Студент магистратуры Потапова Ксения Александровна
1 курс, факультет «Информационных технологий»
МИРЭА - Российский технологический университет
Россия, г. Москва

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ МОДУЛЯ МОНИТОРИНГА ЦЕЛОСТНОСТИ ОБЪЕКТОВ ЗАЩИТЫ

Аннотация: *Модуль мониторинга целостности не только помогает отслеживать опасный «трафик», но и позволяет администраторам удобно следить за объектами и их контрольными суммами. Однако удобство пользования приложением полностью зависит от программной реализации модулей. Реализация модуля подсчета контрольной суммы файла была реализована на языке «высокого уровня» Java.*

Ключевые слова: *программа, мониторинг, целостность, реализация, модуль*

Annotation: *The integrity of monitoring module not only helps to track dangerous "traffic", but also allows administrators to conveniently monitor objects and their checksums. However, the usability of the application depends entirely on the software implementation of the modules. The implementation of the file checksum calculation module was implemented in a «high level» Java language.*

Key words: *program, monitoring, integrity, implementation, module*

```
int MyHashFunc(string word)
{
  int sum = 0;
  for (int k = 0; k < word.length(); k++)
  {
    sum = sum + int(word[k]);
  }

  return sum % word.length();
}
```

Рисунок 1. Программная реализация метода суммирования хэш-функции

Выбор базы данных для работы с модулем мониторинга целостности объектов защиты зависел от решений, существующих на рынке в данный момент.

Для реализации была выбрана база данных PostgreSQL — это объектно-реляционная система управления базами данных (ОРСУБД, ORDBMS), СУБД с открытым исходным кодом. Она поддерживает большую часть стандарта SQL и предлагает множество современных функций:

- сложные запросы
- внешние ключи
- триггеры
- изменяемые представления
- транзакционная целостность
- многоверсионность

У базы данных PostgreSQL имеются следующие преимущества перед аналогами:

- Открытое ПО соответствующее стандарту SQL - PostgreSQL - бесплатное ПО с открытым исходным кодом. Эта СУБД является очень мощной системой.
- Большое сообщество - существует довольно большое сообщество в котором вы запросто найдёте ответы на свои вопросы
- Большое количество дополнений - несмотря на огромное количество встроенных функций, существует очень много дополнений, позволяющих разрабатывать данные для этой СУБД и управлять ими.
- Расширения - существует возможность расширения функционала за счет сохранения своих процедур.
- Объектность - PostrgreSQL это не только реляционная СУБД, но также и объектно-ориентированная с поддержкой наследования и много другого

Для начала работы с модулем пользователь должен перейти в модуль целостности объектов защиты, нажав на поле ПМ МЦОЗ.

