SP-crypted

Система независимого «прозрачного» зашифровывания данных «SP-crypted» комплекса SysPro.d

Это новейшая система мер по организации защиты коммерческой информации
от нежелательного доступа и прочих форс-мажорных обстоятельств.

syspro-d.group SysPro • d

Базовые принципы SP-crypted:

Сервис комплекса SysPro.d, и в первую очередь системы зашифровывания SP-crypted, сформировался опираясь на реальный опыт организации мер по защите конфиденциальной информации.

Выработанные принципы составляют основу всего проекта.

1

Обеспечение «**прозрачного**» **зашифровывания** (расшифровывания) информации при **включении или перезагрузке** компьютера (от отдельного файлового хранилища до операционной системы целиком).

2

НЕОБЯЗАТЕЛЬНОЕ наличие у пользователя ключей для расшифровывания информации, что делает невозможным ситуации востребования ключей доступа.

3

В чрезвычайных ситуациях гарантированно **предоставляет время** для принятия обдуманных решений о доступе к значимым данным.

4

Возможность **удалённого управления доступом** и настройки шифрованных данных.

5

Контроль доступа к зашифрованной информации по географическому расположению – **геолокация**.

Невозможность автоматического расшифровывания при несанкционированном изменении географического расположения зашифрованных данных без ведома владельца.

6

Полная свобода принятия решений о собственности и расположении хранения ключей доступа, а также полная конфиденциальность информации о конфигурации системы шифрования.

7

НЕОБЯЗАТЕЛЬНОСТЬ использования сервиса зашифровывания данных – т.е. наличие на сервере комплекса SysPro.d **не означает факт наличия** какой-либо зашифрованной информации.

Комплекс SysPro.d это сервис управления сервером данных. Предоставляемый сервис предполагает необязательное использование системы зашифровывания. В нём представлен полезный функционал для облегчения и стандартизации текущих задач по управлению и контролю за серверами, такой как:

– Smart-BackUp – инкрементный (только изменения) двухуровневый backup для высоконагруженных файловых хранилищ с функцией восстановления на определённую дату;*

– отслеживание S.M.A.R.T.-данных дисков;

– доступ к консоли сервера находящегося за NAT, к которому нет доступа по внешнему IP.

* В MAC OS похожий сервис называется «TimeMachine», предоставляющий возможность восстановления данных на указанную дату, рассчитанный для локальной рабочей станции. Smart-BackUp комплекса SysPro.d – сервис УДАЛЁННОГО управления BackUp-ом сервера (также и рабочей станции).

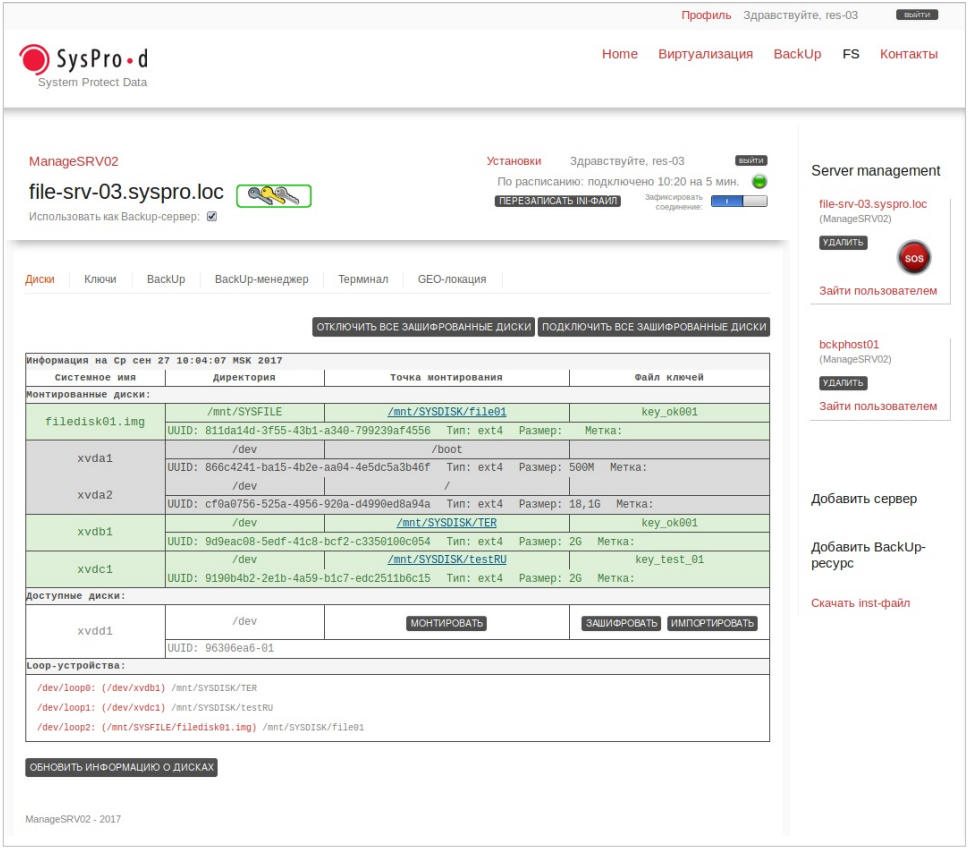
Система независимого «прозрачного» зашифровывания данных SP-crypted

