Антивирус для интернет сайтов САНТИ

версия 0.4

руководство пользователя

«САНТИ», 2013

Автор: Игорь Митрофанов

Сайт: http://santivi.com

ICQ: 375156472

Электронная почта: info@santivi.com

Оглавление

Введение

САНТИ – бесплатная система безопасности интернет-сайтов с понятным интерфейсом и простейшей установкой. Основная цель системы – мониторинг целостности файлов на сайте, состояния сайта в поисковых системах, изменений в БД и моментальное предупреждение хозяина о заражении сайта посредством e-mail уведомлений и SMS.

Web-антивирус в автоматическом режиме, по заданным интервалам времени сканирует файлы и БД сайта; делает резервные копии сайта на хостинг и в облако Яндекс.Диск; проверяет блокировку сайта в поисковых системах. Система имеет механизм самозащиты в виде автовосстановления при малейшем вмешательстве в неё.

САНТИ – антивирус для сайта, который помимо слежения за состоянием сайта, содержит в себе множество инструментов для улучшения защищенности сайта и для лечения вирусов - это блокировщик сайта, генераторы паролей/.ftpaccess файлов, новости уязвимостей, редактор файлов, поисковик файлов по датам, автоматический уничтожитель вредоносных вставок (iframe, рекламных блоки, js вставки и т.д.), инструмент бекапа и восстановления сайта и мн.др.

В интерфейс каждого САНТИ входит он-лайн консультант, посредством которого любой пользователь антивируса, не выходя из панели управления, может запросить помощь квалифицированной техподдержки и совместно излечить сайт.

Антивирус САНТИ имеет простой и удобный интерфейс, который станет понятен любому пользователю, независимо от его

технической подготовки. Для установки САНТИ на сайт - достаточно просто скопировать его на хостинг и пройти диалог настроек. Все файлы антивируса устанавливаются на сайт, а исходные коды открыты для его доработки.

Открытость САНТИ преследует целью сделать его мощной непробиваемой стеной для злоумышленников, благодаря совместной работе над web-антивирусом сообществом специалистов по IT-безопасности.

1. Установка системы

1.1 Системные требования

САНТИ создан для защиты большинства сайтов в Интернете, а так как большинство сайтов написаны на PHP + MySQL и работают на Apache серверах, то и требования вытекают из этого:

- Apache;
- 4.3.2 >=PHP 5.2 и ваше;
- Пожелания: Memory_limit: минимальное значение 16, рекомендованное 32 и выше;
- Для САНТИ БД не требуется, но если требуется защита БД сайта, то работает с MySQL;
- Права файлов и папки 644.

САНТИ протестирован на большинстве известных в СНГ и за его пределами хостингах.

1.2 Процедура установки САНТИ

Установка САНТИ займет не более 10 минут времени и потребует минимального числа шагов:

1. Получите серийный номер на сайте http://santivi.com, введя URL сайта и e-mail.

2. Скачайте на странице “Скачать” архив с последней версией web-антивируса.

3. Создайте на хостинге в корне сайта папку для файлов антивируса, рекомендуется не использовать простые названия папки.

4. Скопируйте файлы САНТИ из архива в папку на хостинге.

5. Должен получиться URL к антивирусу вида: http://сайт.ru/папка сантивирусом/, пройдите по получившейся ссылке в антивирус посредством любого браузера. Если всё в порядке, перед вами возникнет окно входа, рис.1.

6. Если вы не увидели входа в антивирус, проверьте права папки и файл .htaccess на предмет блокировки доступа к папкам.

7. Первоначальный логин admin, пароль 12345 ОБЯЗАТЕЛЬНО СМЕНИТЬ.

Рисунок 1. Вход в САНТИ

1.3 Первый запуск, настройка САНТИ

При первом входе, система Вам не даст ничего делать, пока Вы не пройдёте диалог настроек от начала и до конца, рис.2. Диалог настроек содержит подсказки и пояснения ко всем пунктам и не составит труда его пройти, проделаем это.

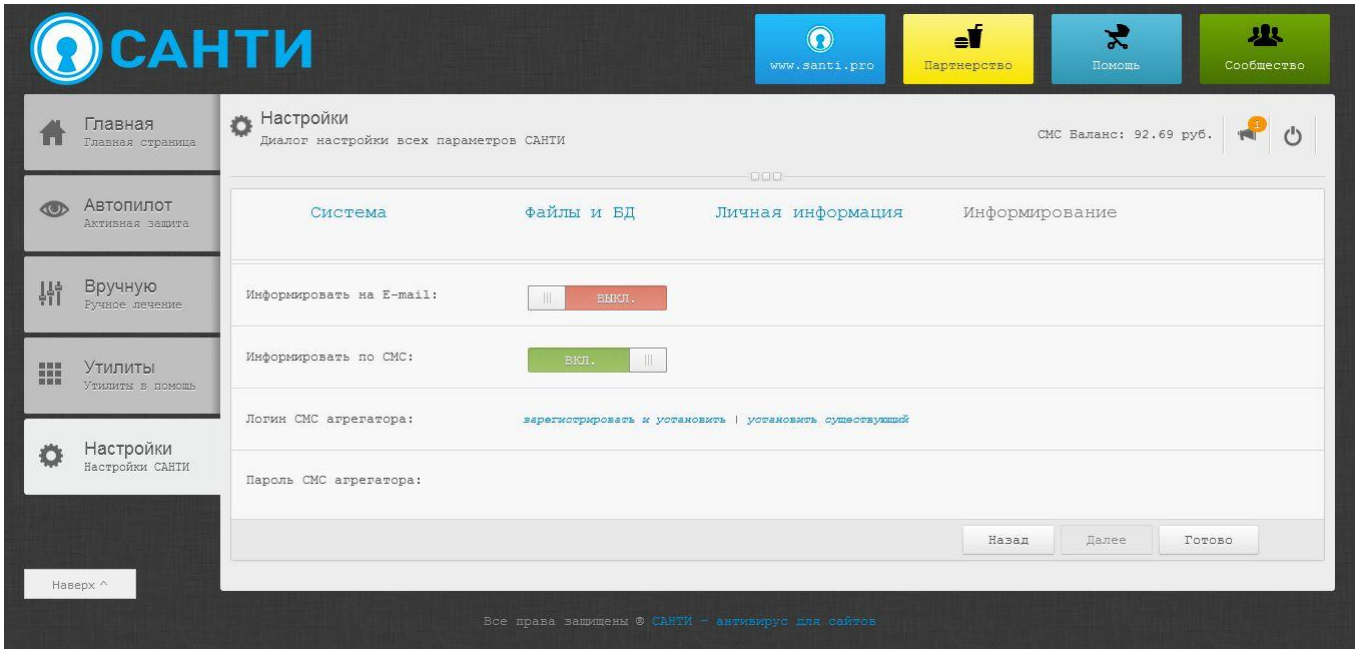

Рисунок 2. Диалог настроек

1. Вкладка “Система”, все поля должна быть заполнены обязательно:
    a. “Логин” для входа в систему – вводим свой логин на замену логину “admin”;
    b. “Пароль” для входа в систему – не скупитесь на сложность пароля, если не хватает фантазии воспользуйтесь утилитой “Генератор паролей”;
    c. “Адрес сайта” – адрес сайта на котором установлен САНТИ в формате http://сайт.ru, если забыли – посмотрите на подсказку под полем ввода;
    d. “Имя папки антивируса” – папка в которой лежат файлы САНТИ;

e. “Серверный путь к сайту” – важный пункт с которым нельзя ошибиться, подсказка под полем ввода, но она может ошибаться, проверяйте.

2. Вкладка “Файлы и БД”:

   a. “Кодировка БД” – пункт, необходимый для работы сканера изменений в БД;

   b. “Логин от Яндекс.Диск” – логин от вашего аккаунта в Яндекс.Диск, обязательное поле, если вы включаете автопилот бекапа сайта в облачное хранилище;

   c. “Пароль от Яндекс.Диск” – пароль от вашего аккаунта в Яндекс.Диск, обязательное поле, если вы включаете автопилот бекапа сайта в облачное хранилище;

   d. “Файл или папка исключение” – папка или файл, исключающиеся при бекапинге и сканировании – настоятельно рекомендуется указать имя папки САНТИ.

3. Вкладка “Личная информация”:

   a. “SANTI ID” – серийный номер SANTI, полученный вами через сайт http://santivi.com/ на почту, если ключ не будет введен – будут недоступны автопилоты, он-лайн консультант;

   b. “E-mail” – ваш почтовый ящик, на которые будут присылаться антивирусом уведомления, при обнаружении заражения сайта;

   c. “Моб.телефон” – номер мобильного телефона, на который САНТИ будет отправлять смс уведомления, при обнаружении заражения сайта.