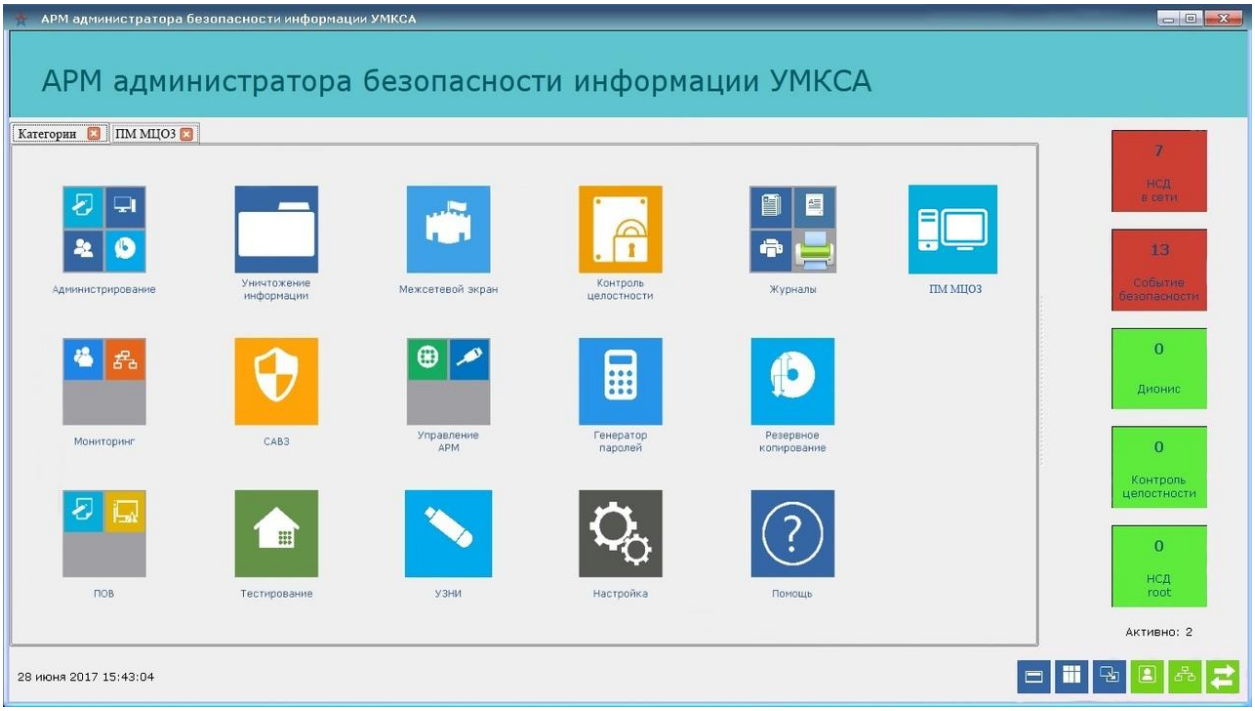

Рисунок 2. – Интерфейс КП УСЗИ

Далее пользователь должен выбрать объект защиты и его тип, кликнув на поле выбор объекта.

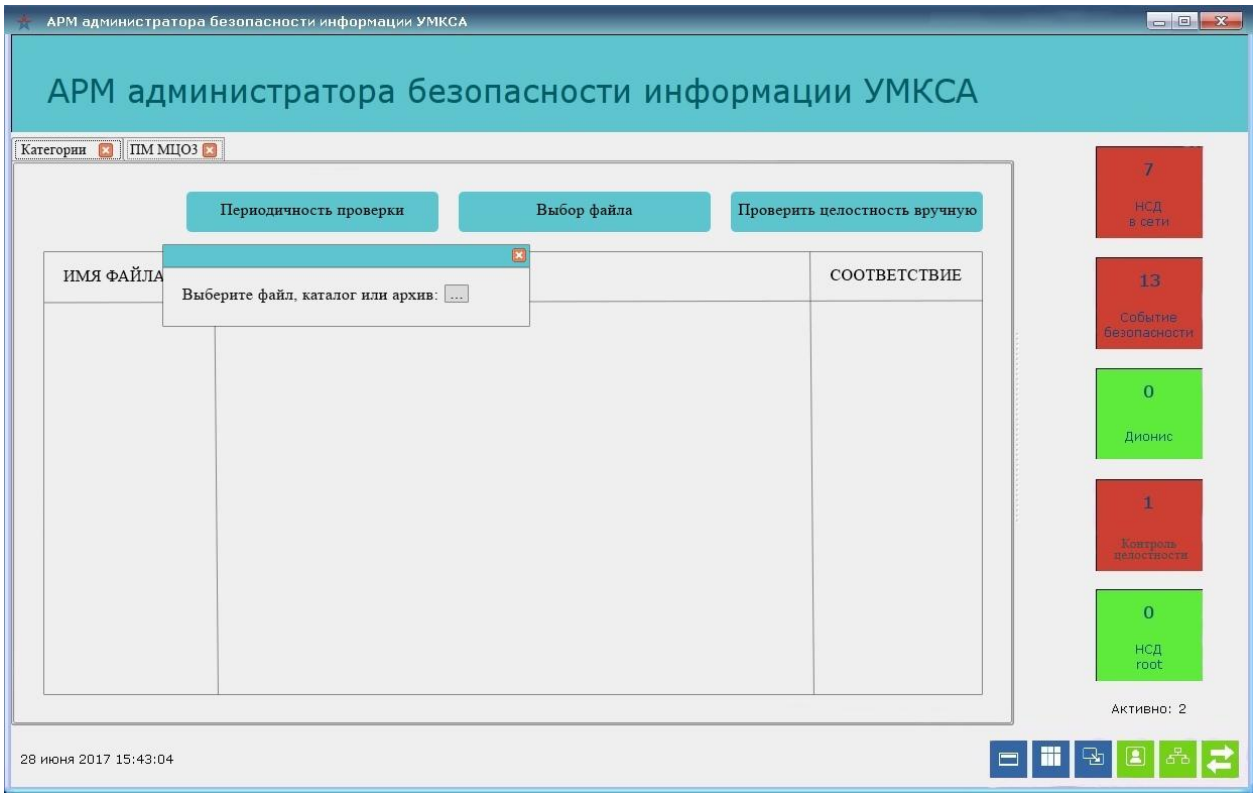

Рисунок 3. – Окно выбора типа объекта защиты

После выбора объекта и пути к нему, пользователь должен выбрать частоту проверки целостности объекта.