В концепции SP-crypted инициатором расшифровывания является файловый сервер (рабочая станция) – **расшифровывание происходит «по запросу»**:

1. Файловый сервер при перезагрузке (включении) подключается к SysPro.d и запрашивает ключи;

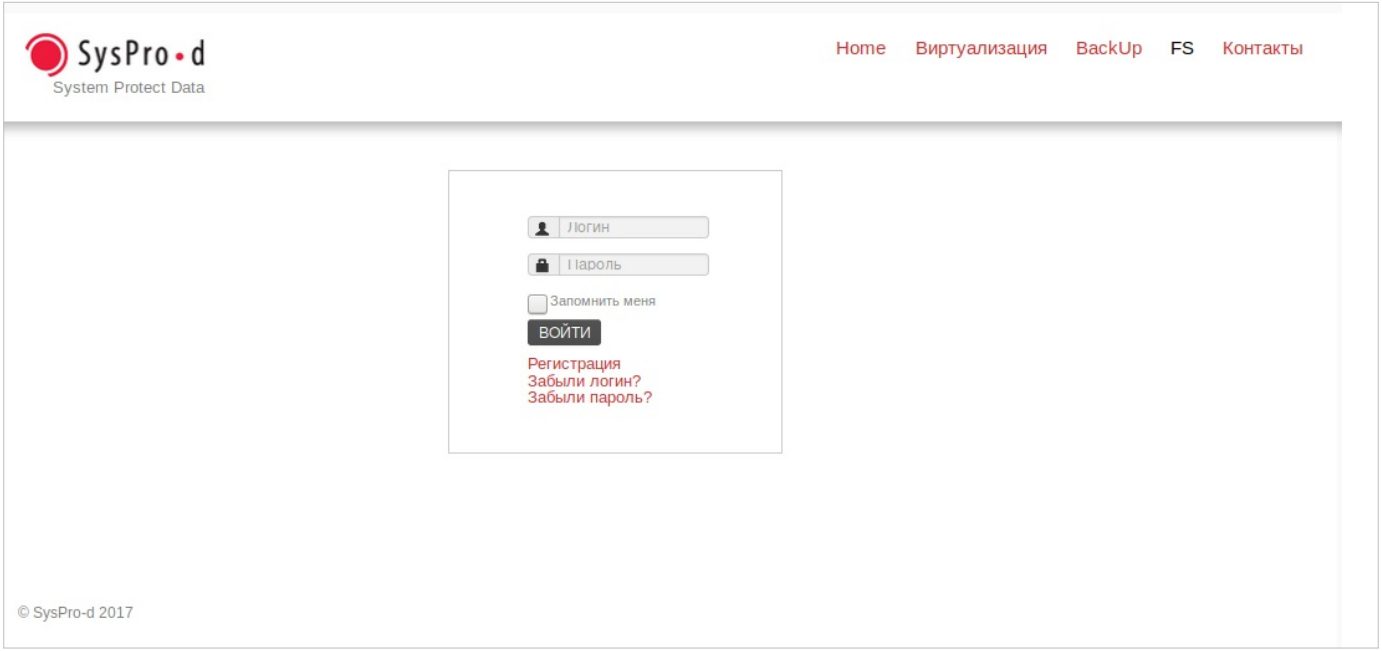
2. SP-crypted на основе проверки параметров валидации (среди которых «геолокация») принимает решение о предоставлении ключей;

