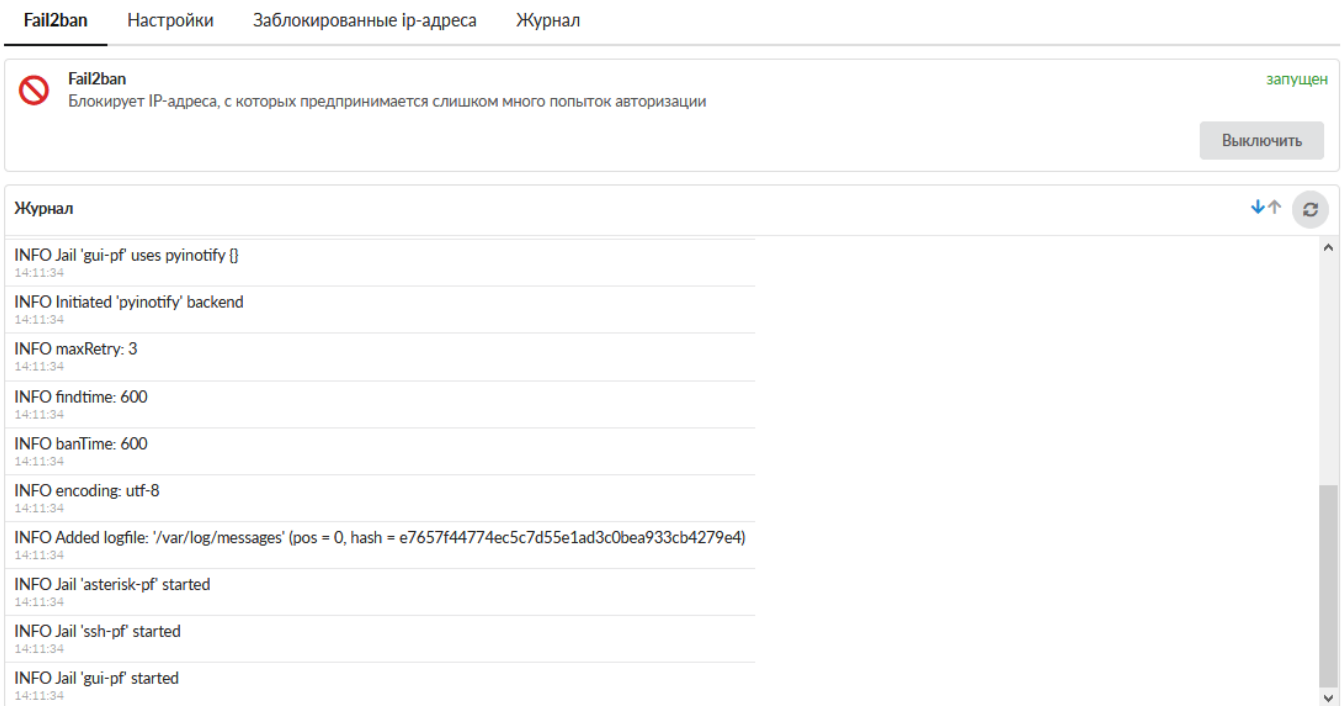
Fail2ban

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.

