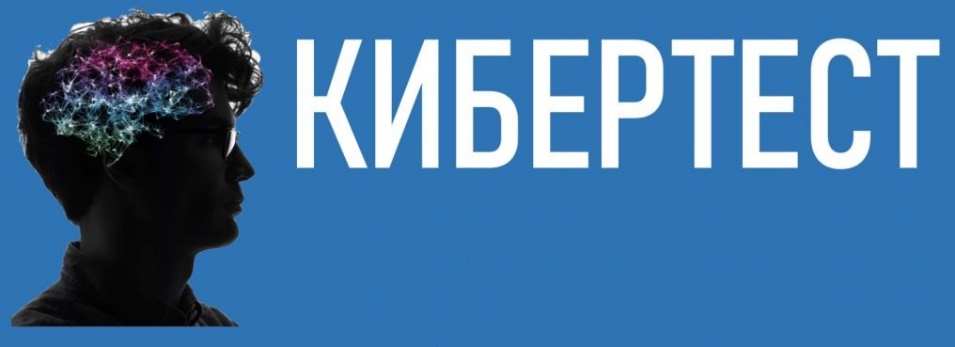
Общество с ограниченной ответственностью

КИБЕРТЕСТ

**ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ**

**«СЕРВИС ПОИСКА ДУБЛИКАТОВ ПАРОЛЕЙ ЛОКАЛЬНЫХ ПОЛЬЗОВАТЕЛЕЙ»**

**ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ**

**Листов 20**

**2023 год**

**АННОТАЦИЯ**

Настоящий документ содержит описание действий Пользователя программного обеспечения «Сервис поиска дубликатов паролей локальных пользователей».

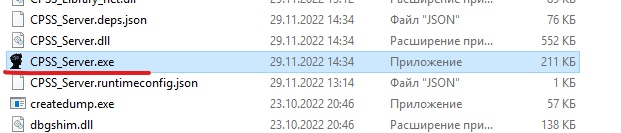
**СОДЕРЖАНИЕ**

|  |  |
| --- | --- |
| **1 1 Первый запуск программы………………………………………………………….** | **4** |
| **1 2 Раздел «Настройки сервера»……………………………………………………….** | **5** |
| **1 3 Настройка HTTPS, подключение сертификата…………………………………** | **6** |
| **1 4 Экспорт отчета………………………………………………………………………….** | **8** |
| **1 5 Ключ программы……………………………………………………………………….** | **10** |
| **1 6 Автоматизация процессов…………………………………………………………..** | **10** |
| **1 7 Раздел «Пользователи»……………………………………………………………...** | **12** |
| **1 8 Раздел «Анализ»……………………………………………………………………….** | **13** |
| **1 9 Раздел «База паролей»……………………………………………………………….** | **14** |
| **1 10 Работа программы, Анализ………………………………………………………..** | **14** |
| **1 11 Раздел «Проверка»…………………………………………………………………..** | **17** |
| **1 12 Раздел «Импорт базы»……………………………………………………………...** | **18** |
| **1 13 Файл с настройками…………………………………………………………………** | **19** |
| **1 14 Список сокращений и обозначений……………………………………………...** | **19** |

**1 Работа с интерфейсом**

**1 1 Первый запуск программы**

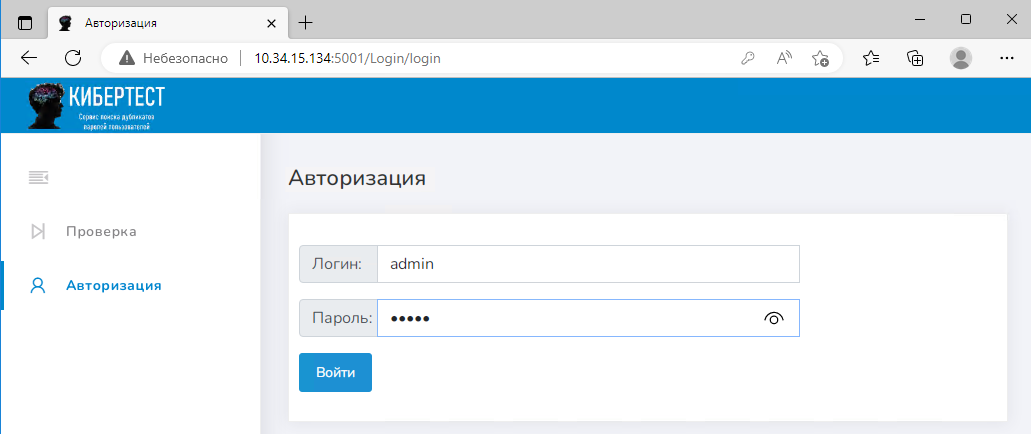
После установки программа должна запуститься автоматически. Если этого не произошло, необходимо запустить ее вручную.



*Рис. 1. Запуск программы вручную*

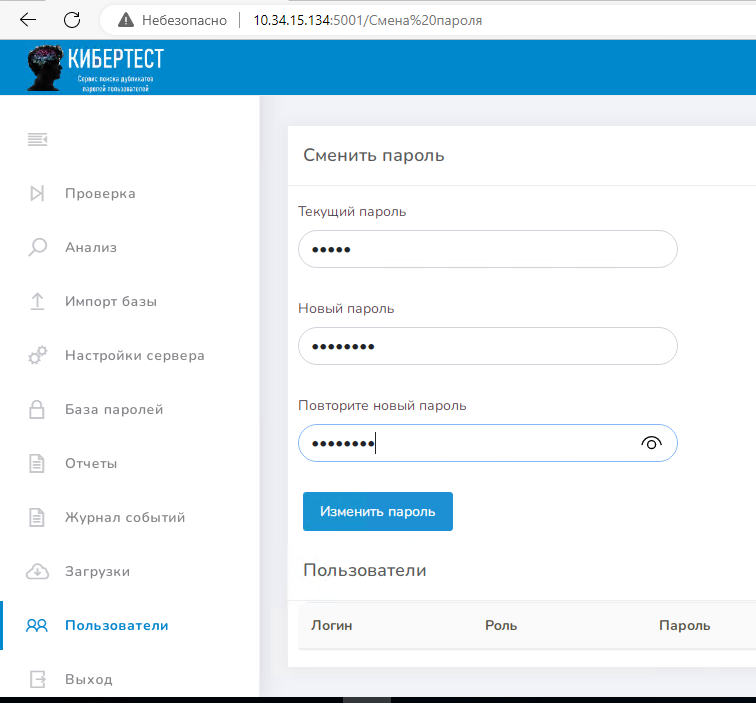
Далее необходимо открыть браузер и перейти по ip-адресу сервера через порт *5001 – localhost:5001*. Так же доступно подключение по сети: *AA.BB.CC.DD:5001*, где вместо *AA.BB.CC.DD* необходимо указать адрес целевого сервера, на котором были распакованы файлы программы.

Далее необходимо выполнить вход под начальными данными: логин *admin*, пароль *admin*.