3. SP-crypted предоставив доступ к ключам, расшифровывает диски на файловом сервере.



Портал syspro-d.group

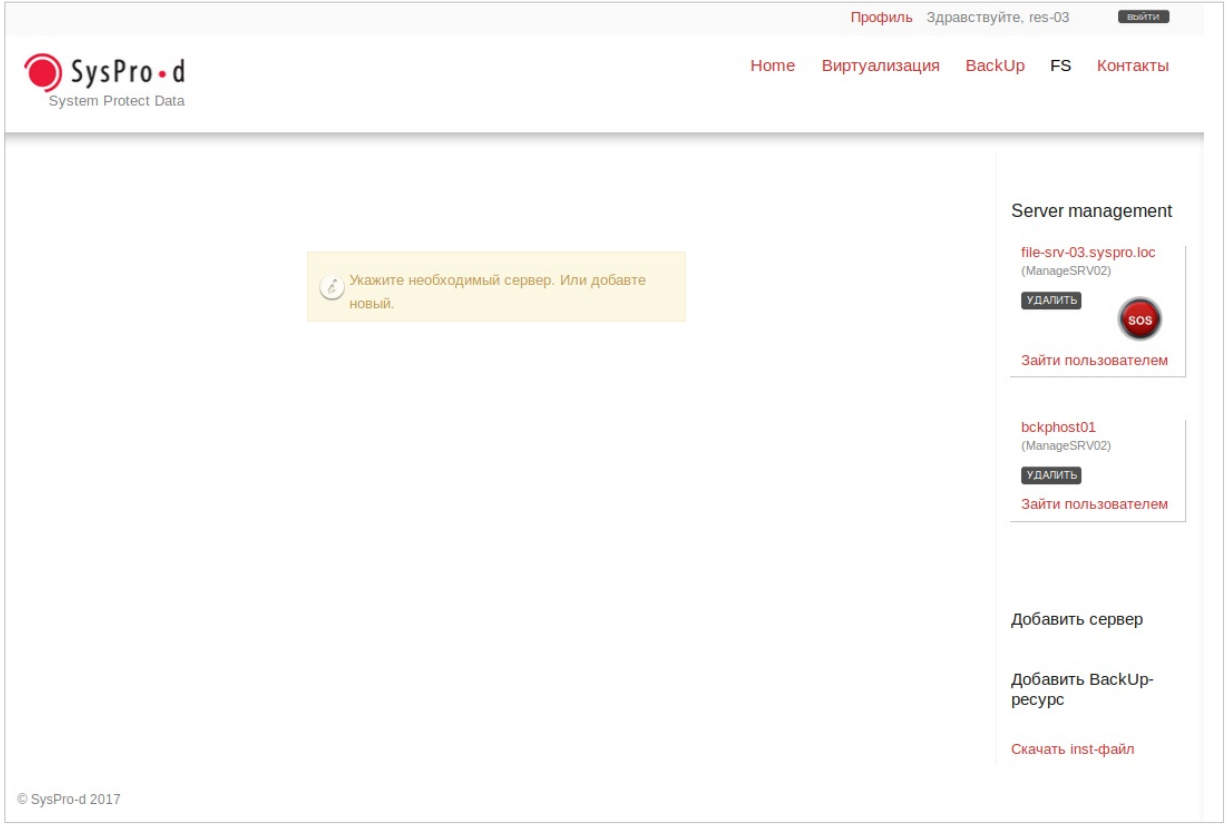
Вход в личный кабинет пользователя (для регистрации, управления и мониторинга) осуществляется через страницу пользователя на портале syspro-d.group, закладка «FS».



Портал syspro-d.group

В личном кабинете предоставляется возможность зарегистрировать сервер и зайти в панель управления сервером (рабочей станцией) на менеджер ключей («Ключницу»).

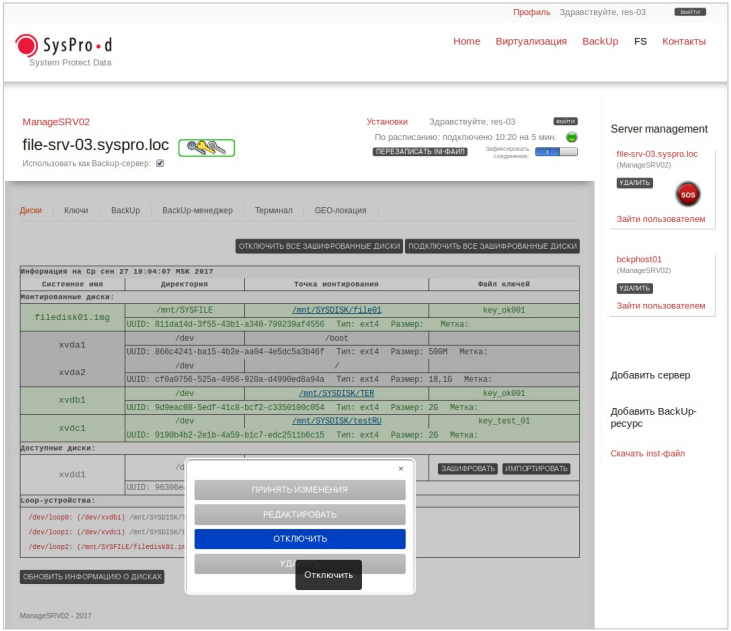
А также, при возникновении форс-мажорных обстоятельств, **воспользоваться «красной кнопкой»** для блокировки ключей и экстренной перезагрузки сервера (рабочей станции).

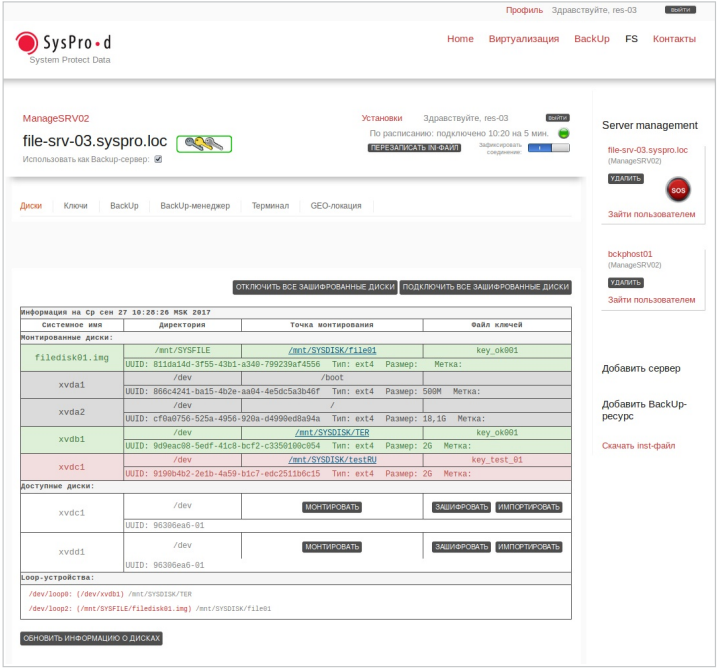


Менеджер управления сервером («Ключница»)

В личном кабинете сервера, на «Ключнице», производится подключение дисков, настройка параметров зашифровывания, управление хранилищами ключей и самими ключами, настройка BackUp и т. д.