Также пользователь может проверить вручную целостность объекта защиты выбрав поле проверить целостность. Далее пользователю необходимо выбрать объект и подтвердить свой выбор. После система выдаст новые и старые данные объекта – его имя, автора, версию и его контрольную сумму.

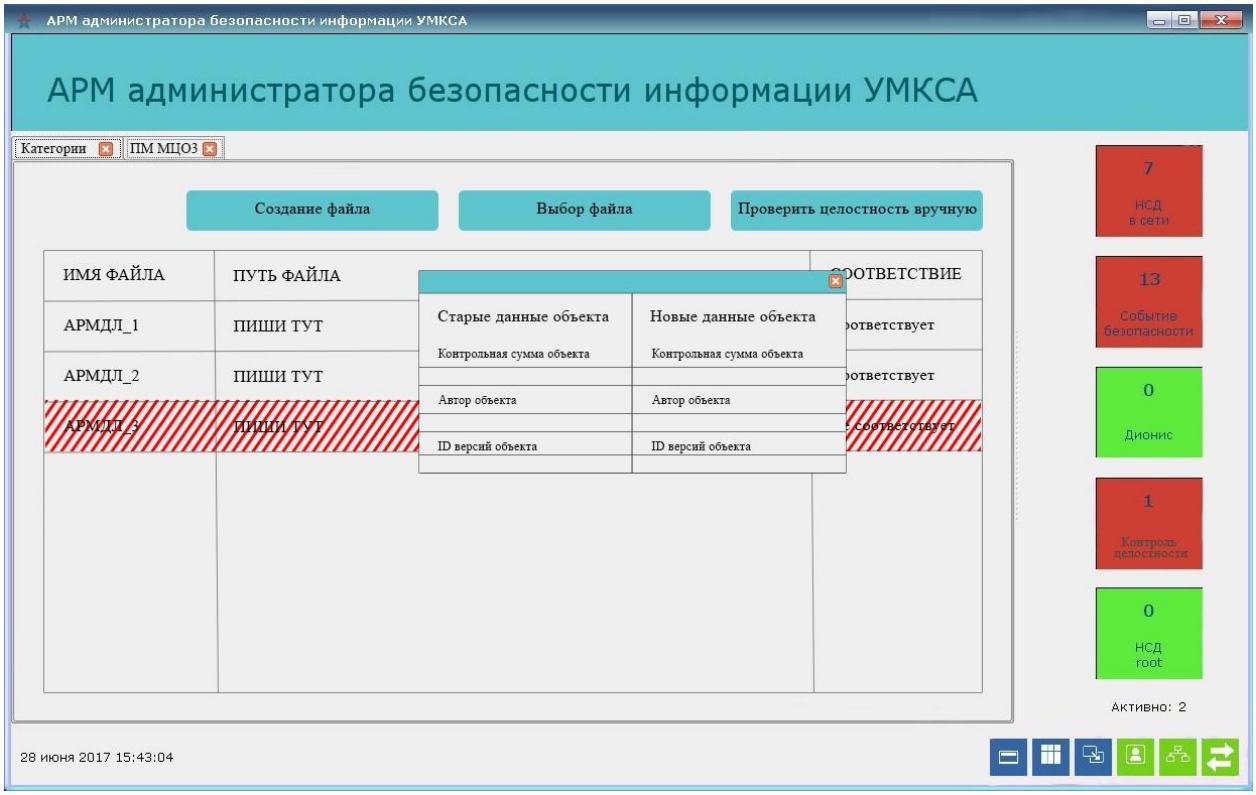

Рисунок 4 – Окно сравнения старых и новых данных объекта

Также пользователь может установить новое или удалить старое расписание проверки целостности объекта, нажав на поле создание расписания

