ZECURION

Руководство
администратора

Zecurion DLP Linux Agent

версия 11.0

Zecurion DLP Linux Agent

Руководство администратора.

Компания Zecurion

Почтовый адрес: 129164, Российская Федерация,
Москва, Ракетный бульвар, 16

Телефон: +7 495 221-21-60

E-mail: info@zecurion.ru

Web: http://www.zecurion.ru

Оглавление

Введение

В настоящем документе описываются функционал, процесс установки и параметры настройки клиентских модулей **Device Control**, **Traffic Control** и **Staff Control**, устанавливаемых на компьютерах под управлением OS Linux.

Данные клиентские модули входят в состав системы информационной безопасности Zecurion DLP версии 11.0 и предназначены для выполнения тех же задач, что и их аналоги на Windows:

Device Control for Linux: модуль предназначен для контроля доступа к USB- и CD/DVD-устройствам, принтерам, перехвата клавиатурного ввода, буфера обмена и сохранения снимков экрана, а также для контроля запуска приложений.

Traffic Control for Linux: модуль предназначен для контроля интернет-трафика и почтовых сообщений.

Staff Control for Linux: модуль предназначен для контроля активности пользователей за компьютером и учета рабочего времени.

Требования к программно-аппаратному обеспечению

Сервер Zecurion DLP

Аппаратные и программные средства	Требуемые ресурсы
Процессор:	Intel Core и выше
Оперативная память:	2 ГБ и выше
Свободный объем на жестком диске:	500 МБ
Операционная система:	Microsoft Windows 7/8/10, Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016
Прочие программные средства:	Microsoft SQL Server 2008, 2008 R2, 2012, 2014, 2016; PostgreSQL 9.6 и выше

Пользовательские компьютеры

Аппаратные и программные средства	Требуемые ресурсы
Процессор:	Pentium 4 и выше
Оперативная память:	1 ГБ и выше
Свободный объем на жестком диске:	40 МБ
Операционная система:	64-разрядные версии следующих OS Linux: • AstraLinux SE 1.5 • AstraLinux SE 1.6 • AstraLinux SE 1.7 • AstraLinux CE 2.12 • RedOS 7.1 • RedOS 7.2 • RedOS 7.3 • ALT Linux p8 (рабочая станция) • ALT Linux c8 • ALT Linux p9 (рабочая станция) • ALT Linux p10 (рабочая станция) • Ubuntu 16.04 LTS а также модификации Kubuntu / Xubuntu / Lubuntu / Edubuntu 16.04 LTS и LinuxMint 18 • Ubuntu 18.04 LTS а также модификации Kubuntu / Xubuntu / Lubuntu / Edubuntu 18.04 LTS и LinuxMint 19 • Ubuntu 20.04 LTS а также модификации Kubuntu / Xubuntu / Lubuntu / Edubuntu 20.04 LTS и LinuxMint 20 • GosLinux IC3

1 ОБЩИЕ СВЕДЕНИЯ

Контроль компьютеров под управлением ОС Linux производится с помощью клиентских модулей **Device Control**, **Traffic Control** и **Staff Control**, установленных на данных компьютерах и взаимодействующих со следующими компонентами системы информационной безопасности Zecurion DLP:

Сервер Zecurion DLP – обеспечивает централизованное управление настройками, справочниками и политиками всей системы информационной безопасности.

Сервер Zecurion Reports – обеспечивает доступ к базам данных, содержащим информацию об инцидентах.

В состав клиентских модулей, устанавливаемых непосредственно на компьютеры с ОС Linux, входят следующие пакеты:

- zlock
- kernel-modules
- zgate
- zservice-staffcontrol
- zpolicy
- zservice
- zpolicy-wbclient
- ztools-go

Первые два (zlock и kernel-modules) относятся к модулю **Device Control**, пакет zgate относится к **Traffic Control**, пакет zservice-staffcontrol к **Staff Control**, следующие четыре должны быть установлены в составе любого из модулей.