*Рис. 2. Вход под начальными данными*

Далее необходимо сменить пароль для входа в систему



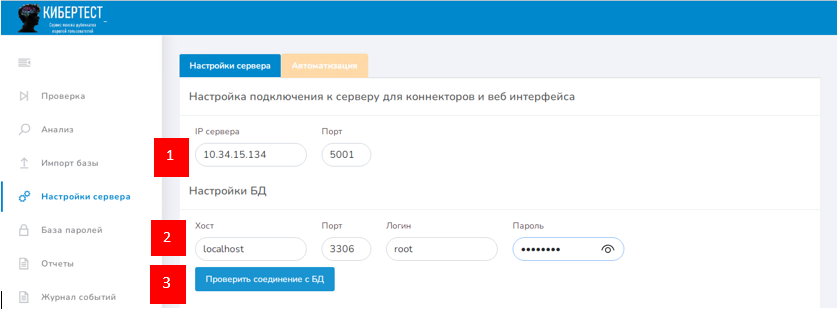
*Рис. 3. Смена пароль для входа в систему*

**1 2 Раздел «Настройки сервера»**

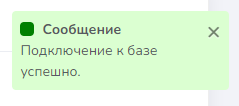
1. IP сервера – необходимо задать адрес, откуда будет запускаться само серверное приложение CPSS. Чаще всего адрес совпадает с адресом web-сервера, но это зависит от разделения установки. По умолчанию они идут вместе.

Этот параметр очень важный, так как его данные будут помещены в выгружаемый файл конфигурации *Connector.cfg*, который используется для коннектора. При изменении данного параметра, файл конфигурации для коннектора необходимо выгружать повторно.

1. Указать хост, порт, логин и пароль для подключения к *MariaDB*.
2. Нажать «Проверить соединение с БД».



*Рис. 4. Настройки вкладки «Настройка сервера»*

В случае успешной проверке появляется сообщение 

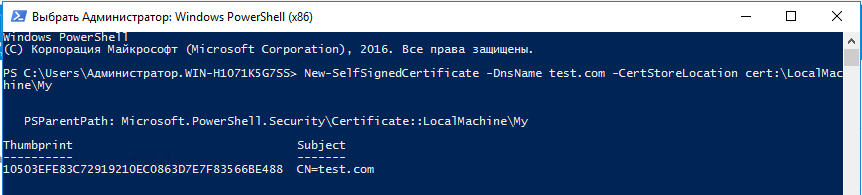
**1 3 Настройка HTTPS, подключение сертификата**

Существует возможность настроить доступ по защищенному протоколу HTTPS. Для этого необходимо разместить сертификат с расширением *\*.pfx* в корне файлов программы, а в самой программе в поле «Настройка HTTPS» указать его наименование полностью с расширением *«Cert\_For\_CPSS.pfx»* и пароль. Далее – перезагрузить программу. Соответственно, после этих действий доступ будет осуществляться по защищенному протоколу *https://AA.BB.CC.DD.*

Далее эти настройки представлены подробнее.

Для создания сертификата необходимо запустить PowerShell от имени администратора. Чтобы создать новый SSL сертификат типа *SSLServerAuthentication* (по умолчанию), например, для DNS имени *test.com* и поместить его в список персональных сертификатов компьютера, необходимо выполнить команду:

*New-SelfSignedCertificate -DnsName test.contoso.com -CertStoreLocation cert:\LocalMachine\My*



*Рис. 5. Выполнение команды*

Для экспорта полученного сертификата c закрытым ключом в \*.pfx-файл нужно указать пароль защиты сертификата и преобразовать его в [формат SecureString](https://winitpro.ru/index.php/2018/10/18/shifrovanie-paroley-v-skriptah-powershell/). Ввести следующую команду, а вместо *“YourPassword”* указать ваш пароль.

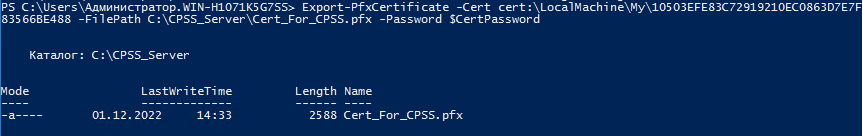
*$CertPassword = ConvertTo-SecureString -String “YourPassword” -Force –AsPlainText*



*Рис. 6. Ввод команды*

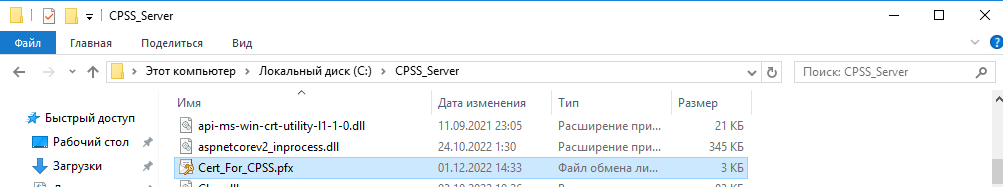
Далее для экспорта полученного сертификата c закрытым ключом в *pfx*-файл необходимо указать ранее полученный сертификат (значение *Thumbprint* нужно скопировать из результатов выполнения команды *New-SelfSignedCertificate*). Также необходимо указать путь и наименование создаваемого *pfx* файла (в примере это *C:\CPSS\_Server\Cert\_For\_CPSS.pfx*).

*Export-PfxCertificate -Cert cert:\LocalMachine\My\2779C0490D558B31AAA0CEF2F6EB1A5C2CA83B30 -FilePath C:\CPSS\_Server\Cert\_For\_CPSS.pfx -Password $CertPassword*



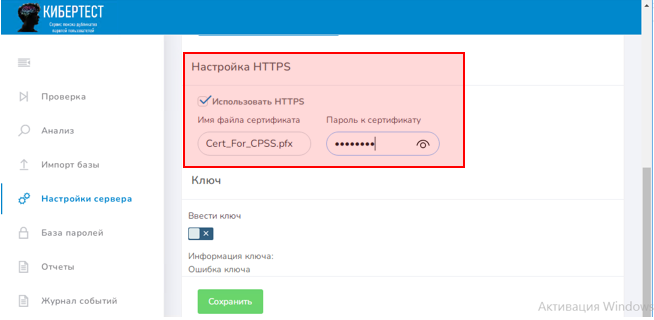
*Рис. 7. Результат ввода команды*

После выполнения всех вышеуказанных действий необходимый сертификат *Cert\_For\_CPSS.pfx* появится в корневом каталоге программы *C:\CPSS\_Server.*



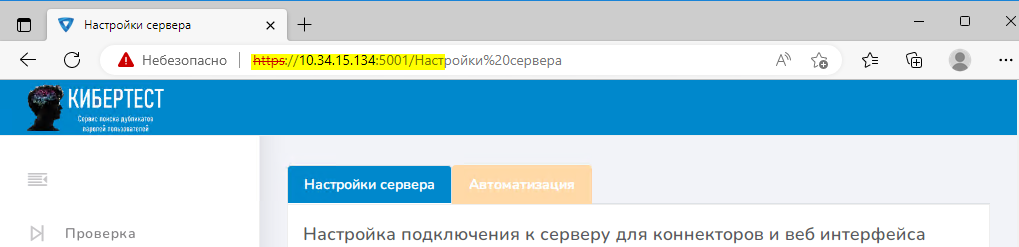
*Рис. 8. Расположение сертификата*

Теперь для установки полученного сертификата необходимо установить галочку на пункте «Использовать HTTPS». В поле «Имя файла сертификата» необходимо указать имя сертификата полностью, включая расширение. В поле «Пароль к сертификату» необходимо ввести пароль, который был указан при его получении. После чего нажать «Сохранить».