4. Вкладка “Информирование”:

   a. “Информировать на E-mail” – тумблер, включающий e-mail уведомления от САНТИ;

   b. “Информировать по СМС” – тумблер, включающий СМС уведомления от САНТИ;

c. “Логин СМС агрегатора” – логин от аккаунта в сервисе отправки СМС. Зарегистрироваться возможно не выходя из системы нажатием по ссылке “зарегистрировать и установить”, если аккаунт имеется – то нажми ссылку “установить существующий”.

d. “Пароль СМС агрегатора” - логин от аккаунта в сервисе отправки СМС, устанавливается при выборе ссылки “ зарегистрировать и установить” или “ установить существующий”

После заполнения всех полей и выставления всех тумблеров – нажимаем “ГОТОВО”. САНТИ сохранит все настройки, запомнит свой образ для автозащиты, просканирует ваш сайт и позволит работать дальше.

Антивирус установлен, можно переходить к изучению его функционала.

2. Знакомство с системой САНТИ

САНТИ установлен и настроен и теперь есть доступ ко всем разделам интерфейса сайта.

Web-антивирус для сайтов САНТИ - это совокупность автопилотов для проверки целостности файлов, инструментов для ручного сканирования/лечения сайта, утилит для лечения сайта и улучшения безопасности сайта.

Антивирус имеет систему самозащиты, при обнаружении вмешательства в свои файлы он удаляет все свои файлы и откатывает первоначальную, функционирующую корректно, версию.

САНТИ имеет в интерфейсе чат-менеджер для общения со специалистами по лечению сайтов. Отображает новости продукта и информирует, если пора обновиться.

Главный страница интерфейса антивируса (рис. 3) отображает список подозрительных действий или событий и позволяет просмотреть/отредактировать/вылечить любой из скриптов сайтов, поставить ему статус. Под списком подозрительных файлов отображается график обнаружений подозрительных объектов на защищаемом сайте.

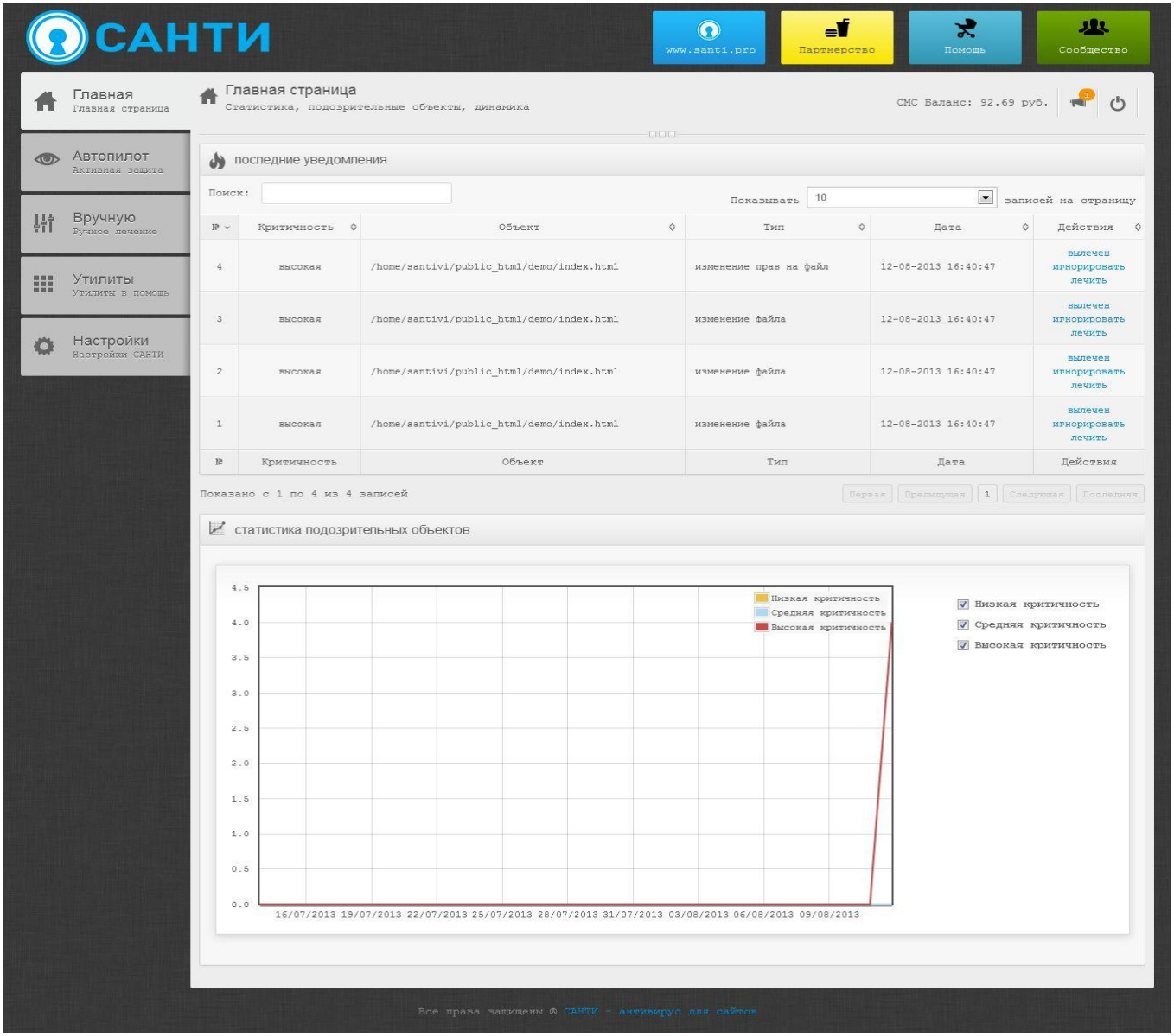

Рисунок 3. Главная страница САНТИ

Автопилоты – это проактивная защита вашего сайта:

- Мониторинг файлов сайта;
- Бекапинг файлов сайта на хостинг или в облако;
- Мониторинг базы данных сайта;
- Проверка сайта глазами поисковых систем;
- Проверка сайта глазами десктопных антивирусов;
- Проверка сайта по сигнатурам.

Защита вручную – быстрая ручная проверка файлов сайта на вирусы/изменения/соответствие сигнатурам:

- Проверка по сигнатурам;
- Поиск изменений в файлах;
- Проверка блокировки в ПС;
- Поиск файлов по дате изменения;
- Удаление вредоносных вставок по маске.

Утилиты – набор полезного инструментария:

- Date-поиск файлов;
- Поиск и удаление вредоносных вставок;
- Бекап и восстановление;
- Редактор файлов;
- .htaccess блокировка сайта;
- .ftpaccess конфигуратор;
- Генератор паролей;
- PHP info;
- Новости САНТИ и уязвимостей сайтов с разрешения http://securitylab.ru/.

В интерфейсе САНТИ в шапке справа располагаются блоки дополнительного меню:

- Блок перехода на сайт антивируса;
- Блок перехода “Партнерство” на страницу обратной связи с разработчиком системы;
- Блок “Он-лайн помощь” – вызов окна чатменеджера с IT-специалистом антивируса САНТИ для помощи в лечении сайта;
- Блок “Сообщество” – при нажатии открывает форум сообщества САНТИ.

В информационной области интерфейса САНТИ, справа от заголовка, на всех страницах антивируса, расположены:

- Кнопка выхода из системы;
- Раздел срочных уведомлений – в нем выводятся по мере появления срочные уведомления от проекта САНТИ и уведомления о необходимости обновления web-антивируса;
- Информация о балансе в СМС сервисе.

Версию установленного у вас САНТИ всегда можно посмотреть в подвале системы.

Таков не полный список возможностей и инструментов системы безопасности и он будет постоянно расширяться.

3. Работа с системой САНТИ

3.1 Автопилот

Раздел интерфейса САНТИ (рис.4), позволяющий активировать необходимые автоматические инструменты, определять их параметры, задать периодичность выполнения автопилотов. Для

работы автопилотов должен быть указан в настройках корректный для защищаемого сайта SANTI ID.