Управление дисками



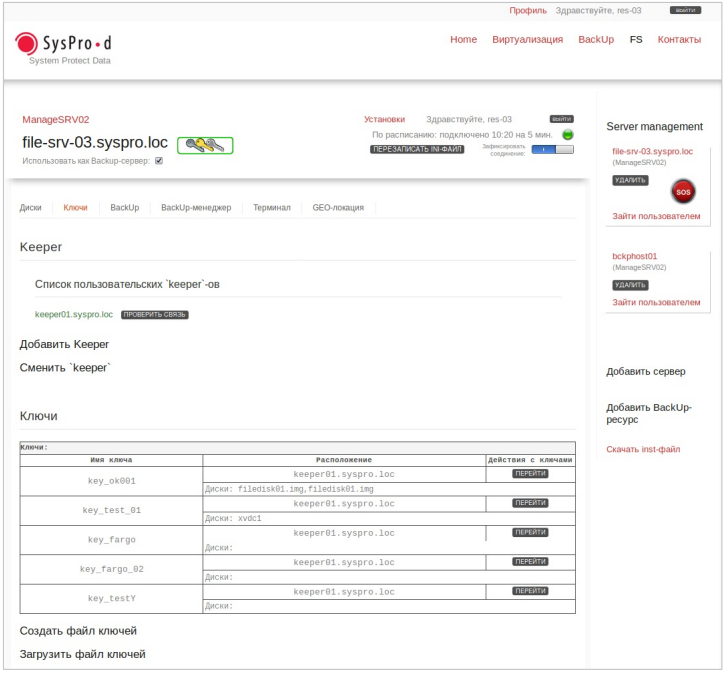


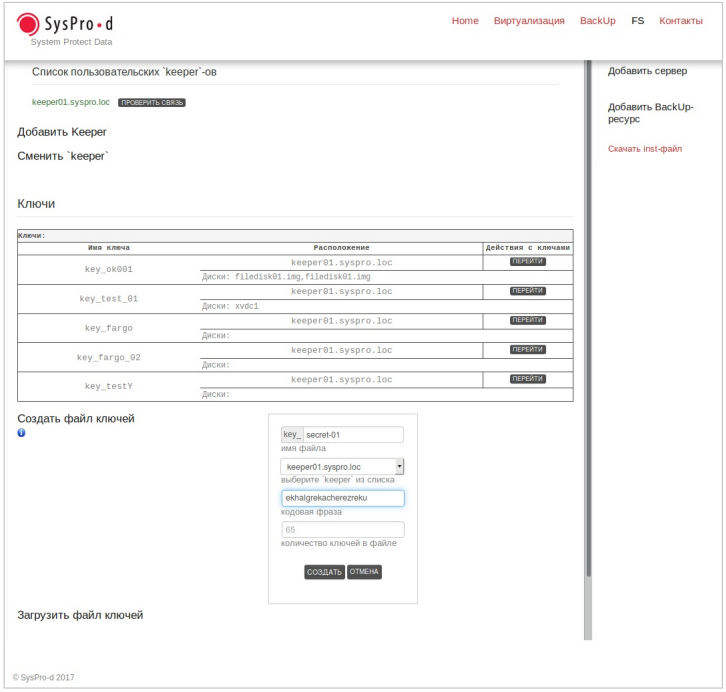
Менеджер управления сервером («Ключница»)

«Ключница» позволяет гибко настраивать расположение хранения ключей: возможно как использование общедоступных хранилищ, так и создание своих хранилищ, расположенных на **удобных для пользователя площадках**, и в полном его управлении.

Создаваемые файлы ключей содержат набор самостоятельных ключей, участвующих в зашифровывании одного диска (по умолчанию 65, возможно иное количество). Используется один из надёжнейших алгоритмов шифрования с большой глубиной шифрования.

Управление ключами и хранилищем ключей





Менеджер управления сервером («Ключница»)

«Ключница» предоставляет уникальный сервис организации резервного копирования – **Smart-BackUp**:

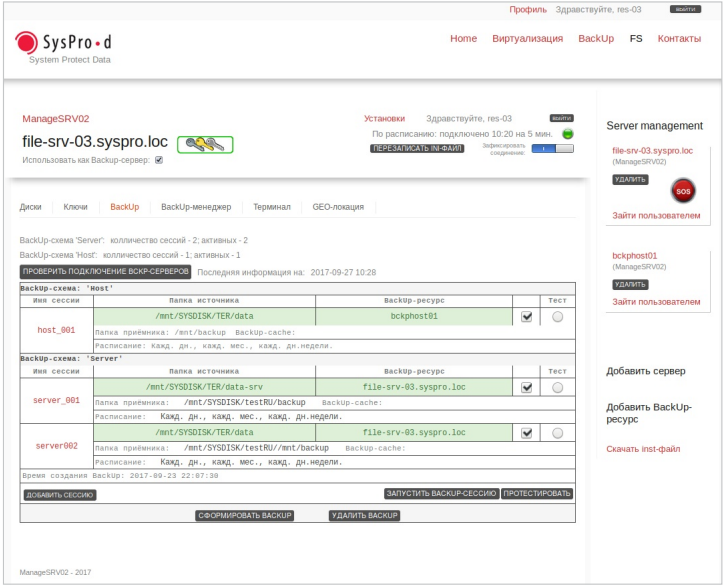
1. Инкрементная (только изменения) синхронизация данных.

