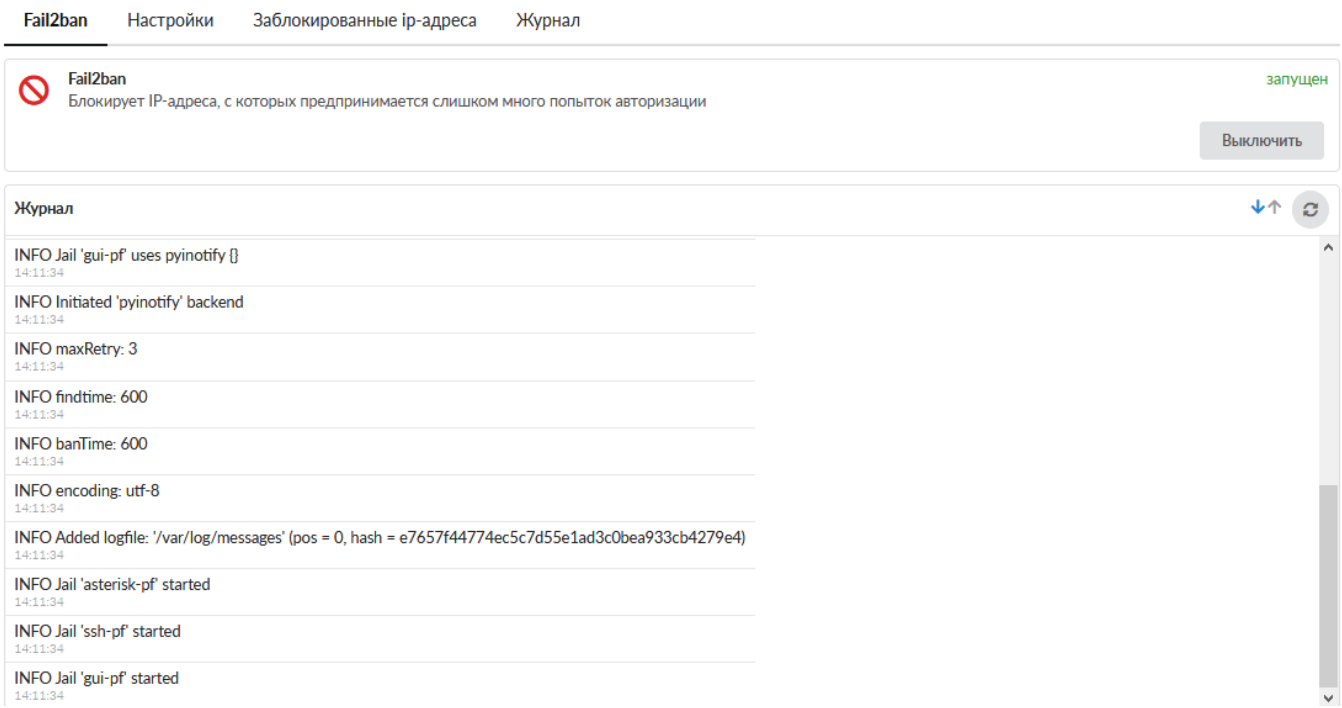
Fail2ban

Fail2ban - сканирует лог-файлы и блокирует IP-адреса, которые ведут себя подозрительно, к примеру, делая слишком много попыток входа с неверным паролем в попытках найти уязвимость. Данная атака часто называется брутфорсом.

