МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

Проверка и устранение признаков заражения сайта

Для технических специалистов и администраторов сайтов

Если сайт уже отключён администратором площадки, то до окончания очистки его страницы и административная часть CMS недоступны. Работать с сайтом можно через ISPmanager, его файлы и базу данных. В рекомендациях приведены действия для первичной проверки и очистки. В большинстве случаев для полной очистки нужен специалист с опытом администрирования сайтов и баз данных, который понимает устройство CMS и может читать PHP, JavaScript и SQL хотя бы на базовом уровне.

1. Что доступно при отключённом сайте

Отключение сайта не закрывает учётную запись ISPmanager. Ответственный специалист организации может продолжать работу с файлами и базой данных сайта.

Доступно	Для чего использовать
Главное меню → Файлы	Просмотр, копирование, загрузка, распаковка, замена и изменение прав на файлы сайта.
Главное меню → Базы данных	Просмотр параметров базы и переход в phpMyAdmin.
Инструменты → Резервные копии	Просмотр доступных точек восстановления и загрузка отдельных файлов или базы.
Настройки сайта в ISPmanager	Просмотр выбранной версии PHP и доступных пользователю модулей. Серверные настройки менять не требуется.

Кому нужны доступы. Доступ к ISPmanager получает ответственный работник организации или выбранный ею исполнитель. ЦПО Самарской области и техподдержке площадки доступы передавать не нужно.

Временный SSH-доступ. Если для очистки нужны консольные инструменты, организация может запросить временное включение SSH-доступа. Доступ включается на период работ. Техподдержка не подбирает команды для очистки и не выполняет работы через SSH.

Термины

1. **CMS:** система управления сайтом, например WordPress или Joomla.
2. **Каталог сайта:** папка, в которой находятся файлы выбранного сайта.
3. **База данных:** таблицы с пользователями, страницами, настройками и другими данными CMS.
4. **phpMyAdmin:** инструмент для просмотра и изменения базы данных MySQL или MariaDB.
5. **Резервная копия:** сохранённое состояние файлов и базы на определённую дату. В копии может сохраняться заражение.

6. **Карантин:** папка, которую пользователь создаёт за пределами каталога сайта и использует для временного хранения подозрительных файлов.
7. **Планировщик, cron:** задание, которое запускает команду по расписанию. На сайте таких заданий может не быть.
8. **.htaccess:** файл с правилами обработки запросов и перенаправлений.
9. **.user.ini:** необязательный файл с настройками PHP. Он работает только в отдельных режимах PHP. Если такого файла нет, создавать его не нужно.
10. **auto_prepend_file:** параметр PHP для подключения файла перед выполнением страниц сайта. Неизвестный путь в таком параметре нужно проверить.
11. **Каталог загрузок:** папка с изображениями и документами, например wp-content/uploads в WordPress или images в Joomla.

2. Что сделать до изменений

На площадке резервные копии создаются каждую ночь и хранятся 14 дней. Самая новая копия могла быть создана после заражения. Перед восстановлением нужно выбрать подходящую дату и проверить, какие более новые материалы придётся вернуть вручную.

12. **Посмотрите доступные даты копий.** Если известна примерная дата появления проблемы, отметьте более раннюю точку восстановления. Не восстанавливайте её вслепую: можно потерять более новые документы и новости.
13. **Создайте папку для карантина.** Откройте раздел «Файлы» в ISPmanager и создайте папку вне каталога сайта, например quarantine_site. Перед изменением подозрительного файла скопируйте его в эту папку и добавьте к имени дату.
14. **Перед изменением базы сделайте экспорт.** В phpMyAdmin экспортируйте всю базу либо только таблицу, которую собираетесь менять. Не редактируйте таблицу без такой копии.
15. **Полный бэкап можно не скачивать.** Он пригодится для анализа на рабочем компьютере или передачи выбранному исполнителю. Наличие скачанной копии не показывает, была ли она создана до заражения.
16. **ISPmanager, работа с резервными копиями:** https://www.ispmanager.ru/docs/ispmanager/rezervnye-kopii
17. **ISPmanager, копия и восстановление одного сайта:** https://www.ispmanager.ru/docs/ispmanager/reservnoe-kopirovanie-odnogo-saita

3. Базовый порядок действий при признаках заражения

3.1. Определите состав сайта

18. **Откройте каталог сайта.** В разделе «Сайты» выделите нужный сайт и нажмите «Файлы сайта». ISPmanager откроет его корневой каталог. Начните проверку с него. Заражённые файлы могут находиться и за его пределами: в домашнем каталоге учётной записи, папках tmp, cache, backups или каталогах других сайтов той же учётной записи. После проверки корня

просмотрите доступные соседние каталоги, прежде всего недавние и неизвестные исполняемые файлы. Не изменяйте файл, пока не установлено, к какому сайту или программе он относится.

19. **Определите CMS и её версию.** Названия служебных папок обычно позволяют узнать CMS. Для WordPress характерны wp-admin, wp-content и wp-includes. Для Joomla характерны administrator, components, modules и plugins. Версию ищите в служебных файлах CMS или в документации её разработчика.
20. **Составьте перечень компонентов.** Запишите темы, плагины, модули и расширения, которые действительно используются. Неизвестные и давно неиспользуемые компоненты отметьте для удаления.

3.2. Замените программные файлы чистыми

21. **Скачайте чистые файлы у разработчика.** Для первого восстановления возьмите ту же версию CMS, темы или компонента, которая была установлена на сайте. Так меньше риск получить ошибку из-за несовместимости версий.
22. **Заменяйте компонент целиком через диспетчер файлов.** Загрузите архив, распакуйте его во временную папку, уберите старый каталог компонента в карантин и перенесите чистый каталог на его место. Не копируйте чистые файлы поверх заражённых: посторонний файл может остаться.
23. **Не заменяйте пользовательские данные.** Сохраняйте конфигурационный файл сайта и каталог загрузок. Не переносите из старой копии PHP-файлы, неизвестные скрипты или изменённые файлы компонента.
24. **Обновление выполните после очистки.** После замены заражённых файлов установите поддерживаемые версии CMS и компонентов. Проверить работу страниц и форм получится после включения сайта.

3.3. Проверьте каталог загрузок и изображения

25. **Проверьте расширения файлов.** Обратите внимание на .php, .phtml, .phar, .cgi, .pl, .sh, неожиданные .js и .html, а также двойные расширения, например photo.jpg.php. Такие файлы могли появиться в каталоге без обычной загрузки через CMS.
26. **Проверьте содержимое изображений.** В файл .jpg, .jpeg, .png или .gif можно дописать скрытый PHP-код. Такой файл иногда продолжает открываться как картинка. Подозрительны строки <?php, eval(, base64_decode(и gzinflate(. Сравните файл с исходным изображением. Если исходника нет и назначение вставки непонятно, оставьте файл в карантине. Не отправляйте подозрительные файлы в техподдержку площадки.
27. **Начните с недавних изменений.** В разделе «Файлы» отсортируйте содержимое по дате изменения. Сначала проверьте период, когда площадка зафиксировала заражение. Посторонний файл может называться почти как легальный, отличаясь одной или двумя буквами, либо иметь имя из случайного набора символов. Необычное имя помогает выбрать файл для проверки, но само по себе не доказывает заражение.

28. **Автоматизируйте проверку большого каталога.** Скачайте архив каталога загрузок на рабочий компьютер. Обновлённый антивирус используйте как дополнительную проверку: он может найти известные веб-угрозы, но результат «угроз не обнаружено» не подтверждает, что каталог чист. Для тысяч файлов используйте функцию «Найти в файлах» в текстовом редакторе и ищите строки из предыдущего пункта по всей распакованной папке. Файлы при проверке не запускайте.
29. **Сначала переносите в карантин.** Сохраните путь подозрительного файла, затем перенесите его в созданную папку карантина. Не удаляйте изображения массово по одному совпадению.

3.4. Проверьте доступные конфигурационные файлы

30. **.htaccess:** ищите неизвестные перенаправления, длинные нечитаемые вставки и правила, отправляющие посетителя на чужой домен.
31. **.user.ini:** проверяйте этот файл только при его наличии. В некоторых режимах PHP он не используется. Не создавайте его специально. Если внутри указан auto_prepend_file с неизвестным путём, сохраните копию файла и выясните назначение подключения.
32. **Файл конфигурации CMS:** проверьте адрес базы, префикс таблиц и неизвестные подключения. Не публикуйте пароль базы и секретные ключи в тикете или поисковом запросе.
33. **Планировщик:** если в ISPmanager есть задания cron, оставьте только известные команды. Перед отключением неизвестного задания сохраните его команду и расписание. Если заданий нет, этот пункт пропустите.
34. **PHP в ISPmanager:** проверьте выбранную версию и модули, доступные в интерфейсе.

