

УТВЕРЖДЕН

RU.64509942.00215-01 93 01-ЛУ

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «АТОМ.КОНТЕНТ»

Руководство Администратора

RU.64509942.00215-01 93 01

Листов 29

Инв № подл.	Подп. и дата	Взамен инв. №	Инв № дубл.	Подп. и дата

АННОТАЦИЯ

В данном документе описано руководство для технического обслуживания и прикладного администрирования программного обеспечения «Атом.Контент» (далее – ПО «Атом.Контент» или Система). В данном документе не рассматриваются вопросы установки и настройки сопутствующего ПО, в том числе ОС, СУБД, СХД.

СОДЕРЖАНИЕ

1. Общие сведения.....	5
1.1. Полное наименование программы	5
1.2. Краткое наименование программы	5
2. Действия по приемке поставленной системы	6
2.1. Проверка комплектности	6
2.2. Проверка маркировки и упаковки.....	7
2.3. Проверка соответствия контрольных сумм дистрибутива.....	7
3. Условия применения.....	8
3.1. Требования к техническому обеспечению	8
3.1.1. Описание технического обеспечения.....	8
3.1.1.1. Техническое обеспечение.....	8
3.1.1.2. Требования к оборудованию рабочих станций.....	8
3.1.1.3. Требования к пропускной способности каналов связи с ИС.....	9
3.1.2. Требования к ПО	9
3.1.2.1. Требования к системному ПО рабочих станций.....	9
3.1.2.2. Требования к ПО серверного оборудования	9
3.1.3. Требования к квалификации обслуживающего персонала.....	9
3.2. Принципы безопасной работы.....	10
4. Системное администрирование	12
4.1. Учетные записи на серверах для установки и администрирования	12
4.2. Установка и настройка ПО	12
4.2.1. Окружение для установки ПО.....	12
4.2.2. Установка и настройка системного ПО	13
4.2.3. Установка и настройка прикладного ПО	14
4.2.3.1. Размещение конфигурационных файлов из дистрибутива на сервере приложения .	14
4.2.3.2. Параметры application.properties.....	15
4.2.3.3. Загрузка образа приложения.....	17
4.2.3.4. Запуск приложения	17
4.2.4. Установка и настройка клиентского ПО.....	17
4.3. Операции по обслуживанию.....	17

<десятичный номер>

4.3.1. Мероприятия по текущему обслуживанию ПО «Атом.Контент».....	17
4.3.1.1. Порядок остановки системы	17
4.3.1.2. Порядок запуска системы.....	17
4.3.1.3. Смена паролей системных пользователей.....	18
4.3.2. Администрирование	19
4.3.2.1. Логирование	19
4.3.2.2. Обслуживание прикладной части Системы	19
4.3.2.3. Добавление файлового хранилища	19
4.3.3. Настройка способов аутентификации	20
4.3.3.1. Добавление SSL сертификатов для подключений по OAuth 2.0 или LDAPS.....	20
4.3.3.2. LDAP и LDAPS	20
4.3.3.3. OAuth 2.0.....	21
4.3.4. Обновление ПО «Атом.Контент»	22
4.3.4.1. Общие замечания по процедуре обновления ПО «Атом.Контент».....	22
4.3.4.2. Установка обновлений.....	22
4.3.4.3. Установка обновления на клиентские рабочие станции	23
4.4. Ошибки работы системы и способы их устранения	23
4.4.1. Вход в Систему невозможен из-за ввода неправильного имени пользователя.....	23
4.5. Превышение количества неуспешных попыток входа	23
4.6. Аварийные ситуации и действия по их устранению.....	24
Перечень терминов.....	25
Перечень сокращений.....	27

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Полное наименование программы

Полное название программы – программное обеспечение «Атом.Контент».

1.2. Краткое наименование программы

Краткое название программы – ПО «Атом.Контент».

2. ДЕЙСТВИЯ ПО ПРИЕМКЕ ПОСТАВЛЕННОЙ СИСТЕМЫ

После получения дистрибутива ПО «Атом.Контент» перед установкой администратор должен произвести приемку. Приемка Системы состоит из следующих действий:

- проверка комплектности;
- проверка маркировки и упаковки;
- проверка соответствия контрольных сумм дистрибутива.

2.1. Проверка комплектности

При проверке комплектности состав Системы должен соответствовать составу, представленному ниже (Таблица 1).

