

READY
FOR
ASTRA



АСТРА

СЕРТИФИКАТ СОВМЕСТИМОСТИ

SELF-CERTIFICATION

№15792/2024

Настоящим сертификатом ООО «РусБИТех-Астра» подтверждает работоспособность и корректность совместного функционирования операционной системы специального назначения Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7) с программным обеспечением

Защищенный программный комплекс IIoT.Istok(серверная часть) - 1.0.1

компании Istok (АО «НПП «Исток» им. Шокина»)

на основании результатов совместных испытаний, указанных
в протоколе №15792/2024 от 15.05.2024.

Протокол является неотъемлемой частью сертификата.



16 июля 2024 года

Директор департамента
сопровождения
ООО «РусБИТех-Астра»



Алексей Трубочев

Проверить Сертификат вы можете на сайте www.astragroup.ru

ПРОТОКОЛ № 15792/2024

проведения совместных испытаний программного обеспечения «Защищенный программный комплекс ПоТ.Istok (серверная часть)» версии 1.0.1 и операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.7)

г. Москва

15.05.2024

1 Предмет испытаний

1.1 В настоящем протоколе зафиксирован факт проведения в период с 13.05.2024 по 15.05.2024 совместных испытаний программного обеспечения «Защищенный программный комплекс ПоТ.Istok (серверная часть)» версии 1.0.1 (далее – ПО), разработанного АО «НПП «Исток» им. Шокина», и операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.7) с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 2023-1023SE17 (оперативное обновление 1.7.5) (далее – Astra Linux SE 1.7.5), разработанной ООО «РусБИТех-Астра».

2 Объект испытаний

2.1 Перечень компонентов, эксплуатировавшихся в ходе проведения данных испытаний, относящихся к ПО, представлен в Таблице 1.

Таблица 1 – Перечень компонентов, относящихся к ПО

Описание	Наименование	MD5	Источник
Файл программного пакета дистрибутива ПО	ApacheDirectoryStudio	1061a8281ca21a414dfa4af2b7d9c40	Ресурс в сети «Интернет», адрес: « https://directory.apache.org/studio »
Файл архива, содержащий файлы дистрибутивов дополнительных модулей ПО	Cloud.jar	b6cd9e568546a2c6fc1922ec019f9e0d	Сторона разработчика ПО
Файл архива, содержащий файлы дистрибутивов дополнительных модулей ПО	Platform.jar	10f1ce9e018674605ca5195088072320	Сторона разработчика ПО
Официальное руководство по эксплуатации ПО в электронном формате	«Руководство пользователя по работе в платформе интернета вещей ПоТ.ISTOK_17.10.2023.docx»	-	Сторона разработчика ПО

3 Ход испытаний

3.1 В ходе проведения настоящих испытаний были выполнены проверки корректности функционирования ПО в среде Astra Linux SE 1.7.5 в объеме, указанном в Приложении 1.

3.2 Перечень используемых репозиторий приведен в Приложении 2.

3.3 С целью проведения проверок при включённом режиме ЗПС использовался файл открытого ключа разработчика ПО.

3.4 Проверка корректности функционирования ПО в условиях ненулевого уровня конфиденциальности механизма мандатного разграничения доступа (далее – МРД) указанных сред не проводилась по причине отсутствия поддержки ПО соответствующей функциональности ОС. Информация об отсутствии упомянутой поддержки была заявлена стороной разработчика ПО.

3.5 Проверка корректности функционирования ПО в условиях низкой целостности не проводилась по причине отсутствия поддержки ПО соответствующей функциональности ОС. Информация об отсутствии упомянутой поддержки была заявлена стороной разработчика ПО.

4 Результаты испытаний

4.1 ПО корректно функционирует в среде Astra Linux SE 1.7.5.

5 Вывод

5.1 ПО и операционная система специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.7) совместимы, принимая во внимание информацию, содержащуюся в разделах 3, 4 и Приложении 2.

6 Состав рабочей группы и подписи сторон

6.1 Данный протокол составлен участниками рабочей группы:

Баринов А. П. – архитектор программных систем отдела автоматизированных систем управлений АО «НПП «Исток» им.Шокина»;

Сапего Д. К. – младший программист отдела автоматизированных систем управлений АО «НПП «Исток» им.Шокина»;

АО «НПП «Исток» им.Шокина»	
архитектор программных систем отдела автоматизированных систем управлений	
(должность)	
 (подпись)	Баринов А. П. (фамилия, инициалы)

Перечень проверок совместимости ПО и Astra Linux SE 1.7.5

[illegible]

Инструкция по установке и удалению ПО в среде Astra Linux SE 1.7.5

1 Используемые репозитории:

в Astra Linux SE 1.7.5:

- deb https://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.5/repository-base/ 1.7_x86-64
main contrib non-free

2 Установка ПО:

2.1 выполнить системные команды, действия:

Установка виртуальной машины Java

Для установки Liberika JDK необходимо выполнить следующую команду: `sudo dpkg -i bellsoft-jdk*-linux-amd64.deb`, где * - актуальная скачанная версия Liberika JDK, из директории, с находящемся там репозиторием Liberika JDK

После установки добавить системные переменные JAVA_HOME и PATH. Пример:

```
echo 'export JAVA_HOME=/usr/lib/jvm/java-8-openjdk-amd64' > /etc/profile.d/jdk.sh
```

```
echo 'export PATH=$JAVA_HOME/bin:$PATH' >> /etc/profile.d/jdk.sh
```

```
echo 'export PATH=$JAVA_HOME/jre/bin:$PATH' >> /etc/profile.d/jdk.sh
```

После чего необходимо применить переменные среды: `source /etc/profile.d/jdk.sh`

В случае ошибки прав необходимо предоставить полные права на директорию, выполнив команду: `sudo chmod 777 /etc/profile.d`

Важно: не выделять права на всю директорию /etc, т. к. это повлечет удаление настроек сети.

• Установка сервера LDAP

Для установки ApacheDS, необходимо перейти в каталог с дистрибутивом:

`cd /ваш_путь` (для удобства выбора директории, возможно использование Tab, которое позволяет автоматически подставлять название директорий).

Дополнительно необходимо предоставить права, на выполнение: `chmod +x ./apacheds-2.0.0.AM26-64bit.bin`

После чего выполнить установку: `sudo ./apacheds-2.0.0.AM26-64bit.bin`

На этапе выборе пользователя для установки, указать актуального пользователя, и его группу

Для запуска сервера ApacheDS, необходимо выполнить команду:

```
sudo /etc/init.d/apacheds-2.0.0.AM26- default start
```

Для включения автозагрузки ApacheDS, необходимо выполнить команду: `sudo update-rc.d apacheds-2.0.0.AM26- default defaults`

Для проверки запуска ApacheDS, необходимо выполнить команду: `nc -v localhost 10389 -w 0`

Для установки ApacheDirectoryStudio, необходимо перейти в каталог с дистрибутивом: `cd /ваш_путь` (для удобства выбора директории, возможно использование Tab, которое позволяет автоматически подставлять название директорий).

После чего выполнить установку: `tar zxvf ApacheDirectoryStudio-2.0.0.v20180908-M14-linux.gtk.x86_64.tar.gz`

Для запуска выполнить команду: `./ApacheDirectoryStudio &`

- Создание пользователей в LDAP

Для создания пользователей нужно открыть Apache Directory Studio и создать соединение (LDAP, New Connection) со следующими свойствами:

- Hostname: ip-адрес(имя) компьютера, где установлен Apache DS (например, localhost)
- Port: 10389
- Bind DN or user: uid=admin, ou=system
- Bind password: secret

Подключиться к сохраненному соединению.

Для создания новой учетной записи, проще всего скопировать существующую, например, можно выбрать учетную запись uid=admin и скопировать ее

Выделить раздел ou=people и вставить учетную запись

Выбрать Object (Only the copied entry), OK

Переименовать учетную запись и поменять поля: cn, sn, Display Name, mail, userPassword

В случае отсутствия нужно поля добавить его выбрав действие «New Attribute»

- Установка базы данных

Для установки ApacheDirectoryStudio, необходимо перейти в каталог с дистрибутивом: `cd /ваш_путь` (для удобства выбора директории, возможно использование Tab, которое позволяет автоматически подставлять название директорий).

Дополнительно необходимо предоставить права, на выполнение: `chmod +x ./postgresql-10.6-1-linux-x64.run`

После чего выполнить установку:

```
sudo ./postgresql-10.6-1-linux-x64.run
```

Параметры, указываемые при установке (рекомендованные):

- port: 5432
- password: sa
- кодировка: UTF-8

Для старта сервера выполнить команду: `service postgresql start`

Запуск при перезагрузке: `update-rc.d postgresql enable`

В случае, если данные команды не выполняются, значит они не требуются, и сервер PostgreSQL автоматически запущен.

Для запуска утилиты PgAdmin4, в отличии от PgAdmin3, необходимо использовать веб-браузер. Для подключения необходимо запустить утилиту PgAdmin4 (из меню пуск - fly-start-panel, либо левый нижний угол экрана).

Во вкладке «утилиты», либо «прочее», выбрать утилиту PgAdmin4.