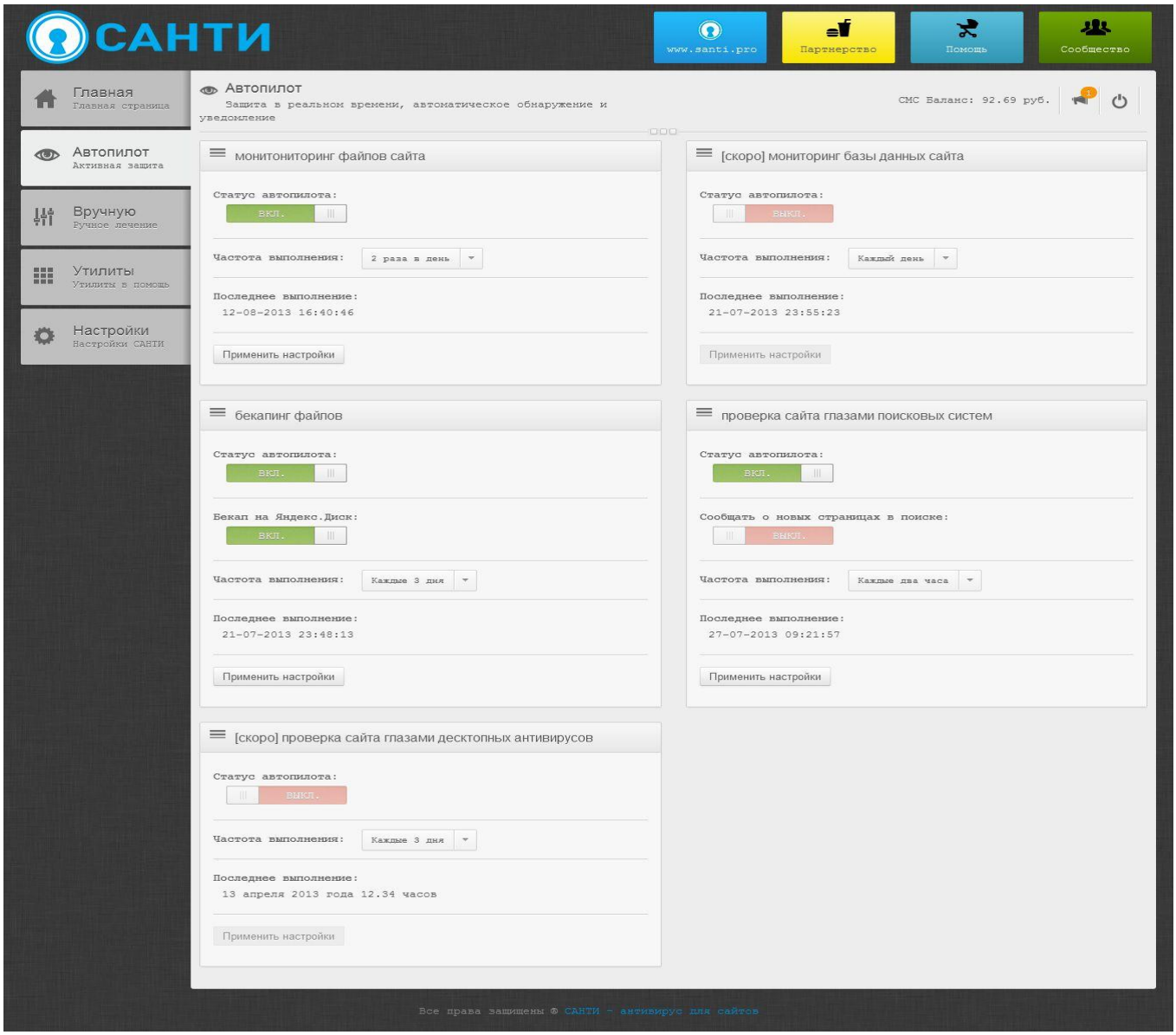

Рисунок 4. Раздел "Автопилот"

3.1.1 Самозащита

Самозащита САНТИ включена на автоматическое выполнение сразу после применение настроек. Через определенные интервалы времени антивирус проверяет целостность своих файлов, за исключением постоянно меняющихся нескольких файлов, и при первом обнаружении вмешательства – возвращает файлы в исходное состояние.

3.1.2 Мониторинг файлов сайта

Автопилот, сканирующий файлы/скрипты сайта на целостность, в сравнении с предыдущим образом файлы, изображения, папки исключения, большие файлы, исключает часто изменяемые файлы, такие как error логи.

Реагирует на разницу в дате изменения файла, в размере файла, в контрольной сумме файла, на появление новых файлов и папок, на удаление файлов. При обнаружении изменений уведомляет пользователя по e-mail и СМС, создает запись в свою базу данных и отображает события и файлы в списке обнаруженных объектов на главной странице САНТИ.

3.1.3 Проверка сайта глазами поисковых систем

Если сайт заражен вирусом и несет опасность для его посетителей, то многие поисковые системы и в частности Яндекс и Google блокируют сайт в поисковой выдаче, выдавая пользователям сообщение о вредоносности и опасности сайта, и занося сайт в список подозрительных. Часто поисковые системы ошибаются. Результатом таких мер является потеря доверия людей к сайту и падение посещаемости.

Автопилот САНТИ по сканированию поисковых систем проверяет через определенные пользователем интервалы времени состояние сайта в ПС Яндекс, Google и уведомляет при обнаружении блокировки о таковой по СМС и e-mail. Уведомление позволяет вовремя среагировать на блокировку, принять меры и написать в ПС об исправности сайта.

3.1.4 Бекапинг файлов сайта

Автопилот бекапа файлов сайта архивирует весь сайт через заданные пользователем интервалы времени и сохраняет их либо на сайте в папке САНТИ по адресу http://сайт/санти/datas/backups/ в файл с расширением .sabu, либо сохраняет архив в облаке Яндекс.Диск (при включенном тумблере Я.Д. и заданных в настройках параметрах аккаунта Яндекс). При архивации игнорируется папка с антивирусом, сохраняются права на файлы, структура сайта.

Для распаковки архива с файлами сайта используется утилита бекапинга/восстановления сайта из раздела “Утилиты” САНТИ. Так же в разделе “Скачать” сайта http://santivi.com/ доступна версия приложения для Windows, позволяющая распаковать файлы .sabu на ПК пользователя.

3.2 Вручную

Раздел (рис. 5), позволяющий не дожидаясь срабатывания автопилота просканировать изменения в файлах и структуре сайта, запустить проверку состояния в поисковых системах и при обнаружении критических изменений – сразу перейти к лечению сайта.

Раздел содержит возможность перехода к утилите поиска файлов по интервалу дат изменений, к утилите удаления вредоносных вставок по маске, к инструменту редактирования файлов. Принцип работы с вышеназванными утилитами смотрите в соответствующих разделах документации к САНТИ.

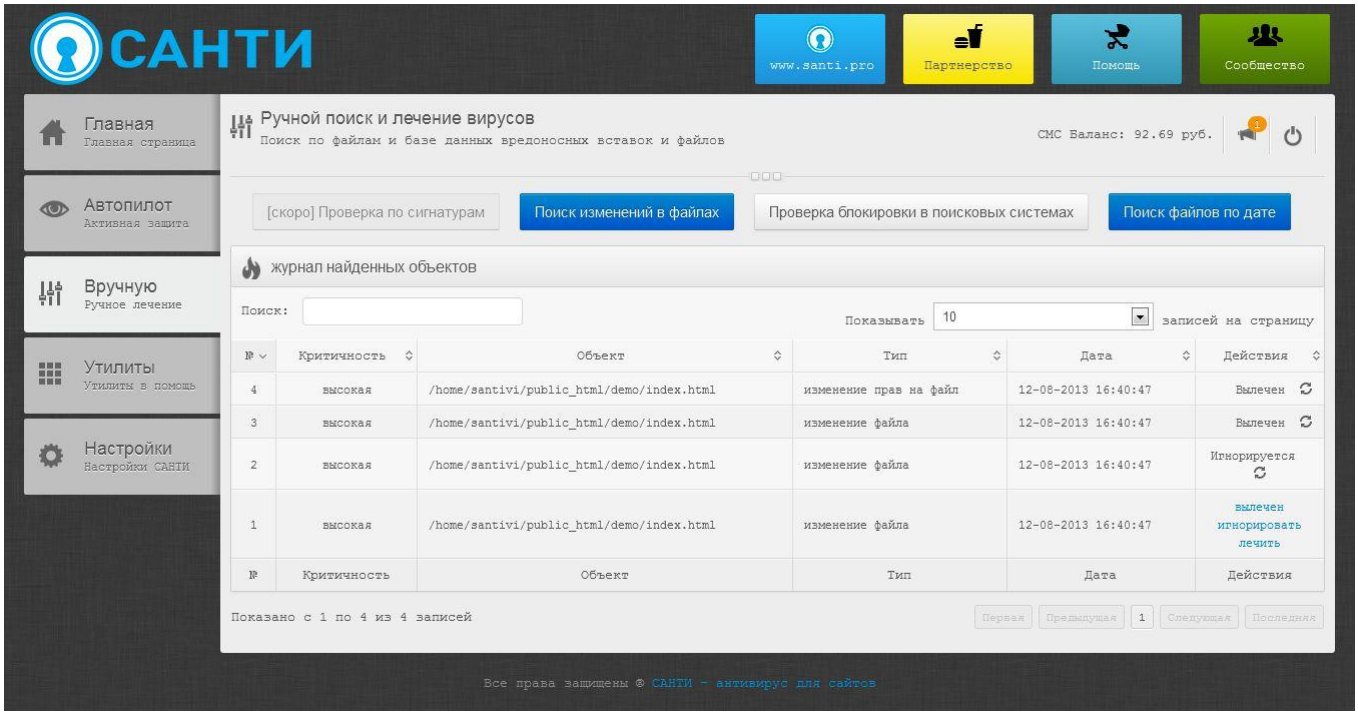

Рисунок 5. Раздел "Вручную"

3.3 Процесс лечения файлов

Система безопасности сайтов САНТИ очень гибкий инструмент, позволяющий использовать его в лечении сайта и как вспомогательное средство, которое не было установлено до заражения интернет-проекта, так и как средство реактивного обнаружения заражений и восстановления сайта будучи установленным. Рассмотрим обзорно оба названных варианта.