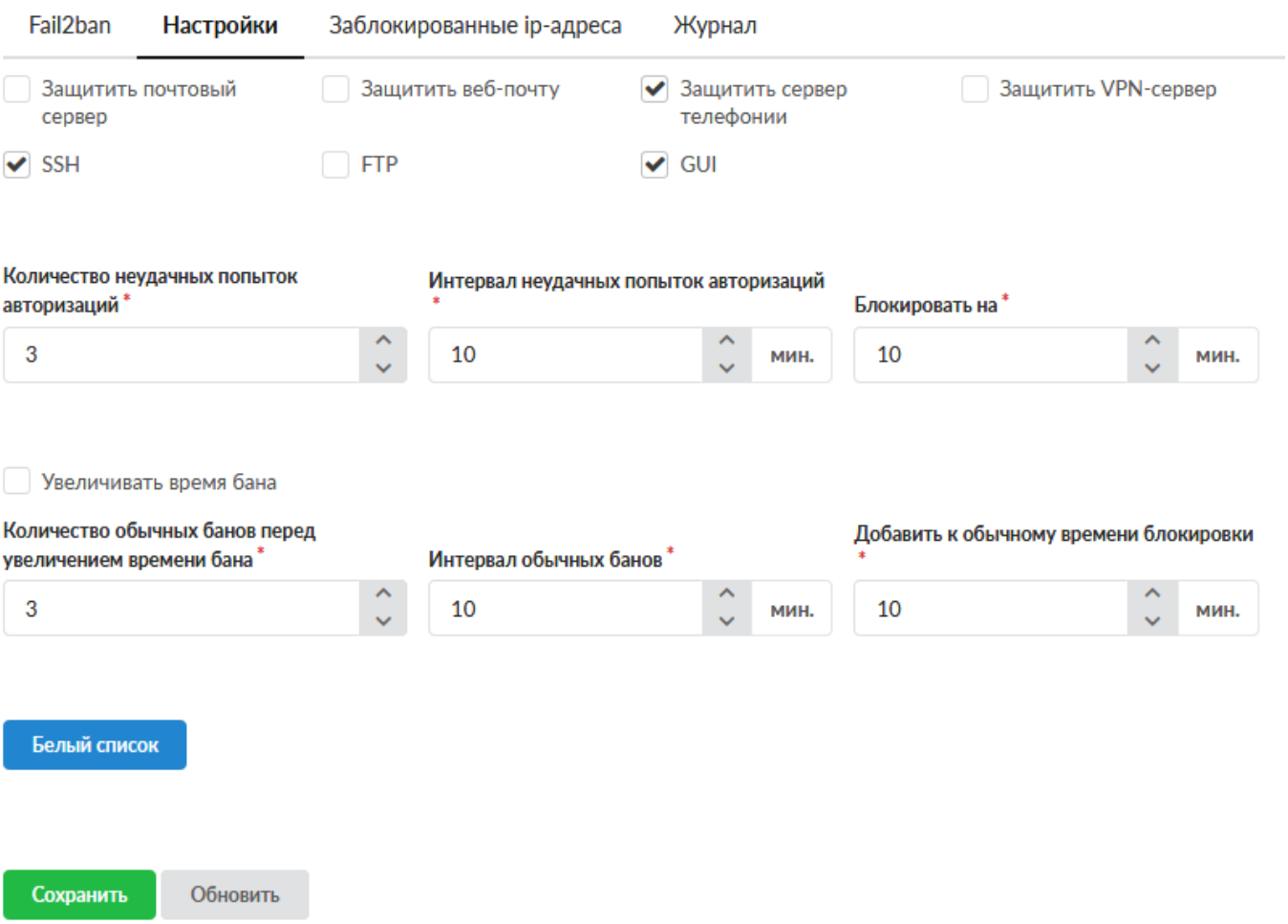
Модуль «Fail2ban» расположен в Меню «Защита», и имеет четыре вкладки: «Fail2ban», «Настройки», «Заблокированные ip-адреса», и «Журнал».

Общие сведения



На данной вкладке отображается состояние модуля (включен/выключен/не настроен), кнопка «Выключить» (или «Включить» если модуль выключен) и последние сообщения в журнале модуля.