*Рис. 9. Настройки для установки сертификата*

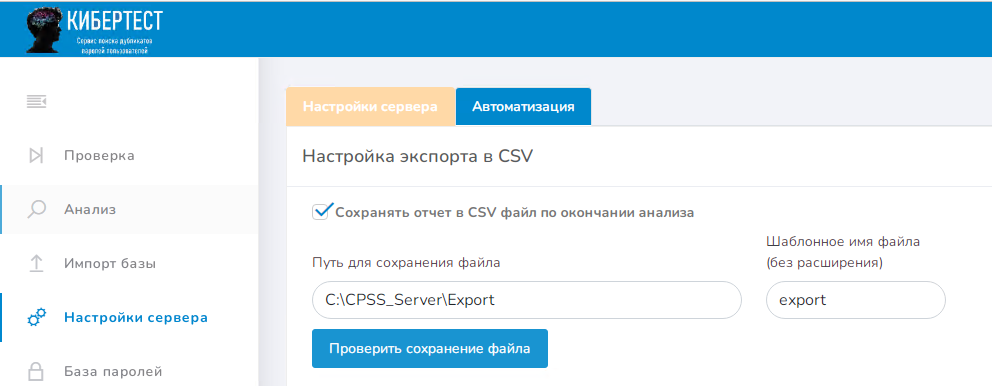
Для применения настроек HTTPS необходимо перезапустить программу в диспетчере задач. После чего осуществить подключение к ней по протоколу HTTPS *https://AA.BB.CC.DD:5001*.



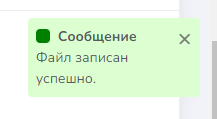
*Рис. 10. Подключение к программе.*

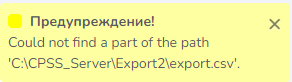
**1 4 Экспорт отчета**

Далее – раздел экспорта отчета в файл CSV. Необходимо создать каталог, в который будет сохраняться отчет. Перейти во вкладку «Автоматизация». Поставить галочку в пункте «Сохранять отчет в CSV файл по окончании анализа». Указать путь к созданному каталогу (например, *C:\CPSS\_Server\Export*) и название файла (например, *export*).

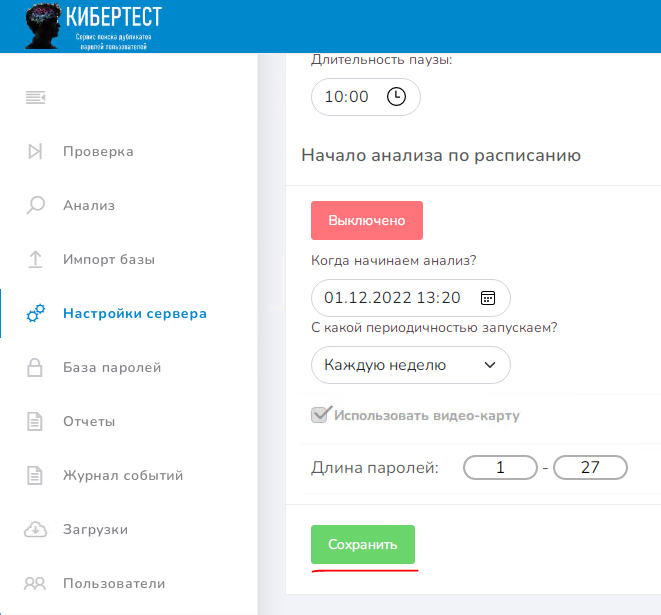


*Рис. 11. Экспорт отчёта*

При нажатии на кнопку «Проверить сохранение файла», происходит проверка указанного пути. Если путь существует, то получаем ответ 

Если в пути файла ошибка, или его не существует, то выводится предупреждение.

Для фиксирования заданных изменений в разделе «Настройки сервера», необходимо нажать кнопку сохранить.



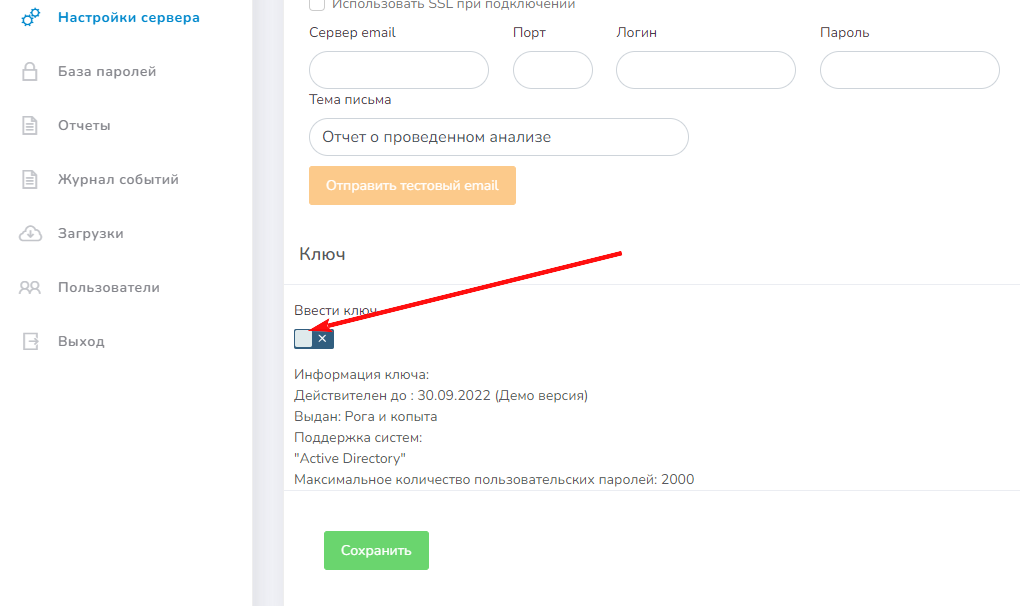
*Рис. 12. Кнопка «Сохранить»*



При успешном сохранении появится сообщение

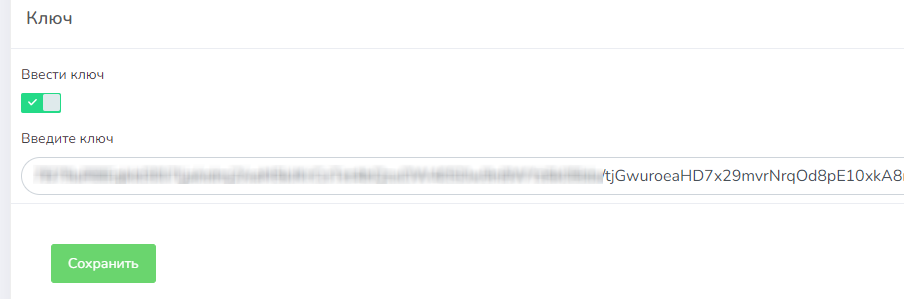
**1 5 Ключ программы**

В разделе «Настройки сервера» необходимо нажать на элемент, после чего появится поле, в которое необходимо ввести ключ – лицензию.



