Экз.№_____

СЕРВИС АВТОМАТИЗАЦИИ ВЫПУСКА СЕРТИФИКАТОВ

СПЕЦИАЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ АВТОМАТИЗАЦИИ ВЫПУСКА СЕРТИФИКАТОВ TRUSTCIA (СПО TRUSTCIA)

Руководство администратора

Листов 36

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

2025

Литера _____

АННОТАЦИЯ

Настоящий документ является руководством администратора и содержит сведения о специальном программном обеспечении автоматизации выпуска сертификатов TrustCIA Сервиса автоматизации выпуска сертификатов, а также порядке его установки, настройки и администрирования.

СОДЕРЖАНИЕ

ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

1.1. В документе используются следующие термины и определения:

МП	–	Мобильное или десктопное приложение банка для работы клиента с платформой цифрового рубля, установленное на устройстве пользователя
Пользователь	–	Клиент банка-участника Платформы цифрового рубля - физическое лицо, юридическое лицо или индивидуальный предприниматель, имеющие доступ к платформе цифрового рубля в целях совершения операций с цифровыми рублями
Потребитель	–	Кредитные организации (банки), являющиеся участниками Платформы цифрового рубля
ПУЦ	–	Подчиненный УЦ для выпуска сертификатов УНЭП пользователям
Сервер ДБО	–	Сервер ДБО, обеспечивающий аутентификацию Пользователя как клиента банка и маршрутизацию запросов из МП в сервис автоматизации выпуска сертификатов.
Сервис автоматизации выпуска сертификатов (САВС)	–	Сервис автоматизации процесса выпуска сертификатов безопасности и сертификатов УНЭП Пользователям
Сертификат безопасности	–	TLS-сертификат для обеспечения построения двухстороннего ГОСТ-TLS соединения
УЦ безопасности	–	УЦ для выпуска сертификатов безопасности пользователям
TLS	–	Протокол защиты транспортного уровня.
TLS-сертификат	–	Цифровой сертификат, позволяющий использовать зашифрованное соединение с использованием протокола TLS

1.2. В документе используются следующие сокращения:

ДБО	–	Дистанционное банковское обслуживание
ЕСИА	–	Единая система идентификации и аутентификации
ОС	–	Операционная система
ПлЦР	–	Платформа Цифрового рубля Банка России
ПУЦ	–	Подчиненный УЦ
САВС	–	Сервис автоматизации выпуска сертификатов
СКЗИ	–	Средство криптографической защиты информации
СПО	–	Специальное программное обеспечение
СПО TrustCIA	–	Специальное программное обеспечение автоматизации выпуска сертификатов
УНЭП	–	Усиленная неквалифицированная электронная подпись
УЦ	–	Удостоверяющий центр
ЦР	–	Цифровой рубль
TLS	–	Transport Layer Security (англ.)
ЦП	–	Цифровой профиль гражданина

1. ОБЩИЕ СВЕДЕНИЯ

1.1 Наименование и обозначение

Полное наименование: Специальное программное обеспечение автоматизации выпуска сертификатов TrustCIA.

Краткое наименование: СПО TrustCIA.

1.2 Область применения

Специальное программное обеспечение автоматизации выпуска сертификатов TrustCIA (далее - СПО TrustCIA) применяется в Сервисе автоматизации выдачи сертификатов (далее – САВС), целью которого является предоставление потребителям возможности автоматизации выпуска сертификатов безопасности и сертификатов УНЭП, создаваемых на базе российских криптографических алгоритмов и используемых пользователями для работы на Платформе Цифрового рубля Банка России (далее – ПлЦР).

Потребителями САВС являются кредитные организации (банки), являющиеся участниками ПлЦР.

Пользователями САВС являются физические лица, физические лица-самозанятые, юридические лица, являющиеся клиентами потребителей и желающие получить доступ к Платформе цифрового рубля с целью совершения операций с Цифровым рублем.

САВС состоит из следующих компонентов:

1. СПО TrustCIA;
2. Специальное программное обеспечение TrustGate с расширением для работы с ЦП (далее – СПО TrustGate);
3. Средство криптографической защиты информации – ViPNet CSP 4, класса КС3 (далее – ViPNet CSP).

1.3 Комплект поставки

В комплект поставки СПО TrustCIA входят:

- дистрибутив СПО;
- документы «TrustCIA. Руководство администратора», «TrustCIA. Руководство программиста»

СПО TrustCIA поставляется в виде, требующем установки и настройки. Установка СПО выполняется администратором.