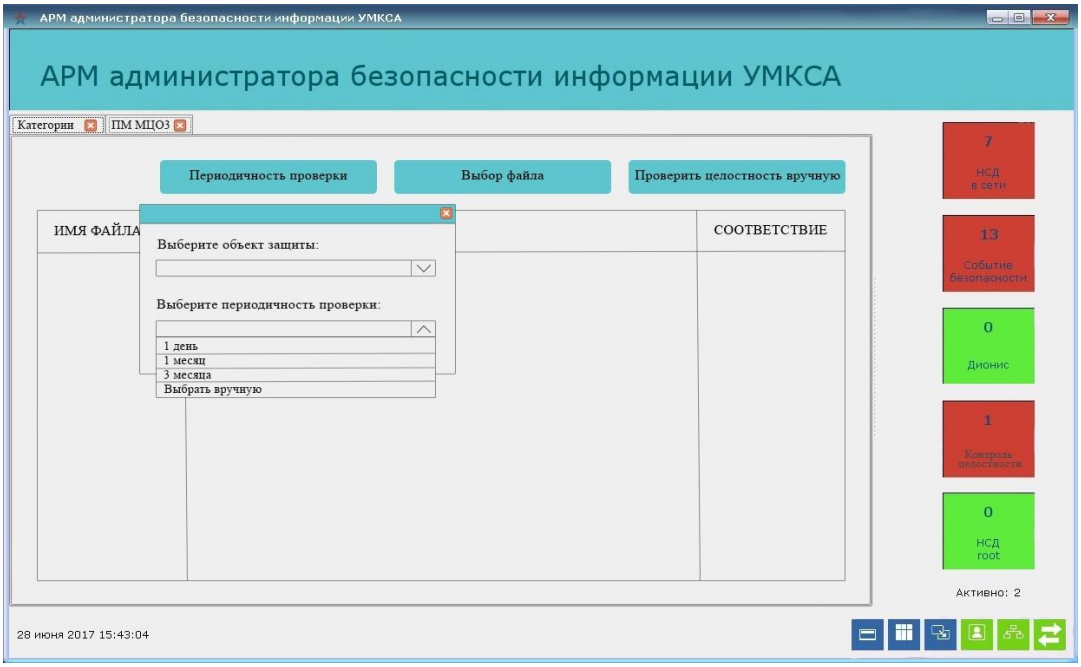

Рисунок 5 – Окно выбора частоты проверки целостности объекта защиты

В случае если какой-то из объектов окажется изменен, поле где отображаются данные объекта загорится красным и модуль отправит оповещение администратору.

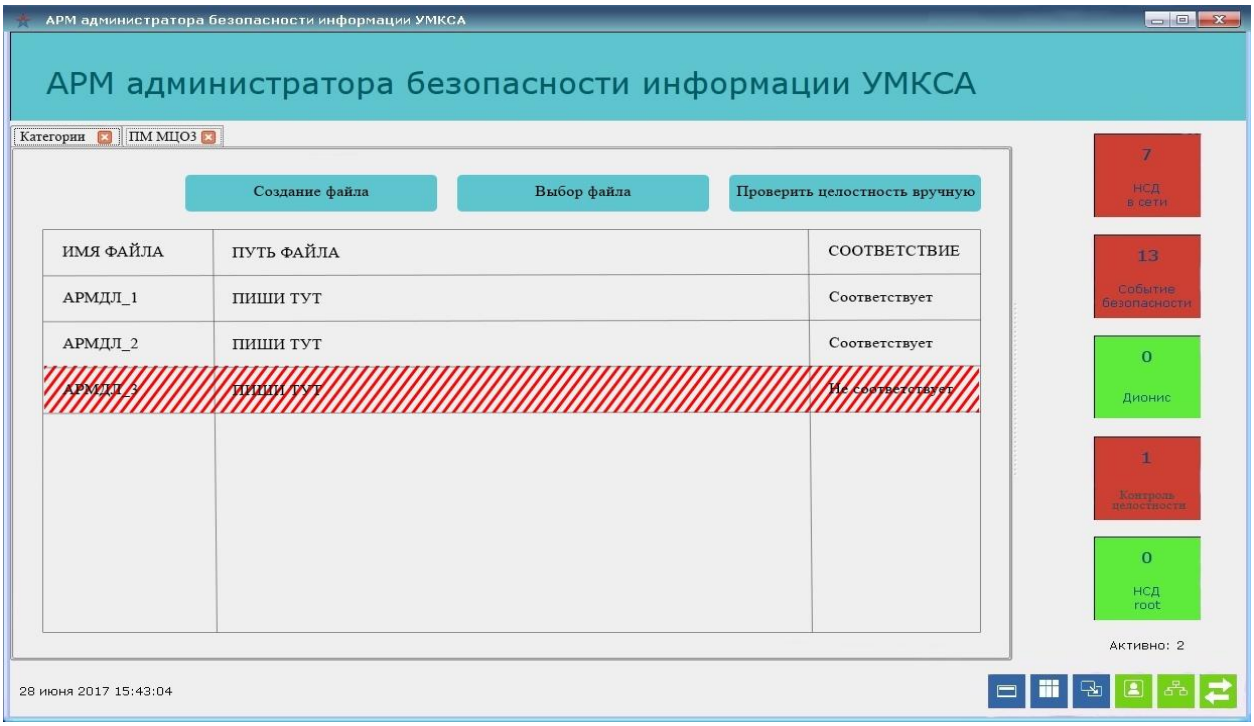

Рисунок 6 – Отображение оповещении об изменении целостности объекта защиты

Список используемой литературы:

1. Техническая документация на КП УСЗИ
2. ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности».