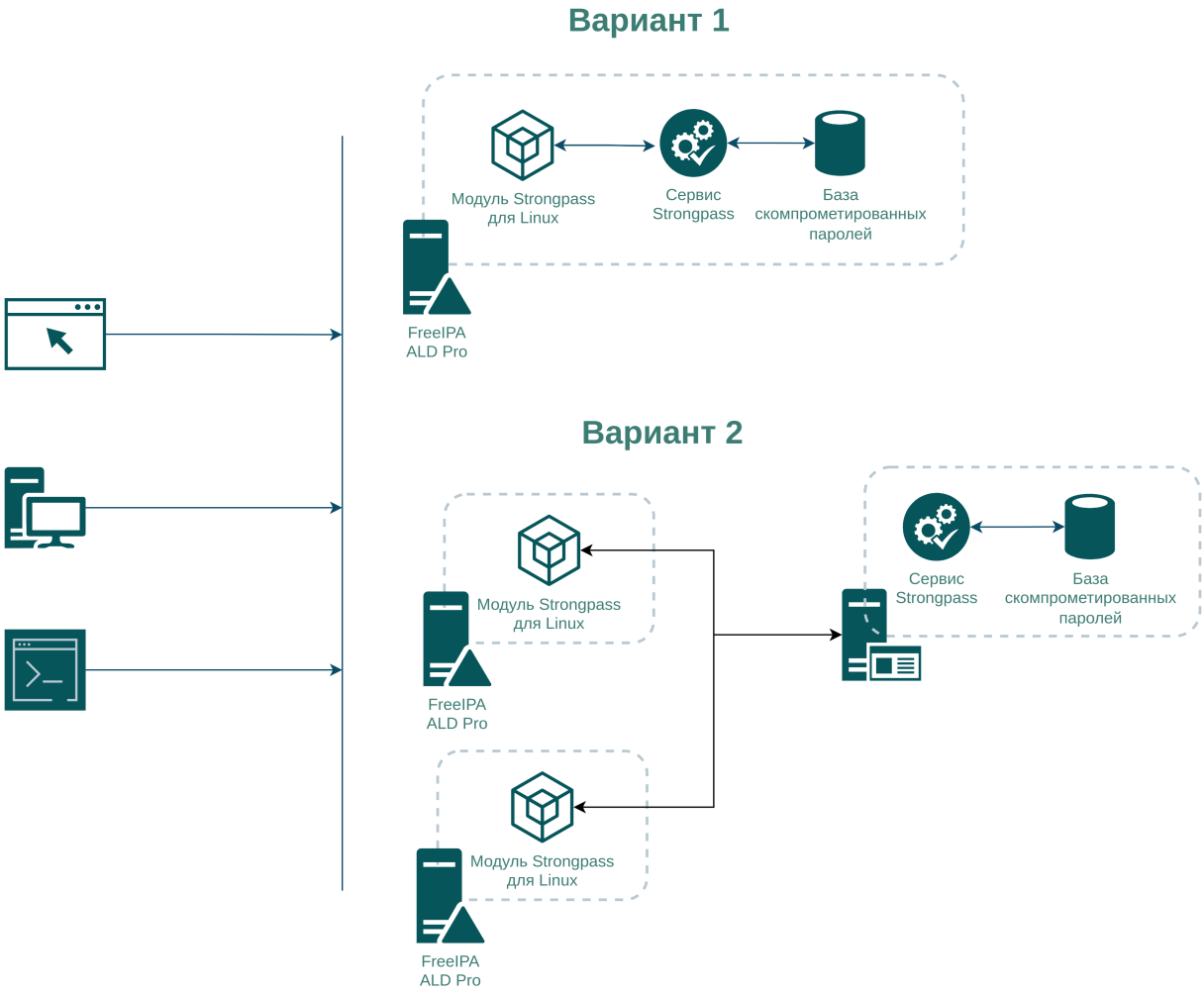

Рисунок 1: Варианты развертывания продукта

4.1.2. Подготовительные действия

Последнюю актуальную версию Strongpass можно скачать со страницы https://strongpass.ru/download/.

Перед установкой продукта необходимо запросить временную демонстрационную лицензию или купить постоянную лицензию. Без файла лицензии (временной или постоян-

ной) проверки паролей проводиться не будут. Сообщения об отсутствии лицензии можно увидеть в журнале сообщений Strongpass.

4.1.3. Вариант 1. Все компоненты на одном сервере

4.1.3.1. Загрузка файлов на сервера.

Все компоненты должны быть установлены на всех контроллерах домена.

1. Загрузите во временный каталог на **все** контроллеры домена файл `strongpass.tar.gz`
2. Распакуйте файл

```
tar -xzf strongpass.tar.gz
```

3. Распакуйте файл `strongpass-integration-module.tar.gz` в каталог `/opt/strongpass` командами:

```
mkdir -p /opt/strongpass
tar xzf strongpass-integration-module.tar.gz -C /opt/strongpass
```

5. Распакуйте файл `strongpass-service.tar.gz` в каталог `/opt/strongpass` командами:

```
mkdir -p /opt/strongpass
tar xzf strongpass-service.tar.gz -C /opt/strongpass
```

4.1.3.2. Настройка и запуск сервиса

1. При необходимости отредактируйте конфигурационный файл `/opt/strongpass/config/config.yml`. Конфигурационный файл позволяет установить настройки журналирования, адрес и порт на котором будет работать сервис.
2. Скопируйте файл лицензий. Файл лицензий должен располагаться по пути `/opt/strongpass/config/strongpass.lic`
3. Скопируйте файл сервиса systemd:

```
cp /opt/strongpass/install/strongpass.service /etc/systemd/system
```

4. Активируйте и запустите сервис

```
systemctl enable strongpass
systemctl start strongpass
```

5. Проверьте состояние сервиса.

```
systemctl status strongpass
```

6. Проверьте журнал сообщений сервиса на наличие сообщений об ошибках. По умолчанию сообщения записываются в файл `/var/log/strongpass/strongpass.log`

В случае ошибок для диагностики выполните команды ниже и проанализируйте сообщения на предмет причин ошибок. В случае отсутствия ошибок считается, что сервис запустился успешно.

```
journalctl -u strongpass -n 100
cat /var/log/strongpass/strongpass.log
```

4.1.3.3. Добавление модуля интеграции в FreeIPA/ALD Pro

Данную процедуру необходимо выполнить на всех контроллерах домена.

1. Добавьте модули интеграции в FreeIPA/ALD Pro с помощью двух команд. При выполнении команд необходимо будет ввести пароль администратора домена.

```
ldapmodify -h localhost -p 389 -a -D cn="Directory Manager" -W -f /opt/
strongpass/install/config_preop.ldif
ldapmodify -h localhost -p 389 -a -D cn="Directory Manager" -W -f /opt/
strongpass/install/config_preextop.ldif
```

При успешном добавлении модулей вы получите сообщения:

```
adding new entry "cn=strongpass_preop,cn=plugins,cn=config"
adding new entry "cn=strongpass_preextop,cn=plugins,cn=config"
```

2. Установите права на каталог журнала сообщений.

Модуль интеграции запускается под учетной записью LDAP сервера, поэтому используется учетная запись и группа `dirsrv`.

```
mkdir -p /var/log/strongpass
chown dirsrv:dirsrv -R /var/log/strongpass
```

3. Перезапустите службу LDAP сервера. `[ваш_домен]` - ваш домен.

```
systemctl restart dirsrv@[ваш_домен].service
```

4. Проверьте статус сервера.

```
systemctl status dirsrv@[ваш_домен]
```

5. Проверьте наличие ошибок и сообщений в журнале LDAP сервера.

```
grep -P '(WARN|ERR|INF).*strongpass__plugin' /var/log/dirsrv/slapd-[ваш-
домен]/errors
```

В случае успешного запуска модуля интеграции в журнале LDAP сервера вы увидете сообщения:

```
```

```
strongpass__preexop плагин успешно запущен.
strongpass__preop плагин успешно запущен.
```

6. Проверьте наличие ошибок и сообщений в журнале сообщений Strongpass.

