**Дозор.**

**Мониторинг систем безопасности рабочей станции для Alt Linux и Astra Linux.**

***Руководство пользователя***

Ростов-на-Дону

2022

# Введение

Данный документ описывает порядок подготовки к работе и эксплуатации программного продукта «Дозор. Мониторинг систем безопасности рабочей станции» (далее – ПП).

Инструкция относится к релизу ПП: 1.0.0.

# Назначение и основные возможности ПП

## Назначение и структура

Программный продукт «Дозор. Мониторинг систем безопасности рабочей станции» предназначен для автоматизации мониторинга состояния безопасности рабочих станций путём контроля установки и настройки антивирусной защиты, ограничения доступа к запрещенным сайтам, а также проведения сканирования и отображения информации об установленном программном обеспечении (далее – ПО).

ПП поставляется в электронном виде и включает в себя следующий набор файлов:

* Dozor.1.0.0.rpm (для Alt Linux) или Dozor.1.0.0.deb (для Astra Linux) содержит файлы установки.
* Руководство пользователя (данный документ).

Электронная почта для вопросов по продукту: [info@cr-obr.ru](mailto:info@cr-obr.ru).

ПП включает в себя три модуля, обладающих следующими функциями:

* Модуль проверки антивирусной защиты ПК:
  + Автоматическое формирование перечня установленных на рабочей станции антивирусных пакетов.
  + Автоматическое определение и отображение каждого установленного антивирусного пакета.
* Модуль проверки доступа к запрещённым сайтам:
  + Проверка наличия доступа к интернет-ресурсам, содержащим информацию, запрещённую к распространению в образовательных организациях (далее – «запрещённые интернет-ресурсы»), с текущей рабочей станции.
  + Настройка параметров проверки:
    - Расписание проверки: временные интервалы проверки в течение дня, периодичность повторных проверок.
    - Скорость проверки: низкая, средняя, высокая.
    - Задержка между проверками сайтов (в секундах).
  + Если проверка была прервана (например, рабочая станция была выключена до окончания проверки доступности всех интернет-ресурсов из списка), при следующем запуске проверка возобновляется с той позиции в списке, на которой был прерван предыдущий сеанс.
  + Формирование отчётности о результатах проверки доступа к запрещённым интернет-ресурсам:
    - Сводный отчёт - включает информацию об общем количестве ресурсов в перечне, количестве проверенных ресурсов и количестве доступных интернет-ресурсов из перечня.
    - Детализированный отчёт – включает перечень всех запрещённых интернет-ресурсов. Для каждого ресурса выводится его доменное имя, дата и время проверки, результат проверки (доступен или не доступен).
  + Сохранение детализированного отчёта в файл в формате CSV.
  + Автоматическое обновление перечня запрещённых интернет-ресурсов.
* Модуль проверки программного обеспечения (далее - ПО) на доверие:
  + Поиск и отображение установленных пакетов на ПК пользователя.
  + Отображение пользователю списка, установленных пакетов на персональном компьютере пользователя, с известной информацией о них с базы ПП.
  + Возможность отправки скорректированной записи ПО на рассмотрение оператору по внесению изменений в запись.
  + Возможность сортировки списков:
    - По наименованию ПО.
    - По доверию.
  + Отображение информации о версии используемой информационной базы ПП.
  + Выгрузка отчетности по ПО, установленному на персональном компьютере пользователя, в формате CSV.
  + Автоматизированная загрузка с сервера актуальной базы ПО.
  + Предоставление вместе с ПП списка базового ПО с дополнительной информацией по программным средствам (может использоваться при запуске программы без Интернет-соединения).
  + Возможность сокрытия модулей программы через Настройки.

## Технические требования

#### Операционная система

Linux, поддерживающая .NET 5:

* Alt Linux Рабочая станция 9
* Alt Linux Рабочая станция 10
* Alt Linux Образование 9
* Alt Linux Образование 10
* ASTRA LINUX COMMON EDITION РЕЛИЗ «ОРЕЛ»

**Процессор**: от 1 ГГц

#### Оперативная память

Рекомендуемый объём ОЗУ: 8 Гб.

**Жёсткий диск**: для установки и работы ПП требуется наличие свободного места размером не менее 300 МБ на диске.

#### Наличие доступа в Интернет

Для обновления информационных баз, используемых ПП, и их последующей проверки требуется интернет-соединение со скоростью от 64 Кбит/сек.