2. Возможность использовать разные схемы расположения сервера резервного копирования: как «сервер» или как «хост», что даёт возможность работать с BackUp-сервером не организуя к нему внешний доступ (сервер располагается за NAT).

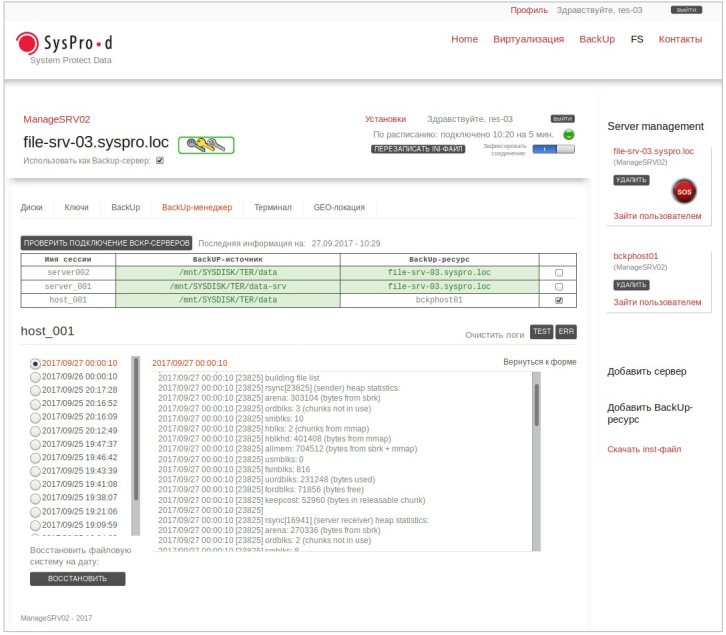
3. Возможность организации двухуровневой схемы резервного копирования (BackUp-cache) для высоконагруженных серверов.

4. Сервис «BackUp-менеджер» предоставляет возможность восстановления данных на определённую дату как выборочно, определённых файлов, так и целиком файловую систему.