Полный путь до журнала сообщений указан в файле `/opt/strongpass/config/config.yml`. По умолчанию файл журнала Strongpass располагается по пути `/var/log/strongpass/strongpass.log`.

При успешном запуске модулей интеграции в журнале Strongpass будет два сообщения:

```
strongpass__preexop плагин успешно запущен.
strongpass__preop плагин успешно запущен.
```

Установка Strongpass для Linux завершена. Продукт готов к работе.

4.1.4. Вариант 2. Сервис проверки на выделенном сервере

На своем компьютере распакуйте файл, скачанный с сайта

```
tar -xzf strongpass.tar.gz
```

4.1.4.1. Установка и запуск сервиса

1. Подготовьте сервер для установки сервиса.
2. Загрузите файл `strongpass-service.tar.gz` на подготовленный сервер.
3. Распакуйте файл `strongpass-service.tar.gz` в каталог `/opt/strongpass` командами:

```
mkdir -p /opt/strongpass
tar xzf strongpass-service.tar.gz -C /opt/strongpass
```

4. Отредактируйте конфигурационный файл `/opt/strongpass/config/config.yml`. Конфигурационный файл позволяет установить настройки журналирования, адрес и порт на котором будет работать сервис. Укажите IP-адрес и порт, на которых будет работать сервис.
5. Скопируйте файл лицензий. Файл лицензий должен располагаться по пути `/opt/strongpass/config/strongpass.lic`
6. Скопируйте файл сервиса systemd:

```
cp /opt/strongpass/install/strongpass.service /etc/systemd/system
```

7. Активируйте и запустите сервис

```
systemctl enable strongpass
systemctl start strongpass
```

8. Проверьте состояние сервиса.

```
systemctl status strongpass
```

9. Проверьте журнал сообщений сервиса на наличие сообщений об ошибках. По умолчанию сообщения записываются в файл `/var/log/strongpass/strongpass.log`

В случае ошибок для диагностики выполните команды ниже и проанализируйте сообщения на предмет причин ошибок. В случае отсутствия ошибок считается, что сервис запустился успешно.

```
journalctl -u strongpass -n 100
cat /var/log/strongpass/strongpass.log
```

4.1.4.2. Загрузка и настройка модуля интеграции

Модуль интеграции необходимо установить на всех контроллерах домена.

1. Загрузите на **все** контроллеры домена файл `strongpass-integration-module.tar.gz`
2. Распакуйте файл `strongpass-integration-module.tar.gz` в каталог `/opt/strongpass` командами:

```
mkdir -p /opt/strongpass
tar xzf strongpass-integration-module.tar.gz -C /opt/strongpass
```

Стандартный конфигурационный файл для модуля выглядит следующим образом:

```
bypass_errors: false
log:
  file: /var/log/strongpass/strongpass.log
  level: info
service:
  address: 127.0.0.1
  port: 9876
```

В конфигурационном файле укажите IP-адрес сервера, на котором запущен сервис, и порт, на котором слушает сервис.

4.1.4.3. Добавление модуля интеграции в FreeIPA/ALD Pro

Данную процедуру необходимо выполнить на всех контроллерах домена.