1.4 Краткое описание функций

САВС обеспечивает выполнение следующих основных и сервисных функций:

1. Основные функции:
   - прием запросов на проведение идентификации и аутентификации в ЕСИА и получение данных Цифрового профиля, поступающих от внешних систем;
   - прием запросов на выпуск сертификатов безопасности и сертификатов УНЭП, поступающих от внешних систем;
   - форматно-логический контроль структуры и состава данных запросов на сертификат и выпускаемых сертификатов;
   - проверка ЭП под файлами запросов на сертификат;
   - передача в ПУЦ и УЦ безопасности запросов на выпуск сертификатов;
   - предоставление информации о статусе запросов на выпуск сертификатов по запросам от внешних систем;
   - прием запросов на отзыв сертификатов безопасности и сертификатов УНЭП, поступающих от внешних систем;
   - передача в ПУЦ и УЦ безопасности запросов на отзыв сертификатов;
   - предоставление информации о статусе запросов на отзыв сертификатов по запросу от внешних систем;

- предоставление актуальных файлов списков отозванных сертификатов (далее – CRL) по запросу от внешних систем;
- регистрация событий.

2. Сервисные функции:
   - предоставление информации о работоспособности сервиса.

В целях реализации функций САВС, СПО TrustCIA обеспечивает:

1. Прием из внешних ИС (ДБО):
   - запросов в рамках проведения аутентификации пользователя ФЛ в ЕСИА и получение данных цифрового профиля;
   - запросов на первичное получение сертификатов пользователем, включающих самоподписанные запросы на выпуск сертификатов в формате #pkcs10;
   - запросов на получение нового сертификата на основании действующего, включающих самоподписанные запросы на выпуск сертификатов в формате #pkcs10, и откреплённые подписи запроса на сертификат ключом действующего сертификата в формате #pkcs7;
   - запросов на отзыв сертификатов пользователя, включающих файл отзываемого сертификата;
   - запросов получения статусов обработки запросов;
   - запросов на получение файлов CRL.
2. Передачу в СПО TrustGate:
   - запросов в рамках проведения аутентификации пользователя ФЛ в ЕСИА и получение данных цифрового профиля;
   - запросов проверки электронных подписей;
   - запросов формирования электронных подписей, требуемых для организации взаимодействия с ПУЦ / УЦ безопасности.
3. Прием из СПО TrustGate:
   - ответов в рамках проведения аутентификации пользователя ФЛ в

ЕСИА и получение данных цифрового профиля;

- результатов проверки электронной подписи;
- электронных подписей, требуемых для организации взаимодействия с ПУЦ / УЦ безопасности.

4. Передачу во внешние ИС (ДБО) в рамках ответов на запросы:
   - ответов в рамках проведения аутентификации пользователя ФЛ в ЕСИА и получение данных цифрового профиля;
   - информации о статусе запроса на выпуск сертификата, включающей в случае успеха файл выпущенного сертификата;
   - информации о статусе запроса на отзыв сертификата;
   - файлов CRL.
5. Валидацию запросов на сертификатов в объеме:
   - проведение форматно-логического контроля полей запроса на сертификат;
   - проверка соответствия данных ФИО, СНИЛС пользователя из запроса на сертификат с его ФИО, СНИЛС, полученными в рамках проведения аутентификации пользователя ФЛ в ЕСИА и получения данных цифрового профиля;
   - проверка соответствия данных пользователя из запроса на сертификат с его данными, переданными их внешней ИС (ДБО) в рамках запроса выпуска сертификата;
   - проверка соответствия данных пользователя из запроса на сертификат с данными владельца сертификата, указанными в действующем сертификате, которым был подписан запрос на сертификат.

6. Передачу успешно прошедших проверку запросов в УЦ Безопасности/ПУЦ:
   - запросов на сертификаты;
   - запросов на отзыв сертификатов

7. Получение из УЦ Безопасности/ПУЦ:
   - файлов выпущенных сертификатов;
   - статусов приема запросов на отзыв сертификатов;
   - файлов CRL.

8. Валидацию выпущенных сертификатов путем форматно-логического контроля полей выпущенного сертификата на соответствие стандарту «ПлЦР. Правила заполнения полей сертификатов»;

9. Мониторинг работоспособности используемых экземпляров средств УЦ.

Примечание. Мониторинг работоспособности не осуществляется в случае использования в качестве средств УЦ Программного комплекса «ViPNet Удостоверяющий центр 4» (версия 4.6.9).

В СПО TrustCIA реализована регистрация следующих событий:

- получение запросов в рамках проведения аутентификации пользователя ФЛ в ЕСИА и получение данных цифрового профиля;
- получение запросов на выпуск сертификата;
- результат проверки корректности запроса на сертификат;
- результат проверки подписи запроса на сертификат;
- направление запроса на выпуск сертификата в УЦ Безопасности/ПУЦ;
- направление запроса на отзыв сертификата в УЦ Безопасности/ПУЦ;
- получение результата обработки запроса на выпуск сертификата в УЦ Безопасности/ПУЦ;
- получение результата обработки запроса на отзыв сертификата в УЦ Безопасности/ПУЦ;
- результат проверки выпущенного сертификата на соответствие стандарту «ПлЦР. Правила заполнения полей сертификатов»;
- получение ошибок при выполнении основных сценариев использования.

В журнале сохраняются следующие сведения о зарегистрированном событии:

– дата и время события;

– тип события;

– содержание события.

1.5 Уровень подготовки администратора

Для правильной и бесперебойной работы СПО TrustCIA и САВС в целом, администратор должен:

1. Обладать практическим опытом выполнения работ по установке, настройке и администрированию программных и технических средств, серверного оборудования и программного обеспечения.

2. Знать:

- основы функционирования операционных систем (далее – ОС) Linux, Windows Server, Windows, а также СУБД PostgreSQL и Microsoft SQL Server;

- содержание и порядок настройки аппаратной части ПЭВМ и серверов;

- принципы работы сетевых протоколов и построения компьютерных сетей;

- основы организации данных, способы и механизмы управления ими;

- порядок настройки и работы программ, входящих в состав САВС;

- содержание эксплуатационных документов.

1.6 Ограничения по установке общесистемного и специального ПО на сервер СПО

К установке общесистемного и специального ПО на сервер СПО TrustCIA допускаются администраторы, изучившие эксплуатационную документацию на соответствующее ПО и на СПО TrustCIA.

На сервер СПО TrustCIA допускается устанавливать и использовать только лицензионное ПО фирм-производителей.

Запрещается устанавливать средства отладки, разработки и трассировки ПО. Если средства отладки приложений необходимы для технологических

потребностей эксплуатирующей организации, то их использование должно быть санкционировано администратором ИБ.

Кроме того, на сервер СПО TrustCIA запрещается также устанавливать и использовать ПО, позволяющее:

- модифицировать содержимое произвольных областей памяти;
- модифицировать собственный код и код других подпрограмм;
- модифицировать память, выделенную для других подпрограмм;
- передавать управление в область собственных данных и данных других подпрограмм;
- несанкционированно модифицировать файлы, содержащие исполняемые коды, при их хранении на жестком диске;
- повышать предоставленные пользователям привилегии;
- модифицировать настройки ОС;
- использовать недокументированные фирмой-разработчиком ОС функции;
- отслеживать и запоминать нажатия клавиш и другие действия пользователя.

1.7 Требования к эксплуатации сервера

При эксплуатации сервера, на котором развернуто СПО TrustCIA, следует руководствоваться следующими рекомендациями:

1) Размещение сервера, специальное оборудование, организация режима и охраны места установки, эксплуатации и хранения сервера, должны обеспечивать:

- безопасность информации, обрабатываемой сервером;
- невозможность доступа лиц, не допущенных к работе с СПО TrustCIA, к наблюдению за работой с СПО и его эксплуатационной документации;
- исключение возможности умышленного повреждения или кражи сервера с СПО.

2) Должны быть приняты меры по исключению несанкционированного доступа (далее – НСД) к серверу СПО посторонних лиц. Порядок допуска к серверу

должен определяться внутренней инструкцией, которая разрабатывается с учетом специфики и условий функционирования эксплуатирующей организации.

3) При эксплуатации СПО TrustCIA в эксплуатирующей организации должны выполняться требования по эксплуатации компонентов, входящих в состав САВС.

2. НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ

2.1 Назначение

СПО TrustCIA предназначено для автоматизации процессов выпуска сертификатов безопасности и сертификатов УНЭП, создаваемых на базе российских криптографических алгоритмов, для пользователей платформы цифрового рубля в рамках инфраструктуры САВС.

2.2 Условия применения

СПО TrustCIA предназначено для функционирования в среде ОС Astra Linux Special Edition версия 1.7.

СПО TrustCIA предназначено для эксплуатации на серверном оборудовании, поддерживающем архитектуру x86, x86-64 с минимальной рекомендуемой производителем ОС аппаратной конфигурацией.

На серверном оборудовании должно быть установлено дополнительное программное обеспечение, указанное в таблице .

Таблица 1 – Перечень требуемого дополнительного программного обеспечения

Название	Версия	Назначение
Redis	Последняя стабильная версия	Предназначен для хранения кэша. Может использоваться как брокер сообщений. Рекомендуется использовать кластер
PostgreSQL	Последняя стабильная версия	Реляционная база данных Рекомендуется использовать кластер
docker	20.10.2+	Предназначен для сборки образов и запуска контейнеров
docker-compose	1.29.2+	Предназначен для использования при запуске контейнеров
zip	Последняя стабильная версия	Предназначен для разархивации дистрибутива

Установка, предварительная настройка и эксплуатация СПО TrustCIA осуществляется в соответствии с эксплуатационной документацией, входящей в комплект поставки.

СПО TrustCIA может быть установлено на виртуальные машины, имеющие характеристики не хуже указанных для аппаратных (техническим) средств.

При установке СПО TrustCIA рекомендуется дополнительно руководствоваться документацией на ОС. На сервере перед установкой СПО TrustCIA должен быть установлен актуальный пакет обновления ОС и все известные критические обновления, опубликованные производителем ОС.

Перед началом эксплуатации СПО TrustCIA необходимо установить все доступные обновления используемых версий ПО среды функционирования.

2.3 Режим работы

Режим работы СПО TrustCIA – непрерывный, круглосуточный (24/7/365).

Максимально допустимое время приостановления работы СПО TrustCIA для выполнение технических работ, а также в случаях сбоев и отказов функционирования, – не более 2 часов. Для достижения заданных показателей оборудование СПО TrustCIA может находиться в «холодном» и «горячем» резерве.