Для установки бэкапа базы, она должна быть совместима с 10 версией PostgreSQL

Параметры восстановления включают в себя следующие параметры:

- Format – Custom or tar
- Role name – postgres
 - Установка IIoT Cloud

Для установки IIoT Cloud необходимо перейти в директорию с дистрибутивом: `cd /ваш_путь/setup`

Выполнить команду для установки:

```
sudo java -jar ./IIoTCloud.5.1.0.jar
```

- Настройка подключения к IIoT Cloud

Для настройки подключения IIoT Cloud к IIoT Storage необходимо отредактировать следующие параметры в файле: `standalone.xml` в директории `IIoTCloud\config\cloud\datacenter`

`id="CloudDataCenterInetAddress"` - IP сервера на котором установлен IIoT Cloud

`id="CloudDataCenterUser"` - Имя пользователя для доступа к кэш хранилищу. По умолчанию `value="cassandra"`

`id="CloudDataCenterPassword"` - Пароль для доступа к кэш хранилищу. По умолчанию `value="cassandra"`

`id="CloudDataCenterKeyspace"` - Идентификатор ключей кэш хранилища. По умолчанию `value="IIoT"`

- Запуск IIoT Cloud и IIoT Storage

Последовательность запуска: 1 – IIoT Storage 2 – IIoT Cloud.

Запуск IIoT Storage состоит из нескольких этапов:

Разрешение выполнения исполняемых файлов (при первом запуске):

```
sudo chmod u+x /home/IIoT/IIoTCloud/storage/3.11.11/bin/cassandra
```

```
sudo chmod u+x /home/IIoT/IIoTCloud/storage/3.11.11/bin/nodetool
```

Для запуска кэш хранилища выполнить команду:

```
sudo /home/IIoT/IIoTCloud/storage/3.11.11/bin/cassandra -R
```

По завершению загрузки появится команда: INFO [main] 2022-07-07 10:34:53,823

AuthCache.java:172 - (Re)initializing CredentialsCache (validity period/update interval/max entries) (2000/2000/1000).

Для проверки состояния запуска используйте команду: sudo

```
/home/IIoT/IIoTCloud/storage/3.11.11/bin/nodetool status
```

Для остановки кэш хранилища используйте команду

```
sudo /home/IIoT/IIoTCloud/storage/3.11.11/bin/nodetool stopdaemon
```

Для запуска IIoT Cloud, необходимо выполнить следующие команды:

Разрешение выполнения исполняемых файлов (при первом запуске):

```
sudo chmod +x /home/IIoT/IIoTCloud/bin/start.sh
```

Для запуска IIoT Cloud выполнить: sudo /home/IIoT/IIoTCloud/bin/start.sh

После появления сообщения «IIoT – LogicServer ready (in ... ms)» IIoT Cloud готов к работе.

Для остановки IIoT Cloud используйте комбинацию клавиш Ctrl+C, либо с помощью команды sudo kill -9 *номер процесса*

- Установка IIoT Platform

Для установки IIoT Platform необходимо перейти в директорию с дистрибутивом:

```
cd /ваш_путь/setup
```

Выполнить команду для установки: sudo java -jar ./IIoTPlatform.5.1.0.jar

- Настройка подключения к IIoT Platform

Для настройки подключения IIoT Platform к IIoT Storage необходимо отредактировать следующие параметры в файле: standalone.xml в директории IIoTPlatform\config\cloud\datacenter

id="CloudDataCenterInetSocketAddress" IP сервера на котором установлен IIoT Cloud

id="CloudDataCenterUser" Имя пользователя для доступа к кэш хранилищу. По умолчанию value="cassandra"

id="CloudDataCenterPassword" Пароль для доступа к кэш хранилищу. По умолчанию value="cassandra"

id="CloudDataCenterKeyspace" Идентификатор ключей кэш хранилища. По умолчанию value="IIoT"

Для настройки подключения IIOT Platform к IIOT Cloud необходимо отредактировать следующие параметры в файле: standalone.xml в директории IIoTPlatform\config\connection

id="IIoTCloudConnectorHost" IP сервера на котором установлен IIOT Cloud

id="IIoTCloudConnectorPort" Порт, который используется для подключения и отключения устройств. По умолчанию value="81" (рекомендуется оставить без изменений)

id="IIoTCloudConnectorType" Тип подключения. WS – websocket, WSS – websocket secured. По умолчанию value="ws" (рекомендуется оставить без изменений)

id="IIoTCloudConnectorAppId" Основной URL префикс IIOT Cloud (рекомендуется оставить без изменений)

Для запуска IIoT Platform необходимо отредактировать следующие параметры в файле start.sh в директории IIoTPlatform\bin

IIOT_HOME Каталог установки IIOT Platform. По умолчанию

"IIOT_HOME=/usr/local/IIoT/IIoTPlatform"