Для установки и настройки ПП компьютер должен быть оснащён манипулятором «мышь».

## Система лицензирования и защиты

Лицензия «Дозор. Мониторинг систем безопасности рабочей станции» разрешает использование ПП на указанном в лицензии количестве рабочих мест в течение 1 года.

# Первоначальная настройка

## Настройка параметров и расписания проверки

При первом запуске программы на каждом компьютере необходимо настроить параметры и расписание проверки. В дальнейшем эти параметры можно изменять только в случае необходимости.

Для настройки параметров необходимо в главном окне программы нажать «Настройки». После чего откроется окно настроек.

В окне настроек необходимо выбрать один из режимов проверки (по умолчанию - медленный):

* Медленный – проверка сайтов будет происходить поочередно, время проверки увеличится, нагрузка на сеть и компьютер уменьшится.
* Обычный – проверка будет происходить по нескольким сайтам одновременно (кол-во одновременно проверяемых сайтов зависит от количества физических ядер процессора), время проверки уменьшится, нагрузка на сеть и компьютер увеличится.
* Быстрый – проверка будет происходить по нескольким сайтам одновременно (кол-во одновременно проверяемых сайтов равно количеству ядер процессора, умноженному на 4), время проверки уменьшится, нагрузка на сеть и компьютер увеличится.

Диапазоны времени, в которые будет производится проверка, настраиваются в нижней части окна «Настройки» (рисунок 5). По умолчанию время проверки зафиксировано на период с 00:00 до 23:59 – полные сутки.

Для добавления нового диапазона необходимо выбрать начальное и конечное время, после чего нажать кнопку «Добавить».

Для удаления диапазона необходимо нажать кнопку, которая расположена справа от каждого диапазона.

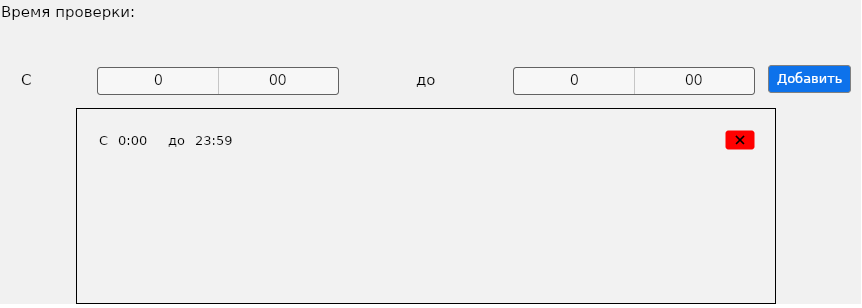


Рис. 5

Настройки повторения находятся в окне «Настройки» на вкладке «Настройки повторения» (см. рисунок 6). В левой части окна расположен переключатель режимов повторения:

* Ежедневно – проверка будет производиться каждый день.
* Еженедельно – проверка будет производиться каждую неделю в выбранный день.
* Ежемесячно – проверка будет производиться в заданное число месяца.