Модули **Device Control** и **Traffic Control** получает от сервера Zecurion DLP политики, распространенные на данный компьютер и, в соответствии с политиками выполняют следующие действия:

Модуль **Device Control**:

— разрешает, запрещает или ограничивает чтение и запись данных на указанных в политиках USB-устройствах и CD/DVD-устройствах;
— разрешает или запрещает печать на указанных в политиках принтерах;
— перехватывает ввод текста с клавиатуры;
— перехватывает содержимое буфера обмена;
— с указанной периодичностью делает снимки с экрана;
— осуществляет сохранение инцидентов с соответствующими параметрами на сервере Zecurion Reports. Также в состав инцидентов могут быть включены

файлы, в отношении которых были совершены действия, текст с клавиатуры или снимки экрана;
- разрешает или запрещает запуск приложений, указанных в политиках контроля приложений.

Модуль **Traffic Control**:
- перехватывает HTTP(S)-трафик;
- перехватывает FTP -трафик;
- перехватывает пересылаемые сообщения электронной почты (SMTP, POP3, IMAP);
- осуществляет сохранение инцидентов, включая в них при необходимости перехваченные сообщения и прикрепленные файлы.

Модуль **Staff Control**:
- контролирует активность пользователей за компьютером и ведет учет рабочего времени.
- осуществляет сохранение событий, связанных с учетом рабочего времени (включение, выключение или блокировка компьютера, переход в режим скринсейвера) и фиксирует время активности пользователя в различных приложениях, а также при посещении различных сайтов.

2 УСТАНОВКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

2.1 Установка и удаление серверных компонентов

К серверным компонентам системы информационной безопасности Zecurion DLP относятся **Zecurion DLP Server** и **Zecurion Reports**. Подробная информация о них содержится в документах **Руководство администратора Zecurion DLP** и **Руководство администратора Zecurion Reports**.

Для установки или обновления перечисленных серверных компонентов необходимо запустить файл **Setup.exe** из соответствующего раздела дистрибутивного пакета и следовать его указаниям.

Удаление серверных компонентов выполняется с помощью стандартных средств Windows.

2.2 Установка и удаление клиентских модулей

В зависимости от дистрибутива Linux для установки клиентских модулей используется пакетный менеджер DPKG (см. *2.2.1 Установка и удаление клиентских модулей в ОС, использующих пакетный менеджер DPKG*) или пакетный менеджер RPM (см. *2.2.2 Установка и удаление клиентских модулей в ОС, использующих пакетный менеджер RPM*).

Технические подробности о конфигурации программного обеспечения и расположении файлов, содержащих диагностические данные, описаны в разделе *Приложение 1* настоящего документа.

> ***Внимание***
>
> *После удаления модулей командой **apt-get remove** (см. далее) остаются конфигурационные файлы пакетов, что позволяет выполнить повторную установку или обновление без ввода дополнительной информации (такой, как адрес сервера конфигурации).*
>
> *Для полного удаления необходимо выполнить команду **apt-get purge** <список пакетов>.*

2.2.1 Установка и удаление клиентских модулей в ОС, использующих пакетный менеджер DPKG

Установка

Важно!

*Перед установкой модулей Zecurion DLP под **ОС Astra Linux SE** версии **1.6 и выше** в режиме замкнутой программной среды необходимо выполнить предварительную настройку системы. Для этого следует руководствоваться указаниями раздела 3.2 Настройка ОС Astra Linux SE при работе в режиме замкнутой программной среды.*

Для установки модулей в заранее подготовленную папку необходимо скопировать файлы пакетов с расширением **.deb**, после чего по очереди ввести команды:

```
dpkg -i ztools-go-#.#.#-###.x86_64.deb
```

***Внимание:** Версия пакета **ztools-go** может не совпадать с версиями остальных пакетов.*

Если используется интеграция с AD при помощи сервисов sssd, то необходимо установить пакет **zpolicy-wbclient-sssd**:

```
dpkg -i zpolicy-wbclient-sssd-#.#.#-##.x86_64.deb
```

во всех остальных случаях необходимо установить пакет **zpolicy-wbclient-samba**:

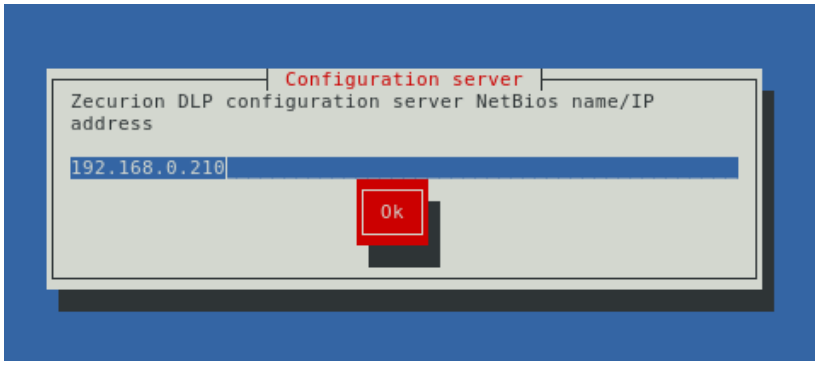
```
dpkg -i zpolicy-wbclient-samba-#.#.#-##.x86_64.deb
dpkg -i zpolicy-#.#.#-##.x86_64.deb
dpkg -i zservice-#.#.#-##.x86_64.deb
dpkg -i kernel-modules-zlock-[...].deb
dpkg -i zlock-#.#.#-##.x86_64.deb
dpkg -i zgate-#.#.#-##.x86_64.deb
dpkg -i zservice-staffcontrol-#.#.#-##.x86_64.deb
```

Внимание

В случае отсутствия в системе библиотек, необходимых для работы модулей, во время установки появится соответствующее уведомление, содержащее имя пакета недостающей библиотеки. Процесс установки при этом будет прерван.

Указанные библиотеки необходимо установить из дистрибутивного пакета операционной системы, после чего вновь запустить команду установки модулей.

В процессе установки в появившемся диалоговом окне необходимо указать имя или IP-адрес сервера DLP:



После завершения установки пакетов необходимо перезагрузить компьютер.

Удаление

Для удаления всех модулей ввести команду:

```
apt-get remove zpolicy ztools-go zservice zlock zgate kernel-modules*
```

2.2.2 Установка и удаление клиентских модулей в ОС, использующих пакетный менеджер RPM

Установка

Для установки модулей в заранее подготовленную папку необходимо скопировать файлы пакетов с расширением **.rpm**, после чего по очереди ввести команды:

```
rpm -ihv ztools-go-#.#.#-###.x86_64.rpm
```

Если используется интеграция с AD при помощи сервисов sssd, то необходимо установить пакет **zpolicy-wbclient-sssd**:

```
rpm -ihv zpolicy-wbclient-sssd-#.#.#-##.x86_64.rpm
```

во всех остальных случаях необходимо установить пакет **zpolicy-wbclient-samba**:

```
rpm -ihv zpolicy-wbclient-samba-#.#.#-##.x86_64.rpm
rpm -ihv zpolicy-#.#.#-##.x86_64.rpm
rpm -ihv zservice-#.#.#-##.x86_64.rpm
```

Внимание

*Одновременно с пакетом **zlock** должен быть установлен пакет **kernel-modules**. Версия пакета должна соответствовать версии ядра ОС, на которой устанавливаются пакеты.*