IIOT_IP IP адрес IIOT Platform. По умолчанию "IIOT_IP=192.168.56.105"

Для добавления новых пользователей в IIOT Platform необходимо отредактировать следующие параметры в файле standalone.xml в директории IIoTPlatform\config\ldap

id="IIoT.security.ldap.host" Адрес LDAPv3 сервера с указанием корневого каталога. По умолчанию "ldap://localhost:10389/dc=example,dc=com"

id="IIoT.security.ldap.password.algorithm" Алгоритм шифрования паролей. По умолчанию "SHA"

id="IIoT.security.ldap.login" Наименование атрибута LOGIN (логин) в LDAP. По умолчанию «uid»

id="IIoT.security.ldap.mail" Наименование атрибута MAIL (эл.почта) в LDAP. По умолчанию «mail»

id="IIoT.security.ldap.displayname" Наименование атрибута DISPLAY_NAME (описание или отображаемое наименование) в LDAP. По умолчанию «displayName»

Пример для настройки подключения к серверу LDAP MS AD: IIoTPlatform\config\appserver\standalone.xml

- LDAP сервер: DC2019.factory.local с портом 389

- Пользователь для подключения: iiotadmin из каталога OU=Admins, OU=Users, DC=factory, DC=local
- Пароль: iiotadmin
- Поиск осуществляется в DC=factory, DC=local и во всех вложенных каталогах IIoTPlatform\config\ldap\standalone.xml
- LDAP сервер: DC2019.factory.local с портом 389
- Шифрование пароля – SHA
- Поле логина – sAMAccountName
- Поле почты – userPrincipalName
- Поле отображаемого имени – name

- Настройка СУБД IIoT Platform

Для настройки базы данных необходимо создать нужные для работы IIoT Platform таблицы, индексы и данные в них.

Для это запустите приложение по администрированию выбранной СУБД и выполните все SQL скрипты по созданию таблиц из каталога «IIoTPlatform/install/DB». Внимание: в скрипте для таблицы IIOTUser параметр «Dn» должен соответствовать установленному значению DN в используемом LDAP. Там же можно сразу указать требуемый часовой пояс (параметр «TimeZone»). Перечень допустимых для использования часовых поясов представлен в разделе «Часовые пояса» настоящего документа.

Для Oracle DB все файлы скриптов должны быть сохранены в кодировке ANSI. По умолчанию для преемственности в ОС Unix файлы сохранены в кодировке UTF-8

Для настройки подключения к базе данных необходимо отредактировать следующие параметры в файле standalone.xml в директории IIoTPlatform\config\appserver

pool-name="IIoTDS" PostgreSQL

pool-name="IIoTOraDS" Oracle Database

pool-name="IIoTMSDS" Microsoft SQL Serve

- Добавления файлов лицензий

Добавление лицензионных файлов выполняется простым копированием в каталог IIoTPlatform\settings\IIoT\license\

Посмотреть детальные сведения о добавленных лицензиях можно в IIoT Platform в разделе «Администрирование» -> «Управление лицензиями»

- Запуск IIoT Platform

IIoT Platform должен запускаться только после запуска IIoT Storage и IIoT Cloud.

Для запуска IIOT Platform необходимо следующее:

Выполнить команду для выдачи прав на выполнение: `sudo chmod +x`

`/usr/local/IIoT/IIoTPlatform/bin/start.sh`

Осуществить запуск: `sudo /usr/local/IIoT/IIoTPlatform/bin/start.sh`

В случае использования сервера LDAP отличного от стандартного (Apache DS) необходимо отредактировать колонку DN в таблице IIOTUser в соответствии значению DN используемого в LDAP сервере.

В свойствах таблицы необходимо указать «имеет OID»

- отредактировать столбец DN в соответствии с местонахождением пользователя `iiotadmin` (либо другого, в таком случае отредактировать колонку «login») в сервере LDAP
- при необходимости, в колонке «TimeZone» можно указать часовой пояс для каждого пользователя

3 Удаление ПО:

3.1 выполнить системные команды, действия:

```
sudo rm -Rf /usr/local/Platform
```

```
sudo rm -Rf /usr/local/IIoT_CLOUD
```

Приложение 3 к Протоколу № 15792/2024**Перечень используемых сокращений**

Astra Linux SE 1.7.5 – операционная система специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.7) с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 2023-1023SE17 (оперативное обновление 1.7.5);

ДВиС – дирекция внедрения и сопровождения;

ЗПС – замкнутая программная среда;

КСЗ – комплекс средств защиты;

МКЦ – мандатный контроль целостности;

МРД – мандатное управление доступом;

ОС – операционная система;

ПО – программное обеспечение «Защищенный программный комплекс ПоТ.Istok (серверная часть)» версии 1.0.1.