Приложение 1

Рекомендации ФСТЭК России по обеспечению безопасности информации информационных ресурсов

1. Обеспечение безопасной конфигурации серверной части информационной системы, включающее:

применение сертифицированных средств криптографической защиты информации для шифрования конфиденциальной информации и хеширования паролей;

ограничение доступа к файловой системе;

использование стойкого пароля администратора веб-сервера и системы управления контентом;

обеспечение двухфакторной аутентификации администраторов при доступе к электронному почтовому ящику, к которому привязан аккаунт системы управления контентом;

применение актуальных версий программного обеспечения веб-сервера, системы управления контентом, библиотек и другого программного обеспечения;

использование операционных систем с актуальной версией ядра и актуальными обновлениями безопасности.

2. Минимизация прав доступа к функциональности веб-приложения и файлам на сервере.

3. Обеспечение защиты учетных данных пользователей с административными привилегиями (включая учетные данные для доступа к панели управления на сайте хостинг-провайдера, а также учетные данные администраторов веб-сервера, системы управления контентом, веб-приложения) и контроля действия указанных пользователей.

4. Обеспечение подтверждения всех критичных действий пользователей с административными привилегиями, связанных с доменным именем и доступом к системам управления информационных систем (восстановление пароля, передача управления доменом и другие действия).

5. Веб-интерфейсы администрирования должны быть доступны только с ограниченного числа рабочих станций администраторов.

6. Обеспечение идентификации и аутентификации внешних пользователей (граждан) при их доступе к информационным системам, а также назначение минимальных прав доступа к информационным системам указанным внешним пользователям (гражданам). В частности, для исполняемых файлов веб-приложений и директорий должны быть установлены права на чтение без прав на запись (за исключением директорий для хранения файлов, загруженных внешними пользователями (гражданами)).

7. Обеспечение доступа внешних пользователей к информационным ресурсам с использованием защищенных протоколов сетевого взаимодействия (HTTPS, SSH и других протоколов). Рекомендуется

использовать только актуальные версии таких протоколов. Также не рекомендуется использовать ссылки на сайты с заголовками HTTP даже в теле страниц веб-приложения, поскольку при переходе по такой ссылке есть риск перехвата значений cookies пользователей.

8. Обеспечение проверки входных данных, поступающих в информационные системы.

9. Проведение регулярного анализа уязвимостей программного обеспечения, обеспечивающего функционирование информационных систем (в том числе средств виртуализации, веб-приложений) и обеспечение оперативного устранения выявленных в таком программном обеспечении критических уязвимостей.

10. Обеспечение фильтрации трафика с целью исключения возможности подключения внешних пользователей к TCP-интерфейсам систем управления базами данных и интерфейсам удаленного управления компонентами информационной системы. Рекомендуется оставлять доступными для подключения внешних пользователей только веб-интерфейсы 443/TCP (HTTPS) и 80/TCP (с принудительным перенаправлением на порт 443/TCP с HTTPS).

11. Обеспечение фильтрации трафика прикладного уровня с применением средств межсетевого экранирования уровня приложения (web application firewall (WAF)), установленных в режим противодействия атакам.

12. Обеспечение отказоустойчивости и резервирования компонентов информационных систем, обеспечивающих возможность продолжения работы системы при выходе из строя отдельных ее компонентов (например, серверов, каналов связи и других компонентов систем).

13. Обеспечение устойчивости информационных систем к распределенным атакам, направленным на отказ в обслуживании (ddos-атакам).

14. Организация защиты и мониторинга DNS серверов, отвечающих за делегирование доменного имени информационной системы.

15. Обеспечение антивирусной защиты информационных систем.

16. Мониторинг событий безопасности информационных систем, включая мониторинг показателей нагрузки на вычислительные мощности информационных систем, и ведение журналов регистрации событий безопасности.

17. Обеспечение возможности оперативного реагирования и принятия мер защиты информации при возникновении компьютерных инцидентов.