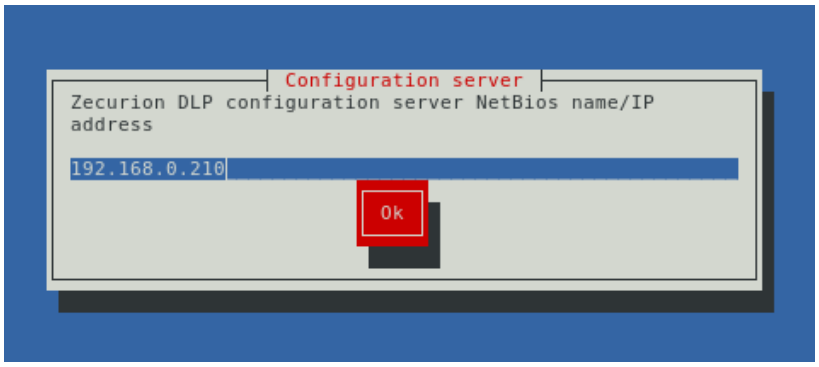
```
rpm -ihv kernel-modules-zlock-[...].rpm zlock-#.#.#-##.x86_64.rpm
rpm -ihv zgate-#.#.#-##.x86_64.rpm
rpm -ihv zservice-staffcontrol-#.#.#-##.x86_64.rpm
```

Внимание

В случае отсутствия в системе библиотек, необходимых для работы модулей, во время установки появится соответствующее уведомление, содержащее имя пакета недостающей библиотеки. Процесс установки при этом будет прерван.

Указанные библиотеки необходимо установить из дистрибутивного пакета операционной системы, после чего вновь запустить команду установки модулей.

В процессе установки в появившемся диалоговом окне необходимо указать имя или IP-адрес сервера DLP:



После завершения установки пакетов необходимо перезагрузить компьютер.

Удаление

Для удаления всех модулей ввести команду:

- Для ОС, использующих пакетный менеджер YUM:

  ```
  yum remove zpolicy ztools-go zservice zlock zgate zservice-staffcontrol kernel-modules*
  ```

- Для ОС, использующих пакетный менеджер APT:

  ```
  apt-get remove zpolicy ztools-go zservice zlock zgate zservice-staffcontrol kernel-modules*
  ```

3 НАСТРОЙКА КОНФИГУРАЦИИ

3.1 Настройка сервера Zecurion DLP

Настройки клиентских модулей **Device Control**, **Traffic Control** и **Staff Control** задаются на сервере Zecurion DLP и распространяются на указанные в настройках компьютеры.

Сервер Zecurion DLP предназначен для:

- централизованного управления настройками и конфигурациями модулей;
- определения политик информационной безопасности в отношении различных каналов передачи и обработки данных;
- создания и модификации средств контентного и контекстного анализа – словарей, цифровых отпечатков и списков устройств.

Подробная информация о сервере Zecurion DLP изложена в документе **Руководство администратора Zecurion DLP**.

3.1.1 Запуск веб-интерфейса сервера Zecurion DLP

Доступ к серверу Zecurion DLP осуществляется через веб-интерфейс в окне интернет-браузера. Запуск веб-интерфейса возможен на локальном компьютере или через удаленное соединение по сети в случае наличия соответствующих прав доступа.

1. Запуск веб-интерфейса на локальном компьютере в окне браузера по умолчанию осуществляется через пункты меню **Пуск → Zecurion → Zecurion DLP**. Также для запуска веб-интерфейса можно ввести в адресной строке браузера *http://localhost:1294*, где **1294** – номер порта HTTP сервера Zecurion DLP по умолчанию. В дальнейшем номер порта HTTP можно изменить. Также в настройках можно настроить порты для подключения по протоколу HTTPS, в этом случае в адресной строке браузера следует набирать *https://localhost:https_port*, где **https_port** — номер порта HTTPS.
2. Для запуска веб-интерфейса через удаленное соединение по сети необходимо в адресной строке браузера набрать

