Тестовый план для Учета критических ошибок в компьютерной сети

1. Обнаружение ошибок

1.1. **Цель:** Проверить функциональность автоматического обнаружения критических ошибок в компьютерной сети.

1.2. **Шаги тестирования:**

- Запустить систему мониторинга.
- Имитировать сбой в сетевом оборудовании или атаку.
- Проверить, что система успешно обнаруживает ошибку.

1.3. **Ожидаемый результат:** Система должна оперативно выявлять критические ошибки в сети.

2. Анализ данных

2.1. **Цель:** Проверить возможность системы проводить анализ данных для выявления причин и последствий ошибок.

2.2. **Шаги тестирования:**

- Запустить систему анализа данных.
- Подать в систему данные о критической ошибке.
- Проверить, что система анализирует данные и выдает информацию о причинах и последствиях ошибки.

2.3. **Ожидаемый результат:** Система должна успешно анализировать данные о критических ошибках и предоставлять информацию об их причинах и последствиях.

3. Регистрация и отслеживание ошибок

3.1. **Цель:** Проверить функциональность системы ведения журнала событий с подробной информацией о критических ошибках.

3.2. **Шаги тестирования:**

- Запустить систему регистрации ошибок.
- Создать несколько тестовых критических ошибок.

- Проверить, что система регистрирует ошибки и сохраняет подробную информацию о них.

3.3. **Ожидаемый результат:** Система должна вести журнал событий с подробной информацией о критических ошибках.

4. Оповещение и уведомление

4.1. **Цель:** Проверить функциональность оповещения администраторов о возникновении критических ошибок.

4.2. **Шаги тестирования:**

- Запустить систему оповещения.
- Имитировать возникновение критической ошибки.
- Проверить, что система успешно оповещает администраторов о ошибке.

4.3. **Ожидаемый результат:** Система должна оперативно оповещать администраторов о возникновении критических ошибок.

5. Интеграция с существующими информационными системами

5.1. **Цель:** Проверить возможность интеграции системы с существующими системами мониторинга сети и журналирования событий.

5.2. **Шаги тестирования:**

- Подключить систему к тестовой сетевой инфраструктуре.
- Проверить, что система успешно интегрируется с существующими информационными системами.

5.3. **Ожидаемый результат:** Система должна без проблем интегрироваться с существующими системами мониторинга сети и журналирования событий.

6. Тестирование безопасности

6.1. **Цель:** Проверить безопасность системы.

6.2. **Шаги тестирования:**

- Попытаться получить доступ к системе без прав доступа.

- Протестировать уязвимости системы на наличие уязвимостей.

6.3. **Ожидаемый результат:** Система должна успешно защищать доступ и не иметь уязвимостей.