*Рис.13. Элемент для ввода ключа*

После ввода ключа нажать «Сохранить».

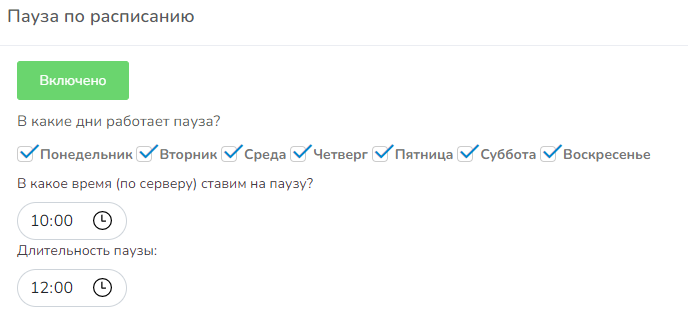


*Рис. 14. Сохранение введенного ключа*

**1 6 Автоматизация процессов**

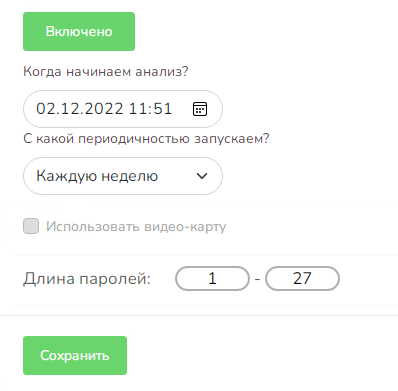
В Настройках сервера в разделе «Автоматизация» можно настроить паузу по расписанию и начало анализа по расписанию.

Пауза по расписанию позволяет на заданное время в определенные дни недели ставить на паузу анализ пользователей. Для этого нужно выбрать необходимые дни недели и указать время начала и окончания паузы. После чего нажать на кнопку «Выключено», чтобы перевести ее в статус «Включено». Затем нажать кнопку «Сохранить» внизу раздела.



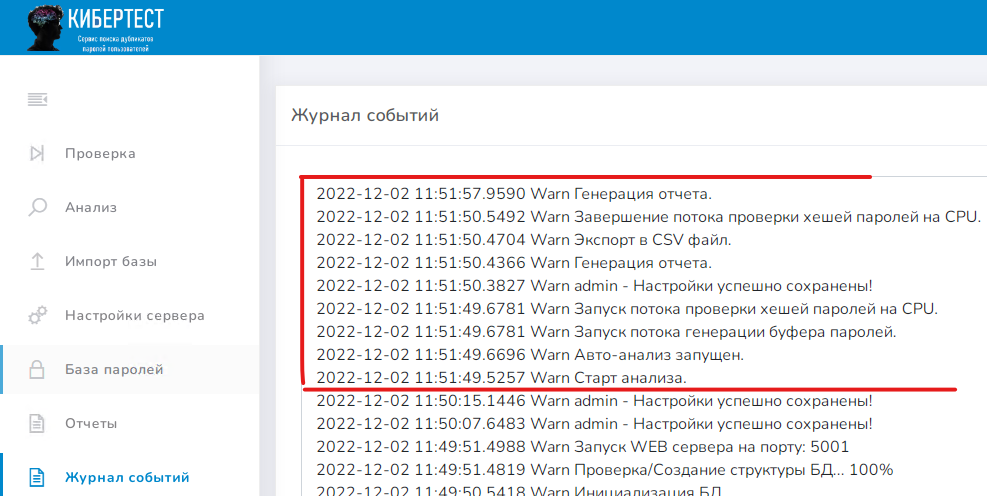
*Рис.15. Настройка паузы по расписанию*

Начало анализа по расписанию настраивается для автоматического анализа пользователей в заданное время. Необходимо указать дату и время начала анализа и периодичность запуска. После чего нажать на кнопку «Выключено», чтобы перевести ее в статус «Включено». Затем нажать кнопку «Сохранить».



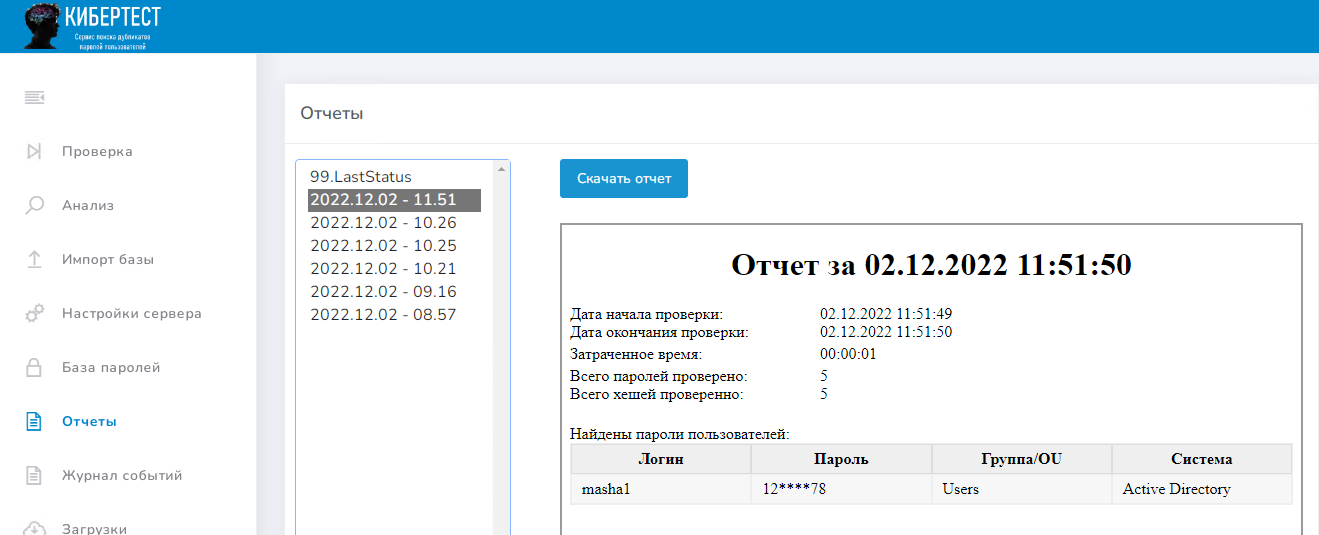
*Рис.16. Настройка анализа по расписанию*

После автоматического анализа в Журнале событий выводятся сообщения об успешной загрузке отчета.



*Рис. 17. Вывод событий в Журнале*

Сам отчет можно посмотреть в разделе «Отчеты».



*Рис. 18. Отчёты*

**1 7 Раздел «Пользователи»**

После добавления ключа, в программе появляется новый функционал и дополнительные возможности.