3.5. Проверьте базу данных через phpMyAdmin

35. **Выберите базу именно этого сайта.** Имя базы и префикс таблиц указаны в конфигурационном файле CMS. Если они не совпадают с выбранной базой, остановитесь.
36. **Проверьте администраторов.** В WordPress пользователи находятся в таблице с окончанием _users, роли находятся в _usermeta. В Joomla пользователи находятся в таблице с окончанием _users, группы находятся в _user_usergroup_map. Сверьте логины и адреса электронной почты со списком легальных администраторов организации.
37. **Не удаляйте пользователя по одной найденной строке.** Сначала экспортируйте таблицы пользователей и ролей. Затем найдите порядок удаления именно для своей CMS и версии: одна учётная запись может быть связана с несколькими таблицами. Удаляйте или блокируйте только точно установленную постороннюю запись.
38. **Проверьте содержимое страниц и настроек.** Поиск в таблицах используйте для неизвестных доменов, script, iframe и посторонних перенаправлений. Удаляйте только подтверждённую постороннюю вставку; массовую замену по всей базе не выполняйте.
39. **Не редактируйте сериализованные данные вручную.** В отдельных ячейках CMS хранит массивы и настройки в специальном формате. В WordPress такие значения встречаются в параметрах и метаданных, в Joomla настройки могут храниться в JSON. Изменение части строки может нарушить её длину или структуру и повредить данные. Если значение начинается с a:, s:

или O: с указанием длины либо содержит сложную структуру JSON, используйте способ, предназначенный для этой CMS, или передайте работу специалисту.

40. **Смените пароли и завершите прежние сеансы.** Для каждой CMS порядок свой. Инструкции для WordPress приведены в разделе 6. Для другой CMS ищите руководство разработчика по запросу с названием и версией системы. Техподдержка площадки не составляет запросы к базе и не проверяет их перед выполнением.

Что искать по работе с базой. Добавьте в запрос точное название и версию CMS: «удалить пользователя через phpMyAdmin», «таблицы пользователей и ролей», «поиск вредоносной вставки в базе», «сериализованные данные базы». Сначала ищите документацию разработчика CMS. Не выполняйте SQL-запрос из статьи, если в нём отличаются префикс таблиц, версия CMS или назначение полей.

3.6. Проверьте права доступа

На площадке для каталогов обычно используются права 755, для файлов 644. У конфигурационных файлов могут быть более строгие права 600 или 640. Оставьте их без изменения, если сайт работал с такими значениями. Права 777 устанавливать нельзя.

4. Что проверять в первую очередь

Уведомление об отключении сайта может содержать общее описание заражения без перечня файлов. Ответственный специалист начинает с проверки файлов, базы данных и настроек по разделу 3. Если при самостоятельной проверке найден один из признаков ниже, используйте соответствующую строку таблицы.

Что найдено при проверке	Что проверить при отключённом сайте	Когда нужен исполнитель с опытом
Подозрительный файл	Сохранить путь, определить компонент, заменить компонент чистым дистрибутивом и проверить соседние свежие файлы.	Файл не относится к известному компоненту или появляется снова.
Переход на чужой сайт	Проверить .htaccess, имеющийся .user.ini, точки входа, тему, плагины и базу на чужой домен.	Источник не найден либо вставка восстанавливается.
Неизвестный администратор	Проверить таблицы пользователей и ролей, экспортировать их, удалить запись только при уверенной идентификации.	Неизвестны легальные администраторы или связанные таблицы.
PHP в uploads/images	Поместить файл в карантин, проверить весь каталог по расширениям и датам, проверить задания cron.	Файлы создаются снова или их назначение неясно.
Ошибка после замены файлов	Вернуть сохранённый каталог компонента, проверить точность версии и доступный журнал ошибок.	Нужна правка кода или причина не определяется.
Признак появился повторно	Проверить задания, конфигурацию, доступы и другие сайты в той же учётной записи.	Повторное заражение требует более глубокой диагностики.

5. Проверка результата до включения сайта

Пока сайт отключён, его страницы, формы и административную часть нельзя проверить в браузере. До обращения в техподдержку проверяются файлы, база данных, настройки и задания, доступные через ISPmanager.

41. **Сверьте программные файлы.** Ядро CMS и каталоги компонентов должны происходить из официальных дистрибутивов; старые каталоги не должны оставаться внутри корня сайта.
42. **Повторите поиск подозрительных файлов.** Проверьте исполняемые расширения в каталогах загрузок, свежие изменения и первоначально указанные пути. При возможности повторите антивирусное сканирование.
43. **Повторно просмотрите базу.** Должны остаться только легальные администраторы; подтверждённые чужие домены, script, iframe и перенаправления должны быть удалены.
44. **Проверьте доступные задания и конфигурацию.** Неизвестные cron-задания, подключения и правила перенаправления не должны оставаться активными.
45. **Проверьте, не возникают ли новые изменения.** Если при отключённом сайте снова создаётся подозрительный файл или учётная запись, причина не устранена и повторную проверку запрашивать рано.

Результат повторной проверки. Если признаков заражения не найдено, администратор площадки включает сайт. Если признаки сохраняются, сайт остаётся отключённым и организации нужно продолжить очистку. После включения организация проверяет страницы, вход в CMS, документы, поиск, формы и другие функции.