Таблица 1 – Комплектность

Исполнение	Наименование составной части и его обозначение	Примечание
1	Дистрибутив «Программное обеспечение «Атом.Контент» Исполнение 1» RU.64509942.00215-01	Поставляется на оптическом диске (DVD-R) в конверте для хранения. Установку программного обеспечения на аппаратную платформу выполняет изготовитель
2	Дистрибутив «Программное обеспечение «Атом.Контент» Исполнение 2» RU.64509942.00215-02	
№	Поставляемая документация на изделие	Примечание
	Комплект программной и конструкторской документации в составе на оптическом диске (DVD-R): <ul style="list-style-type: none"> – Спецификация RU.64509942.00215-01; – Технические условия RU.64509942.00215-01 90 01 ТУ; – Текст программы RU.64509942.00215-01 12 01; – Описание программы RU.64509942.00215-01 13 01; – Описание применения RU.64509942.00215-01 31 01; – Руководство системного программиста RU.64509942.00215-01 32 01; – Руководство программиста RU.64509942.00215-01 33 01; – Руководство оператора RU.64509942.00215-01 34 01; – Руководство по техническому обслуживанию RU.64509942.00215-01 91 01; 	1 шт.

	– заверенная копия выданного ФСТЭК России сертификата соответствия Системы сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00	1 шт.
	Формуляр RU.64509942.00215-01 30 01	1 шт., на бумажном носителе

2.2. Проверка маркировки и упаковки

Проверка маркировки и упаковки включает в себя:

- проверку целостности пластикового футляра и оптического диска;
- проверку маркировки комплекта поставки на наличие:
 - заводского номера;
 - товарного знака и наименования фирмы-разработчика;
 - наименования продукции;
 - года и месяца выпуска;
- проверку наличия в формуляре (раздел 10) идентификатора сертифицированной продукции, имеющего вид: РОСС RU.01.XXXXXX.YYYYYYY, где XXXXXX – номер сертификата соответствия на изделие, а YYYYYYY – заводский (серийный) номер изделия.

2.3. Проверка соответствия контрольных сумм дистрибутива

Проверка соответствия контрольных сумм файлов дистрибутива Системы проводится путем подсчета контрольных сумм файлов дистрибутива с помощью программы фиксации и контроля исходного состояния программного комплекса «ФИКС» (версия 2.0.2) по алгоритму «Уровень-1 программно».

Проверка считается успешной, если рассчитанные контрольные суммы совпадают с контрольными суммами, указанными в документе RU.64509942.00215-01 30 01 «Программное обеспечение «Атом.Контент». Формуляр».

3. УСЛОВИЯ ПРИМЕНЕНИЯ

3.1. Требования к техническому обеспечению

3.1.1. Описание технического обеспечения

3.1.1.1. Техническое обеспечение

Минимальные системные требования для функционирования изделия приведены ниже (Таблица 2).

Таблица 2 – Минимальные системные требования к серверам

Тип	Наименование
Процессор Оперативная память	2.5 ГГц, 4 ядра; 8 Гб ОЗУ
Жёсткий диск (свободное пространство, HDD)	Не менее 40 Гб
Сетевой адаптер	Ethernet

3.1.1.2. Требования к оборудованию рабочих станций

Таблица 3 – Минимальные системные требования к рабочим станциям клиентов

Тип	Наименование
Процессор Оперативная память	2 ГГц, 2 ядра; 4 Гб ОЗУ
Жёсткий диск (свободное пространство, HDD)	Не менее 40 Гб
Сетевой адаптер	Сетевая карта 100Mbit и выше

3.1.1.3. Требования к пропускной способности каналов связи с ИС

Таблица 4 – Требования к каналу связи с ИС

Характеристика канала связи	Показатель
Минимальная пропускная способность канала связи на одного пользователя	Не менее 98 кбит\с
Сетевая задержка при передачи данных в одном\двух направлениях	< 200мс
Потеря пакетов	<0,5

3.1.2. Требования к ПО

3.1.2.1. Требования к системному ПО рабочих станций

Минимальные системные требования к АРМ клиентской части: веб-браузер – Chromium версии 80 и выше, Яндекс.Браузер версии 20.2.3 и выше.

3.1.2.2. Требования к ПО серверного оборудования

- РЕД ОС версия 7.2 и выше;
- СУБД одна из:
 - Oracle Database версии 12с с используемыми компонентами Oracle Advanced Security и Oracle Database Vault;
 - Postgres Pro Enterprise Certified версии 11.7.4 и выше;
 - Postgres Pro Enterprise версии 12.2.1 и выше;
- OpenJDK/JRE 8 и выше.