2.4 Ограничения по применению

СПО TrustCIA используется совместно с СПО TrustGate в рамках инфраструктуры САВС.

На сервере СПО TrustGate должен быть размещен контейнер с ключами ЭП СПО TrustCIA для обеспечения формирования электронных подписей, требуемых для организации взаимодействия с экземплярами средств УЦ.

СПО TrustCIA может использоваться со следующими средствами УЦ:

- Программный комплекс «ViPNet Удостоверяющий центр 4» (версия 4.6.9);
- Изделие «Программно-аппаратный комплекс «Удостоверяющий центр «КриптоПро УЦ» версии 2.0» (варианты исполнения 5, 6, 9, 10, 15, 16).
- Программно-аппаратный комплекс «ViPNet Удостоверяющий центр 5» (версия 5.1.0).

Для взаимодействия СПО TrustCIA со средствами УЦ требуется обеспечить защищенное ГОСТ-TLS соединение средствами среды функционирования САВС в соответствии с Правилами пользования на указанные средства удостоверяющего центра.

Примечание. Для реализации защищенного ГОСТ-TLS соединения со средствами удостоверяющего центра рекомендуется использовать следующее программное обеспечение:

- Nginx и ViPNet OSSL.
- Nginx и ViPNet PKI Client.
- Stunnel и ViPNet OSSL.

При использовании программно-аппаратного комплекса «Удостоверяющий центр «КриптоПро УЦ» версии 2.0» в исполнении 15, 16 получение списков отозванных сертификатов доступно только при работе СПО TrustCIA с адресами публикации сформированных файлов CRL в среде функционирования потребителя.

СПО TrustCIA поддерживает возможность работы с несколькими экземплярами средств УЦ, обеспечивающих управление жизненным циклом сертификатов одноного типа, в целях реализации отказоустойчивого исполнения САВС.

3. ПОРЯДОК УСТАНОВКИ И НАСТРОЙКИ

3.1 Общие сведения

СПО TrustCIA не имеет графического интерфейса для установки. Установка осуществляется через консоль ОС Astra Linux Special Edition версия 1.7

Для установки и функционирования СПО TrustCIA требуется наличие компонентов и программ, указанных в таблице , подраздела 2.2.

3.2 Установка и запуск программы

Для установки СПО TrustCIA необходимо последовательно выполнить следующие действия:

1. Создать директорию проекта выполнив команды:

```
mkdir savs
cd savs
```

2. Поместить дистрибутив в папку **savs** и распаковать выполнив команду:

```
unzip -o savs.{версия сервиса}.{номер сборки}.zip
```

3. Выполнить подготовительный скрипт:

```
cd savs
bash prepare.sh
```

4. Настроить переменные окружения (см.подраздел 3.3).
   - открыть файл local.env;
   - определить переменные.
5. Запустить сервис командой:

```
docker-compose up -d
```

3.3 Настройка программы

3.3.1 Общие сведения

В СПО TrustCIA выполняется настройка следующих конфигураций:

1. Доступ к СПО TrustGate:
   - адрес сервера TrustGate;
   - логин доступа к TrustGate;
   - пароль доступа к TrustGate;

- области доступа согласия (множественное указание мнемоник);
- цели получения согласия (множественное указание мнемоник);
- действия в рамках согласия (множественное указание мнемоник).

2. Доступ к средствам УЦ:
   - тип УЦ;
   - адрес сервера УЦ;
   - тип выпускаемых сертификатов – УНЭП/безопасности;
   - адрес скачивания CRL;
   - отпечаток сертификата в СПО TrustGate для подписания запросов к УЦ;
   - идентификатор ключа сертификата УЦ (subject key identifier);
   - идентификатор папки для создания пользователей в УЦ[1].
   - идентификатор сертификата УЦ[2].
   - параметры мониторинга и балансировки запросов (в случае эксплуатации нескольких экземпляров средств УЦ для выпуска сертификатов одного типа):
     - приоритет экземпляра;
     - таймаут для обращения к экземпляру;
     - период времени при котором экземпляр считается недоступным в случае обнаружения его неработоспособности;
     - частота мониторинга работоспособности экземпляра.

3. Алгоритм балансировки запросов в случае эксплуатации нескольких экземпляров средств УЦ для выпуска сертификатов одного типа:
   - по приоритету экземпляров от 1 до N (где чем меньше число, тем выше приоритет)

[1]Заполняется только при настройке взаимодействия с Программно-аппаратным комплексом «Удостоверяющий центр «КриптоПро УЦ» версии 2.0

[2]Заполняется только при настройке взаимодействия с Программно-аппаратным комплексом «ViPNet Удостоверяющий центр 5» версии 5.1.0

- случайным распределением по доступным экземплярам;

4. Тип файлового хранилища:
   - жесткий диск сервера:
     - адрес директории хранения;
   - хранилище S3:
     - параметры доступа к хранилищу.
5. Параметры хранения журнала событий:
   - graylog:
     - параметры доступа к graylog;
   - syslog:
     - параметры доступа к syslog.