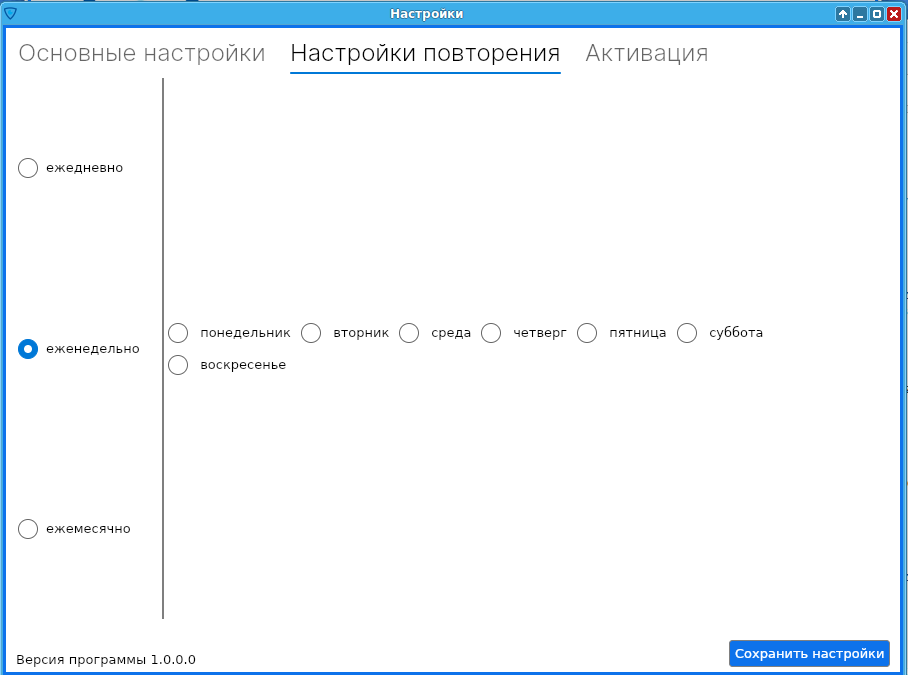


Рис. 6

Для применения настроек необходимо:

* В окне настроек нажать кнопку «Сохранить настройки».
* В главном окне программы (рисунок 7) нажать кнопку «Обновить».

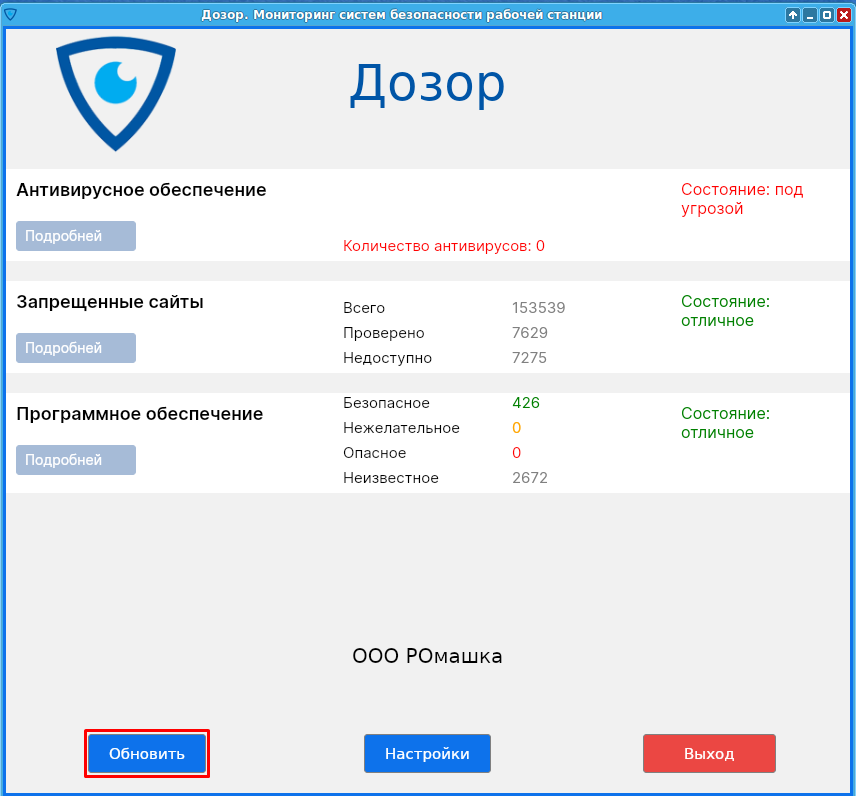


Рис. 7

# Просмотр отчётов о проверках

## Сводная информация о состоянии безопасности

В главном окне отображаются вкладки с информацией по модулям:

* Вкладка «Антивирус» (рисунок 8) – содержит данные о проверке антивируса. Отображается список установленных пакетов антивирусов.

