РЕКОМЕНДАЦИИ
по обеспечению безопасности сайтов

1. В части управления доступом и аутентификации.

1.1. Рекомендуется установить минимальную длину пароля – 10 символов. Пароль должен содержать буквы разного регистра, цифры и специальные символы.

1.2. Рекомендуется ограничить количество неудачных попыток входа до 5 с последующей временной блокировкой учётной записи.

1.3. Права доступа пользователям рекомендуется назначать по принципу "не больше, чем нужно для работы". Периодически проверять список пользователей и удалять неиспользуемые учётные записи.

2. Обновление программного обеспечения.

2.1. Обновления безопасности рекомендуется устанавливать в следующие сроки:

- критические обновления, закрывающие активно эксплуатируемые уязвимости, – как можно быстрее после официального выпуска, убедившись в их стабильности;
- плановые обновления безопасности – в течение 7 календарных дней с момента выпуска;
- перед установкой на рабочий сайт обновление желательно протестировать на копии (тестовом стенде). Если такой возможности нет, рекомендуется выждать не менее 48 часов с момента публикации.

2.2. Неиспользуемые программные компоненты (плагины, модули, темы оформления) рекомендуется удалить.

2.3. Не реже одного раза в квартал рекомендуется проводить инвентаризацию установленного программного обеспечения и его зависимостей – проверять, нет ли среди них компонентов с известными уязвимостями.

3. Сетевая защита.

3.1. Доступ к сайту рекомендуется организовать исключительно по протоколу HTTPS. Настроить принудительную переадресацию с HTTP на HTTPS.

3.2. На сервере рекомендуется настроить HTTP-заголовки безопасности. Основные заголовки: Strict-Transport-Security, X-Frame-Options, X-Content-Type-Options, Content-Security-Policy, Referrer-Policy.

3.3. Доступ к административным интерфейсам сайта ограничить по IP-адресам (белый список) или дополнительным паролем.

4. Резервное копирование.

4.1. Настроить ежедневное автоматическое резервное копирование базы данных и файлов сайта.

4.2. Резервные копии хранить отдельно от основного сервера – на другом физическом носителе или в облаке.

4.3. Не реже одного раза в квартал проводить проверку – пробовать восстановить сайт из резервной копии.

5. Защита от атак.

5.1. Все данные, поступающие от пользователей через формы ввода, рекомендуется проверять и фильтровать на стороне сервера.

5.2. На публичных формах (вход, регистрация, обратная связь) рекомендуется применять защиту от автоматизированного заполнения – CAPTCHA.

5.3. Через пользовательские формы запретить загрузку исполняемых файлов и скриптов (например, .php, .exe, .js, .phtml).

На периметре сети применять межсетевой экран уровня веб-приложений (WAF).