Управление BackUp

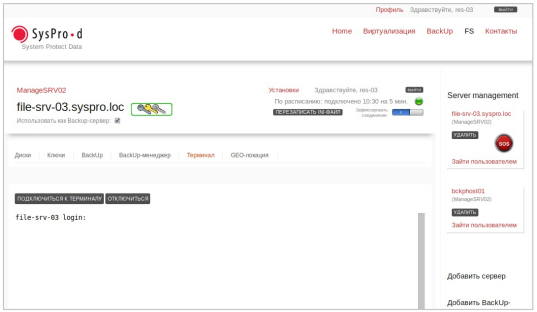


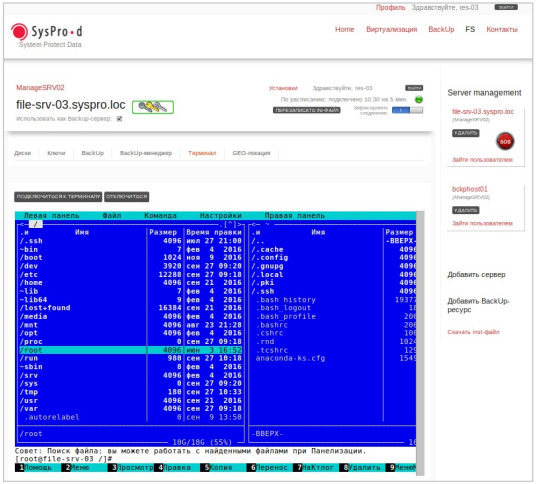
BackUp-менеджер



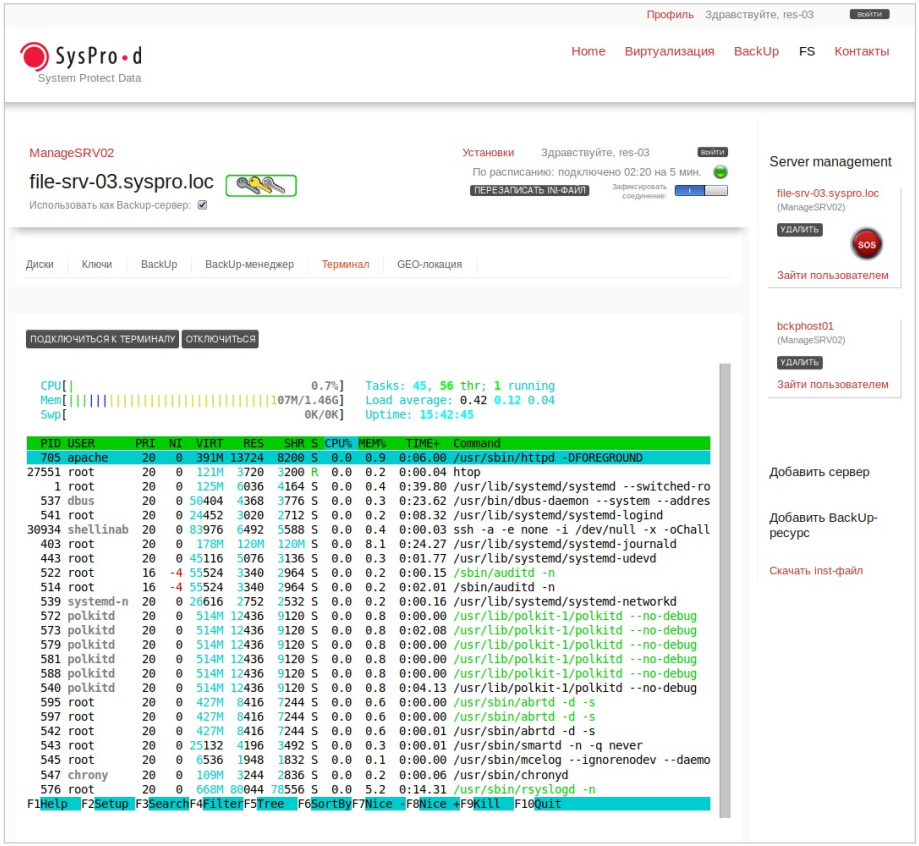
Менеджер управления сервером («Ключница»)

Для управления сервером реализован доступ к **полноценному терминалу**, позволяющему в полном объёме работать с сервером, включая системный мониторинг.





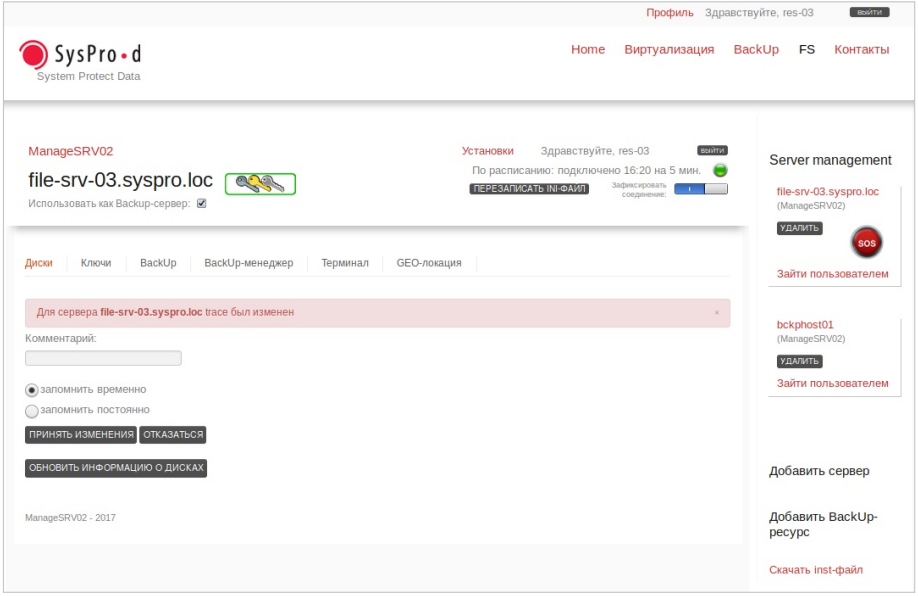
Терминал управления сервером



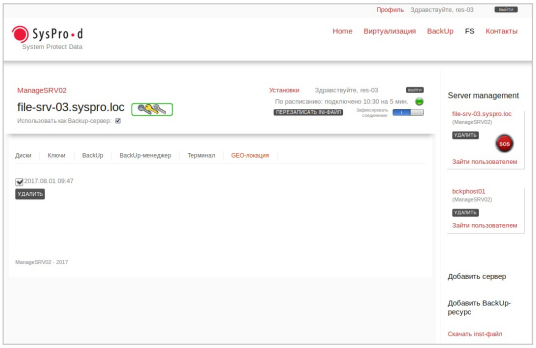
Менеджер управления сервером («Ключница»)

При изменении георасположения сервера владелец имеет возможность **принять новое расположение** и продолжить работу. В противном случае диски расшифрованы не будут.

Принять расположение можно на постоянной и временной основе.