3.3.2 Настройка параметров

Для настройки СПО TrustCIA необходимо:

– определить параметры переменных окружения;

– задать количество воркеров асинхронных задач.

3.3.2.1 Настройка переменных окружения

Для настройки параметров переменных окружения необходимо отредактировать файл local.env и определить переменные. Сведения о переменных указаны в приложении 1.

Примечание. Пример настройки переменных содержится в файле savs/examples/example.env

3.3.2.2 Настройка количества воркеров асинхронных задач

Для настройки количества воркеров асинхронных задач необходимо отредактировать файл .env и определить переменную:

– CELERY_TASK_WORKERS (значение по умолчанию - 4).

3.4 Остановка и перезапуск

Остановка программы выполняется командой:

```
docker-compose down
```

Для перезапуска программы необходимо выполнить ее остановку и последующий запуск.

Порядок запуска описан в подразделе 4.2.

3.5 Обновление программы

Для обновления программы необходимо:

1. Скачать дистрибутив с новой версией программы;
2. Остановить программу (см.подраздел 3.4);
3. Выполнитьустановку и запуск новой версией программы (см.подраздел 4.2).

3.6 Удаление программы

Для удаления СПО TrustCIA необходимо:

1. Выполнить команду:

```
docker-compose down -v
```

Программа будет остановлена и удалена.

2. Удалить папку savs и папку с медиа файлами выполнив команды:

```
cd ..
sudo rm -rf savs
sudo rm -rf /var/lib/savs
```

4. ТРЕБОВАНИЯ К ЭКСПЛУАТАЦИИ

4.1 Общие сведения

При эксплуатации СПО TrustCIA все действия по настройке, мониторингу функционирования и управлению должны выполняться администраторами в соответствии с требованиями и рекомендациями, изложенными в настоящем документе.

Действия по обслуживанию и настройке СПО TrustCIA рекомендуется выполнять только в периоды регламентного обслуживания сервера, на котором развернуто СПО TrustCIA.

4.2 Включение оборудования

Перед включением оборудования, на котором развернуто СПО TrustCIA, администратор обязан убедиться в отсутствии признаков НСД и (или) внешних признаков вскрытия корпуса сервера (нарушения целостности печатей (пломб) сервера при их наличии).

4.3 Контроль целостности сервера и СПО TrustCIA

В СПО TrustCIA не предусмотрено мер контроля целостности и работоспособности сервера.

Данный контроль осуществляется штатными средствами BIOS при холодной перезагрузке сервера и организационными мерами. При включении сервера выполняется:

1. Проверка регистров процессора.
2. Проверка контрольной суммы постоянного запоминающего устройства (ПЗУ).
3. Проверка системного таймера.
4. Тест контроллера непосредственного доступа к памяти (DMA).
5. Тест регенератора оперативной памяти.
6. Тест нижней области оперативного запоминающего устройства (ОЗУ) для проецирования резидентных программ BIOS.
7. Тест стандартного графического адаптера.

8. Тест оперативной памяти.
9. Тест основных устройств ввода.
10. Тест CMOS.
11. Тест основных портов ввода/вывода.
12. Тест жестких дисков.
13. Самодиагностика функциональных подсистем BIOS.

4.4 Контроль целостности сервера с ОС Astra Linux

Организация регламентного контроля целостности ОС Astra Linux и СПО TrustCIA обеспечивается набором программных средств на основе «Another File Integrity Checker», входящих в состав ОС.

Подробная информация о настройке средств регламентного контроля целостности приведена в эксплуатационной документации на ОС Astra Linux Special Edition версии 1.7.

4.5 Контроль за соблюдением правил эксплуатации

Контроль за соблюдением правил эксплуатации возлагается на администратора. При обнаружении фактов нарушения правил пользования администратор обязан принять меры для устранения выявленных нарушений и оценить возможные последствия.

4.6 Восстановление работоспособности при сбоях, действия в нештатных ситуациях

Все действия в нештатных ситуациях, связанных с использованием СПО TrustCIA, а также при восстановлении работоспособности проводятся администратором.

Для восстановления работы СПО TrustCIA в случае нарушения целостности (искажения файлов) необходимо иметь установочный дистрибутив.

В случае выявления нарушения целостности (искажения файлов) СПО TrustCIA необходимо:

1. Выполнить мероприятия по контролю и восстановлению (при необходимости) целостности среды функционирования.

2. Выполнить повторную установку СПО TrustCIA в соответствии с требованиями и рекомендациями.

В случае выхода из строя сервера СПО TrustCIA может быть установлено на другой сервер, соответствующий требованиям. В случае выхода из строя сервера, на котором установлено СПО TrustCIA необходимо:

1. Выполнить по необходимости и при наличии возможности копирование каталога установки СПО TrustCIA на другой сервер – в каталог с теми же путями, что и на вышедшем из строя сервере.

2. Выполнить установку СПО TrustCIA в соответствии с требованиями.