3.1.3. Требования к квалификации обслуживающего персонала

Основными пользователями ПО «Атом.Контент» являются сотрудники организации, осуществляющие сопровождение и техническую поддержку систем, реализованных на базе ПО «Атом.Контент». Также пользователями ПО «Атом.Контент» могут являться сотрудники организации, участвующие в

процессах организации, обслуживаемых системами, реализованных на базе ПО «Атом.Контент».

Для эксплуатации ПО «Атом.Контент» необходимо наличие сотрудников, выполняющих роли:

- программист;
- системный программист;
- технический администратор;
- оператор (администратор);
- оператор (пользователь).

Обслуживание ПО «Атом.Контент» должны выполнять технические администраторы. В состав обслуживающего персонала приложения со стороны Заказчика должны входить специалисты, обученные и сертифицированные в авторизованных центрах подготовки персонала по следующим направлениям:

- администратор серверной ОС (Linux, РедОС);
- администратор системы хранения данных;
- администратор БД (Oracle, PostgresPro);
- администратор прикладных приложений развёрнутых с использованием технологий Java и Docker.

3.2. Принципы безопасной работы

В целях обеспечения безопасности в ходе работы с Системой технические администраторы обязаны:

- соблюдать требования внутренних нормативных и организационно-распорядительных документов по обеспечению ИБ, а также правила работы с Системой;
- не разглашать сведения конфиденциального характера, ставшие известными в ходе работы с Системой;
- выполнять работы в соответствии с установленным технологическим процессом обработки информации;

- осуществлять идентификацию только под своими учетными данными;
- проводить периодическую плановую смену пароля;
- хранить в тайне свои идентификационные и аутентификационные данные (логины и пароли);
- располагать экран монитора в помещении во время работы так, чтобы исключалась возможность ознакомления с отображаемой на них информацией посторонними лицами;
- контролировать работоспособность наложенных средств защиты информации;
- использовать только разрешенные и зарегистрированные съемные машинные носители информации.

4. СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

4.1. Учетные записи на серверах для установки и администрирования

- edms – учётная запись ОС владельца установки приложения;
- учетная запись ОС для обслуживания БД:
 - oracle – учётная запись ОС для обслуживания БД Oracle;
 - pgadm – учётная запись ОС для обслуживания БД PostgresPro;
- admin – учётная запись администратора в ПО «Атом.Контент».

4.2. Установка и настройка ПО

4.2.1. Окружение для установки ПО

Установка библиотек и пакетов осуществляется в соответствии с инструкциями и указаниями поставщиков общесистемного ПО.

Для развёртывания дистрибутива требуется операционная система Ред ОС 7.2 и выше. Предварительно необходимо выполнить следующий набор действий (требуется права доступа root):

- создать учётную запись владельца установки системы (edms);
- создать структуру файлов и папок:
 - mkdir -p /opt/app/opscr/docker-file/logs;
 - mkdir -p /opt/app/opscr/docker-file/config;
 - mkdir -p /opt/app/opscr/docker-storage;
- дать владельцу установки права на созданную структуру файлов и папок:
 - chown -R edms:docker /opt/app/opscr/docker-file;
 - chown -R edms:docker /opt/app/opscr/docker-storage;
- добавить в /etc/security/limits.conf скорректировав лимиты по файлам и процессам, например:
 - edms soft nproc 16384
 - edms hard nproc 16384

- edms soft nofile 65536
- edms hard nofile 65536
- скорректировать sysctl.conf:
 - vm.swappiness=10.

4.2.2. Установка и настройка системного ПО

Подготовка сервера приложений:

- установить ПО docker из репозитория Ред ОС:
 - например: yum install docker-ce.x86_64;
 - сконфигурировать docker согласно стандартам, принятым в рамках инфраструктуры Заказчика;
- включить владельца установки системы в группу docker для получения возможности управления контейнерами:
 - usermod -aG docker edms.

