



УТВЕРЖДЕН

RU.33654484.0003-01 90 01-ЛУ

ПРОГРАММНЫЙ КОМПЛЕКС «СИНОНИКС»

Руководство пользователя

RU.33654484.0003-01 90 01

Листов 16

Ине. № подл.	Подпись и дата	Взам. инв №	Ине. № дубл.	Подпись и дата

2024

Литера

АННОТАЦИЯ

В данном документе приведено руководство пользователя программного комплекса «Синоникс» (далее по тексту – ПК «Синоникс», Изделие). В документе описываются действия пользователя по осуществлению приема/передачи файловой информации (файлов и директорий).

СОДЕРЖАНИЕ

1. Описание и работа в режимЕ «filetransfer»	4
1.1. Назначение и область применения	4
1.2. Требования к уровню подготовки пользователя режима «filetransfer».....	4
1.3. Рекомендуемые характеристики АРМ пользователя	4
1.4. Общие сведения	5
1.5. Доступ к функциональным возможностям ПК «Синоникс» в режиме «filetransfer»	9
1.6. Передача файлов и каталогов	9
1.7. Передача файлов с проверкой целостности посредством цифровой подписи	9
1.7.1. Создание ключа.....	10
1.7.2. Подписание файлов	10
1.7.3. Регистрация публичного ключа.....	11
1.7.4. Передача файлов подписанных ЭЦП.....	11
1.8. Получение файловых объектов	11
1.9. Контроль результатов действий пользователя и завершение работы	12
Перечень сокращений.....	13
Перечень рисунков.....	14
Перечень таблиц.....	15

1. ОПИСАНИЕ И РАБОТА В РЕЖИМЕ «FILETRANSFER»

1.1. Назначение и область применения

В данном документе приведено руководство пользователя программного комплекса «Синоникс», где описываются действия пользователя по осуществлению приема/передачи файловой информации (файлов и директорий); прием/передача файловой информации в терминах ПК «Синоникс» носит название «режим «filetransfer».

Программный комплекс «Синоникс» предназначен для использования в качестве специального программного обеспечения в составе программно-аппаратного средства информационного обмена (СИО), основным назначением которого является автоматизация процессов передачи файловой и потоковой информации между сетевыми приложениями.

Обмен файловой информацией осуществляется пользователями, которые являются авторизованными клиентами СИО по протоколам FTP и SFTP. Взаимодействие пользователя с СИО происходит как с сетевым устройством сети/сегмента сети.

ПК «Синоникс» предназначен для обработки конфиденциальной информации.

1.2. Требования к уровню подготовки пользователя режима «filetransfer»

Пользователь режима «filetransfer» должен обладать практическими навыками работы в командной строке терминала среды функционирования, работы с SFTP-клиентами.

1.3. Рекомендуемые характеристики АРМ пользователя

Действия по осуществлению приема/передачи файловой информации осуществляются с АРМ пользователя; рекомендуемые характеристики аппаратного обеспечения АРМ представлены в таблице 1.

Т а б л и ц а 1 – Рекомендуемые характеристики аппаратного обеспечения АРМ пользователя

Компонент	Характеристика
Процессор	архитектура x86-64 с тактовой частотой 2 ГГц
Оперативная память	8 ГБ
Жесткий диск	128 ГБ
Интерфейсы	– интерфейс для подключения к LAN – интерфейс USB 2.0
Монитор	разрешение экрана при работе с управляющим интерфейсом: 1280x1024 пикселей

Требования к среде функционирования и программным средствам АРМ пользователя представлены в таблице 2.

Т а б л и ц а 2 – Программные средства АРМ пользователя

Компонент	Характеристика
ОС	Linux (например, Astra Linux версии 1.5 и выше), Windows (версии 7 и выше), другие ОС с поддержкой SSH-клиентов (работающих по протоколу SSH-2)
Другое ПО	Свободно распространяемые клиенты для протоколов удаленного доступа, включая SSH, RS-232. (В качестве такого клиента может быть использован «PuTTY» или аналогичный)

1.4. Общие сведения

Для осуществления приема/передачи файловой информации, иных действий, администратор СИО должен передать пользователю режима «filetransfer» следующую информацию:

- параметры подключения к СИО по протоколу SFTP (адрес и порт);
- порядок и параметры авторизации пользователя;
- требования, предъявляемые к передаваемой/принимаемой файловой информации и наименование правил, которые задают эти требования;
- дополнительную служебную информацию (время и периодичность отправки/приема файловых объектов, сроки проведения регламентных работ и др.).