3.3.1 Первичное лечение сайта с САНТИ

Статью о лечении сайта с помощью САНТИ вы можете прочитать на нашем блоге по ссылке http://santivi.com/category/blog-santi .

3.3.2 Лечение сайта при обнаружении угрозы системой САНТИ

Статью о том, что делать, если САНТИ обнаружил и сообщил о вмешательстве в сайт и его заражении, вы можете прочесть на нашем блоге по ссылке http://santivi.com/category/blog-santi .

3.4 Уведомления от антивируса

Так как именно от того, насколько быстро среагирует собственник интернет-проекта и устранит вредоносные скрипты на сайте, зависит сохранность репутации и посещаемости сайта, система безопасности сайтов САНТИ оснащена двумя системами уведомления о угрозе: e-mail уведомления, СМС уведомления.

При обнаружении автопилотом САНТИ вирусов на сайте система отправляет e-mail на почту с информацией об обнаружении и отправляет СМС на телефон хозяина сайта с информацией об обнаружении и критичности события.

Уведомления отправляются автопилотами: “ Мониторинг файлов сайта”, “Проверка сайта глазами поисковых систем”.

Уведомлениями можно управлять через раздел “Настройки” интерфейса системы безопасности, здесь возможно их отключать или активировать.

Для получения СМС сообщений от САНТИ, в разделе “Настройки” необходимо:

- указать номер мобильного телефона в федеральном формате;

- зарегистрироваться в системе СМС отправки, что можно проделать сразу в разделе “Настройки” во вкладке “Информирование”;
- установить логин и пароль доступа к системе СМС отправки – это произойдет автоматически при регистрации в системе;
- пополнить баланс в СМС сервисе, стоимость 1 СМС на день написания инструкции составляла 25 коп./смс..

После регистрации в СМС сервисе у вас будет 10 бесплатных СМС.

3.5 Инструменты системы

Раздел “Утилиты” (рис. 6) содержит в себе массу инструментов для обеспечения безопасности сайта, для лечения сайта, для информационной поддержки пользователя системы. Рассмотрим каждую из утилит подробнее.

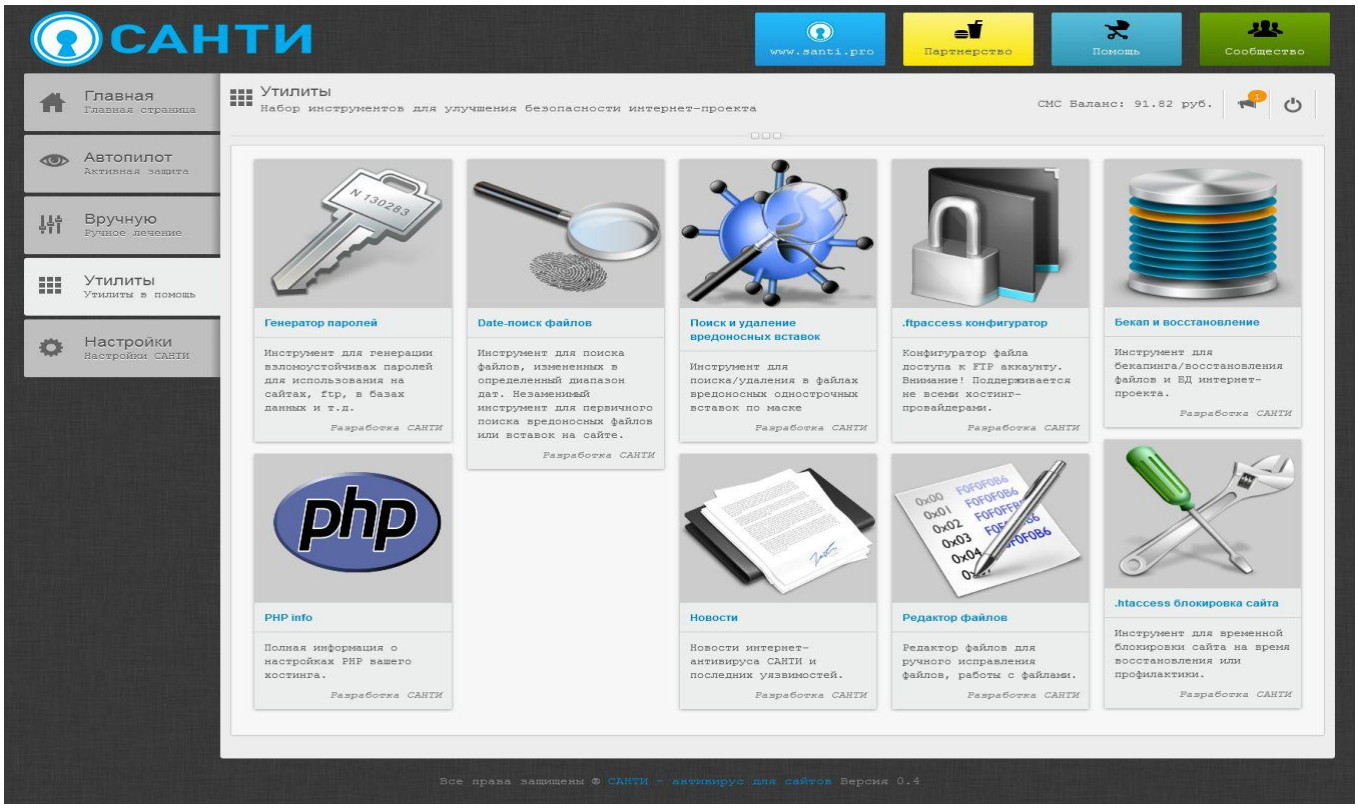

Рисунок 6. Раздел "Утилиты"

3.5.1 Генератор паролей

Инструмент “Генератор паролей” (рис. 7) – незаменимый помощник при нехватке фантазии для создания сложных, взломоустойчивых паролей.

Параметры:

- Длина пароля для генерации;
- Тип пароля
    - Любые символы в любом регистре;
    - Буквы+цифры в верхнем и нижнем регистрах.

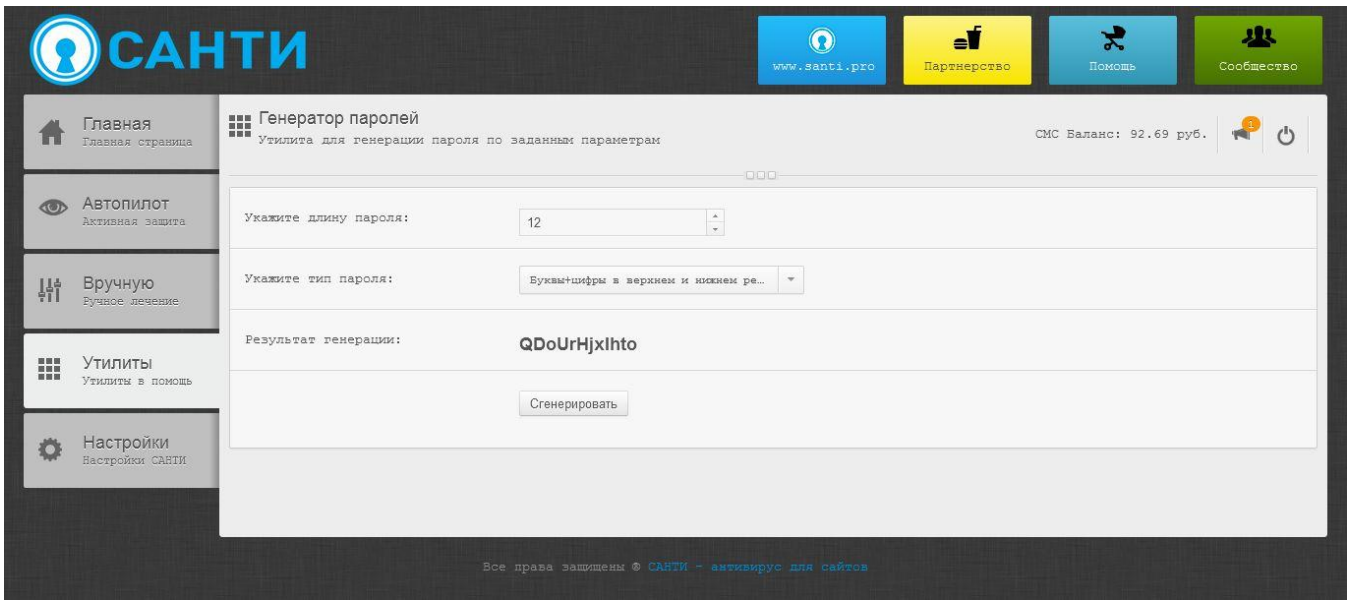

Рисунок 7. Утилита "Генератор паролей"

3.5.2 FTP конфигуратор

Инструмент для настройки и генерации файла управления доступом по FTP к сайту *.ftpaccess* (рис 8.).

Огромная доля взломов сайтов и заражений происходит вследствие “угона” у владельцев сайтов их ftp аккаунтов, панацеей от

подобных взломов может быть настройка файла доступа к FTP *.ftpaccess.* В нем мы можем указать IP дозволенных пользователей FTP, ограничить доступ всем остальным и мн.др..