1. Добавьте модули интеграции в FreeIPA/ALD Pro с помощью двух команд. При выполнении команд необходимо будет ввести пароль администратора домена.

```
ldapmodify -h localhost -p 389 -a -D cn="Directory Manager" -W -f /opt/
strongpass/install/config_preop.ldif
ldapmodify -h localhost -p 389 -a -D cn="Directory Manager" -W -f /opt/
strongpass/install/config_preextop.ldif
```

При успешном добавлении модулей вы получите сообщения:

```
adding new entry "cn=strongpass_preop,cn=plugins,cn=config"
adding new entry "cn=strongpass_preextop,cn=plugins,cn=config"
```

2. Установите права на каталог журнала сообщений.

Модуль интеграции запускается под учетной записью LDAP сервера, поэтому используется учетная запись и группа dirsrv.

```
mkdir -p /var/log/strongpass
chown dirsrv:dirsrv -R /var/log/strongpass
```

3. Перезапустите службу LDAP сервера. `[ваш_домен]` - ваш домен.

```
systemctl restart dirsrv@[ваш_домен].service
```

4. Проверьте статус сервера.

```
systemctl status dirsrv@[ваш_домен]
```

5. Проверьте наличие ошибок и сообщений в журнале LDAP сервера.

```
grep -P '(WARN|ERR|INF).\*strongpass__plugin' /var/log/dirsrv/slapd-[ваш-
домен]/errors
```

В случае успешного запуска модуля интеграции в журнале LDAP сервера вы увидете сообщения:

```
strongpass__preexop плагин успешно запущен.
strongpass__preop плагин успешно запущен.
```

6. Проверьте наличие ошибок и сообщений в журнале сообщений Strongpass.

Полный путь до журнала сообщений указан в файле `/opt/strongpass/config/config.yml`. По умолчанию файл журнала Strongpass располагается по пути `/var/log/strongpass/strongpass.log`.

При успешном запуске модулей интеграции в журнале Strongpass будет два сообщения:

```
strongpass__preexop плагин успешно запущен.
strongpass__preop плагин успешно запущен.
```

Установка Strongpass для Linux завершена. Продукт готов к работе.

4.2. Windows

Последнюю актуальную версию Strongpass можно скачать со страницы https://strongpass.ru/download/.

Перед установкой продукта необходимо запросить временную демонстрационную лицензию или купить постоянную лицензию. Без файла лицензии (временной или постоянной) проверки паролей проводиться не будут. Сообщения об отсутствии лицензии можно увидеть в Windows Event Log.

Продукт необходимо установить на все контроллеры домена, кроме read-only контроллеров.

После установки продукта необходимо на всех серверах, где он установлен:

1. Сохранить лицензионный файл. Путь для сохранения файла:

```
%System32%\strongpass\config\strongpass.lic
```

обычно это путь

```
C:\Windows\System32\strongpass\config\strongpass.lic
```

2. Перезагрузить сервер

Только после перезагрузки сервера начнутся проверки паролей.

5. Последовательность проверок

При попытке смены пароля проверки производятся в следующем порядке.

1. Пользователь находится в файле исключений пользователей (логин пользователя указан в файле excluded-users.txt)? Если ДА, то смена пароля разрешается вне зависимости от того какой пароль использовался.
2. Пароль указан в списке разрешенных паролей (файл excluded-passwords.txt)? Если ДА, то смена пароля разрешается.
3. Производится поиск по базе паролей из публичных утечек. Если пароль найден в базе, то смена пароля запрещается.
4. Производится проверка по списку запрещенных паролей из файла wordlist.txt. Если пароль или часть пароля присутствуют в списке, то смена пароля запрещается.

Если все проверки были успешно пройдены, то пароль считается надежным и смена пароля разрешается.

6. Режимы работы

Strongpass может работать в двух режимах:

– нормальный режим;
– режим тестирования.

Режим тестирования отличается от нормального тем, что реальной блокировки попытки смены пароля (если пароль признан скомпрометированным или слабым) не происходит. При этом:

– производятся все проверки;
– отправляются сообщения в журнал сообщений (в Windows запись производится в Windows Event Log) о результатах проверки или ошибках;

Режим тестирования позволяет безопасно проверить как внедрение Strongpass или изменения в настройках повлияют на пользователей, оценить насколько часто пользователи используют слабые пароли в организации.