Подготовка сервера БД Postgres Pro:

- сконфигурировать БД Postgres Pro согласно стандартам, принятым в рамках инфраструктуры Заказчика;
- специфические требования к БД:
 - кодировка – ru_RU.utf8;
- выполнить создание пользователей и баз данных:

```
CREATE USER uto_product with createdb password 'password';
```

```
CREATE USER uto_product_secondary with createdb password 'password';
```

```
CREATE DATABASE uto_product;
```

```
CREATE DATABASE uto_product_secondary;
```

```
GRANT ALL PRIVILEGES ON DATABASE uto_product TO uto_product;
```

```
GRANT ALL PRIVILEGES ON DATABASE uto_product_secondary TO  
uto_product_secondary;
```

Подготовка сервера БД Oracle:

- сконфигурировать БД Oracle согласно стандартам, принятым в рамках инфраструктуры Заказчика;
- специфические требования к БД:
 - кодировка – AL32UTF8;
- выполнить создание пользователей и баз данных:

```
CREATE USER uto_product IDENTIFIED BY uto_product;
```

```
GRANT RESOURCE, CONNECT, SELECT_CATALOG_ROLE TO uto_product;
```

```
GRANT UNLIMITED TABLESPACE TO uto_product;
```

```
GRANT CREATE MATERIALIZED VIEW TO uto_product;
```

```
GRANT CREATE VIEW TO uto_product;
```

```
GRANT CREATE TABLE TO uto_product;
```

```
CREATE USER uto_product_secondary IDENTIFIED BY uto_product_secondary;
```

```
GRANT RESOURCE, CONNECT, SELECT_CATALOG_ROLE TO
```

```
uto_product_secondary;
```

```
GRANT UNLIMITED TABLESPACE TO uto_product_secondary;
```

```
GRANT CREATE MATERIALIZED VIEW TO uto_product_secondary;
```

```
GRANT CREATE VIEW TO uto_product_secondary;
```

```
GRANT CREATE TABLE TO uto_product_secondary.
```

4.2.3. Установка и настройка прикладного ПО

4.2.3.1. Размещение конфигурационных файлов из дистрибутива на сервере приложения

Разместить конфигурационный файл `application.properties` в директории `/opt/app/opscr/docker-file`.

Разместить контейнер сертификатов приложения Java - `caserts` в директории `/opt/app/opscr/docker-file`.

4.2.3.2. Параметры application.properties

Указываем следующие обязательные параметры в конфигурации application.properties:

- вместо <DBHOST> указываем хост основной БД (например, 1tsdo-s-pg01) в строке параметра primary.spring.datasource.url=jdbc:postgresql://<DBHOST>:5432/uto_product?escapeSyntaxCallMode=callIfNoReturn;
- вместо <DBHOST> указываем хост второй БД (например, 1tsdo-s-pg01) в строке параметра secondary.spring.datasource.url=jdbc:postgresql://<DBHOST>:5432/uto_product_secondary?escapeSyntaxCallMode=callIfNoReturn;
- логины и пароли для подключения к основной и второй БД задаются параметрами:

```
primary.spring.datasource.username=${uto.primary.jdbc.user}
primary.spring.datasource.password=${uto.primary.jdbc.password}
secondary.spring.datasource.username=${uto.primary.jdbc.user}
secondary.spring.datasource.password=${uto.primary.jdbc.password}
```

При необходимости указываем следующие **дополнительные** параметры в конфигурации application.properties:

- (опционально) При первой установке приложения на новый ландшафт с пустой БД или при возникновении необходимости удалить текущую структуру и данные БД и создать структуру БД используются параметры:

```
primary.spring.liquibase.drop-first=true
secondary.spring.liquibase.drop-first=true
```

Перед последующими запусками или рестартами необходимо вернуть значение false для данных параметров.

- (опционально) Для включения планировщика джобов на данном инстансе приложения добавить параметры, например:

```
primary.uto.datastore.job.schedule-enabled=true
```

```
primary.uto.datastore.job.sync-cron=*/30 * * * * *
```

```
secondary.uto.datastore.job.schedule-enabled=true
```

```
secondary.uto.datastore.job.sync-cron=*/30 * * * * *
```

Где `primary.uto.datastore.job.sync-cron` и `secondary.uto.datastore.job.sync-cron` опциональные параметры, позволяющие настраивать частоту опроса планировщиком списка джобов в формате crontab (см. Рисунок 1)

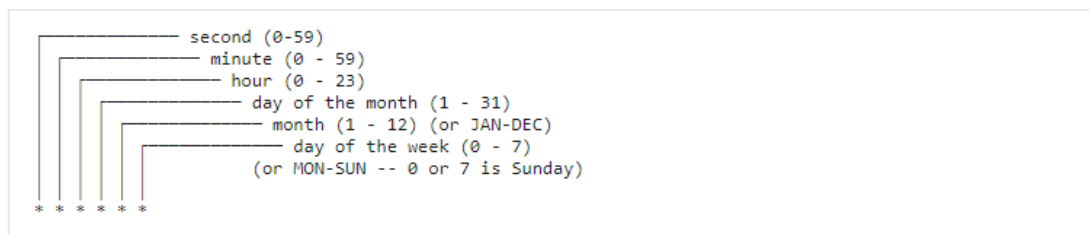


Рисунок 1 – Формат значения для параметров `primary.uto.datastore.job.sync-cron` и `secondary.uto.datastore.job.sync-cron`

Значение по умолчанию для `primary.uto.datastore.job.schedule-enabled` и `secondary.uto.datastore.job.schedule-enabled` – `false`.

- (опционально) Если требуется загрузить демонстрационный набор объектов в структуру репозитория (`demo`) следует заменить параметры:

```
primary.spring.liquibase.change-log=classpath:/db/migration/releases/current.xml
```

```
secondary.spring.liquibase.change-log=classpath:/db/migration/releases/current.xml
```

строками:

```
primary.spring.liquibase.change-log=classpath:/db/migration/demo/current.xml
```

```
secondary.spring.liquibase.change-log=classpath:/db/migration/demo/current.xml
```

после первого запуска приложения вернуть прежние значения параметров (`releases`);

- максимальное количество тредов встроенного сервера приложений регулируется добавлением параметра `server.tomcat.threads.max`, значение по умолчанию:

- `server.tomcat.threads.max=200;`

- допустимое количество неудачных попыток входа для встроенного механизма авторизации:
 - `uto.security.max-auth-attempts=3`;
- интервал смены пароля для встроенного механизма авторизации:
 - `uto.security.password-expires-in-days=90`.

4.2.3.3. Загрузка образа приложения

Разместить полученный вместе с дистрибутивом образ `rafile-app` по пути `/opt/app/opscr/docker-file`.

Выполнить `docker load -i /opt/app/opscr/docker-file/rafile-app`.

4.2.3.4. Запуск приложения

Запустить приложение в соответствии с разделом 4.3.1.2.

4.2.4. Установка и настройка клиентского ПО

Требования к специализированным настройкам на АРМах пользователей (предварительно не требуются).

4.3. Операции по обслуживанию

4.3.1. Мероприятия по текущему обслуживанию ПО «Атом.Контент»

4.3.1.1. Порядок останова системы

- остановить контейнер:
 - `docker stop rafileapp`;
- при необходимости остановить БД.

4.3.1.2. Порядок запуска системы

- убедиться, что БД запущена, если нет – запустить;

- запустить контейнер, для этого выполнить команду следующего вида (параметры и мэппинг атрибутов предварительно скорректировать в соответствии с окружением):
 - `docker run -u `stat -c "%u:%g" /opt/app/opscr/docker-storage` --rm --detach --name rfileapp -e TZ=Europe/Moscow -e JAVA_OPTS='-Xmx12g -Xms6g ' -v /opt/app/opscr/docker-file/logs:/logs -v /opt/app/opscr/docker-file/application.properties:/application.properties -v /opt/app/opscr/docker-file/cacerts: /usr/lib/jvm/jdk-8u292-bellsoft-x86_64/jre/lib/security/cacerts -v /opt/app/opscr/docker-storage:/opt/app/opscr/docker-storage -p8080:8080 rfile-app;`
- проконтролировать запуск приложения по логу:
 - `/opt/app/opscr/docker-file/logs/spring-boot-logger.log`.

4.3.1.3. Смена паролей системных пользователей

Пароли пользователей ОС меняются средствами ОС Linux.

Пароли пользователей БД меняются средствами БД.

Пароли технических учетных записей из ActiveDirectory (LDAPS и внешнего сервиса аутентификации, поддерживающего протокол OAuth 2.0) меняются средствами соответствующего сервиса.

Пароли технических учетных записей системы со способом аутентификации «Внутренний» меняются следующим образом:

- войти в «Модуль администрирования» ПО «Атом.Контент» по ссылке вида `http://hostname:8080/`;
- открыть раздел «Администрирование/Пользователи»;
- развернуть поисковый фильтр и найти нужного пользователя;
- открыть карточку свойств пользователя двойным кликом по строке;
- отредактировать поле пароль;
- нажать «Сохранить» или «Сохранить и закрыть».

4.3.2. Администрирование

4.3.2.1. Логирование

Директории хранения логов безопасности и приложения задается при запуске системы (см. раздел 4.3.1.2):

- `spring-boot-logger.log` – основной лог, в котором фиксируются ошибки в работе `java`-методов и информация для дебага;
- `security.log` – аудит событий безопасности;
- `archived` – каталог, куда перемещаются логи после ротации;
- `docker logs -f rafileapp` – способ посмотреть логи уровня ПО `docker`.

Максимальный объем хранимых логов и необходимость очистки архивный логов определяет Администратор в соответствии с внутренними регламентами предприятия.

4.3.2.2. Обслуживание прикладной части Системы

Контроль свободного места в хранилищах осуществляется в соответствии с инструкциями и рекомендациями поставщика ОС.

4.3.2.3. Добавление файлового хранилища

Авторизоваться в системе (например, `http://hostname:8080/`) с правами Администратора и перейти в структуре:

Администрирование – Данные – Хранилища – Конфигурация – Действия – Создать хранилище.

На выбор:

- файловое хранилище;
- ВЛОВ-хранилище – в БД;
- внешнее хранилище.

При выборе «Файловое хранилище» предварительно потребуется создать:

Администрирование – Данные – Системные пути – Конфигурация – Действия – Создать путь.

При этом важно указать «Полный путь до объекта в хранилище», например, «/opt/app/opscr/docker-storage/storage01». Важно учесть мэппинг данного пути из контейнера в файловую систему основной ОС (см. раздел 4.3.1.2).

4.3.3. Настройка способов аутентификации

4.3.3.1. Добавление SSL сертификатов для подключений по OAuth 2.0 или LDAPS

Получить открытую часть SSL сертификата, используемую для подключения к внешнему сервису аутентификации по OAuth 2.0 или LDAPS, и импортировать данный сертификат в хранилище:

```
keytool -import -keystore /opt/app/opscr/docker-file/config/cacerts -alias <ссылка на приложение> -file certificate.crt
```

Выполнить перезапуск приложения (см. раздел 4.3.1.1 и 4.3.1.2).

4.3.3.2. LDAP и LDAPS

Авторизоваться в системе (например, <http://hostname:8080/>) с правами Администратора и перейти в структуре:

Администрирование – Аутентификация – LDAP – Конфигурация – Действия – Создать LDAP конфигурацию.

Заполнить обязательные поля:

- Имя объекта – название подключения;
- JDBC /IP сервера – адрес подключения;
- Режим SSL – выбираем с TLS;
- TCP-порт (подключение с TLS) – указываем порт для подключения (если порт не изменяли, то указать 636).

4.3.3.3. OAuth 2.0

Авторизоваться в системе (например, http://имя_сервера_приложения:8080/) с правами Администратора и перейти в структуре:

Администрирование – Аутентификация – OAuth2 – Конфигурация – Действия – Создать OAuth2 конфигурацию.

Заполнить обязательные поля:

- Наименование – название подключения;
- Описание – описание подключения;
- Тип авторизации – выбрать один из доступных вариантов согласно спецификации OAuth2 (<https://developers.onelogin.com/openid-connect/>);
- Адрес авторизации (Например: <https://fs.test.local/adfs/oauth2/authorize>);
- Идентификатор клиентского приложения (Например: c78852c1-2526-40cb-b634-88cf176685e7).

Примечание: «Идентификатор клиентского приложения» получаем на стороне внешнего сервиса аутентификации, поддерживающего протокол OAuth 2.0, при настройке группы приложений для соответствующего ландшафта.

- Перенаправление после авторизации (Например: <http://hostname:8080/login/oauth2/code/adfs>).

Примечание: На стороне внешнего сервиса аутентификации, поддерживающего протокол OAuth 2.0, выполняется настройка, разрешающая для «Идентификатор клиентского приложения» выполнить перенаправление по ссылке «Перенаправление после авторизации».

- Имя пользователя;
- Адрес получения информации о пользователе (например: <https://fs.test.local/adfs/userinfo>);
- Адрес получения токена (например: <https://fs.test.local/adfs/oauth2/token>);
- Адрес получения ключа для подписания приложения (например: <https://fs.test.local/adfs/discovery/keys>).