ВНИМАНИЕ! Файл обрабатывается FTP серверами на базе *ProFTPD, Pure-FTP.*

Результат генерации содержимого для файла .ftpaccess необходимо поместить в одноименный файл в корневую директорию вашего сайта, тогда он будет действовать на каталог в котором размещен и на его подкаталоги.

Параметры:

- Запрет доступа всем – при выборе данной настройки вы получите содержимое файла, полностью блокирующее доступ к FTP;
- Запрет доступа для IP – указываем IP адреса, которые хотим заблокировать, через запятую;
- Разрешить доступ для IP – через запятую указываем IP адреса, которым хотим дать доступ к сайту через FTP, например, IP адрес офиса, IP адрес дома;
- Запретить перезапись существующих файлов – параметр который позволяет просматривать по FTP файлы, но не перезаписывать файлы.

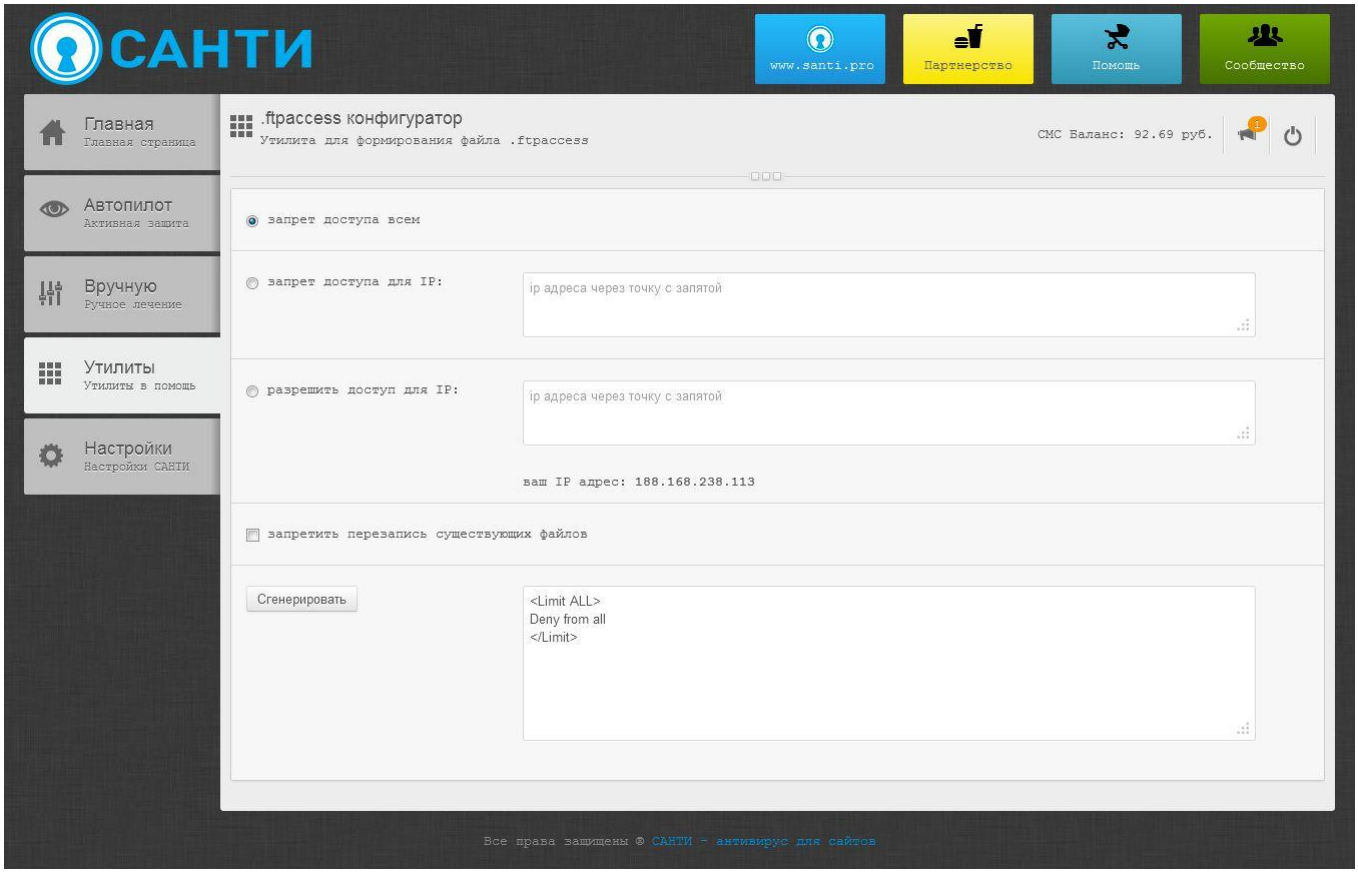

Рисунок 8. Утилита ".ftpaccess конфигуратор"

3.5.3 Бекап и восстановление

Многофункциональная утилита для бекапа/восстановления сайта, на котором установлен САНТИ (рис. 9).

При бекапе файлов сайта утилита упаковывает все файлы в архив с расширением .sabu (gzip архивация), в названии файла помечается дата бекапинга. Архив сохраняется в папке санти/datas/backups/. При архивации утилита сохраняет права файлов и папок, игнорирует указанные папки и мн.др.

Параметры бекапа:

- Имя бекапа – устанавливается автоматически, но можно изменить;

- С какой папки бекапим – автоматически устанавливается корневой каталог сайта, возможно редактирование;
- Исключить папку – папка, которую стоит игнорировать при бекапинге, по умолчанию – папка САНТИ;
- Только с расширением – архивируем файлы с указанным расширением;
- Не более (байт) – ограничение на размер файлов, указываем в байтах максимальный для бекапинга объем файла.

Если мы пользуемся утилитой для восстановления, то вабираем действие “Восстанавливаем”, утилита предложит вам список доступных для распаковки файлов.

Параметры:

- В какую папку восстанавливаем – по умолчанию восстановление идет в папку санти/ datas/unarchive/, этим параметром мы задаем имя папки по вышеназванному пути;
- Существующие бекапы – список доступных в папке backups архивов с бекапами, восстанавливаться будет выбранный.

Формат архива .sabu специфичен и ни одно из существующих средств распаковки архивов не поможет Вам с распаковкой файла, кроме данной утилиты. В ближайшее время будет разработано Windows приложение для распаковки бекап файлов на ПК.

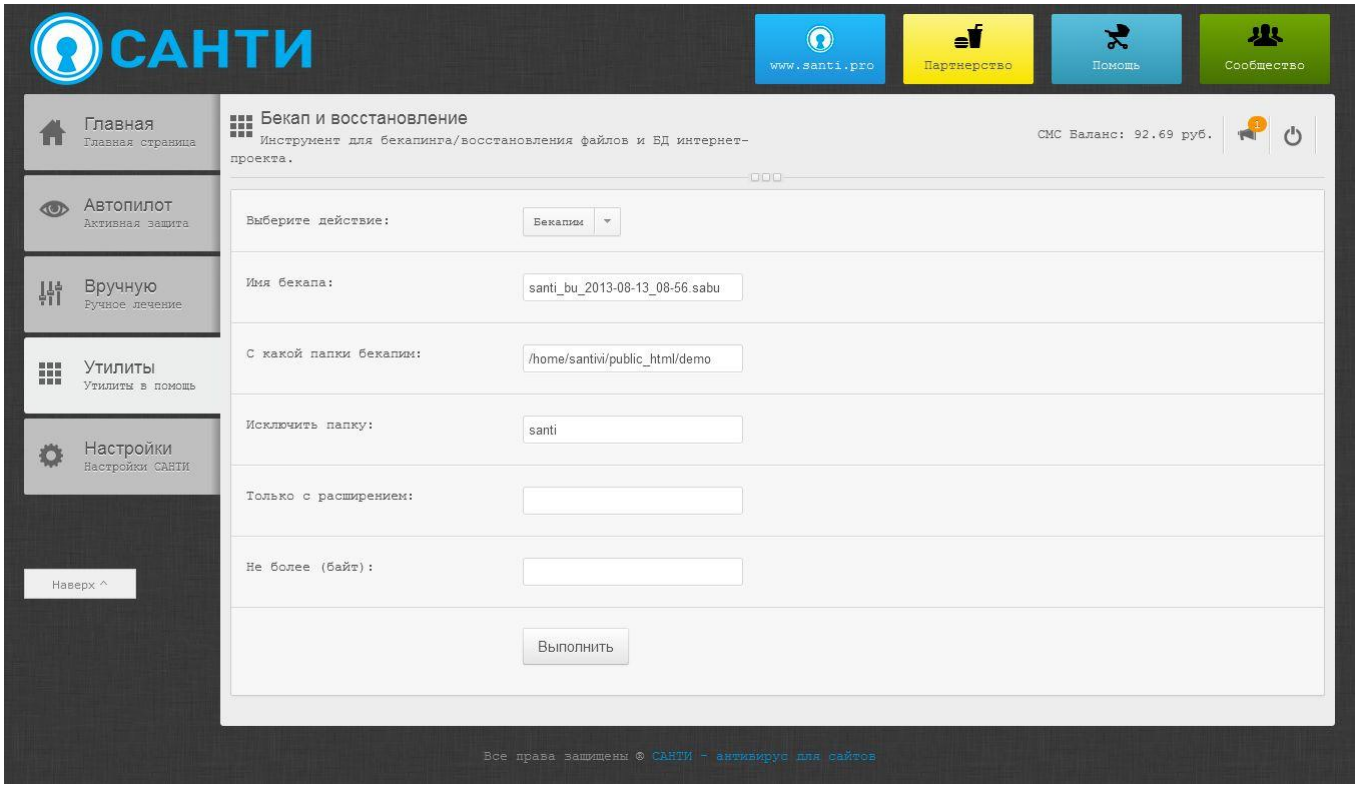

Рисунок 9. Утилита "Бекап и восстановление"

3.5.4 Блокировка сайта

Утилита “.htaccess блокировка сайта” (рис. 10) – инструмент, позволяющий, в одно нажатие заблокировать/разблокировать сайт, на котором установлен САНТИ.