6. Если собственных знаний недостаточно

Образовательная организация является самостоятельным юридическим лицом и отвечает за ведение и техническое сопровождение своего сайта. При нехватке собственных знаний организация выбирает внешнего исполнителя. Министерство, ЦПО Самарской области и техподдержка площадки не подбирают и не рекомендуют конкретных специалистов или организации, а также не очищают сайты организаций.

Если своего специалиста нет. Организации нужно самостоятельно найти исполнителя. До устранения заражения сайт останется отключённым. Опасные изменения в файлах и базе наугад выполнять не следует.

Где искать порядок действий. Для WordPress используйте документацию на wordpress.org. Для Joomla используйте docs.joomla.org. Для плагина или темы откройте сайт её разработчика. В поисковом запросе укажите название CMS, точную версию, название компонента и найденный признак заражения. Пароли, ключи, конфигурационные файлы и персональные данные в запрос не вставляйте.

46. **WordPress, восстановление после заражения:** https://wordpress.org/documentation/article/faq-my-site-was-hacked/
47. **WordPress, смена пароля через phpMyAdmin:** https://wordpress.org/documentation/article/reset-your-password/

48.**Joomla, документация и поиск по версии:** https://docs.joomla.org/

7. Повторная проверка и границы техподдержки

Почему сайт отключён. Площадка отключает сайт после фиксации технических признаков вредоносной активности. Первоначальное уведомление может содержать общее описание заражения без путей к файлам и без перечня обнаруженных объектов. Такой перечень не составляется, поскольку один найденный объект не показывает полный объём заражения.

Какие сведения можно уточнить. По отдельному запросу техподдержка может сообщить общий тип зафиксированного признака или один доступный пример, если эти сведения уже сохранены. Это ориентир для начала проверки. Техподдержка не проводит по запросу дополнительный поиск заражённых файлов и не готовит их полный перечень. Повторные запросы о новых примерах не заменяют самостоятельную проверку сайта.

Что делает техподдержка площадки. После сообщения о завершении работ техподдержка повторно проверяет сайт на технические признаки заражения. Она не подключается к CMS и базе, не определяет, какие файлы удалить, не восстанавливает сайт и не сопровождает очистку. Режим работы: по будням с 9:00 до 17:00. Обращения вне этого времени рассматриваются в ближайший рабочий день.

Когда создавать тикет. Создайте тикет после проверки из раздела 5. До завершения работ тикет нужен только для запроса временного SSH-доступа или уточнения общего типа ранее зафиксированного признака. Порядок очистки конкретного сайта организация определяет сама или вместе с выбранным исполнителем. Ссылки для WordPress и Joomla приведены в разделе 6.

Проверка перед обращением в техподдержку

Что проверить	Что должно быть установлено
Исходный индикатор	Указанный файл, вставка, учётная запись или другой признак проверен; результат зафиксирован.
Программные файлы	Подозрительный компонент заменён чистым дистрибутивом целиком; старый каталог не оставлен в корне.
Загрузки и база	Выполнены доступные проверки исполняемых файлов, легальных администраторов и посторонних вставок.
Конфигурация и задания	Проверены доступные .htaccess, .user.ini и задания cron, если они имеются.
Повторное появление	При наблюдении в отключённом состоянии подозрительные файлы или записи не создаются снова.

Как написать запрос на повторную проверку

Домен, дату и время завершения работ указывать не требуется: сведения об услуге видны техподдержке в BILLmanager. Пароли и копию сайта к тикету не прикладывайте. Укажите только то, что вы фактически нашли и сделали.

Пример: «Обнаружено: [пути файлов, посторонняя учётная запись, вставка или иной подтверждённый признак]. Выполнено: [какие компоненты заменены, какие файлы помещены в карантин, какие записи и задания удалены, какие проверки повторены]. Просим провести повторную техническую проверку».

Результат проверки. Администратор площадки включает сайт, если технические признаки заражения не обнаружены. Если признаки сохраняются, сайт возвращается на дополнительную очистку. Полный перечень заражённых файлов при повторной проверке не формируется. Проверка страниц и функций начинается после включения сайта.

8. После восстановления

49. **Обновляйте CMS и компоненты.** Используйте поддерживаемые версии, а неиспользуемые темы, плагины и модули удаляйте полностью.
50. **Защитите учётные записи.** Смените пароли легальных администраторов, завершите прежние сеансы через CMS и включите двухфакторную защиту, если она поддерживается.
51. **Контролируйте изменения.** Периодически проверяйте администраторов, свежие файлы, задания cron и предупреждения доступных средств защиты.
52. **Учитывайте срок хранения копий.** Автоматические копии площадки хранятся 14 дней. Перед важными изменениями организация может скачать дополнительную копию. Её также нужно проверить на заражение.

Повторная проверка показывает, обнаруживает ли площадка технические признаки заражения на момент проверки. После включения организация продолжает следить за обновлениями, учётными записями и изменениями файлов.