В разделе «Пользователи», можно изменять и создавать новых пользователей. По умолчанию созданы два дополнительных пользователя.

Всего имеется три роли. Admin – полные права. User – возможность запуска проверки, отсутствие возможности изменения настроек. Watcher – режим просмотра.

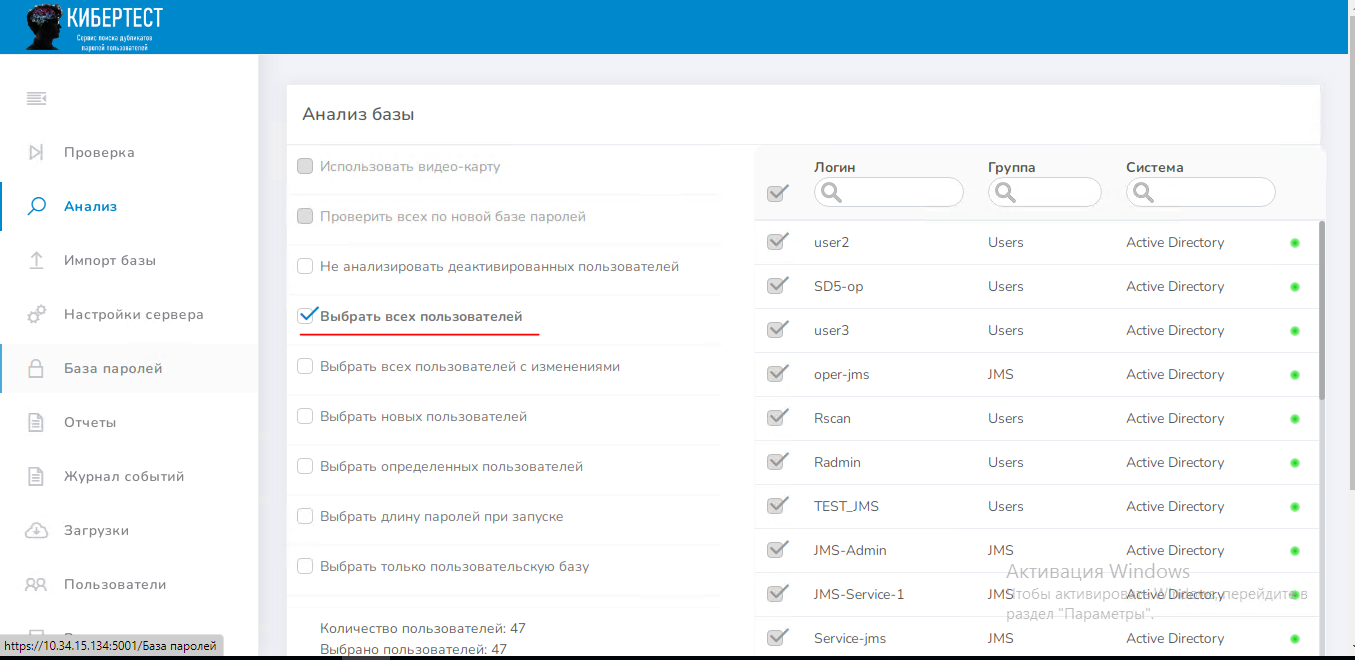
|  |  |
| --- | --- |
|  |  |

*Рис. 19. Роли пользователей*

**1 8 Раздел «Анализ»**

Импорт пользователей происходит при помощи работы коннектора. Описание его работы как для Windows, так и для Linux находятся в отдельной инструкции. Сначала необходимо выполнить действия из инструкции о работе с коннектором.

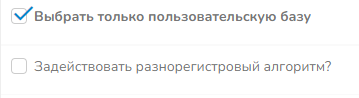
После передачи пользователей необходимо зайти в раздел «Анализ», в котором есть возможность выбора сразу всех пользователей, по которым будет запущена проверка, и далее по значениям.



*Рис. 20. Фильтрация пользователей*

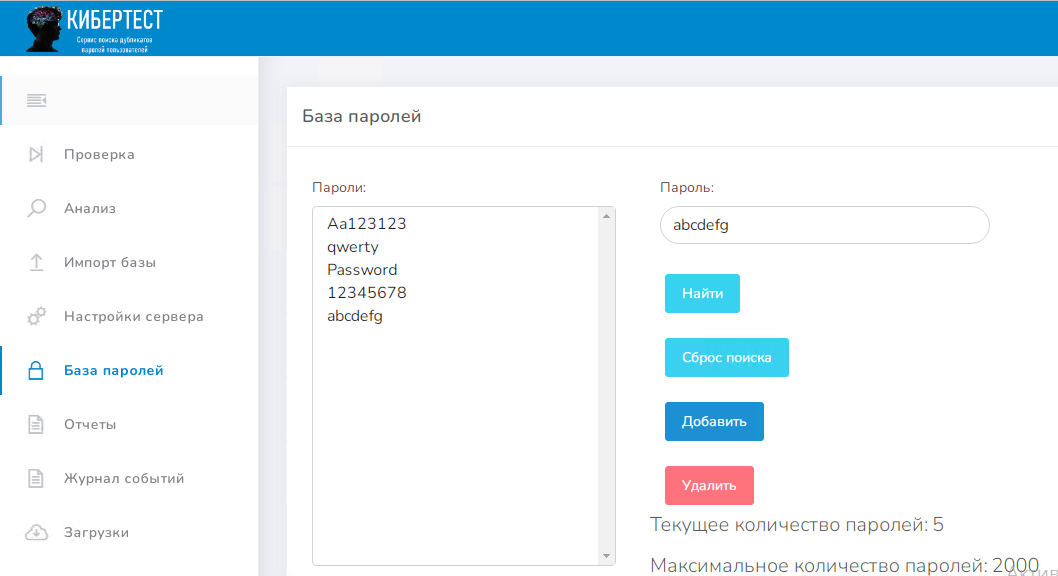
В пункте «Выбрать длину паролей» при запуске можно указать диапазон количества символов, значение которого позволит оптимизировать время, потраченное на проверку:

Пункты «Выбрать только пользовательскую базу» и «Выбор регистра» позволяют выполнить проверку по заранее заведенным паролям вручную.