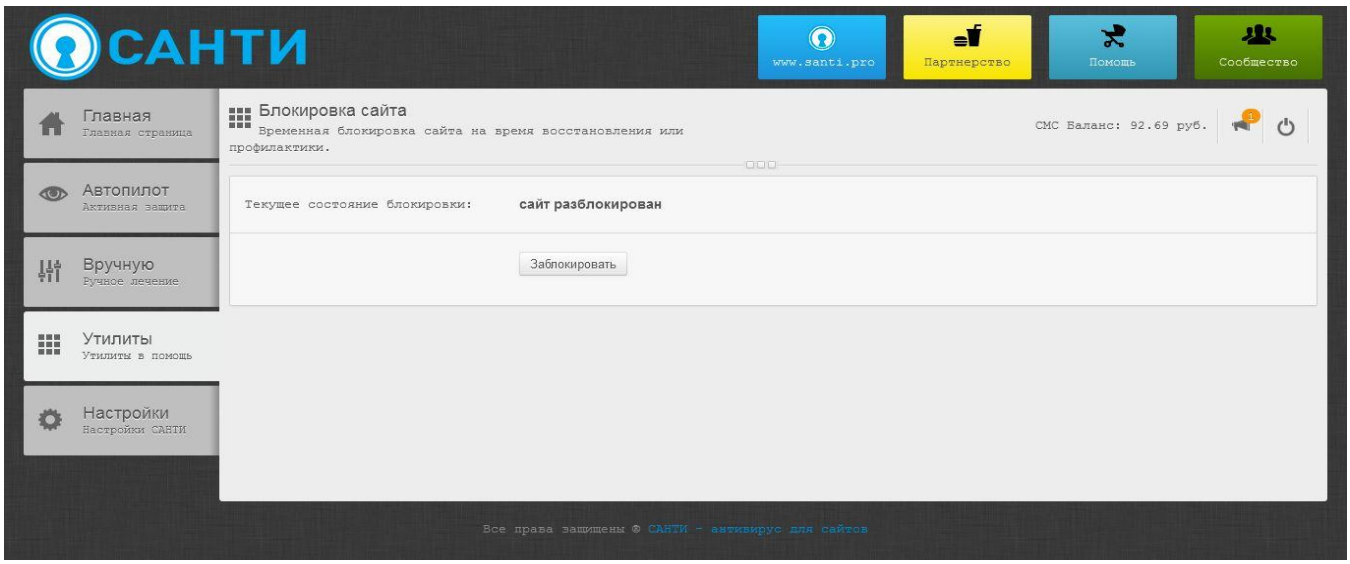

Рисунок 10. Утилита ".htaccess блокировка сайта"

Если сайт заражен, подвергается DDOS атаке или сломан в результате постороннего вмешательства, рекомендуется пользоваться этим инструментом во время лечения или восстановления сайта. Благодаря блокировке сайта вы не ударите в грязь лицом перед посетителями и сохраните их компьютеры невредимыми от вирусов.

При активации блокировки утилита делает временную запись в корневой .htaccess файл сайта и показывает всем посетителям страницу, представленную на рисунке 11.

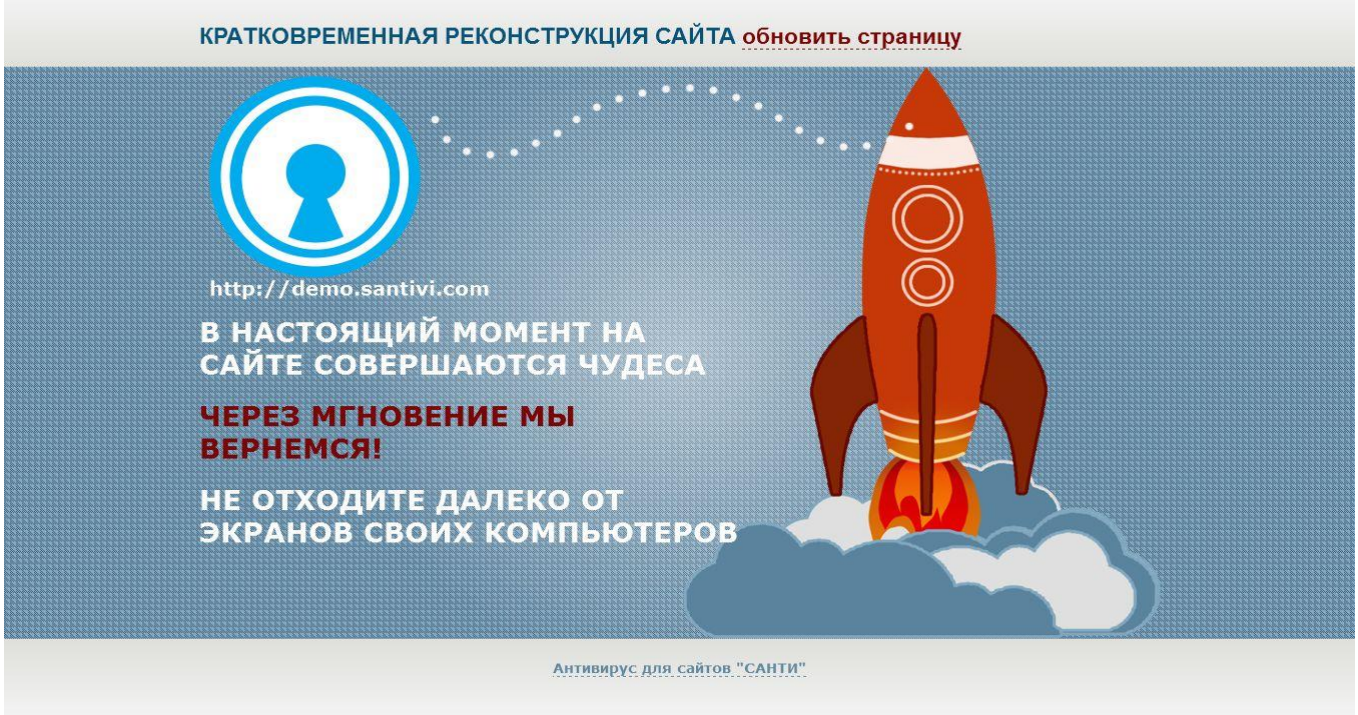

Рисунок 11. Экран блокировки сайта

3.5.5 PHP info

Инструмент, который можно отнести к разряду информационных и часто необходимых веб-администраторам при установке и настройке тех или иных скриптов, когда необходимо посмотреть параметры Сервера/PHP и т.д.. Утилита “PHP info” (рис. 12) теперь

всегда под рукой и покажет Вам всю информацию о вашем хостинге.