Авторизация пользователя может быть выполнена двумя способами (порядок и параметры авторизации пользователю назначает администратор):

- путем использования логина и пароля;
- с помощью публичного ключа SSH.

В случае авторизации с помощью ключа SSH, пользователь по согласованию с администратором выполняет генерацию ключа SSH и передает сгенерированный публичный ключ SSH администратору для настройки доступа; при настроенном доступе по ключу SSH, авторизация пользователя на СИО происходит автоматически после того, как будет установлено SFTP соединение.

Для генерации SSH-ключа следует в терминале и выполнить команду:

```
ssh-keygen -t rsa
```

и далее следовать указаниям системы.

После того, как ключ будет создан, в терминале выполнить команду:

```
cat ~/.ssh/id_rsa.pub
```

На консоль будет выведен ключ.

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDErpqPzYtGgIYj3ujKgp9nxV6/Ehe7koJMTepM5bn/U8UdtqASQanCJiitU17TZXBz0nERvLpEtaQC9Io6GkK14NOZwkbF4sGswGUUvcCCHvK4DzLa+Qr3kcLbxapWKfuocYGc4da8VDyu8oL0/svW50QRXUyYHu2zvHe33uP5P25wAKetXoHmHwnHQJHzmSQezG+mdFarXpDw+HLhXJRI+sDE+E2zUtXdnmgPQoinNzfN+Bo4Rku+86Q1rV/Du/s8bHIBfJYhtt uho/Rz1L03sPZF/90+vonhpkmNSnmGCCgRSuLuP7ZRuuHSY07MxivsT7Hr6VIIdmrKjoQ4WJSzd syn-admin@client-to-syn-b
```

Его следует скопировать и передать администратору для настройки доступа.

Требования, предъявляемые к передаваемой/принимаемой файловой информации задаются администраторами сетей/сегментов сети; такие требования могут не накладывать никаких ограничений, либо представлять комбинацию отдельных требований/ограничений (каждый конкретный набор требований называется «правило» («rule»):

– ограничения, предъявляемые к наименованию передаваемых файлов и каталогов; если в правиле установлен такой вид ограничений, то они следующие:

– список запрещённых символов:

```
":", ". ", "\\ ", "=", "!", "?", "$", "*", "(", ")", "{", "}", "[", "]", "&", "|", ";", ":", "\\", "/", ">", "<", ">", "<", ">", ">", "<"
```

– с каких символов не может начинаться имя файла:

```
" ", "~", "-"
```

– запрещённый разделитель:

```
"~", "-"
```

– запрещены пробелы в конце имени;

– максимально-допустимая длина имени файла: 227 символов;

– ограничения, предъявляемые к размеру передаваемых файлов и каталогов (устанавливаются в Мб);

– требование, обязывающее пользователя подписывать цифровой подписью передаваемые файлы и каталоги;

– ограничения, предъявляемые к разрешенным к передаче типам многопользовательских почтовых расширений (MIMEtype) и (или) расширений файлов;

– а также может быть задано требование по дополнительной верификации передаваемой/принимаемой файловой информации во внешних системах (средства антивирусной защиты, DLP-системы и др.), доступных из сети эксплуатирующей организации по протоколу ICAP.

В случае, если передаваемая/принимаемая информация не удовлетворяет заданным правилам или средствами антивирусной защиты, DLP-системами и др., в ней будут выявлены опасные объекты, ПК «Синоникс» запретит передачу/прием такой информации.

При создании каждого пользователя режима «filetransfer» (выполняется администратором) ему в файловой системе СИО автоматически создаются служебные директории (кроме директорий «rule...»); пример для условного пользователя user1 показан на рисунке 1.

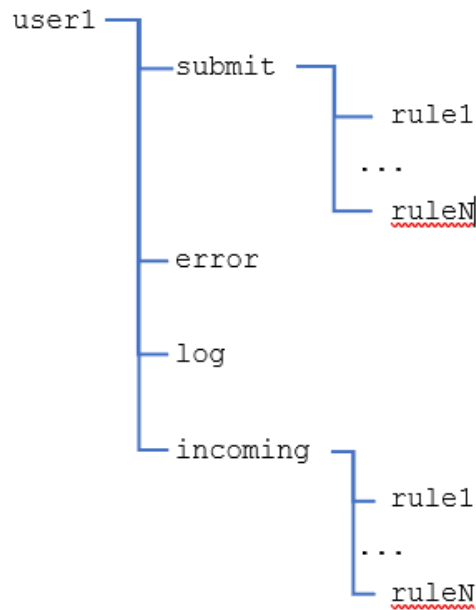


Рисунок 1 – Пример структуры директорий пользователя

Назначение директорий приведено в таблице 3.

Т а б л и ц а 3 – Назначение директорий пользователя

Название директории	Назначение директории
user1	Директория пользователя user1. Название директории совпадает с именем учетной записи пользователя.
submit	Изначально, при создании пользователя, папка submit пуста. В данную директорию помещаются предназначенные для отправки файловые объекты (в соответствующие директории «rule...») Директории «rule...» создаются в директории submit автоматически при создании администратором правил передачи файловых объектов и выполнении действий по ассоциации данных правил с пользователем user1; данным директориям присваиваются имена, идентичные наименованиям созданных правил передачи.
error	Директория, куда помещаются файловые объекты, которые

Название директории	Назначение директории
	пользователь пытался отправить и которые были запрещены к передаче в соответствии с заданными правилами.
log	Директория, в которой хранятся сведения о действиях пользователя: <ul style="list-style-type: none"> – метка времени по данным СИО; – режим (filetransfer); – путь и имя файла (каталога); – статусное сообщение.
incoming	Изначально, при создании пользователя, папка incoming пуста. В дальнейшем она будет наполняться файловыми объектами, отправленными с противоположной сети/сегмента сети и разрешенными к передаче. Принимаемые объекты будут помещены в директории «rule...», наименования которых соответствуют наименованиям правил, созданных на противоположной сети/сегменте сети и в соответствии с которыми производилась их отправка.

Пользователю доступны к просмотру каталоги `error` и `log`. Файлы в каталогах `error` и `log` автоматически удаляются по истечении 15 суток хранения (в 04.00).

Удаление файлов из каталога `incoming` выполняется автоматически, по истечении 15 суток хранения (в 04.00).

Для инициации процесса передачи файла (директории) пользователь должен создать соединение со СИО по протоколу SFTP, выполнить авторизацию, перенести файл (директорию) в соответствующую папку `submit/<rule>` и закрыть подключение.

Передача данных выполняется по следующему алгоритму:

- если на отправляющей стороне передача разрешена (передаваемый файловый объект соответствует установленному на отправляющей стороне правилу `rule`), то происходит его передача (в противном случае, запрещенные к передаче объекты помещаются в директорию `error`).

- на принимающей стороне, пользователь, которому назначен доступ к одноименному правилу передачи `rule`, сможет найти переданные файлы в своей личной директории `incoming/<rule>` в случае, если принимаемый файловый объект соответствует установленному на принимающей стороне правилу `rule`. В противном случае, файловые объекты будут помещены в директорию `error` принимающей стороны.

1.5. Доступ к функциональным возможностям ПК «Синоникс» в режиме «filetransfer»

Для доступа к функциональным возможностям ПК «Синоникс» в режиме «filetransfer» пользователю необходимо:

Шаг 1. Открыть терминал среды функционирования или клиент удаленного доступа с поддержкой режима SFTP.

Шаг 2. Создать соединение используя указанные администратором логин и адрес.

Шаг 3. Ввести пароль учетной записи (в случае, если авторизация производится по логину и паролю).

1.6. Передача файлов и каталогов

Для передачи файла (каталога) пользователю необходимо (пример):

Шаг 1. При установленном соединении с СИО выполнить авторизацию пользователя `test_user` с паролем `test_user!`:

```
sftp -P 20020 test_user@192.85.85.100 (пароль test_user!)
```

Шаг 2. Перенести файл `testfile` в директорию `submit/ rule1`

```
cd submit/rule1  
put testfile
```

Шаг 3. Закрывать подключение комбинацией клавиатуры `Ctrl+D`. Закрытие сессии инициирует процесс передачи файла (каталога).

Примечание. Если файл соответствует параметрам, заданным правилом (в примере это правило `rule1`), то он будет отправлен в противоположную сеть/сегмент сети. Если нет, то файл будет помещен в директорию `Error` (при повторном подключении пользователь может убедиться в этом, выполнив анализ ее содержимого).

1.7. Передача файлов с проверкой целостности посредством цифровой подписи

Изделие позволяет выполнять верификацию целостности передаваемых файлов посредством электронной цифровой подписи (ЭЦП).

Примечание. Для операций контроля целостности, Изделие использует вызов утилиты `openssl` из состава ОС.

Для передачи файлов с цифровой подписью необходимо:

– создать ключ ЭЦП;

– выполнить регистрацию публичного ключа ЭЦП в ПК «Синоникс» (выполняется администратором);

- создать файл контроля целостности предназначенных к отправке файлов;
- выполнить отправку файлов.

1.7.1. Создание ключа

Для создания закрытого ключа (Private Key) RSA с длиной 2048 бита в терминале среды функционирования необходимо выполнить команду:

```
openssl genpkey -algorithm RSA -out private_key.pem -aes256
```

Эта команда создаст закрытый ключ и сохранит его в файле `private_key.pem`, зашифрованным алгоритмом AES-256. В процессе выполнения команды потребуется ввести пароль для защиты закрытого ключа.

Закрытый ключ создается один раз, хранится в безопасной области, передача его запрещена.

Далее следует извлечь открытый ключ (Public Key) из закрытого следующей командой:

```
openssl rsa -pubout -in private_key.pem -out public_key.pub
```

Публичный ключ можно передавать. Он используется при передаче подписанных ЭЦП файлов.

Примечание. В зависимости от принятой в организации политики безопасности создание ключа ЭЦП может выполняться администратором либо непосредственно пользователем.

1.7.2. Подписание файлов

Для подписания файлов необходимо выполнить команду

```
openssl dgst -sha256 -sign private_key.pem -out file_to_sign.sig  
file_to_sign.txt
```

где `file_to_sign.sig` – файл, в котором сохранится цифровая подпись, `file_to_sign.txt`; подписываемый файл (должен находиться в директории в момент выполнения команды).

Для ручной проверки подписи файла необходимо выполнить команду

```
openssl dgst -sha256 -verify public_key.pub -signature file_to_sign.sig  
file_to_sign.txt
```

Для успешного прохождения проверок на подпись, имя файла подписи с расширением `*.sig` должно соответствовать имени проверяемого файла.

1.7.3. Регистрация публичного ключа

Перед передачей файлов, подписанных ЭЦП, необходимо передать публичный ключ, содержащийся в файле `public_key.pub` администратору.

Администратор должен ввести в СИО публичный ключ и уведомить об этом пользователя.

1.7.4. Передача файлов подписанных ЭЦП

Для передачи подписанного ЭЦП файла, пользователю необходимо (пример):

Шаг 1. Авторизоваться на своем сегменте сети СИО:

```
sftp -P 20020 test_user@192.85.85.100 (пароль test_user!)
```

Шаг 2. Перенести файл `testfile`, подписанный ЭЦП и его цифровую подпись `testfile.sig` в директорию `submit/rule1`:

```
cd submit/rule1  
put testfile  
put testfile.sig
```

Шаг 3. Закрывать подключение комбинацией клавиш `Ctrl+D`. Закрывание сессии инициирует процесс передачи файлов.

Примечание. Название передаваемого файла и название цифровой подписи должны совпадать.

1.8. Получение файловых объектов

Передаваемые файлы и каталоги сохраняются в директории `incoming/<имя правила>`. Например, если имя правила передачи `rule1`, то файловые объекты будут помещены в директорию `incoming/rule1`.

Для получения файловых объектов пользователю необходимо (пример):

Шаг 1. Закрывать подключение комбинацией клавиш `Ctrl+D` (если пользователь был подключен в момент передачи файлов).

Шаг 2. Авторизоваться на своем сегменте сети СИО:

```
sftp -P 20020 test_user@192.85.85.100 (пароль test_user!)
```

Шаг 3. Перейти в директорию с переданными файловыми объектами

```
cd incoming/rule1
```

Шаг 4. Скопировать их в целевой ресурс.

Примечания:

1. Передача файла происходит не мгновенно и выполняется каждую минуту в 00 секунд.

2. В программном комплексе также реализована возможность передачи файловых объектов с принимающего Узла на внешний файловый сервер (Push) в режиме файлтранфера. В случае успешного завершения действий по передаче файловых объектов на внешний файловый сервер происходит завершение сессии и удаление доставленных файловых объектов из папки `incoming` на внешний файловый сервер. В случае, если передачу файловых объектов с принимающего Узла на внешний файловый сервер осуществить не удалось, то журналируется ошибка передачи на этапе Push, а сами файловые объекты остаются в папке `incoming` принимающего Узла и в папку `error` не помещаются. Порядок и правила доступа к внешнему файловому серверу устанавливает и доводит до пользователя (при необходимости) администратор.

3. Изделие контролирует расход ресурсов хранения для области передачи файлов. При заполнении хранилища на 90 и более %, пользовательские директории переходят в режим чтения и загрузка файлов блокируется (до момента освобождения ресурсов хранилища); данные события журналируются в папке `error`.

1.9. Контроль результатов действий пользователя и завершение работы

Пользователь, который осуществил отправку файловой информации может убедиться, что файл отправлен, выполнив анализ содержимого директорий `error` и `log`. Критерием успешной передачи файловой информации является отсутствие ее в директории `error`. Информация о результатах передачи содержится в директории `log`, где формируются журналы по каждой сессии передачи.

В случае успешного завершения проверки передаваемых файловых объектов пользователю-получателю они доступны в директории `incoming/<имя правила>`. Информация о результатах передачи содержится в директории `<имя пользователя>/incoming/<имя правила>`.

В случае неуспешного завершения проверки передаваемых файловых объектов информация о ее результатах содержится в директории `<имя пользователя>/incoming/<имя правила>`. Файловые объекты, не прошедшие проверку, помещаются в директорию `<имя пользователя>/incoming/<имя правила>/error`.

Для завершения работы с Изделием необходимо разорвать соединение с СИО.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АРМ	Автоматизированное рабочее место
ОС	Операционная система
ПК	Программный комплекс
ЭЦП	Электронная цифровая подпись
CLI	A Command-Line Interface, интерфейс командной строки
DLP	Data Leak Prevention, технологии предотвращения утечек конфиденциальной информации из информационной системы вовне, а также технические устройства (программные или программно-аппаратные) для предотвращения утечек.
LAN	Local Area Network — локальная вычислительная сеть
ICAP	Internet Content Adaptation Protocol, протокол адаптации интернет-контента
RSA	Rivest, Shamir, Adleman, криптографический алгоритм с открытым ключом.
SFTP	Secure File Transfer Protocol, протокол прикладного уровня передачи файлов, работающий поверх безопасного канала
SSH	Secure Shell, безопасная оболочка, протокол защищенной передачи данных
USB2.0	Universal Serial Bus, последовательный интерфейс версии 2 для подключения периферийных устройств к вычислительной технике

ПЕРЕЧЕНЬ РИСУНКОВ

Рисунок 1 – Пример структуры директорий пользователя..... 7

ПЕРЕЧЕНЬ ТАБЛИЦ

Таблица 1 – Рекомендуемые характеристики аппаратного обеспечения АРМ пользователя	4
Таблица 2 – Программные средства АРМ пользователя	5
Таблица 3 – Назначение директорий пользователя	7