4.3.4. Обновление ПО «Атом.Контент»

4.3.4.1. Общие замечания по процедуре обновления ПО «Атом.Контент»

Для бесперебойной работы ПО «Атом.Контент» должны быть полностью отключены механизмы автоматического обновления системного ПО, прикладного ПО и любого стороннего ПО, участвующего в работе ПО. Установка обновлений должна осуществляться только после проверки на второстепенных средах (тестирования и разработки).

Настоящий регламент не рассматривает процедуру обновления микропрограмм аппаратного комплекса.

Процедура обновления может быть произведена только после разработки Плана проведения работ, включающего:

- подробное описание подготовительных работ для проведения обновления;
- описание шагов выполнения обновления;
- план тестирования функционала ПО после обновления;
- детальный план возврата системы в исходное состояние при неудачном выполнении работ.

Каждый из этапов плана должен иметь заданные временные рамки выполнения и ответственных за выполнение работ специалистов.

4.3.4.2. Установка обновлений

- распаковать дистрибутив;
- выполнить остановку приложения (см. раздел 4.3.1.1);
- выполнить загрузку образа (см. раздел 4.2.3.4);
- выполнить дополнительные инструкции перед запуском приложения, если они прилагались к дистрибутиву;
- выполнить запуск контейнера (см. раздел 4.3.1.2);
- выполнить дополнительные инструкции после запуска приложения, если они прилагались к дистрибутиву.

4.3.4.3. Установка обновления на клиентские рабочие станции

Автоматическое обновление ОС, СрЗИ и браузеров на клиентских рабочих станциях должно быть отключено. При проведении работ по установке обновлений необходимо согласование устанавливаемых версий обновлений браузера с разработчиком ПО «Атом.Контент».

Установка патчей безопасности, системных драйверов выполняется согласно внутренней политике АО «Гринатом».

4.4. Ошибки работы системы и способы их устранения

4.4.1. Вход в Систему невозможен из-за ввода неправильного имени пользователя

Идентификация: при попытке аутентификации пользователю выводится сообщение вида «Неверный логин или пароль».

Способ устранения: убедиться, что пользователь есть в системе и ввести корректное имя пользователя.

4.5. Превышение количества неуспешных попыток входа

Идентификация: при попытке аутентификации пользователю выводится сообщение вида «Ошибка аутентификации. Обратитесь к администратору».

Способ устранения:

- войти в «Модуль администрирования» ПО «Атом.Контент» по ссылке вида <http://hostname:8080/>;
- открыть раздел «Администрирование/Пользователи»;
- развернуть поисковый фильтр и найти нужного пользователя;
- открыть карточку свойств пользователя двойным кликом по строке;
- отредактировать поле «Статус» поставив значение «Активен»;
- нажать «Сохранить» или «Сохранить и закрыть».

4.6. Аварийные ситуации и действия по их устранению

Таблица 5 – Перечень действий администраторов при сбоях ПО «Атом.Контент»

Сервис	Вид сбоя	Последовательность действия для диагностики сбоя	Последовательность действия при сбое
Приложение «Атом.Контент»	Приложение недоступно	Проанализировать лог приложения, см. раздел 4.3.1.1	Выполнить перезапуск, см разделы см. раздел 4.3.1.1 и см. раздел 4.3.1.2

ПЕРЕЧЕНЬ ТЕРМИНОВ

Ниже (Таблица 6) приведены значения терминов, которые используются в настоящем документе, если по тексту прямо не указано иное.

Таблица 6 – Термины и определения

Термин	Определение
Chromium	На основе Chromium создан браузер Google Chrome, а также ряд других альтернативных веб-обозревателей
Oracle Advanced Security	Дополнительный вариант для сред баз данных Oracle. Расширяет возможности Oracle Net Services в области вычислений баз данных, обеспечивая безопасность сети, безопасность корпоративных пользователей, безопасность инфраструктуры с открытым ключом и шифрование данных для пользователей баз данных Oracle
Oracle Database	Объектно-реляционная система управления базами данных компании Oracle
Oracle Database Vault	Опция безопасности базы данных Oracle, позволяющая контролировать или при необходимости исключить доступ администратора СУБД к данным приложений, усилить защиту структур СУБД от несанкционированного доступа и реализовать возможности, обеспечивающие динамическую настройку политик безопасности за счет многофункциональных внутренних механизмов самой СУБД
Postgres Pro Enterprise	Российская коммерческая система управления базами данных для крупных клиентов, базирующаяся на свободной СУБД PostgreSQL
Postgres Pro Enterprise Certified	Сертифицированная версия СУБД Postgres Pro Enterprise (сертификат ФСТЭК №4063)
Авторизация	Процесс предоставления прав, включая предоставление прав на доступ
Администрирование системы	Планирование, установка и обслуживание системы
Аппаратная платформа	Аппаратное обеспечение вычислительных систем, включая тип процессора
Аутентификация	Проверка подлинности предъявленного пользователем идентификатора
База данных	Совокупность данных, хранимых в соответствии со схемой данных, манипулирование которыми выполняют в соответствии с правилами средств моделирования данных

Термин	Определение
Идентификация	Процедура, в результате выполнения которой для субъекта идентификации выявляется его идентификатор, однозначно идентифицирующий этого субъекта в информационной системе
Конфиденциальность	Свойство, заключающееся в том, что информация не может быть доступной или раскрытой для неавторизованных лиц, объектов или процессов
Ландшафт; Системный ландшафт	Группа взаимосвязанных систем, объединенных по признаку функционального предназначения. В рамках данного документа под ландшафтом понимается продуктивная группа систем
Модуль администрирования	Модуль Системы, предоставляющий возможности системного администрирования
Операционная система	Комплекс взаимосвязанных программ, предназначенных для управления ресурсами компьютера и организации взаимодействия с пользователем
Пользователь	Пользователь ПО «Атом.Контент»
Программное обеспечение	Программа или множество программ, используемых для управления компьютером
РЕД ОС	Операционная система на базе ядра Linux, являющаяся составным продуктом, построенным на базе решений с открытым исходным кодом и собственных разработок. Занесена в Единый реестр российских программ
Сведения конфиденциального характера	Сведения, попадающие под понятия «КТ», «ДСП», ПДн», обрабатываемые в ПО «Атом.Контент»
Система	Программное обеспечение «Атом.Контент»
Системное программное обеспечение	Операционная система и входящие в ее состав утилиты

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Ниже (Таблица 7) приведен список сокращений, используемых в настоящем документе, и их расшифровка.

Таблица 7 – Сокращения и расшифровка

Сокращение	Расшифровка
BLOB	Binary Large Object – решение корпорации Майкрософт для хранения объектов в облаке. Хранилище BLOB-объектов оптимизировано для хранения больших объемов неструктурированных данных
FQDN	Fully Qualified Domain Name – полное имя домена, не имеющее неоднозначностей в определении. Включает в себя имена всех родительских доменов иерархии DNS
IP (адрес)	Internet Protocol – уникальный числовой идентификатор устройства в компьютерной сети, работающей по протоколу IP
JDBC	Java Database Connectivity – платформенно-независимый промышленный стандарт взаимодействия Java-приложений с различными СУБД, реализованный в виде пакета java.sql, входящего в состав Java SE. JDBC основан на концепции так называемых драйверов, позволяющих получать соединение с базой данных по специально описанному URL
JDK	Java Development Kit – распространяемый компанией Oracle Corporation комплект разработчика приложений на языке Java, включающий в себя компилятор Java, стандартные библиотеки классов Java, примеры, документацию, различные утилиты и исполнительную систему Java
LDAP	Lightweight Directory Access Protocol – протокол, использующий TCP/IP и позволяющий производить операции аутентификации (bind), поиска (search) и сравнения (compare), а также операции добавления, изменения или удаления записей. Открытый стандартизированный протокол, применяемый для работы с различным реализациям служб каталогов, в том числе и Active Directory
LDAPS	Lightweight Directory Access Protocol Security
OAuth	Открытый протокол (схема) авторизации, который позволяет предоставить третьей стороне ограниченный доступ к защищенным ресурсам пользователя без необходимости передавать ей (третьей стороне) логин и пароль
TCP	TCP (IP идентификатор 6) – «гарантированный» транспортный механизм с предварительным установлением соединения, предоставляющий приложению надежный поток данных, дающий уверенность в безошибочности получаемых данных, перезапрашивающий данные в случае потери и устраняющий дублирование данных
TLS	Transport Layer Security – протокол, который поддерживает

Сокращение	Расшифровка
	защищенную передачу данных между клиентом и сервисом
АРМ	Автоматизированное рабочее место
БД	База данных
ИБ	Информационная безопасность
ОЗУ	Оперативное запоминающее устройство
ОС	Операционная система
ПО	Программное обеспечение
СрЗИ	Средства защиты информации
СУБД	Система управления базами данных
ФСТЭК	Федеральная служба по техническому и экспортному контролю