Настройки



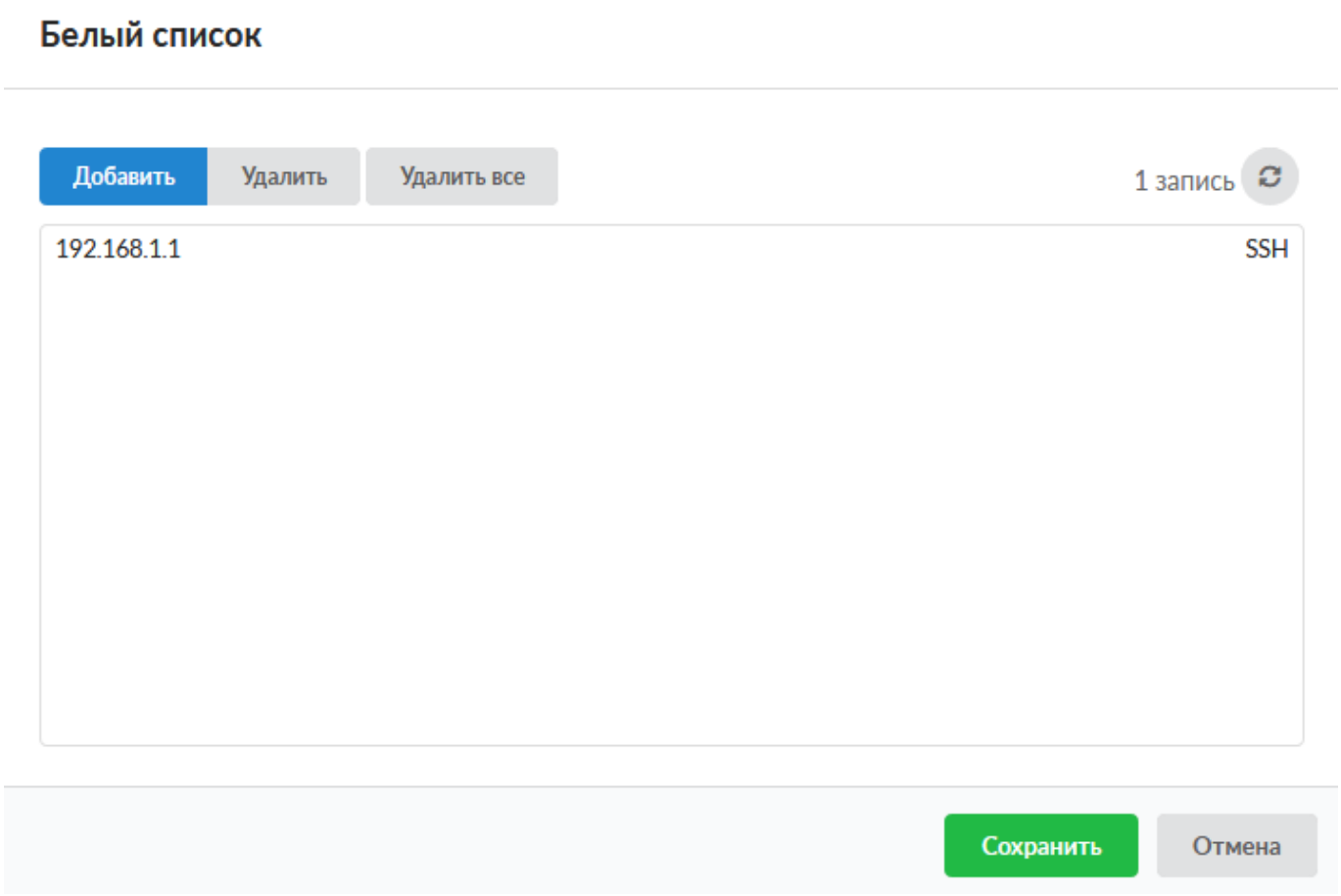
Данная вкладка предназначена для настройки работы модуля «Fail2ban».
Флаги: **«Защитить почтовый сервер», «Защитить веб-почту», «Защитить сервер телефонии», «Защитить VPN-сервер», «SSH», «FTP», «GUI»** - позволяют fail2ban анализировать логи авторизации в соответствующих модулях.
Поле «**Количество неудачных попыток авторизаций**» - позволяет задать количество неудачных попыток авторизации в одном из модулей, отмеченных флагом, после чего ip-адресу будет заблокирован доступ к «ИКС» полностью.
Поле «**Интервал неудачных попыток авторизаций**» - время, в течении которого подсчитывается количество неудачных попыток авторизации, в каждом модуле.
Поле «**Блокировать на**» - При срабатывании блокировки, доступ с ip-адреса, будет прекращен на заданное количество минут.