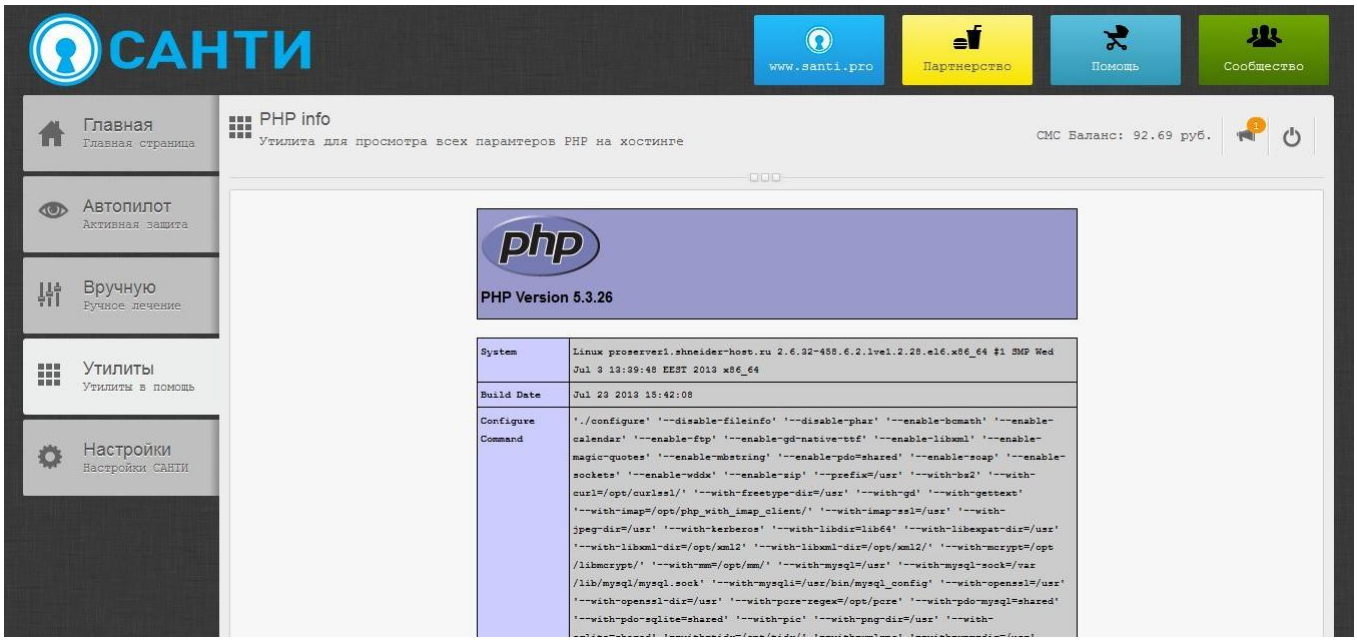

Рисунок 12. Утилита "PHP info"

3.5.6 Новости

Информационная утилита “Новости” (рис. 13) - это RSS ленты новостей уязвимостей популярных CMS и ПО, новостей САНТИ.

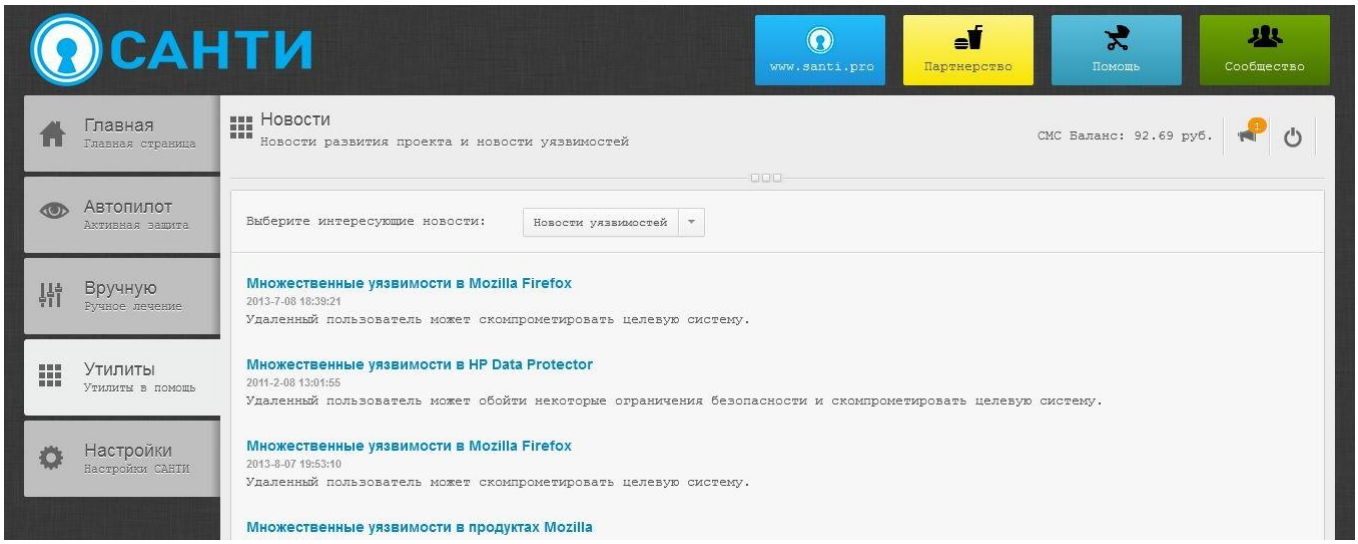

Рисунок 13. Утилита "Новости"

3.5.7 Date-поиск файлов

Утилита для поиска файлов сайта с датой изменения из заданного интервала дат (рис. 14). Поисковый инструмент является незаменимым помощником при поиске зараженных файлов в известный промежуток дат, рекомендуется к использованию, когда Вы установили антивирус на уже зараженный сайт и требуется его излечить с помощью САНТИ.

Почему Date-поиск? Как правило, скрипты сайтов крайне редко изменяются после их загрузки на сервер, частые изменения распространяются только на файлы контента: изображения, документы, конфигурационные файлы, все остальные файлы остаются неизменными с момента их загрузки. Вмешиваясь в файлы, вирусы меняют дату изменения и их легко вычислить при помощи данного инструмента.

Параметры:

- Диапазон дат для поиска – начальная и конечная дата диапазона дат изменений, из которого искать файлы.
- Расширения (через запятую) – список расширений файлов, которые мы можем либо игнорировать, либо обрабатывать, см. параметр ниже;
- Действия с указанными расширениями:
    - Указанные исключить;
    - Указанные проверять;
    - Не учитывать расширения;

В результате работы поисковика вам выдастся список найденных файлов с указанием пути к файлу, даты изменения и кнопкой

редактирования файла. На выбор –можно вылечить его редактированием в САНТИ, либо отредактировать файл по выданному пути через FTP.

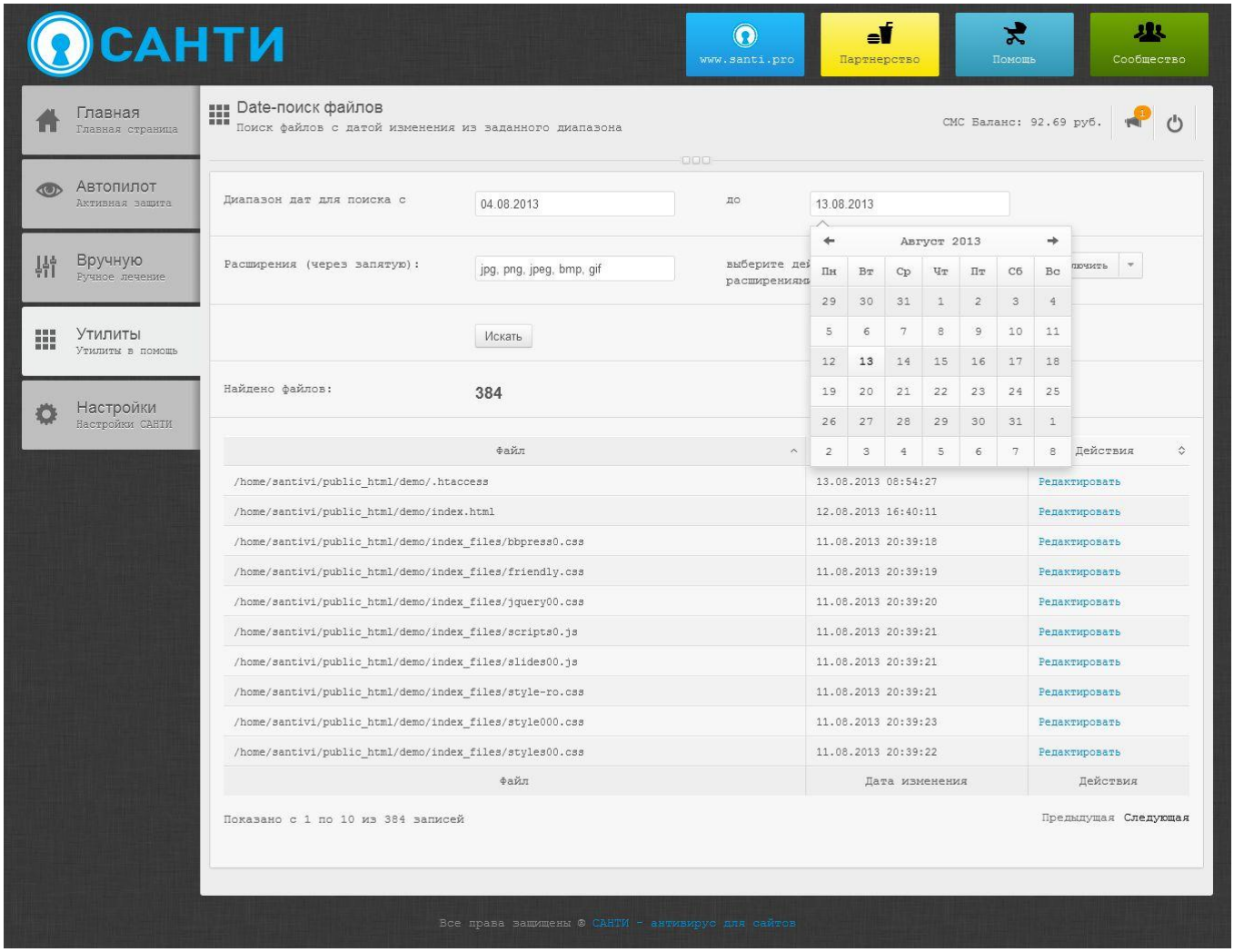

Рисунок 14. Утилита "Date-поиск файлов"

3.5.8 Редактор файлов

Вспомогательная утилита для найденных САНТИ измененных файлов, помогает просматривать и редактировать объекты. Редактор файлов (рис. 15) имеет подсветку кода, автоопределение кодировки файла, которая может ошибаться – !!!всегда задавайте кодировку файла вручную. После редактирования нажмите кнопку

“Сохранить” и файл на хостинге будет изменен. При самостоятельном запуске утилиты, функционал ограничен.