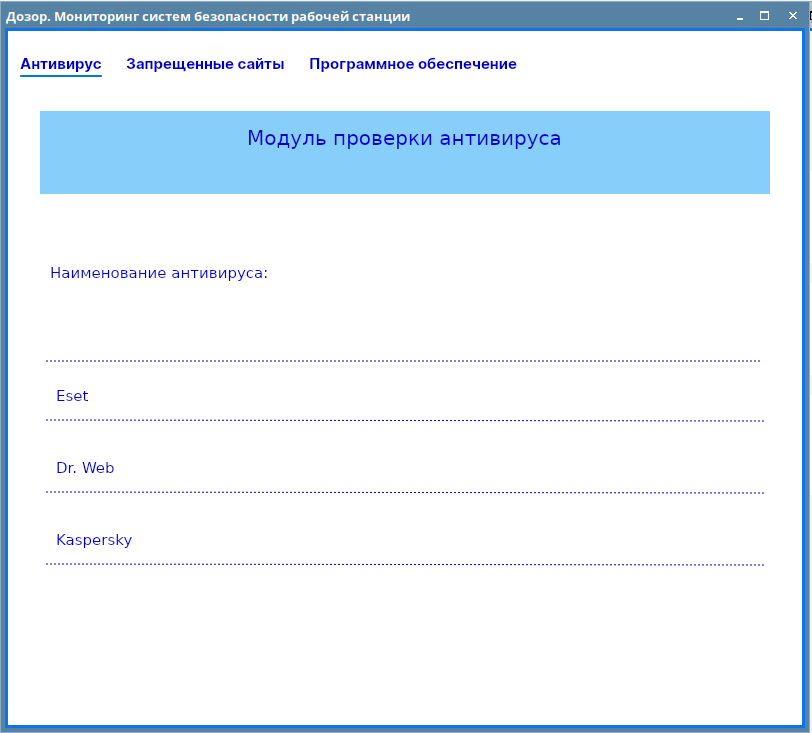


Рис. 8

* Во вкладке «Запрещенные сайты» (рисунок 9) предоставляется информация о проверке запрещённых сайтов. Отображаются показатели:
  + Общее количество сайтов в списке.
  + Количество сайтов из списка, проверенных в текущем сеансе проверки.
  + Количество сайтов, проверенных в текущем сеансе и определённых как недоступные.
  + Процент недоступных сайтов из общего количества сайтов, проверенных в текущем сеансе.

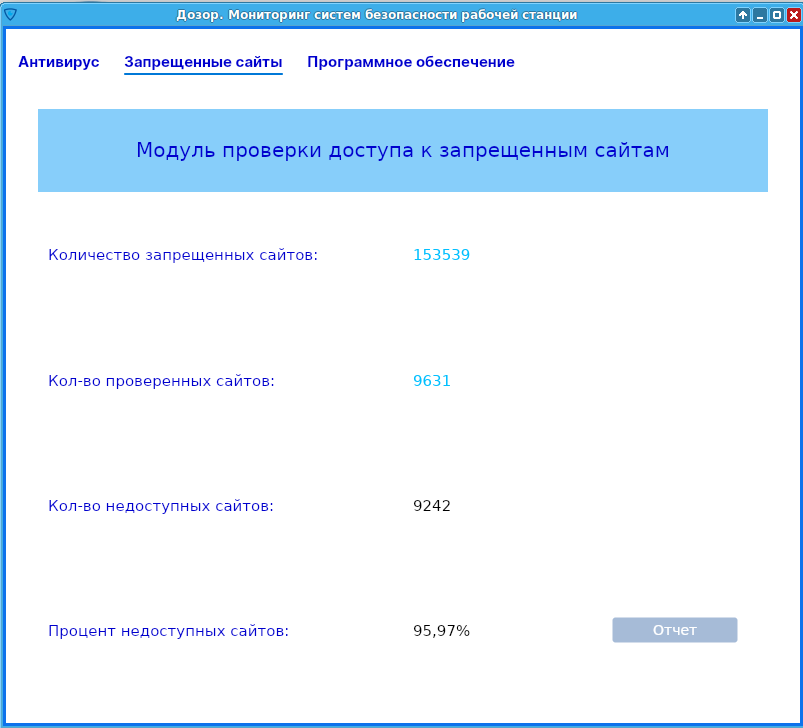


Рис. 9

* Вкладка «Программное обеспечение» (рисунок 10) предоставляет информацию о пакетах, установленных на рабочей станции. Проверка происходит путем сверки ПО клиента и информационной базой ПО, предоставляемой пользователю с ПП. Модуль предоставляет следующую информацию о ПО:
  + Список неизвестного ПО, установленного на ПК.
  + Список ПО на ПК, совпавшего с информационной базой ПП.
  + Версия информационной базы ПО.