**1 9 Раздел «База паролей»**

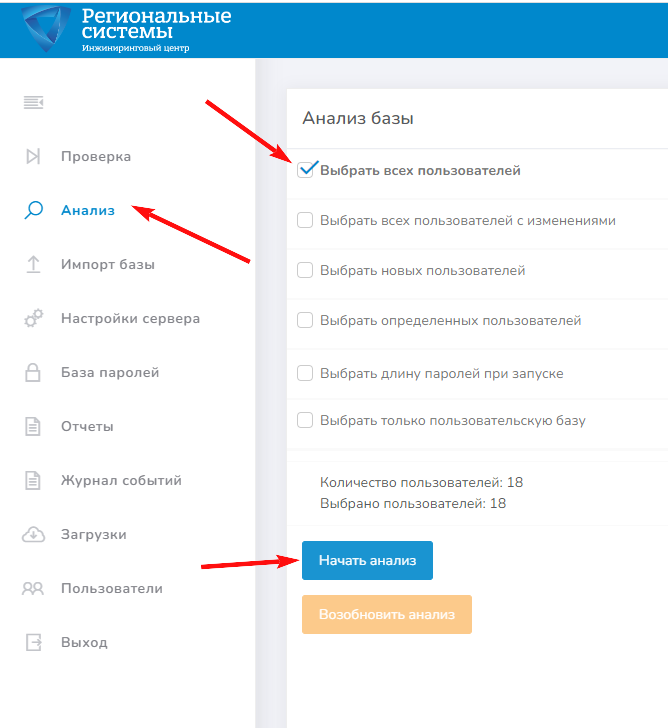
В разделе «База паролей» имеется возможность добавить свои пароли, по которым так же будет выполняться проверка.



*Рис. 21. Раздел База паролей*

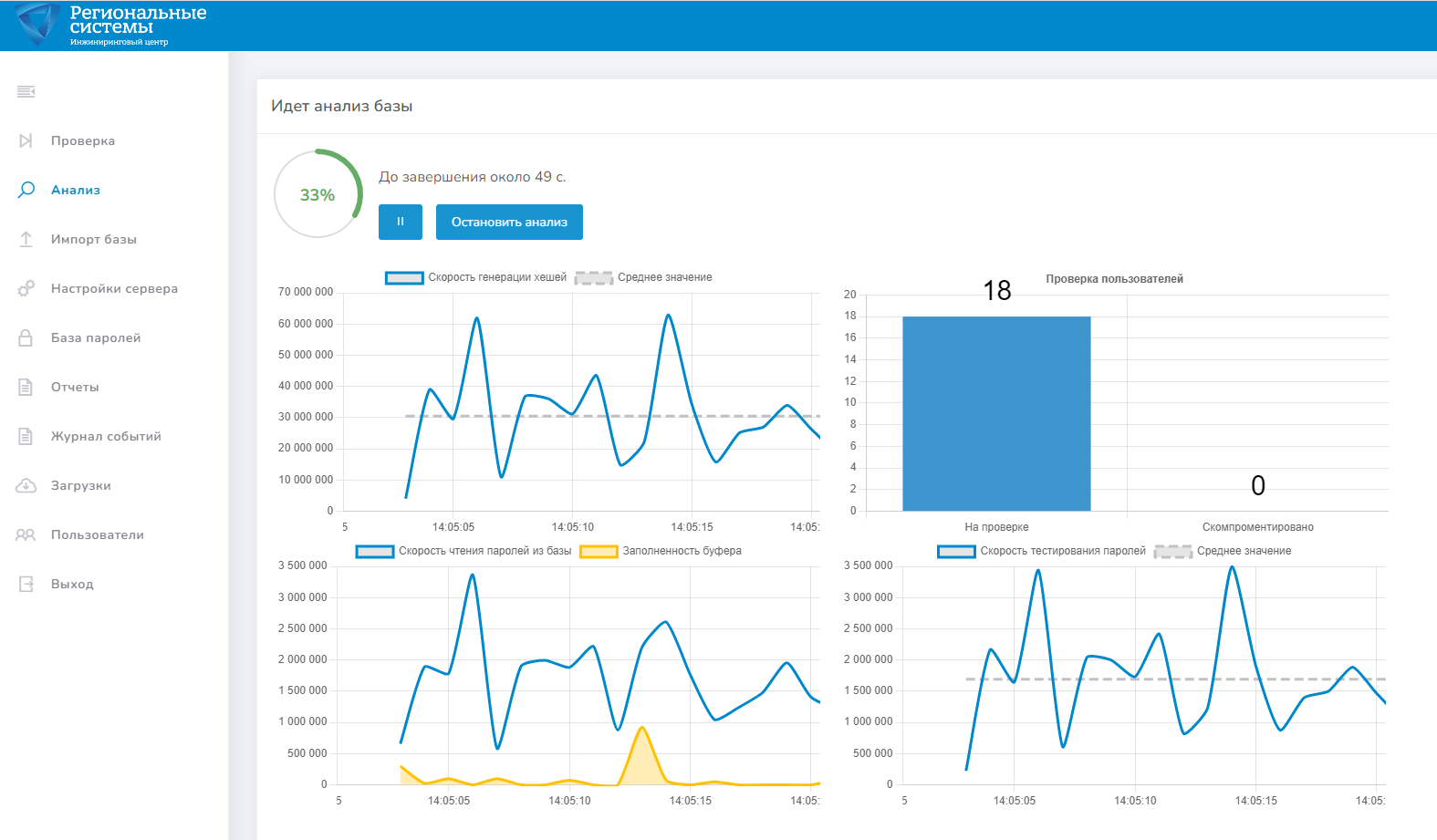
**1 10 Работа программы, Анализ**

Чтобы приступить к самому анализу, необходимо перейти в раздел «Анализ». Далее нужно выбрать всех или определенных пользователей, после чего нажать кнопку внизу области – Начать анализ.