Параметры:

- Кодировка файла.

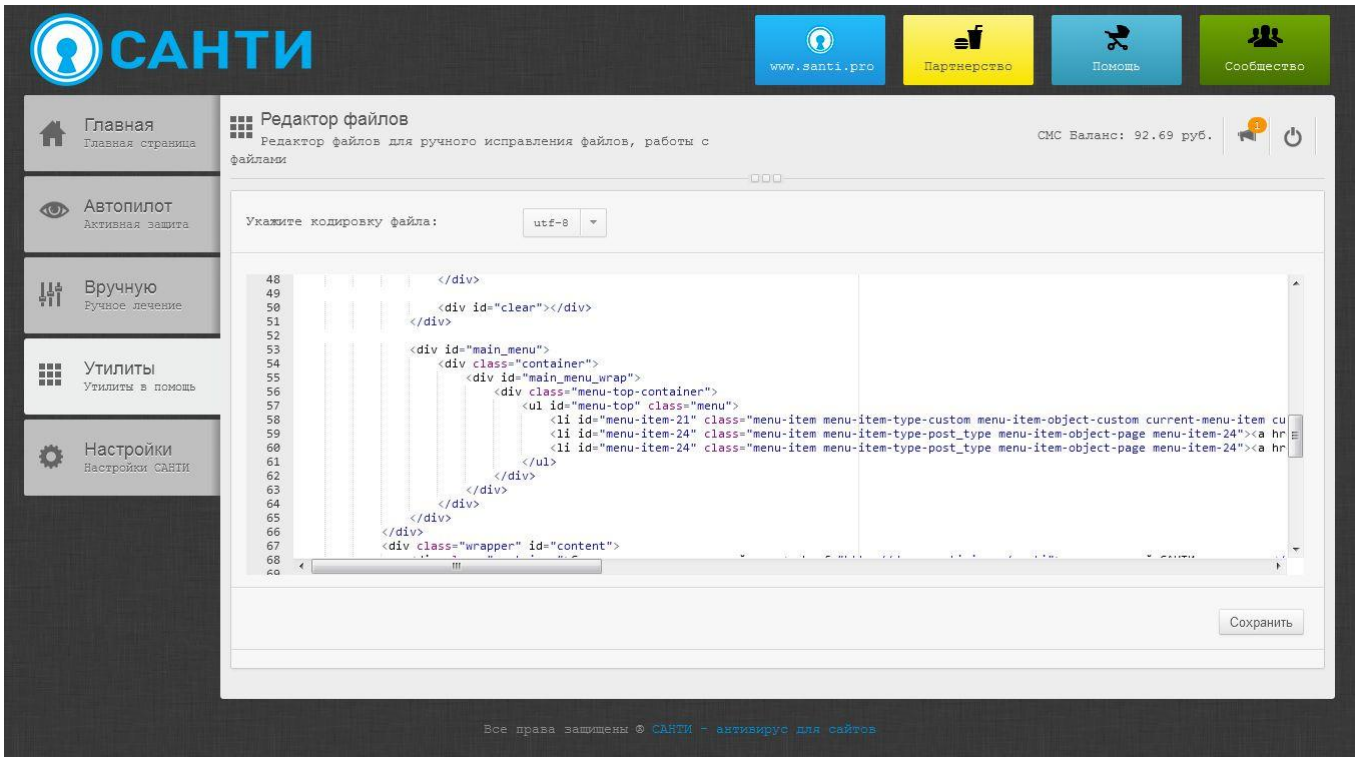

Рисунок 15. Утилиты "Редактор файлов"

3.5.9 Поиск и удаление вредоносных вставок

Утилита для массового поиска/удаления вредоносных вставок в скриптах сайта (рис. 16). Утилита позволяет быстро и легко найти и вылечить все файлы, если известна строка вредоносной вставки. Инструмент помогает при заражении сотен файлов одним и тем же вредоносом, например, распространенный iframe вирусы в .js javascript файлах.

Для работы инструмента достаточно ввести начало вредоносной строки и её конец, по которым можно однозначно идентифицировать эту строку, далее задать параметры и нажать “Выполнить”.

Параметры:

- Начало вредоносной вставки – например, “;document.write(unescape('%3”;
- Конец вредоносной вставки – например, “3E'));”;
- Расширения (через запятую) – список расширений файлов, которые мы можем либо игнорировать, либо обрабатывать, см. параметр ниже;
- Действия с указанными расширениями:
    - Указанные исключить;
    - Указанные обрабатывать;
    - Не учитывать расширения;
- Действие:
    - Ищем;
    - Ищем и лечим.

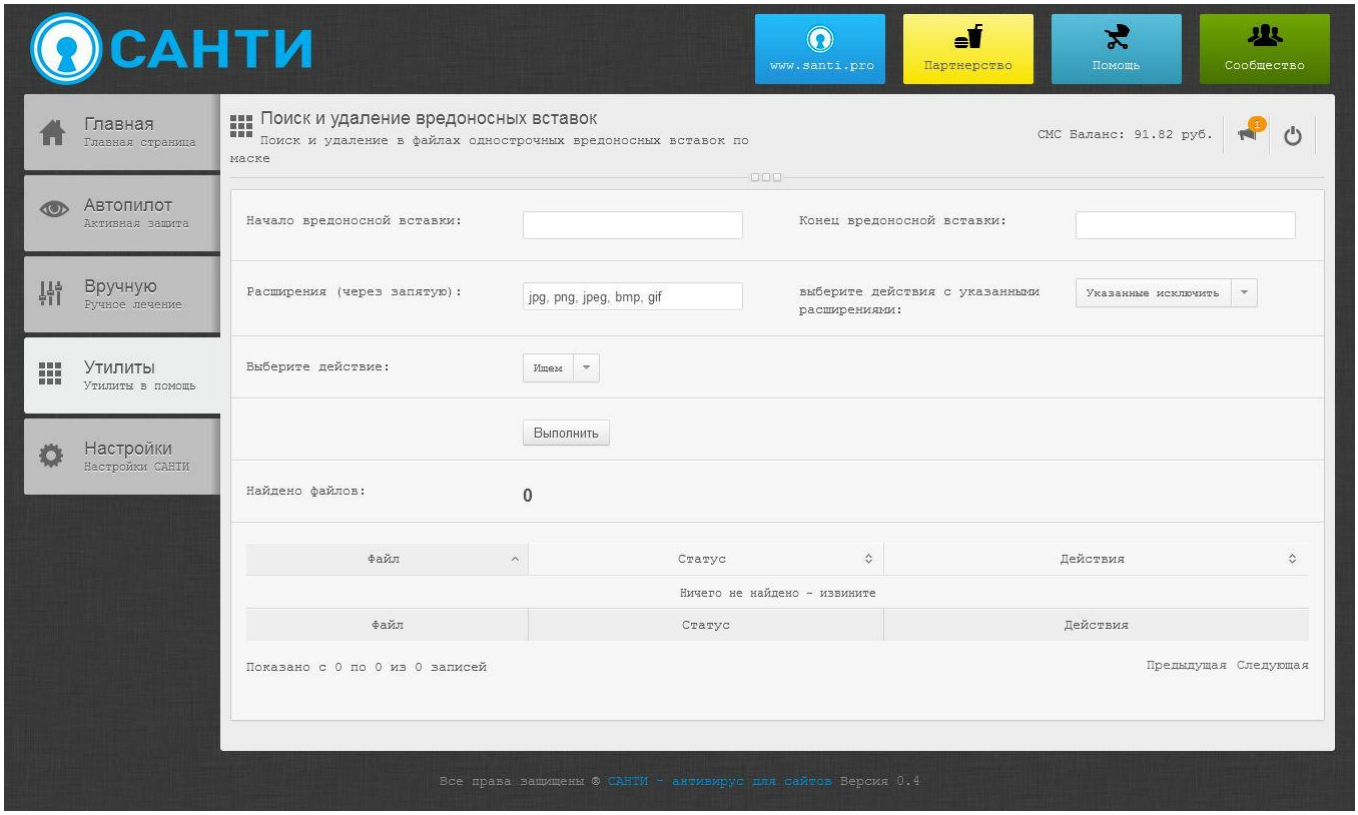

Рисунок 16. Утилита "Поиск и удаление вредоносных вставок"

спасибо!