Флаг «**Увеличивать время бана**» - позволяет включить дополнительные настройки fail2ban («**Количество обычных банов перед увеличением времени бана**», «**Интервал обычных банов**», «**Добавить к обычному времени блокировки**») для инкрементации времени бана. Так при срабатывании бана **n**-раз (указанных в поле «Количество обычных банов перед увеличением времени бана») в течении времени **t** (указанного в «Интервал обычных банов») доступ к «ИКС» ip-адресу будет заблокирован. На **n+1** бане доступ будет заблокирован на время = **t +** значение из поля «Блокировать на».

ВАЖНО

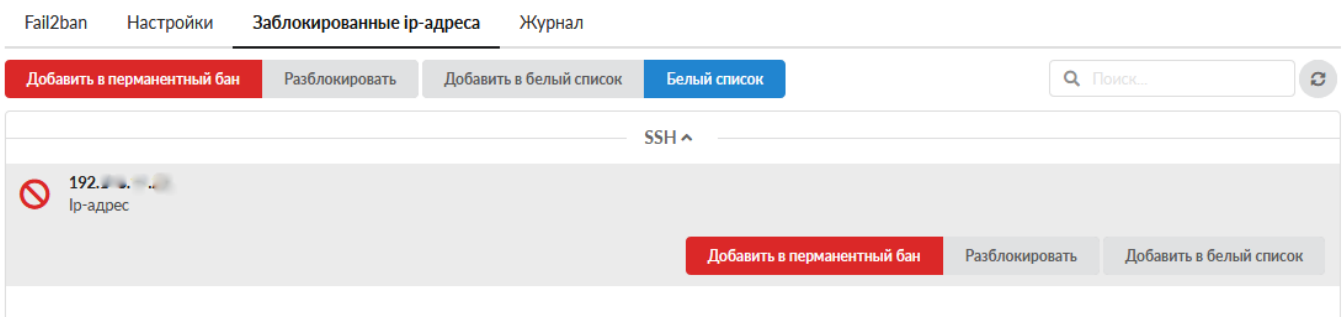
- *Стоит отметить*, что значение указанное в поле «Интервал обычных банов» должно быть *больше*, чем произведение значений полей «Блокировать на» и «Количество обычных банов перед увеличением времени бана».

- Если авторизация на FTP идет через браузер, то количество попыток авторизации, указанное в поле «Количество неудачных попыток авторизаций», будет в два раза меньше. Так как браузер пытается первоначально авторизоваться под учетной записью Anonymous.



Кнопка «Белый список». При нажатии будет открыто новое диалоговое окно, в котором возможно задать соответствие IP-адреса/подсети/диапазона (192.168.1.1 или 192.168.1.1/28 или 192.168.1.1-192.168.1.3) и сервиса/всех сервисов, для которых fail2ban не будет срабатывать.
Стоит отметить, что если fail2ban заблокирует IP-адрес по одному из сервисов, то доступ с IP-адреса к другим сервисам, также будет заблокирован, в том числе добавленным в белый список.