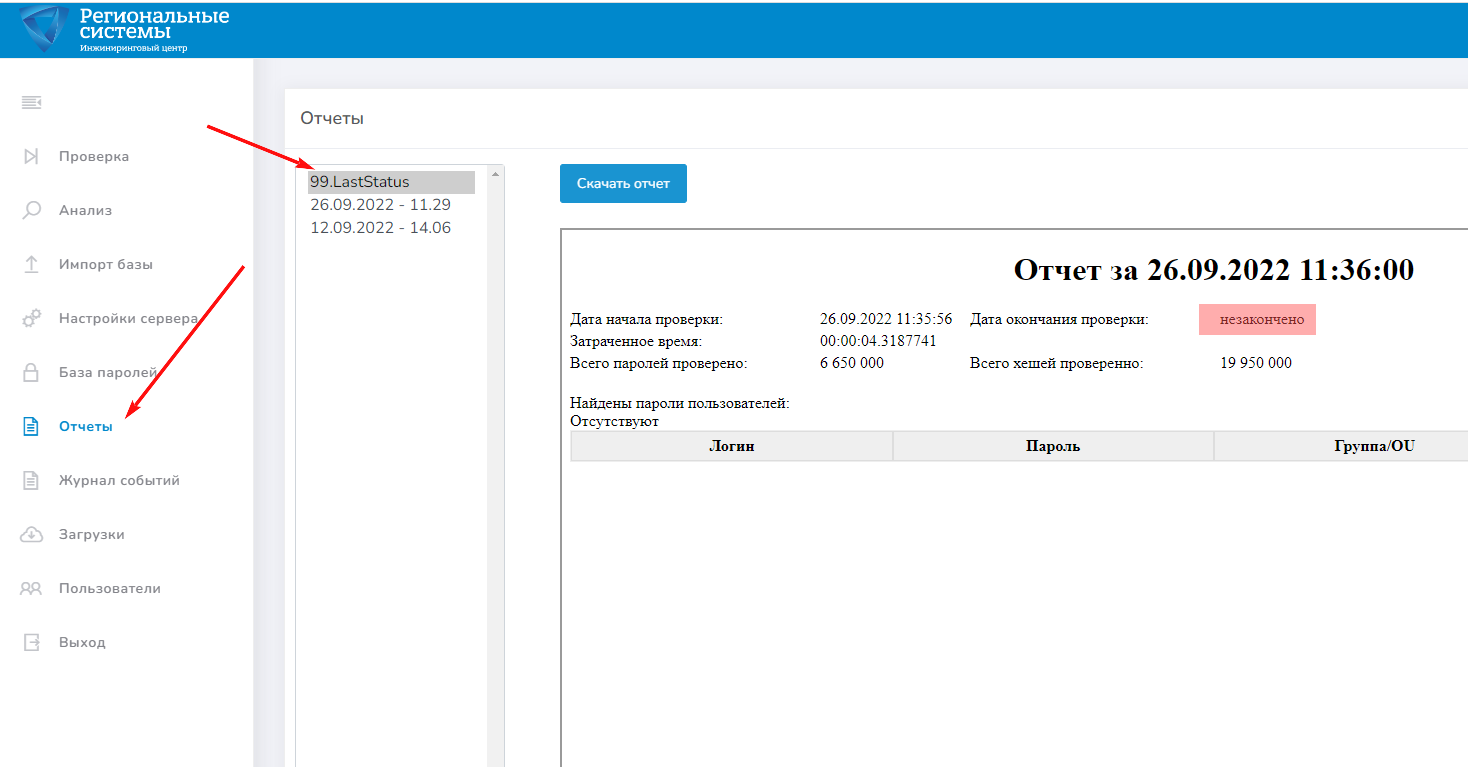
*Рис. 22. Раздел «Анализ»*

Происходит анализ, сравнение хэшей, паролей. Для наглядности и удобства выполнена визуализация в виде графиков. В режиме онлайн также будет показано количество пользователей по мере нахождения у них уязвимостей.



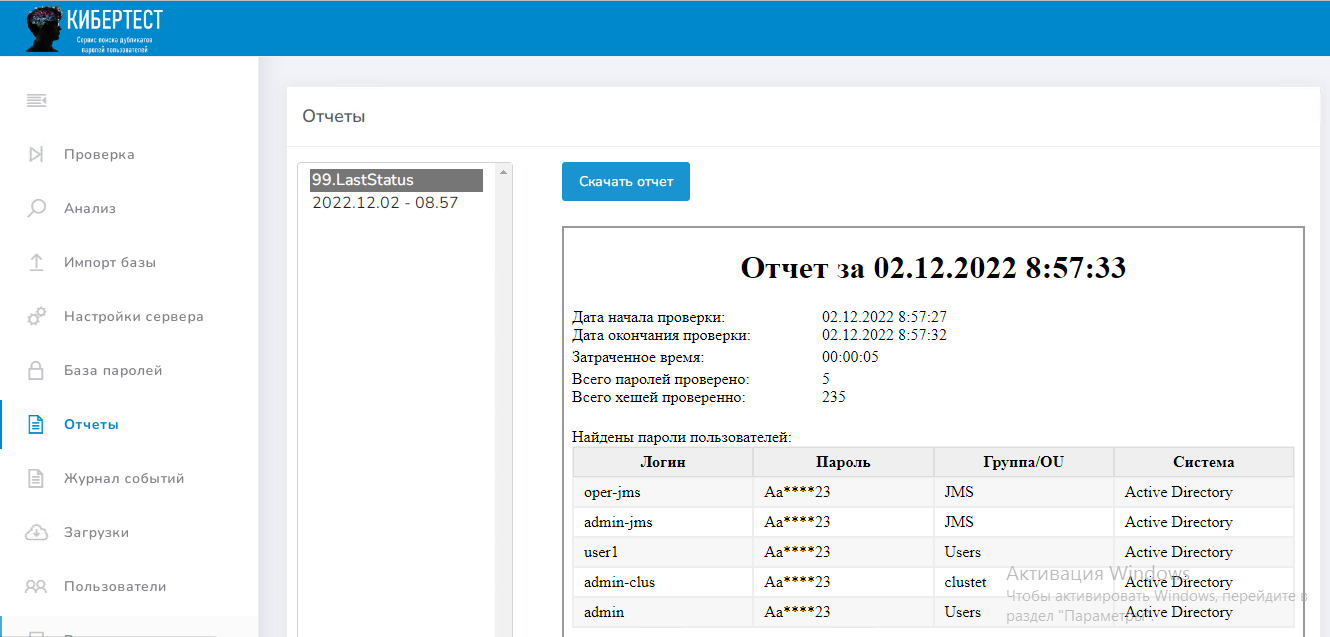
*Рис. 23. Визуализация анализа*

Пока идет анализ в онлайн режиме, можно увидеть ход процесса в виде выполненных действий (в разделе «Отчеты», в выбранном документе 99.**LastStatus**, где дата окончания проверки: не закончено).



*Рис. 24. Ход процесса в виде выполненных действий*

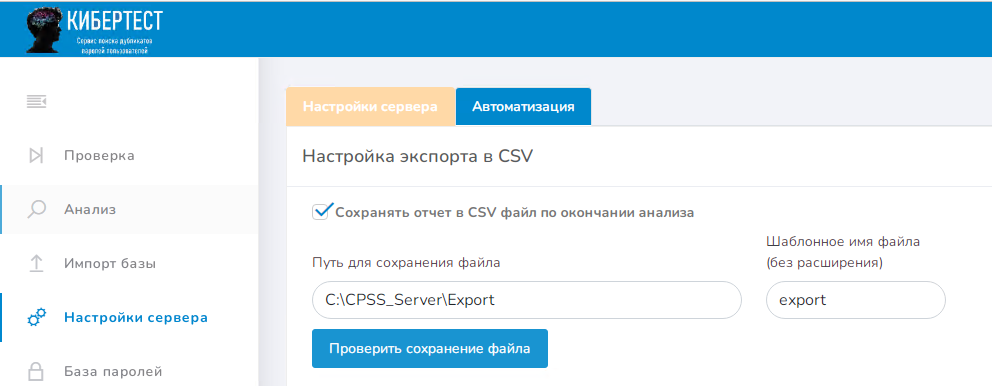
По завершению Анализа программа формирует отчет данными о произведенных вычислениях и затраченном времени, указывая пользователей, чьи пароли совпадают с утекшими. Вся история проведенных проверок сохраняется в данном разделе.



*Рис. 25. Отчёт по итогам проверки*

В разделе «Отчеты» показано текущее состояние процесса проверки (при нажатии на файл из списка с именем **99.LastStatus** отображается информация о затраченном времени и производительности в режиме онлайн).