Геолокация

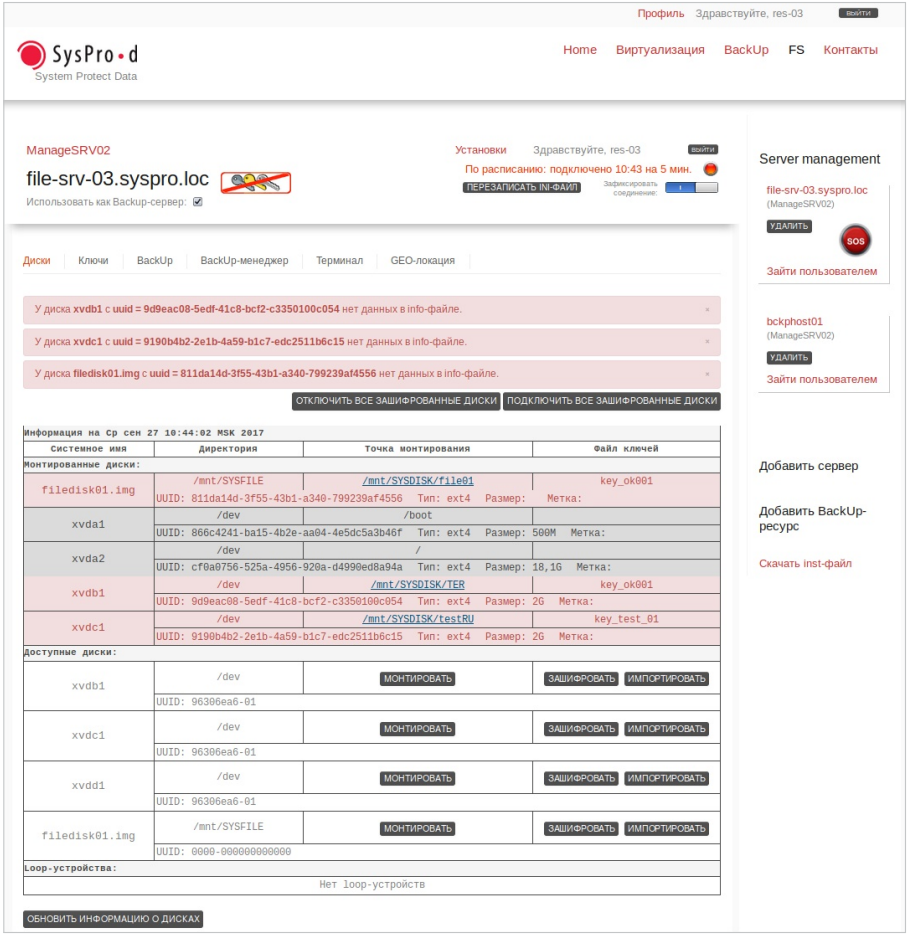


Экстренная блокировка ключей («красная кнопка»)

В **экстренных случаях** владелец может воспользоваться «красной кнопкой» **(SOS)** которая блокирует доступ к ключам и перегружает сервер (рабочую станцию).

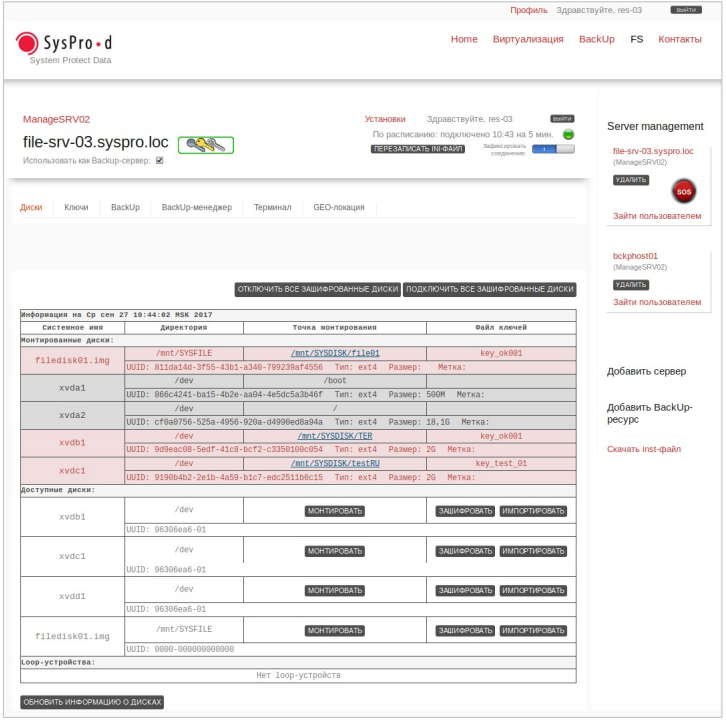
После блокировки ключей **расшифровывание дисков не возможна** до снятия блокировки владельцем сервера (рабочей станции), или может быть принято решение об аннулировании информации о шифрованных дисках. При этом информация о хранилище ключей **становиться не доступна** и может быть возобновлена только владельцем сервера (рабочей станции).

