3.5

|  |  |  |
| --- | --- | --- |
| № | Показатель качества | Объект мониторинга |
| 1. | HTTP-запрос – пришел или не пришел запрос | Будет отображаться в клиентской части сайта |
| 2. | Срок действия сертификата (дата) | Будет отображаться в адресной строке |
| 3. | Срок действия доменного имени (дата) | Будет отображаться на почте, на которую регистрировался домен или проверить самостоятельно с помощью сайта <https://www.reg.ru/whois/> |
| 4. | Время отклика от сервера (секунды) | Сервер и клиентская часть |
| 5. | Адаптация для мобильного устройства | Проверяется есть ли удобная навигация по сайту и функциональность всех кнопок |
| 6. | Система оповещения о проблемах (работает или не работает) | Приходит ли ошибка на сервер о неисправности в работе программы |
| 7. | Корректная работа базы данных | Сохраняются ли значения в базе данных об аккаунте |

3.6

1. Выполнение всех действий с информацией, связанных с обеспечением функциональных требований к системе и/или её отдельному приложению, должно сопровождаться генерацией событий, позволяющих обеспечить контроль характеристик качества этих действий. К таким действиям должны относиться приём, передача данных, их сохранение или чтение из хранилища, преобразование любого характера.

2. Каждое событие должно классифицироваться по уровню значимости:

Critical (Fatal) – сведения о возникших критических ошибках и сбоях, приводящих к нарушению функционирования или недоступности компонента, или функции.

Error – сведения о возникших ошибках.

Warn – сведения о потенциально небезопасных ситуациях, которые могут привести к ошибкам.

Info – информационные сведения о жизненном цикле, обращении к внешним источникам, вызове внутренних сервисов, ключевых действиях пользователя, ключевых операциях.

Debug - подробные сведения о прохождении узлов ветвления, ключевых точек и вычислений алгоритмов, Информация о аргументах вызова функций и результатах выполнения функций.

Trace - максимально подробный уровень отладочных сообщений для получения полной видимости того, что происходит внутри приложения, а также используемых им сторонних библиотек.

3. События должны фиксироваться в журнале событий, а также направляться в стандартные потоки вывода (stdout и stderr).

4. Запись о событии должна быть представлена в формате, доступным для чтения человеком и автоматизированной системой. Следует избегать форматов, содержащих большой объём инструкций форматирования и разметки. Рекомендуется применять стандартные текстовые структурированные форматы, например, JSON или YAML.

5. Должна быть обеспечена возможность ограничения уровня значимости для записи событий в журнал и в поток вывода во избежание излишних нагрузок на приложение и среду его функционирования. По умолчанию, в журнал должны записываться все события от уровня Info и более значимые. Смена уровня должна происходить без необходимости перезапуска приложения или отдельных его компонентов.

6. При выводе данных в журнал или в поток вывода не допускается нарушение требований информационной безопасности, определяемых составом защищаемой информации. В частности, не допускается нарушение требований по обработке персональных данных, требований к защите данных об информационной инфраструктуре, раскрытие сведений, относящихся к государственной и коммерческой тайне.

7. Генерация и запись событий уровней Info, Warn, Error, Critical не должна приводить к нарушению показателей производительности приложения. При включении уровней Debug и Trace показатели производительности могут ухудшиться не более, чем на 5% от целевых значений.

8. Запись журнала, как минимум, должна содержать следующую информацию:

* штамп момента времени, когда произошло событие;
* уровень значимости события;
* источник события;
* уникальный идентификатор процесса, в рамках которого выполняется действие с информацией;
* тип события или/и идентификатор шага процесса;
* сообщение о событии;
* детальную информацию о событии (в зависимости от типа события).

9. Рекомендуемое. Приложением должны генерироваться и фиксироваться события, имеющие практическую ценность для обеспечения наблюдаемости и сопровождаемости системы или отдельного приложения в ней.

10. Рекомендуемое. Должны быть определены метрики и допустимые диапазоны их значений для отслеживания показателей функционирования подсистемы журналирования. Должна быть обеспечена возможность централизованного сбора метрик для их анализа и визуализации системами мониторинга.