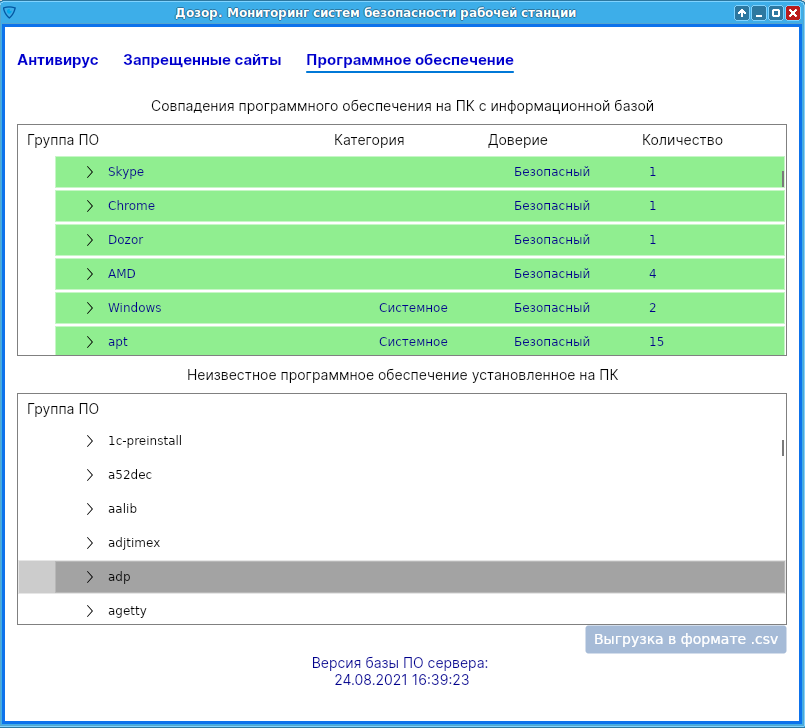
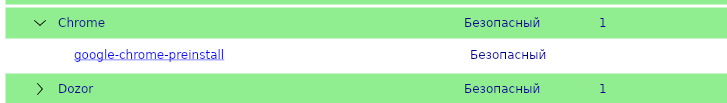


Рис. 10

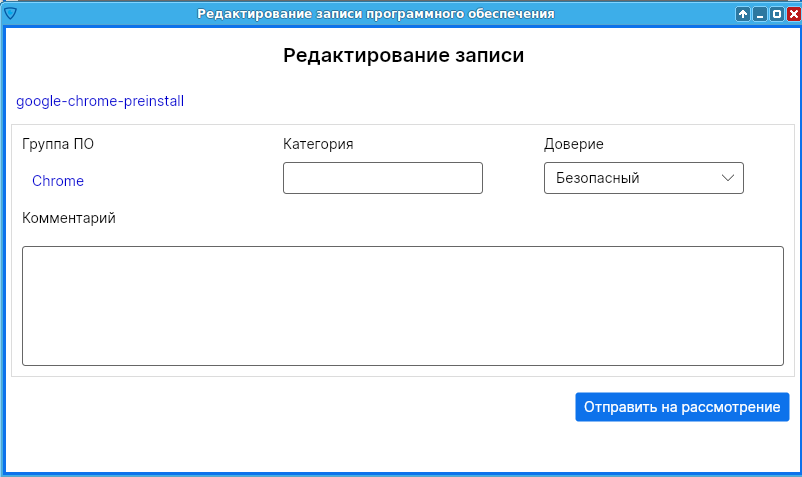
## Отправка изменений по определенному ПО оператору программы

Для изменения информации об определенном ПО необходимо щелкнуть по данному ПО (рисунок 11).



**Рис. 11**

После выбора ПО для редактирования будет отображено окно «Редактирование записи» (рисунок 12).



**Рис. 12**

Для отправки записи необходимо заполнить поле «Комментарий» к проведенным изменениям: «Почему изменено доверие?», «Почему отнесли к такой категории?» и т.д. Иначе, запрос не будет отправлен, так как оператору необходимо принять решение об изменении информации о ПО, основываясь на корректных доводах пользователя.

## Отчёт о результатах проверки доступности запрещённых сайтов

Отчет о результатах проверки запрещённых сайтов формируется в окне «Отчет», переход в которое происходит по кнопке «Отчет» во вкладке «Запрещенные сайты» программы (рисунок 9).