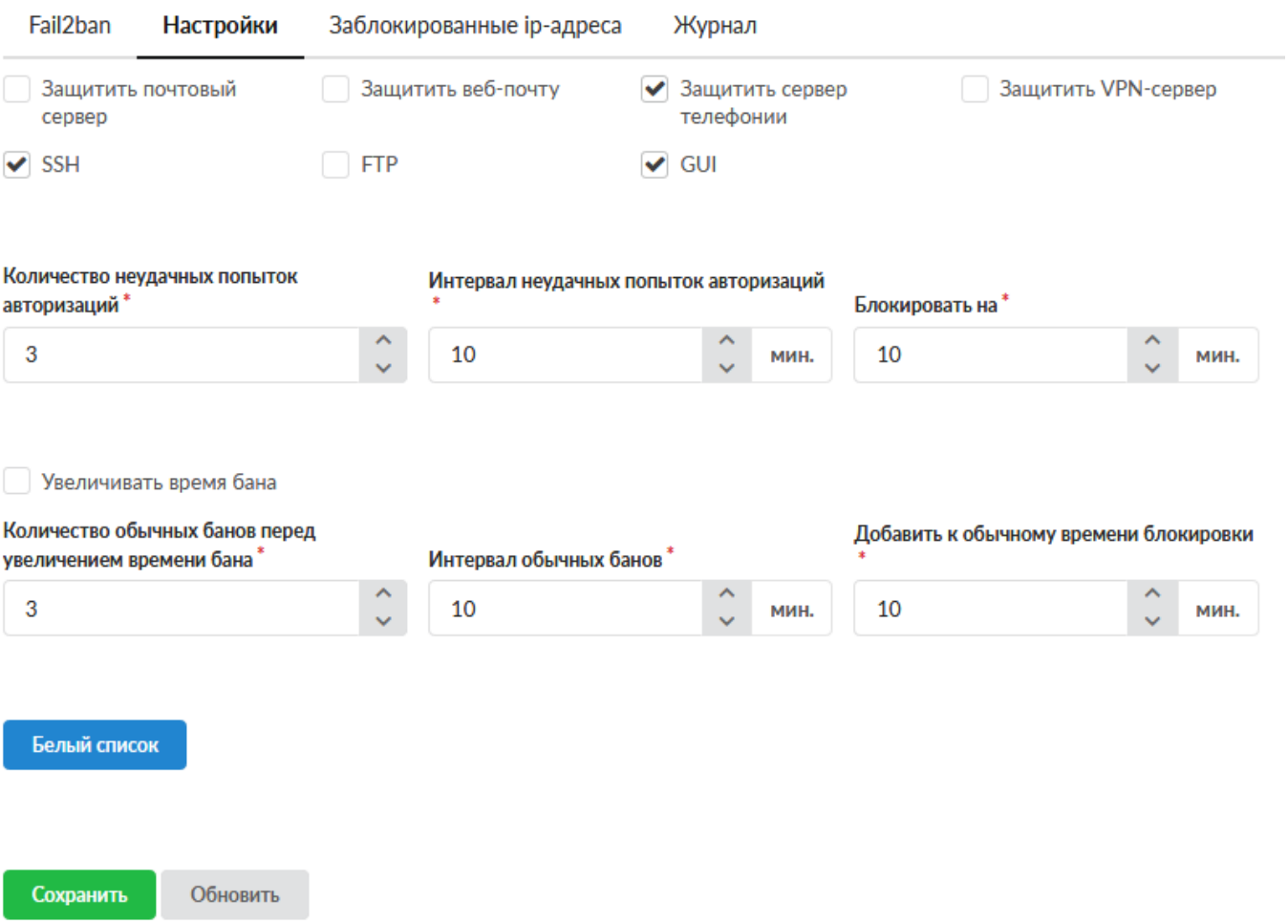
Модуль «Fail2ban» расположен в Меню «Защита», и имеет четыре вкладки: «Fail2ban», «Настройки», «Заблокированные ip-адреса», и «Журнал».

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



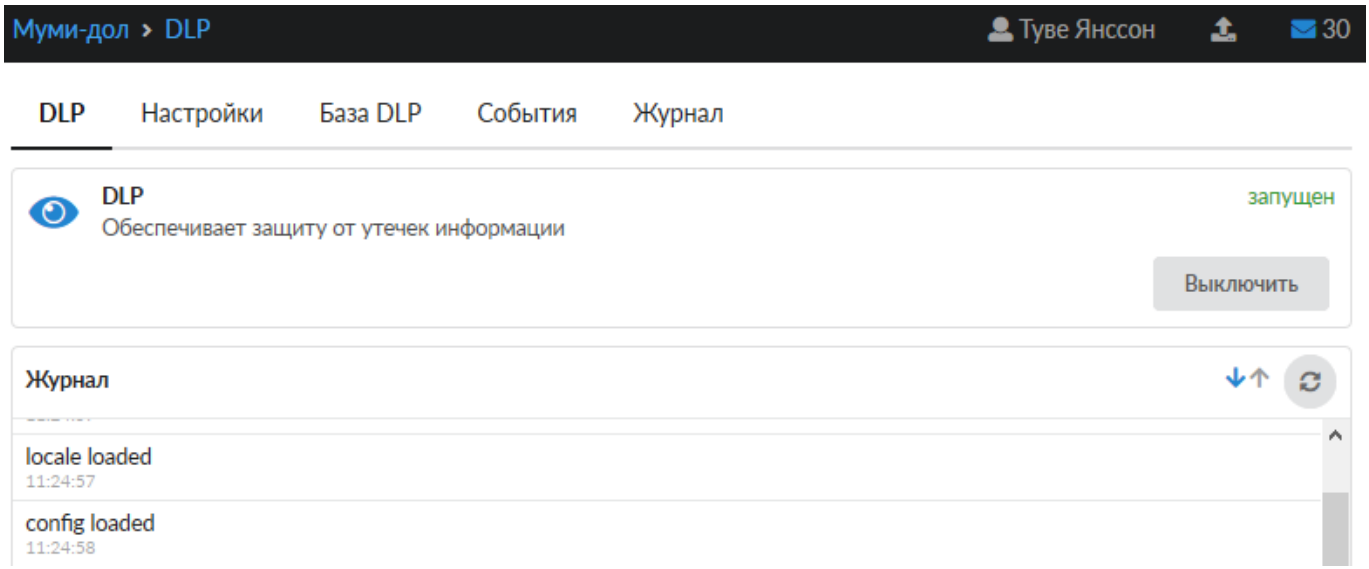
Данная вкладка предназначена для настройки работы модуля «Fail2ban».
Флаги: **«Защитить почтовый сервер», «Защитить веб-почту», «Защитить сервер телефонии», «Защитить VPN-сервер», «SSH», «FTP», «GUI«** - позволяют fail2ban анализировать логи авторизации в соответствующих модулях.
Поле «**Количество неудачных попыток авторизаций**» - позволяет задать количество неудачных попыток авторизации в модуле, отмеченном флагамом, после чего ip-адресу будет заблокирован доступ к «ИКС»
Поле «**Интервал неудачных попыток авторизаций**» - время, в течении которого подсчитывается количество неудачных попыток авторизации
Поле «**Блокировать на**» - При срабатывании блокировки, доступ с ip-адреса будет прекращен на заданной 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 способствования увеличения 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 на время = t + «Блокировать на».
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».