Включение и выключение режима тестирования не требует перезагрузки сервера.

6.1.1.1. Как включить режим тестирования.

Создайте на каждом сервере, где установлен Strongpass, файл:

в Linux:

```
/opt/strongpass/config/demo.mode
```

в Windows:

```
C:\Windows\System32\strongpass\config\demo.mode
```

Все последующие проверки смены пароля будут проходить в режиме тестирования.

6.1.1.2. Как выключить режим тестирования.

Удалите на каждом сервере, где установлен Strongpass, файл:

в Linux:

```
/opt/strongpass/config/demo.mode
```

в Windows:

```
C:\Windows\System32\strongpass\config\demo.mode
```

Все последующие проверки смены пароля будут проходить в нормальном режиме.

7. Настройка

7.1. Конфигурационный файл

Только для редакции работающей в ОС Linux.

Стандартный конфигурационный файл выглядит следующим образом:

```
bypass_errors: false
log:
  file: /var/log/strongpass/strongpass.log
  level: info
service:
  address: 127.0.0.1
  port: 9876
```

Назначение параметров конфигурационного файла.

Параметр	Тип	Комментарии
bypass_errors	Булевый	Возможные значения: `false`, `true`. Определяет логику работы модуля интеграции при наличии ошибок со стороны сервиса Strongpass. При значении `false` - в случае ошибок (например, сервис недоступен) модуль интеграции запретит смену пароля, т.к. проверка не была произведена. При значении `true` - разрешит смену пароля, даже если проверка не была произведена.
log	Словарь	Определяет параметры журналирования
file	Строка	Полный путь до файла журнала
level	Строка	Уровень детализации журналирования. Возможные значения: `error`, `warn`, `info`, `debug`
service	Словарь	Определяет параметры сервиса.
address	IP адрес	Для модуля интеграции указывает на какой IP адрес отправлять запросы на проверку пароля. Для сервиса - на каком IP адресе работать.
port	Число	Для модуля интеграции указывает на какой порт отправлять запросы на проверку пароля. Для сервиса - на каком порту ожидать запросы.

7.2. Дополнительные списки паролей

Дополнительные списки паролей необходимы для того, чтобы точнее настроить парольную политику с учетом особенностей конкретной компании.

Все изменения не требуют перезагрузки и начинают действовать немедленно.

7.2.1. Запрещенные пароли, слова, последовательности символов

Для создания индивидуального списка запрещенных паролей и/или частей паролей создайте текстовый файл в кодировке UTF-8 без BOM-маркеров.

Linux:

```
/opt/strongpass/config/wordlist.txt
```

Windows:

```
%System32%\strongpass\config\wordlist.txt
```

Укажите в файле запрещенные пароли или запрещенные части паролей по одному паролю или части пароля в строке.

Пример файла `wordlist.txt`:

```
#комментарий. Комментарии начинаются с символа "#"
"qaz"
"wsx"
"123"
companyname
october
```

7.2.2. Особенности проверок

Все проверки производится без учета регистра. В зависимости от того как указаны слова, наборы символов в файле возможны два варианта проверки пароля.

7.2.2.1. Точный поиск подстроки.

Если слово или набор символов заключены в двойные кавычки (например «qaz»), то производится только точный поиск подстроки в пароле.

Например:

- пароль `QaZzxc345023!` будет признан небезопасным, т.к. содержит запрещенную подстроку `qaz` из примера выше;
- пароль `Q1Zzxc345023!` будет признан безопасным, т.к. не содержит запрещенную подстроку `qaz`

Такой поиск позволяет запретить использование в пароле последовательности букв, символов, совпадающих с соседними клавишами на клавиатуре, таких как `qaz`, `qwerty` и т.д. Так же это позволяет запретить использование последовательных цифр: `123`, `1234`, `456` и т.д.