   http://hostname:http_port или *https://hostname:https_port*, где

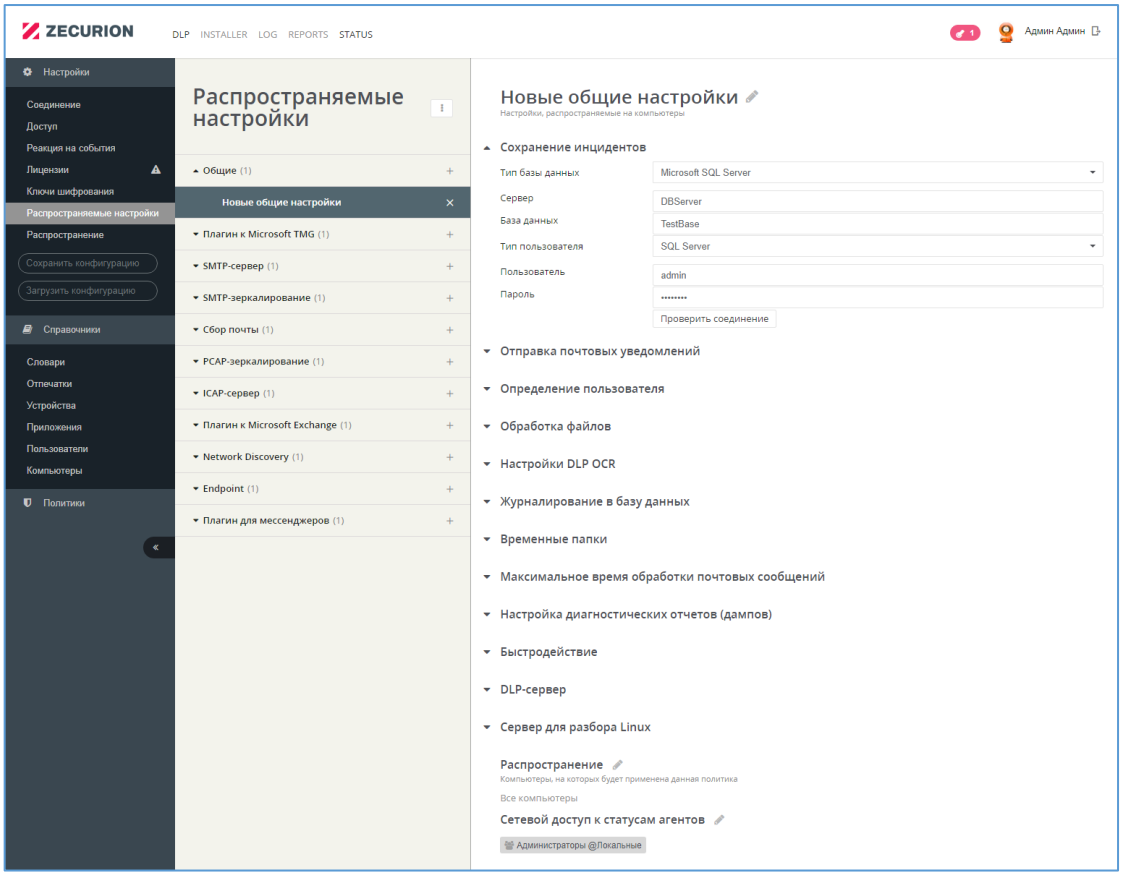
   - **hostname** — имя или IP-адрес компьютера, на котором установлен сервер Zecurion DLP;
   - **http_port** — номер порта для подключения к серверу Zecurion DLP по протоколу HTTP (по умолчанию – 1294);

- **https_port** — номер порта для подключения к серверу Zecurion DLP по протоколу HTTPS (настраивается дополнительно).

3.1.2 Описание веб-интерфейса сервера Zecurion DLP

Левая часть экрана содержит главное меню, состоящее из разделов **Настройки**, **Справочники** и **Политики**.

- В разделе **Настройки** расположены параметры сервера Zecurion DLP, а также модулей системы информационной безопасности Zecurion DLP.
- В разделе **Справочники** расположены инструменты контентного и контекстного анализа, а также каталоги пользователей и компьютеров, находящихся под контролем системы.
- В разделе **Политики** расположены политики, определяющие реакцию системы Zecurion DLP на события информационной безопасности.



При выборе раздела открываются дополнительные панели, содержащие настройки данного раздела или детализированную информацию о связанных с ним объектах.

3.1.3 Настройка модулей

> ***Внимание***
>
> *Необходимо наличие достаточного количества активных лицензий **Traffic Control**, **Device Control** и **Staff Control** для работы соответствующих клиентских модулей (см. раздел **3.4 Лицензии** документа **Руководство администратора Zecurion DLP**).*

Для настройки модулей **Device Control**, **Traffic Control** и **Staff Control** для Linux необходимо зайти в раздел **Настройки** главного меню веб-интерфейса сервера Zecurion DLP и выполнить следующие действия:

1. В пункте **Распространяемые настройки** в разделе **Общие** открыть или создать новую настройку, предназначенную для распространения на компьютеры под управлением ОС Linux.
2. В списке распространения данной настройки указать компьютеры под управлением ОС Linux и сохранить настройку.

Внимание

*Следует учитывать, что функционал некоторых настроек из раздела **Общие** отсутствует в клиентских модулях для Linux. Изменение следующих настроек не оказывает влияния на их работу:*

Определение пользователя.
Временные папки.
Максимальное время обработки почтовых сообщений.

3. В пункте **Распространяемые настройки** в разделе **Endpoint** открыть или создать новую настройку, предназначенную для распространения на компьютеры под управлением ОС Linux.

Внимание

*Следует учитывать, что модуль **Traffic Control** для Linux работает только в режиме зеркалирования.*

1. В секции **Traffic Control** в разделе **Основные** при необходимости заполнить поля **Игнорируемые хосты для SSL** и **Опубликованные хосты**.
2. В секции **Traffic Control** в разделе **Порты** при необходимости изменить значения портов для следующих протоколов: **HTTP**, **FTP**, **POP3**, **SMTP** и **SSL/TSL**.
3. В секции **Device Control** настроить следующие параметры:
   a. **Снимки экрана**: указать **Периодичность** и выбрать **Формат файла**.
   b. **Запись звука**: указать **Минимальный порог громкости для записи**, **Задержку перед началом записи** и **Задержку перед окончанием записи**.
   c. **Прочее**: указать **Email администратора для запроса доступа** и **Текст, отображаемый пользователю, при запросе доступа по телефону**.
   d. **Прочее**: при необходимости включить опции **Запретить печать на нераспознанных принтерах** и **Запретить печать неподдерживаемых форматов**.
4. В секции **Staff Control** настроить опции отслеживания активности приложений и работы в браузере. Учитывать, что при включении опции **Отслеживать работу в браузере** отслеживается работа только в браузерах Chrome/Chromium, Firefox, Vivaldi, Yandex browser.
5. В секции **Дополнительно** при необходимости включить опцию **Скрывать Zecurion DLP от конечных пользователей**.
6. В списке распространения данной настройки указать компьютеры под управлением ОС Linux и сохранить настройку.

Внимание

*Следует учитывать, что все остальные настройки из раздела **Endpoint**, кроме вышеперечисленных, не оказывают влияния на работу модулей для Linux, так как у них отсутствуют соответствующие функциональные возможности.*

3.1.4 Настройка политик

> ***Внимание***
>
> *Подробная информация о настройке политик изложена в документе **Руководство администратора Zecurion DLP**.*
>
> *Не реализовано применение политик к некоторым устройствам и каналам.*

Для настройки политик, распространяемых на модули для Linux необходимо перейти в раздел **Политики** главного меню веб-интерфейса сервера Zecurion DLP и выполнить следующие действия:

1. В разделе **По умолчанию** настроить правила доступа и действия по умолчанию для следующих каналов:
   - Почта.
   - USB-устройства.
   - Принтеры.
   - Экран.
   - Буфер обмена.
   - Клавиатура.
   - Микрофон.
   - DVD и CD дисководы.
   - Съемные носители.
2. В разделе **Контроль устройств** создать и настроить политики, предназначенные для распространения на компьютеры под управлением ОС Linux, на которых установлен модуль **Device Control** с учетом следующих особенностей:
   - Поддерживается контроль каналов **Устройства**, **Экран**, **Буфер обмена**, **Клавиатура** и **Микрофон**.
   - Не поддерживается канал **Веб-камера**.