В случае возникновения нештатных ситуаций в процессе эксплуатации СПО TrustCIA администратор должен выполнить следующие действия:

1. Уведомить уполномоченных лиц эксплуатирующей организации о возникновении нештатной ситуации.

2. Инициировать расследование нештатной ситуации, результаты которого отражаются в отчете о возникновении нештатной ситуации.

3. Созвать комиссию по нештатным ситуациям, в состав которой входят администратор и уполномоченные лица организации.

4. В зависимости от характера нештатной ситуации, выполнить все возможные меры по предотвращению повторного возникновения подобной нештатной ситуации.

В случае возникновения нештатной ситуации, порядок действий при которой не регламентирован настоящим документом, администратором вырабатывается план действий с учетом текущей ситуации.

5. ТРЕБОВАНИЯ К ЗАЩИТЕ ОТ НСД

5.1 Общие положения

Защита аппаратного и программного обеспечения от несанкционированного доступа при установке и использовании СПО TrustCIA является составной частью общей задачи обеспечения безопасности информации в САВС, в состав которого входит программа.

Наряду с применением средств защиты от НСД необходимо выполнение целого ряда мер, включающего в себя организационно-технические и административные мероприятия, связанные с обеспечением правильности функционирования технических средств обработки и передачи информации, а также установлением соответствующих правил для сотрудников, допущенных к работе с конфиденциальной информацией.

В приведенных ниже разделах содержатся основные требования по организации указанных мер защиты.

5.2 Организация работ по защите от НСД

Защита информации от НСД должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости администратором.

При эксплуатации СПО TrustCIA в организации должен быть определен ответственный администратор, на которого возлагаются задачи организации работ по эксплуатации ПО, а также контролю за соблюдением описанных ниже требований.

Правом локального доступа к СПО TrustCIA и его компонентам должны обладать только сотрудники, ознакомленные с настоящим руководством.

5.3 Требования по защите от НСД при эксплуатации СПО TrustCIA

При организации работ по защите информации от НСД необходимо разработать и ввести в действие политику назначения и смены паролей (для входа в ОС, BIOS). Требования к характеристикам паролей определяются принятой в эксплуатирующей организации парольной политикой, но должны как минимум

включать следующие правила:

– Длина пароля должна быть не менее 6 символов.

– В числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.).

– Пароль не должен включать в себя легко подбираемые сочетания символов (имена, фамилии и т. д.), а также общепринятые сокращения (USER, ADMIN, ALEX и т. д.).

– Срок действия пароля не должен превышать 6 месяцев.

– При смене пароля новое значение должно отличаться от предыдущего не менее чем в четырех позициях.

– Пользователь не имеет права разглашать (сообщать кому-либо) личный пароль.

Указанная политика должна распространяться на все учетные записи пользователей ОС.

Запрещается также:

– Оставлять без контроля сервер, на котором установлено СПО TrustCIA, после ввода ключей либо иной конфиденциальной информации.

– Вносить какие-либо изменения в СПО TrustCIA.

Администратор должен выполнить настройки ОС и/или иных установленных на сервер программ, в среде которых планируется использовать СПО TrustCIA, и осуществлять периодический контроль выполненных настроек в соответствии со следующими требованиями:

– Запрещается использовать нестандартные, измененные или отладочные версии ОС.

– Необходимо исключить возможность загрузки и использования ОС, отличной от предусмотренной штатной работой.

– Необходимо исключить возможность несанкционированного удаленного управления, администрирования и модификации ОС и ее настроек.

– На сервере, на котором установлено СПО TrustCIA, должна быть установлена только одна ОС.

– Правом установки и настройки ОС, а также установки СПО TrustCIA и других программ, должен обладать только администратор.

– Необходимо отключить все неиспользуемые ресурсы ОС (протоколы, сервисы, службы и т.п.).

– В ОС должны быть реализованы механизмы защиты информации согласно установленным требованиям безопасности информации, к информационной системе, в которой применяется ПО.

– Необходимо ограничить использование администратором запуска программ с учетом выбранной в организации политики информационной безопасности.

– Должна использоваться система аудита, должен выполняться регулярный анализ результатов аудита.

– Необходимо настроить ОС на завершение работы при переполнении журнала аудита.

– Необходимо предусмотреть меры, максимально ограничивающие доступ к следующим ресурсам системы (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части):

1) Файлы конфигурации, временные файлы;
2) Файлы и каталоги;
3) Журналы системы;
4) Файлы подкачки;
5) Кэшируемая информация (пароли и т.п.).

ПРИЛОЖЕНИЕ 1.