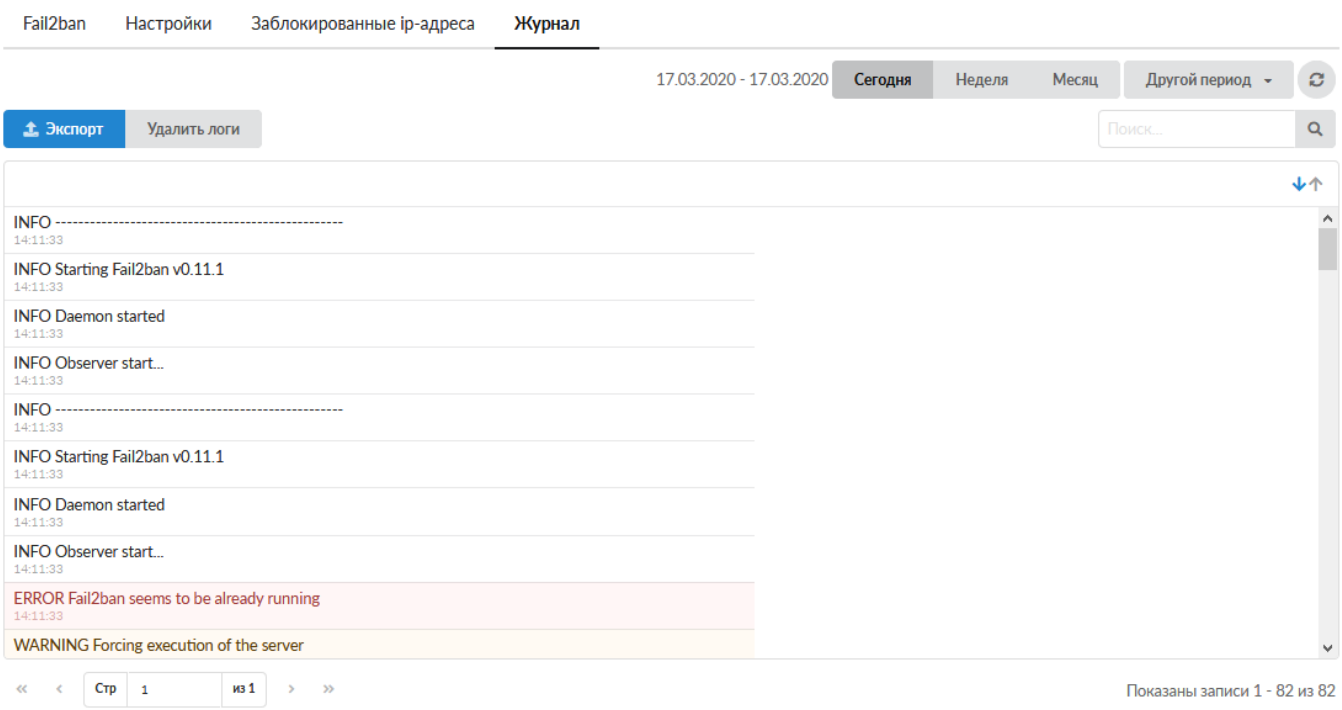
Заблокированные ip-адреса



На данной вкладке отображаются текущие блокировки IP-адресов, распределенные по блокам (модулям), где произошла блокировка. При необходимости, Пользователь с ролью Администратор, может добавить IP-адрес в перманентный бан (т.е. навсегда и по всем сервисам), в белый список (произойдет разблокировка IP-адреса и он не будет проверяться Fail2ban по сервису добавленному в белый список) или разблокировать IP-адрес до истечения бана.

При добавлении в перманентный бан, возможно добавить: IP (например, 192.168.1.1), сеть (например, 192.168.1.1/30), диапазон IP (например, 192.168.1.1-192.168.1.4).

Журнал



Отображает сводку всех системных сообщений модуля «Fail2ban» с указанием даты и времени. Журнал разделен на страницы, кнопками «вперед» и «назад» возможно переходить со страницы на страницу, либо ввести номер требуемой страницы. Записи в журнале выделяются цветом в зависимости от вида сообщения. Обычные сообщения системы отмечены белым цветом, сообщения о состоянии системы (включение/выключение) - зеленым, предупреждения – желтым, ошибки - красным. В правом верхнем углу модуля находится строка поиска, а также возможность выбора периода отображения журнала событий. По умолчанию журнал отображает события за текущую дату. При необходимости можно сохранить данные журнала в файл, нажав кнопку «Экспорт» или удалить данные журнала, за определенный период, нажав кнопку «Удалить логи».