> ***Внимание***
>
> *При выборе канала **Устройства** следует учитывать, что поддерживается контроль только нижеперечисленных типов устройств:*
> - *USB-устройства (из списка типовых устройств).*
> - *DVD и CD дисководы.*
> - *Принтеры.*
> - *Съемные носители.*

3. В разделе **Контроль приложений** создать и настроить политики, предназначенные для распространения на компьютеры под управлением ОС Linux, на которых установлен модуль **Device Control**.
4. В разделе **Контентные** создать и настроить политики, предназначенные для распространения на компьютеры под управлением ОС Linux, на которых установлены модули **Traffic Control** и **Device Control**. Следует учитывать следующее:
   - Блокировка трафика (каналы **Интернет** и **Почта**) или передачи данных на внешний носитель (канал **Устройства**) по результатам контентного анализа не осуществляется. Анализ производится в режиме зеркалирования.
   - Действие **Заблокировать пользователя** не осуществляется.
   - Действие **Шифрование** для канала **Устройства** не осуществляется.
   - Действие **Журналировать** поддерживает только вариант **Запись в SysLog**.
   - Не поддерживаются условия, связанные с отпечатками, созданными на основе:

  - Источника **Изображения**.
  - Источника **Базы данных**.
  - Источника **Текст** с алгоритмом опорных векторов.
- Не поддерживаются условия **Из группы Exchange / Не из группы Exchange** по параметру **Пользователь**.
- Не поддерживается канал **Discovery**.
- Не поддерживается канал **Мессенджеры**.
- Не поддерживается при создании инцидента опция **Сделать снимок экрана**.

В следующей таблице перечислены форматы содержащих текст файлов, из которых может быть извлечена текстовая составляющая, анализируемая при проверке условий по параметру **Текст в файле**. Также перечислены форматы файлов, из которых текстовая составляющая не может быть извлечена:

Форматы файлов, из которых может быть извлечена текстовая составляющая	Форматы файлов, из которых не может быть извлечена текстовая составляющая
DOC (Документ Microsoft Office Word)	ACCDB (База данных Microsoft Access 2007)
DOCX (Документ Microsoft Word 2007)	CHM (Скомпилированный HTML-файл справки Microsoft)
EML (Почтовое сообщение Outlook Express)	DBF (База данных dBase)
HTML (Веб-страница, файл гипертекста)	DJVU (Документ DJVU)
ODP (Презентация OpenOffice.org)	MDB (База данных Microsoft Office Access)
ODS (Электронная таблица OpenOffice.org)	MHT (Веб-архив MHT)
ODT (Текстовый документ OpenOffice.org)	MPP (Файл Microsoft Project)
PDF (Файл документации Adobe Acrobat)	ODB (База данных OpenOffice.org)
PLAIN TEXT (Стандартный текстовый документ)	ODF (Формула OpenOffice.org)
PPT (Презентация Microsoft Office PowerPoint)	ODG (Изображение OpenOffice.org)
PPTX (Презентация Microsoft PowerPoint 2007)	RPT (Crystal Reports)
RTF (Документ Rich Text Format)	SDA (Рисунок StarOffice)
SDC (Электронная таблица StarOffice)	SMF (Математический документ StarOffice)
SDD (Презентация StarOffice)	TEX (Текстовый документ Tex)
SDW (Текстовый документ StarOffice)	VSD (Документ Microsoft Visio)
SGML (Стандартный обобщённый язык разметки)	WPS (Текстовый документ Microsoft Works)
XLS (Электронная таблица Microsoft Office Excel)	WRI (Документ Windows Write)
XLSB (Бинарная электронная таблица Microsoft Office Excel)	XPS (Файл XPS/OXPS)
XLSX (Электронная таблица Microsoft Excel 2007)	
XML (Расширяемый язык разметки)	