СВЕДЕНИЯ О НАСТРОЙКАХ ПЕРЕМЕННЫХ ОКРУЖЕНИЯ

Название	Назначение	Значение по умолчанию	Необходимость переопределения	Пример
PROJECT_NAME	Наименование проекта в swagger	CABC	нет	CABC
TAG	Версия сервиса. Возвращается в методах /version и /healthcheck	= версия дистрибутива	нет	1.0.0.1
STATIC_DIR	Расположение статичных файлов в контейнере	static	нет	static
TIMEZONE	Часовой пояс сервиса	Europe/Moscow	не обязательно	Europe/Moscow
FILE_STORAGE_TYPE	Тип файлового хранилища	FILE_SYSTEM	не обязательно	Может принимать одно из значений: – FILE_SYSTEM - сохранение файлов на жесткий диск сервера в папку /var/lib/savs/media – S3 - сохранение файлов в s3. При выборе s3 в обязательно порядке нужно заполнить следующие параметры доступа к хранилищу: • AWS_ACCESS_KEY_ID • AWS_SECRET_ACCESS_ KEY • AWS_STORAGE_BUCKET_NAME • AWS_S3_ENDPOINT_URL • AWS_S3_SIGNATURE_ VERSION

Название	Назначение	Значение по умолчанию	Необходимость переопределения	Пример
FILE_STORAGE_PATH	Путь для сохранения файлов при локальной разработке	../files	нет	../files
AWS_ACCESS_KEY_ID	AWS ключ доступа	Отсутствует	Обязательно при FILE_STORAGE_TYPE=S3	OUHXMEC-YSR3Z3EIKZ-P
AWS_SECRET_ACCESS_KEY	AWS секретный ключ доступа	Отсутствует	Обязательно при FILE_STORAGE_TYPE=S3	PuXmpnyDZWatppkCSFj2r2tFQimtsGb7k4uqDRP3
AWS_STORAGE_BUCKET_NAME	Наименование корзины для хранения файлов	Отсутствует	Обязательно при FILE_STORAGE_TYPE=S3	savs
AWS_S3_ENDPOINT_URL	Адрес s3	Отсутствует	Обязательно при FILE_STORAGE_TYPE=S3	http://s3.my-domain.ru
AWS_S3_PROXIES	Словарь с прокси для доступа к s3	Отсутствует	не обязательно	{"http":"localhost:9000"}
AWS_S3_SIGNATURE_VERSION	Используемая версия подписи	s3v4	не обязательно	s3v4
AWS_S3_VERIFY	Проверять ли сертификат при подключение к s3	false	не обязательно	false
REQUEST_SIGNATURE_VERIFY	Проверять ли самоподписанную подпись запроса на сертификат	true	не обязательно	true

Название	Назначение	Значение по умолчанию	Необходимость переопределения	Пример
CHECK_SUBJECT_OID_ORDER	Выполнять ли проверку порядка oid subject в выпущенном сертификате	true	не обязательно	true
SYSLOG_HOST	Адрес syslog	Отсутствует	да	10.0.10.100
SYSLOG_PORT	Порт syslog	Отсутствует	да	515
SYSLOG_FACILITY	Средство, используемого для ведения журнала	local6	не обязательно	local6
GRAYLOG_HOST	Адрес graylog	Отсутствует	не обязательно	10.0.10.101
GRAYLOG_PORT	Порт graylog	Отсутствует	не обязательно	5046
LOG_DATE_FORMAT	Формат времени при логировании	%Y-%m-%d %H:%M:%S,uuu	не обязательно	%Y-%m-%d %H:%M:%S,uuu
LOG_LEVEL	Уровень логирования	INFO	не обязательно	Может принимать одно из значений: – NOTSET – DEBUG – INFO – WARNING – ERROR – CRITICAL
DATABASE_HOST	Адрес БД	localhost	да	localhost
DATABASE_PORT	Порт БД	5432	да	5432
DATABASE_USER	Пользователь БД	savs	да	savs
DATABASE_PASSWORD	Пароль пользователя БД	111111	да	111111
DATABASE_NAME	Наименование БД	savs	да	savs

Название	Назначение	Значение по умолчанию	Необходимость переопределения	Пример
SQLALCHEMY_DATABASE_URL	Адрес доступа к БД	postgresql+psycopg://savs:savs@localhost:5432/savs	Формируется автоматически	postgresql+psycopg://{DATABASE_USER}:{DATABASE_PASSWORD}@{DATABASE_HOST}:{DATABASE_PORT}/{DATABASE_NAME}
DATABASE_POOL_SIZE	Размер пула для доступа к БД	5	не обязательно	5
REDIS_HOST	Адрес redis	localhost	да	localhost
REDIS_PORT	Порт redis	6379	да	6379
REDIS_DB	Номер БД redis	0	да	0
REDIS_URL	Адрес доступа к redis	redis://localhost:6379	Формируется автоматически	redis://{REDIS_HOST}:{REDIS_PORT}/{REDIS_DB}
CELERY_BROKER_URL	Адрес брокера для хранения асинхронных задач	= REDIS_URL	да	amqp://guest:guest@10.0.36.102:5672/savs
AUTHORITY_SETTINGS	Массив настроек взаимодействия с экземплярами УЦ	Отсутствует	да	Заполняется в формате «параметр»: «значение» для каждого используемого экземпляра УЦ. Параметры настройки: – type - тип УЦ: • vipnet; • vipnet_5; • crypto_pro_rest; • crypto_pro_soap; – url - адрес доступа к УЦ: – cert_type - тип выпускаемого сертификата: • UNEP;