7.2.2.2. Нечеткий поиск

Если вы хотите дополнительно усилить требования к паролям, то укажите слово, последовательность символов без кавычек.

В этом случае производится поиск:

- подстроки
- обратной подстроки
- подстроки с учетом до трех замен символов включительно.

Например, если вы указали в списке запрещенных паролей слово `company`, тогда при проверках пароли содержащие подстроки ниже, будет признаны небезопасными:

```
COMPANY (регистр не учитывается)
CoMpAnY (регистр не учитывается)
company99! (подстрока)
упарmос! (обратная подстрока)
compani (замена одной буквы)
C0mpany (замена одной буквы)
c0mp4ny (замена двух букв)
1com2pany3 (изменение трех букв)
yn@pm0c! (обратная подстрока и изменение трех букв)
```

7.3. Разрешенные пароли

Для разрешенных паролей создайте текстовый файл в кодировке UTF-8 без BOM-маркеров. Укажите пароли, которые вы считаете безопасными по одному паролю в строке.

Linux:

```
/opt/strongpass/config/excluded-passwords.txt
```

Windows:

```
%System32%\strongpass\config\excluded-passwords.txt
```

Важно! В отличие от списка запрещенных паролей, пароли в файле `excluded-passwords.txt` проверяются по точному совпадению без учета регистра.

Например, если вы указали в файле пароль `qazxcv` то именно такой пароль без учета символа будет считаться разрешенным. Пароль `qazxcv123` будет признан небезопасным, так как находится в базе паролей из публичных утечек, хотя и содержит в себе подстроку из списка разрешенных паролей.

7.4. Исключение отдельных пользователей из проверок

Strongpass позволяет исключать из проверок конкретных пользователей. Все изменения настроек не требуют перезагрузки и начинают действовать немедленно.

Для исключения отдельных пользователей из проверок создайте текстовый файл в кодировке UTF-8 без BOM-маркеров. Укажите в файле имена доменных пользователей (аттрибут `sAMAccountName` или `uid` в Linux) по одному имени в строке.

Linux:

```
/opt/strongpass/config/excluded-users.txt
```

Windows:

```
%System32%\strongpass\config\excluded-users.txt
```

Пример файла `excluded-users.txt`:

```
ivan-ivanov
user11
user
```

Для пользователей, перечисленных в файле, проверка паролей не будет производиться.

8. Журналирование

8.1. Linux

По умолчанию файл журнала расположен по пути `/var/log/strongpass.log` и может быть изменен в конфигурационном файле.

В журнал записываются:

- результаты проверки пароля (разрешена ли смена пароля или попытка заблокирована);
- ошибки связанные с лицензией (окончание срока действия лицензии, повреждение или отсутствие файла лицензии);
- другие ошибки и сообщения, связанные с работой приложения.

Для изменения уровня журналирования см. Раздел 7.1

8.2. Windows

Strongpass отправляет сообщения об ошибках и результатах проверки в Windows Event Log

Сообщения от Strongpass можно посмотреть через стандартный Event Viewer в разделе `Windows Logs -> Application`. При фильтрации сообщений указать в поле `Event sources` значение `Strongpass`.

В Windows Event Log записываются:

- результаты проверки пароля (разрешена ли смена пароля или попытка заблокирована).
- ошибки связанные с лицензией (окончание срока действия лицензии, повреждение или отсутствие файла лицензии).

Из командной строки журнал сообщений можно посмотреть командой:

```
wevtutil qe Application "/q:\*[System [Provider[@Name='StrongPass']]]" /
f:text /uni:true
```

Сохранить сообщения в текстовый файл:

```
wevtutil qe Application "/q:\*[System [Provider[@Name='StrongPass']]]" /
f:text /uni:true > strongpass.log
```

Файл будет сохранен в кодировке UTF-16LE с BOM-маркером.