3.1.5 Просмотр статуса агента

Просмотр статуса агента осуществляется только с актуального (указанного при установке агента) DLP-сервера, при условии, что на сервере авторизован пользователь

AD, который присутствует в списке настройки **Сетевой доступ к статусам агентов** группы **Общие** распространяемых настроек DLP-сервера.

Если запрос на просмотр статуса отправляется не с актуального DLP-сервера, то запрос отклоняется с сообщением "**доступ с данного сервера запрещен**".

Если запрос на просмотр статуса отправляется с актуального DLP-сервера, но на сервере авторизован пользователь AD, который не присутствует в списке настройки **Сетевой доступ к статусам агентов**, то запрос отклоняется с сообщением "**доступ для данного пользователя запрещен**".

3.2 Настройка ОС Astra Linux SE при работе в режиме замкнутой программной среды

В ОС Astra Linux SE поддерживается особый режим замкнутой программной среды (ЗПС), в котором запускаются только приложения, исполняемые файлы которых подписаны цифровой подписью разработчика, чей открытый ключ добавлен в перечень ключей, которым доверяет ОС.

По умолчанию клиентские модули Zecurion, поставляемые для исполнения в среде Astra Linux SE, подписаны цифровой подписью компании **СекьюрИТ**, а открытый ключ для этой цифровой подписи автоматически добавляется в перечень доверенных при установке программы. В результате этого клиентские модули Zecurion должны корректно запускаться при активизации режима ЗПС в ОС Astra Linux SE версии 1.5.

Однако, в связи с тем, что в ОС Astra Linux SE версии 1.6 механизм подписи был изменен, для обеспечения корректного запуска сервисов Zecurion в режиме ЗПС в ОС Astra Linux SE версии 1.6 и выше необходимо выполнить следующие шаги для предварительной настройки системы:

1. Поместить открытый ключ компании **СекьюрИТ** в каталог **`/etc/digsig/keys`**. Ключ поставляется вместе с дистрибутивом DLP Linux Agent в файле **securit_rusbitech_pub.key**.
2. Выполнить команду:

```
# update-initramfs -k all -u
```

3. Перезагрузить систему.

ПРИЛОЖЕНИЕ 1

- На клиентских компьютерах программное обеспечение компании Zecurion устанавливается в каталог **`/opt/zecurion`**
- Конфигурация Zservice находится в файле **`/etc/zservice.conf`**
- Основная конфигурация Device Control находится в файле **`/etc/zlockd.conf`**
- Основная конфигурация Traffic Control находится в файле **`/etc/zgate.conf`**

Диагностика

Ведутся следующие журналы (в каталоге **`/var/log/`**):

- **zservice.log** - протокол работы zservice (обмен с сервером DLP, а также работа агента).
- **zlock.log** и **messages** (для Astra Linux) или **journalctl** (для RedOS, Ubuntu и ALT Linux) - протокол работы Device Control.
- zgate.log - протокол работы Traffic Control.

- При включении режима диагностики в консоли статуса агента (см. **3.7.1 Статус агентов** в документе **Руководство администратора Zecurion DLP**) данные, передаваемые в базу данных Zecurion Reports, по умолчанию сохраняются в следующем каталоге:

  `/var/spool/zservice/archive/<dd.mm.yyyy>/`

  Каждый пакет хранится в zip-архиве вида **`{guid}.zip`**. Каталог для хранения архива можно изменить в конфигурационном файле **`/etc/zservice.conf`**

```
[service]
ArchiveData = true
ArchivePath = /path/to/archive
```