Чек-лист | Эксперт

Чек-лист по безопасности вебсайта

Вы долго и кропотливо работали над вебсайтом, и в один из дней узнаете, что его взломали или еще хуже заразили вирусом… Зачем это делают? Кто-то, потому что руки чешутся, кто-то, чтобы получить доступ к сайту и использовать ресурсы вашего сервера, кто-то – для распространения вредоносных программ, а может быть и вовсе это ваш конкурент сделал из зависти. Этот чек-лист необходимо использовать в работе, в нем собраны несложные способы защиты веб-сайта.

- [ ] Выбрать хороший и проверенный хостинг
  Необходимо изначально обеспечить сайт надежным фундаментом. Рекомендовано использовать VDS, в данном случае сайт будет работать в автономном режиме
- [ ] Скачивать расширения с официальных сайтов, не использовать шаблоны
  Скачивайте все расширения только с официальных сайтов их разработчиков
- [ ] Включить SEF (человеко-понятные урлы)
  Включив функцию SEF, вы прячете адреса типа «index.php?option=com_content» и формируете вместо них человеко-понятные
- [ ] Не хранить пароли в FTP клиентах и браузерах
  FTP сам по себе небезопасный протокол, поэтому кража сохранённых паролей здесь – для взломщиков это дело 5 минут
- [ ] Проверить права на папки и файлы
- [ ] Проверить логин и пароль администратора
  Логин администратора НИ в коем случае НЕ должен быть «admin», а пароль должен содержать буквы и цифры
- [ ] Спрятать административную панель Joomla

Это можно сделать при помощи расширения Jsecure Lite или AdminExile

- [ ] Запретить прямое обращение к скриптам

  Воспользуйтесь кодом, который защитит вас от прямого использования информации

- [ ] Делать по возможности регулярное резервное копирование

  Это можно сделать при помощи компонента Akeeba Backup или настроить резервное копирование в панели хостинга. Актуальная резервная копия - это единственная 100% защита вашего сайта

- [ ] Подключить ЯндексВебмастер и GoogleВебмастер

  Это позволит вам довольно оперативно получить информацию о наличии неполадок на сайте или о содержании вредоносного ПО

- [ ] Следить за обновлениями расширений

  В обновлениях часто выходят исправления ошибок, в том числе и ошибок безопасности

- [ ] Использовать качественный платный антивирус на компьютере

  Базы антивирусных сигнатур для платных антивирусов обновляются чаще, поэтому риск заражения меньше

- [ ] Изменить пароль пользователя базы данных

  На многих хостингах пароль пользователя БД, совпадает с паролем аккаунта. Чтобы себя обезопасить необходимо воспользоваться сразу разными паролями, или изменить их