В отчете отображены следующие данные: ссылка на сайт, дата проверки и статус проверки. Для сохранения отчета необходимо нажать на кнопку «Сохранить» (рисунок 13). После чего откроется окно сохранения (рисунок 14), в котором необходимо указать имя файла и место сохранения. Отчёт сохраняется в формате XLSX и CSV (текстовый файл со значениями, разделёнными точками с запятой). Сохраненный файл можно открыть для просмотра и обработки либо в текстовом редакторе, либо в программе Microsoft Excel или её бесплатных аналогах.

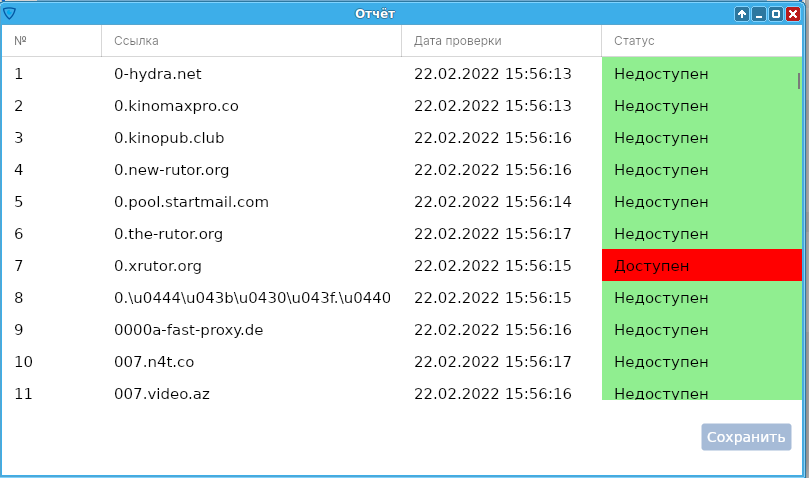


Рис. 13

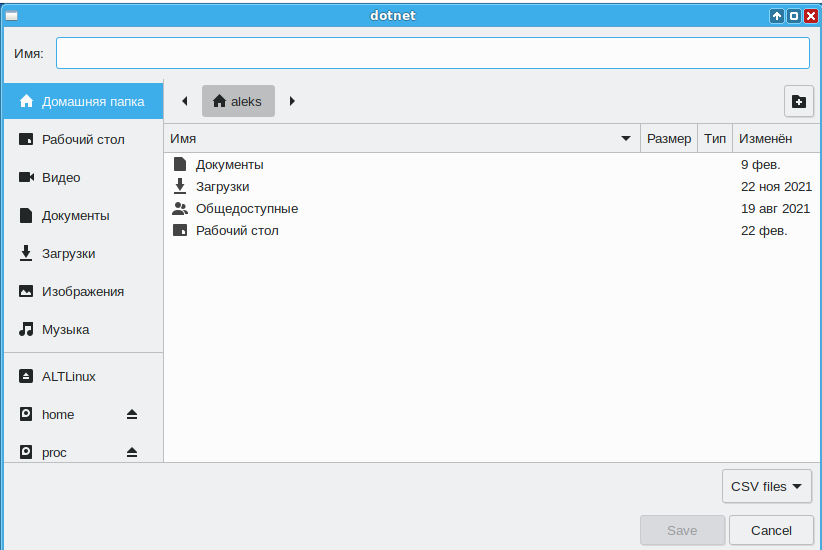


Рис. 14

## Отчёт о результатах проверки программного обеспечения

Отчет о результатах проверки ПО на ПК пользователя можно выгрузить по кнопке «Выгрузка в формате .csv» во вкладке «Программное обеспечение» программы (рисунок 10). После чего откроется окно сохранения (рисунок 14), в котором необходимо указать имя файла и место сохранения. Отчёт сохраняется в формате CSV (текстовый файл со значениями, разделёнными точками с запятой). Сохраненный файл можно открыть для просмотра и обработки либо в текстовом редакторе, либо в программе Microsoft Excel или её бесплатных аналогах. Отчет включает в себя информацию о ПО, разделенную по следующим колонкам (рисунок 15): имя ПО, категория, описание и доверие.

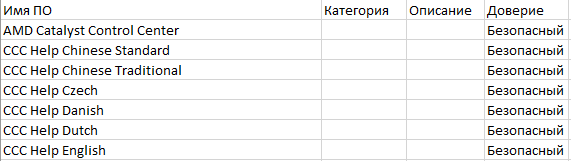


Рис. 15