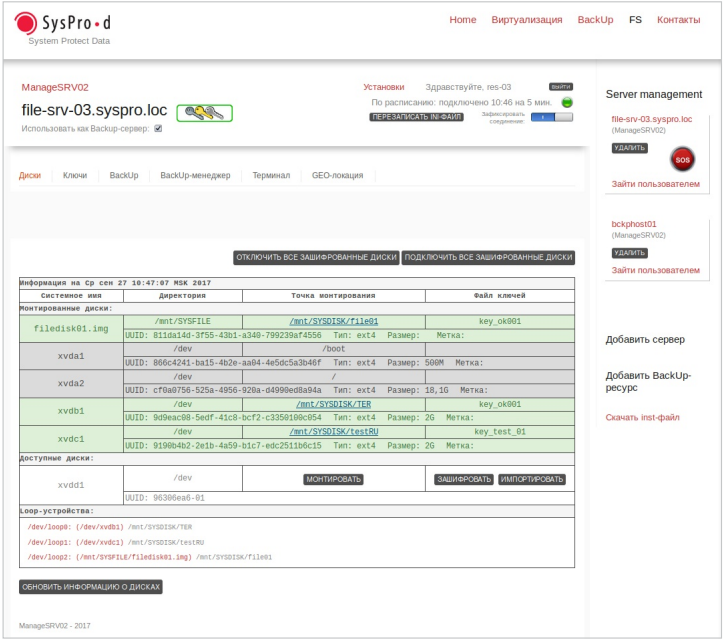
Для того чтобы воспользоваться сервисом «красной кнопки» нет необходимости заходить на «Ключницу» – **для экономии времени** блокировка происходит через личный кабинет на портале syspro-d.group.



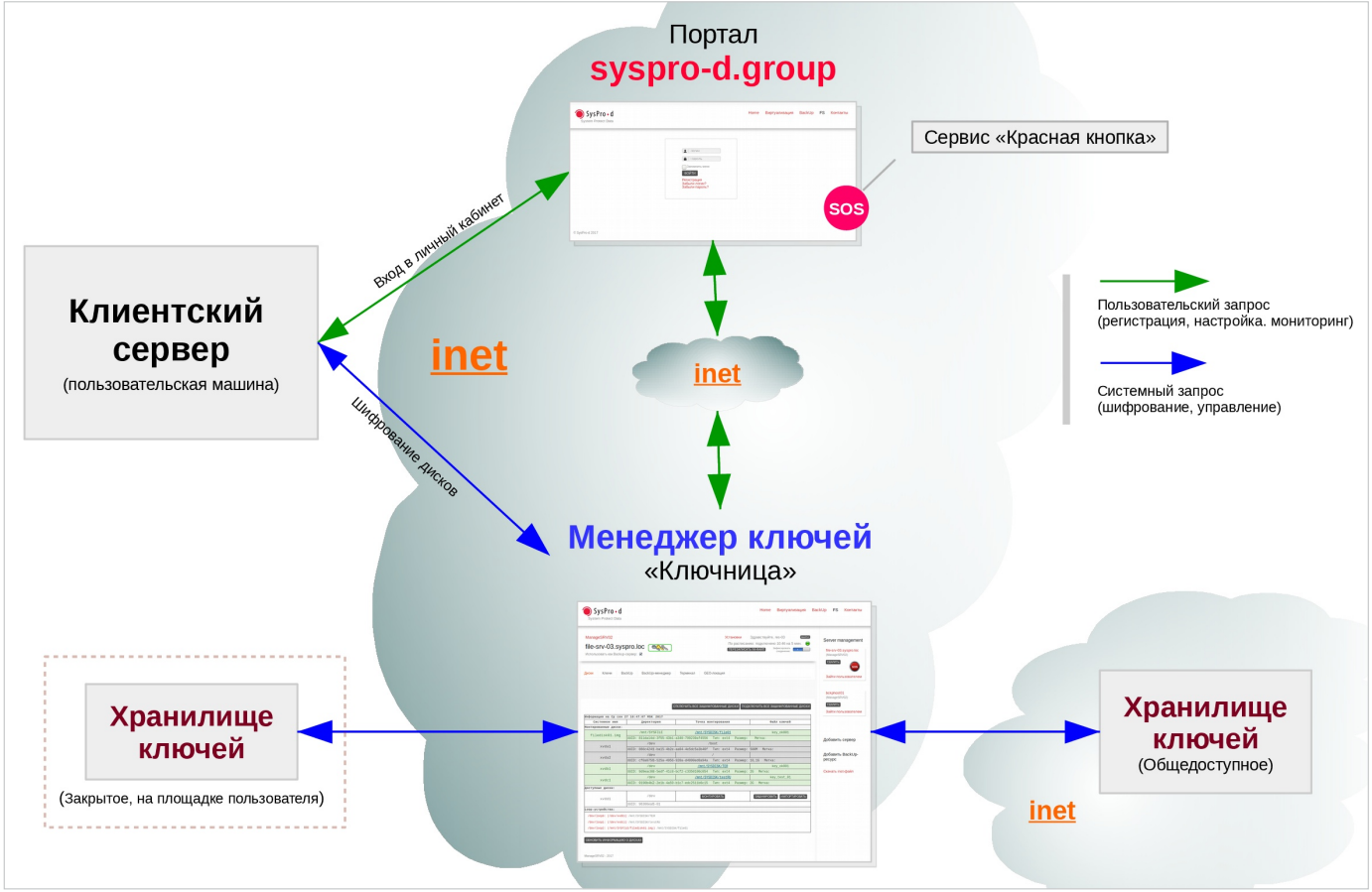
Экстренная блокировка ключей («красная кнопка»)

После снятия блокировки возможно запустить расшифровывание всех дисков или **просто перегрузить сервер** (ПК).





Структура комплекса SysPro.d



+7 965 009 08 76
info@syspro-d.group
http://syspro-d.group

2017 г.

SysPro • d