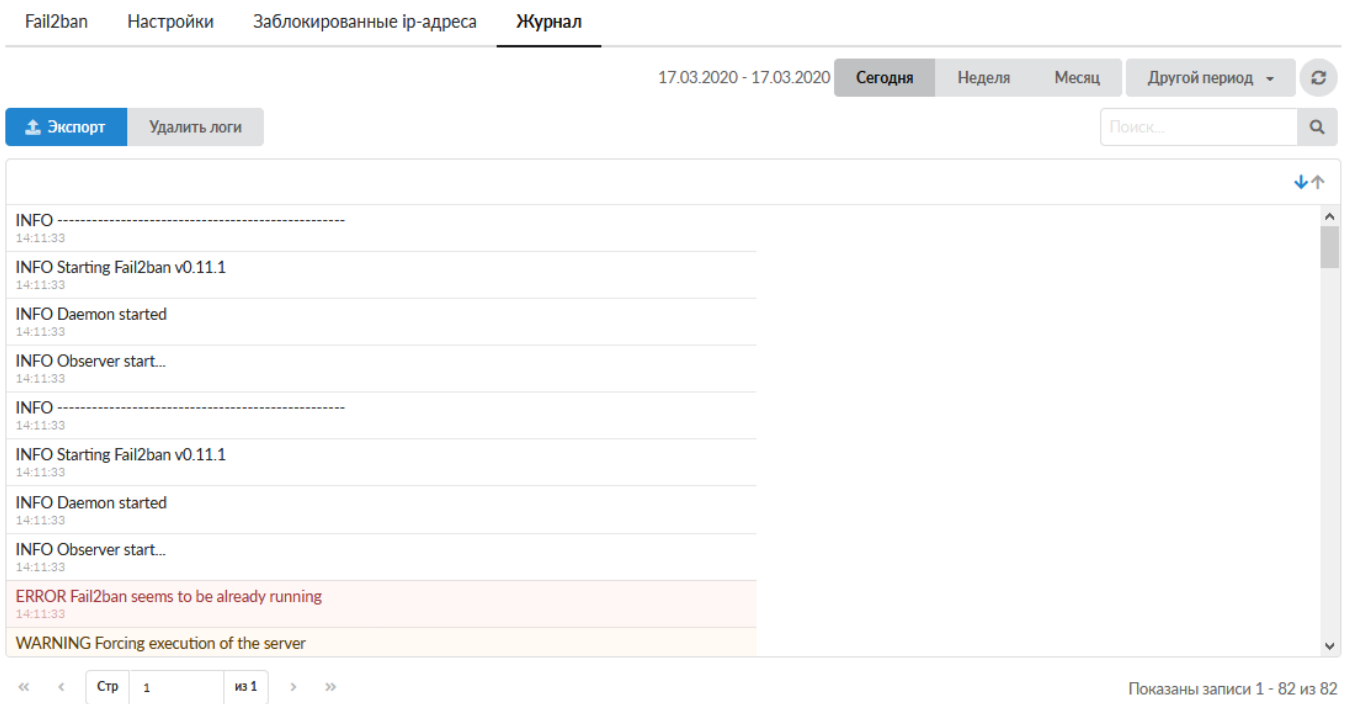
Кнопка «Белый список». При нажатии будет открыто новое диалоговое окно, в котором возможно задать соответствие ip-адреса и сервиса/всех сервисов, для которых fail2ban не

будет срабатывать.

Заблокированные ip-адреса



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».