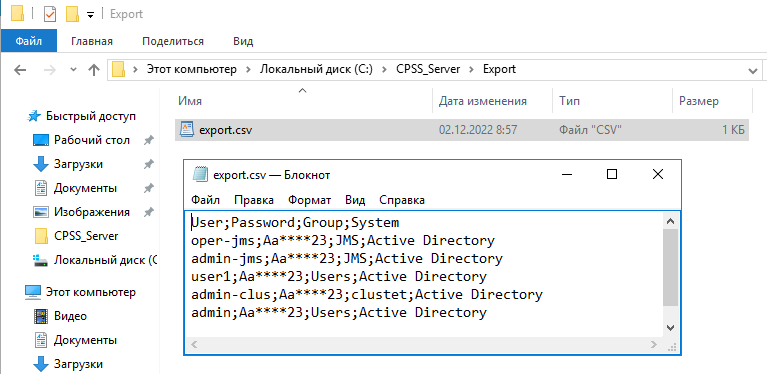
Отчет можно сохранить по кнопке «Скачать отчет». А также можно настроить автоматическое сохранение отчета по указанному пути (описание настроек было описано ранее). Также можно настроить отправку отчета на email (в разделе «Настройки сервера»). В этом случае по завершению анализа автоматически произойдёт сохранение отчета в формате CSV в заранее определенном каталоге и пересылка его на указанную почту).



*Рис. 26. Настройка экспорта отчёта*

Отчет сохраняется в файл csv с указанным заранее именем и отправляется на email.

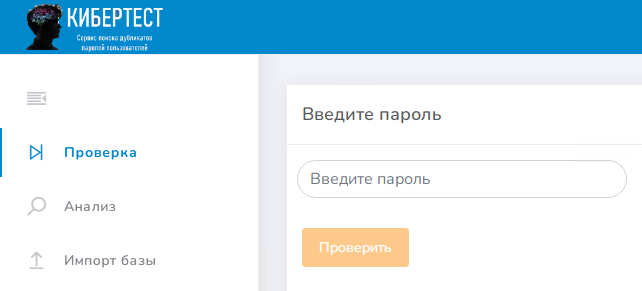
Ниже показан сам файл, находящийся по указанному ранее адресу и его содержимое.



*Рис. 27. Содержимое файла экспорта*

**1 11 Раздел «Проверка»**

Существует дополнительная возможность проверки определенного пароля (раздел «Проверка»).



*Рис. 28. Проверка определенного пароля*

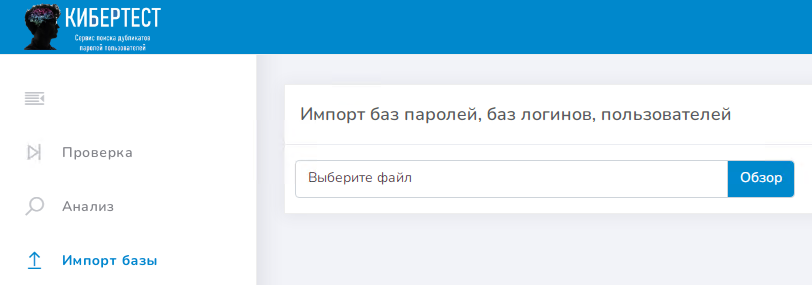
Для этого нужно ввести пароль. Пример предупреждения, что пароль в базе обнаружен, показан ниже.

|  |  |
| --- | --- |
|  |  |

*Рис. 29. Пример предупреждения*

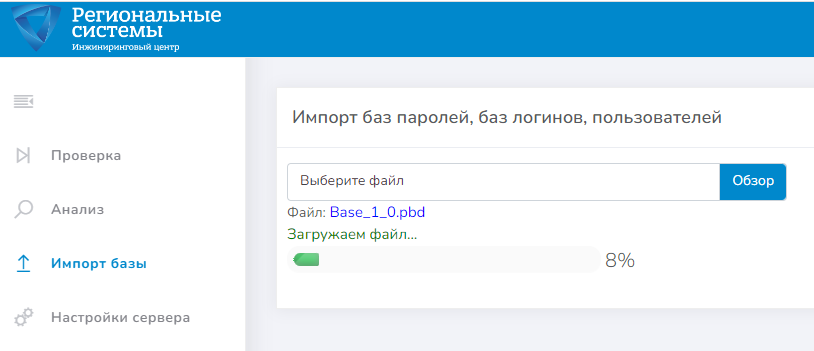
**1 12 Раздел «Импорт базы»**

Раздел «Импорт базы» позволяет загружать файлы базы данных с паролями.



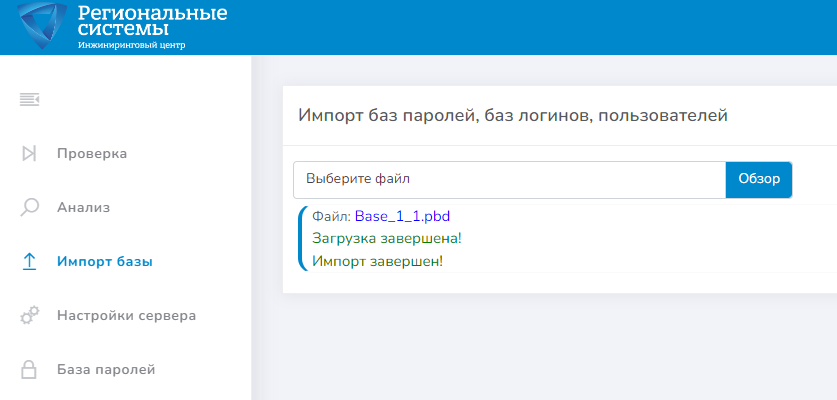
*Рис. 30. Раздел «Импорт базы»*

Необходимо выбрать файл базы и добавить его. Загрузка будет проходить в автоматическом режиме.



*Рис. 31. Процесс загрузки базы паролей*

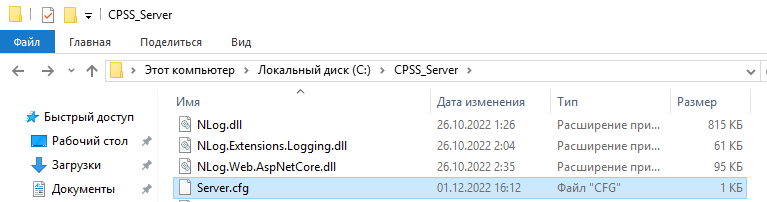
Информация о завершении загрузки базы паролей.



*Рис. 32. Завершение процесса загрузки базы паролей*

**1 13 Файл с настройками**

Все настройки программы хранятся в файле конфигурации **Server.cfg**, который расположен в корневом каталоге папки с программой. Он формируется при запуске программы. Если необходимо сбросить все установленные настройки, то достаточно его просто удалить. И при запуске программы данный файл формируется и создаётся вновь.



*Рис. 33. Файл с настройками в каталоге*

**1 14 Список сокращений и обозначений**

|  |  |
| --- | --- |
| БД | - база данных |
| CSV | - Comma-Separated Values (значения, разделённые запятыми) |
| DNS | - Domain Name System (система доменных имён) |
| HTTPS | - HyperText Transfer Protocol SECURED (протокол передачи гипертекста ЗАЩИЩЕННЫЙ) |
| IP | - Internet Protocol (межсетевой протокол) |
| SSL | - Secure Sockets Layer (уровень защищённых сокетов) |