Название	Назначение	Значение по умолчанию	Необходимость переопределения	Пример
				• Secure; – crl_url - адрес для скачивания crl УЦ; – thumbprint - отпечаток сертификата в СПО TrustGate, используемого для верификации запросов к УЦ; – key_identifier – идентификатор ключа сертификата УЦ (subject key identifier); – folder - название папки в случае типа УЦ crypto_pro_rest или guid папки в случае типа УЦ crypto_pro_soap; – ca_cert_id - идентификатор сертификата УЦ для типа УЦ = vipnet_5; – priority - приоритет УЦ для типа балансировки = "priority"; – timeout_seconds - таймаут для обращения к УЦ; – downtime_seconds - период времени при котором УЦ считается недоступным в случае обнаружения его неработоспособности; – monitoring_period_seconds - частота мониторинга работоспособности УЦ.
AUTHORITY_BALANCING_METHOD	Тип балансировки нагрузки к УЦ	priority	нет	Допускаются следующие типы балансировки запросов:

Изм.	№ Док.	Подп.	Дата

Название	Назначение	Значение по умолчанию	Необходимость переопределения	Пример
				– priority – по приоритету от 1 до N, где чем меньше число, тем выше приоритет экземпляра; – random – выбирается случайный из доступных
TRUST_GATE_URL	Адрес СПО TrustGate	Отсутствует	да	https://10.0.10.103
TRUST_GATE_LOGIN	Пользователь СПО TrustGate	Отсутствует	да	api
TRUST_GATE_PASSWORD	Пароль пользователя СПО TrustGate	Отсутствует	да	111111
TRUST_GATE_AUTH_RETRY_LIMIT	Максимальное количество попыток авторизации в СПО TrustGate	3	не обязательно	3
TRUST_GATE_AUTH_RETRY_DELAY	Задержка между попытками авторизации в СПО TrustGate	1	не обязательно	1
TRUST_GATE_RETRY_LIMIT	Максимальное количество попыток выполнения запроса (кроме авторизации) в СПО TrustGate	1	не обязательно	1
TRUST_GATE_RETRY_DELAY	Задержка между попытками выполнения запроса (кроме авторизации) в СПО TrustGate	1	не обязательно	1

Название	Назначение	Значение по умолчанию	Необходимость переопределения	Пример
TRUST_GATE_ESIA_AUTH_CREATE	Параметры запроса для авторизации в ЕСИА и получения данных цифрового профиля, передаваемые в СПО TrustGate	{"scopes":["openid"],"permissions":[{"sysname":"DIGITAL_RUBLE","scopes":[{"sysname":"fullname"},{"sysname":"birthdate"},{"sysname":"inn"},{"sysname":"snils"},{"sysname":"id_doc"},{"sysname":"addresses"}],"purposes":[{"sysname":"DIGITAL_RUBLE"}],"actions":[{"sysname":"ALL_ACTIONS_TO_DATA"}]}],"need_logout":false}	не обязательно	{"scopes":["openid"],"permissions":[{"sysname":"DIGITAL_RUBLE","scopes":[{"sysname":"fullname"},{"sysname":"birthdate"},{"sysname":"inn"},{"sysname":"snils"},{"sysname":"id_doc"},{"sysname":"addresses"}],"purposes":[{"sysname":"DIGITAL_RUBLE"}],"actions":[{"sysname":"ALL_ACTIONS_TO_DATA"}]}],"need_logout":false}
TASK_SETTINGS	Настройки для асинхронных задач взаимодействия с СПО TrustGate и УЦ			Объект, со следующими параметрами: – TRUST_GATE_CHECK_SIGNATURE_MAX_RETRIES - максимальное количество попыток для задачи проверки подписи – TRUST_GATE_CHECK_SIGNATURE_RETRY_BACKOFF_SECONDS - начальная задержка для задачи проверки подписи – TRUST_GATE_CHECK_SIGNATURE_RETRY_BACKOFF_MAX_SECONDS - максимальная задержка между

Изм.	№ Док.	Подп.	Дата

Название	Назначение	Значение по умолчанию	Необходимость переопределения	Пример
				попытками для задачи проверки подписи – TRUST_GATE_SIGN_MAX_RETRIES - максимальное количество попыток для задачи создания подписи – TRUST_GATE_SIGN_RETRY_BACKOFF_SECONDS - начальная задержка для задачи создания подписи – TRUST_GATE_SIGN_RETRY_BACKOFF_MAX_SECONDS - максимальная задержка между попытками для задачи создания подписи – AUTHORITY_CERT_ISSUE_MAX_RETRIES - максимальное количество попыток для задачи выпуска сертификата – AUTHORITY_CERT_ISSUE_RETRY_BACKOFF_SECONDS - начальная задержка для задачи выпуска сертификата – AUTHORITY_CERT_ISSUE_RETRY_BACKOFF_MAX_SECONDS - максимальная задержка между попытками для задачи выпуска сертификата