

# Руководства пользователя

Для прохождения самооценки по защите персональных данных:

1. В открывшемся окне нажмите на кнопку “Пройти оценку уровня защищенности”. См. Рис.1.

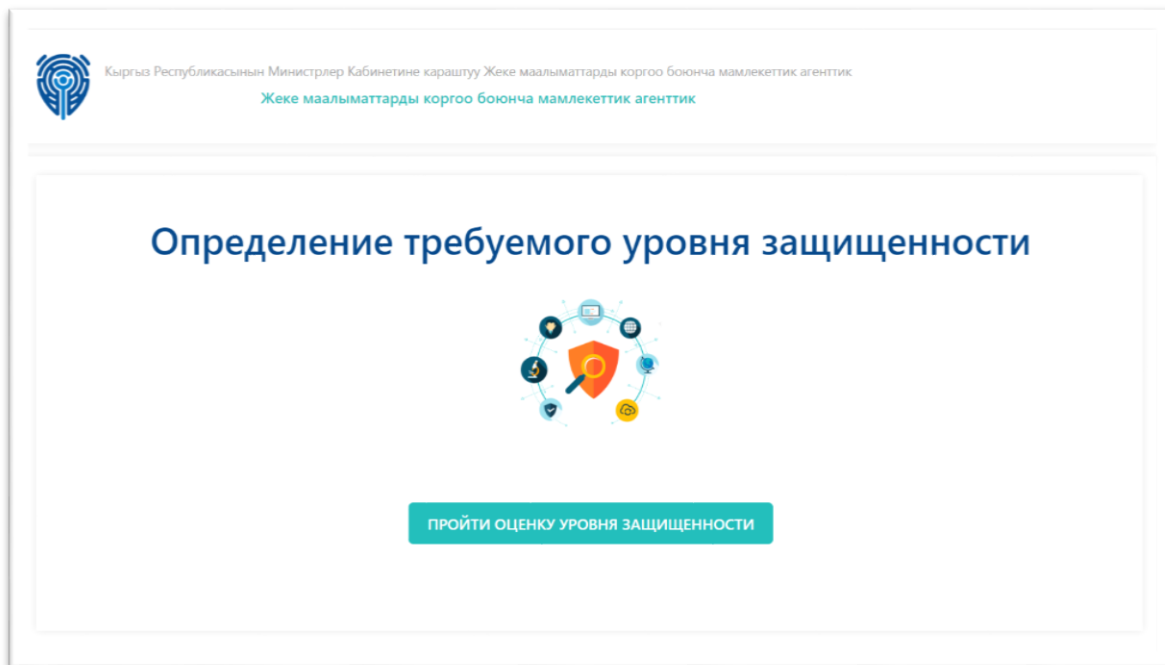


Рис.1. Окно приветствия.

2. Пройдите опросник по всем угрозам. См. Рис.2.

Рис.2. Опросник.

3. В самом конце нажмите на кнопку “Завершить самооценку”. См. Рис.3.

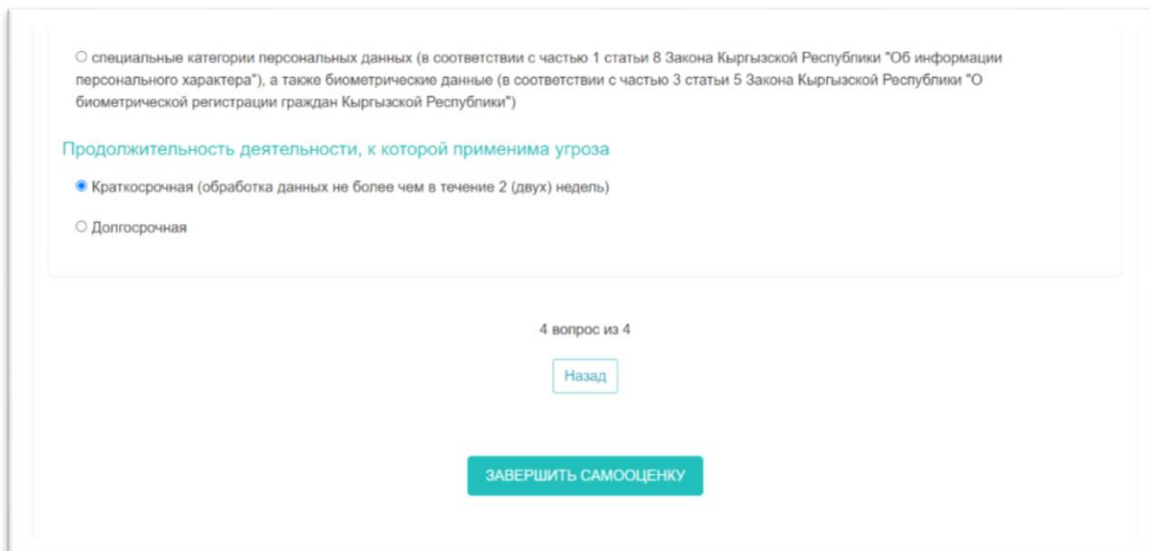


Рис.3. Кнопка “Завершить самооценку”.

4. В появившемся окне посмотрите на результаты. См. Рис.4.

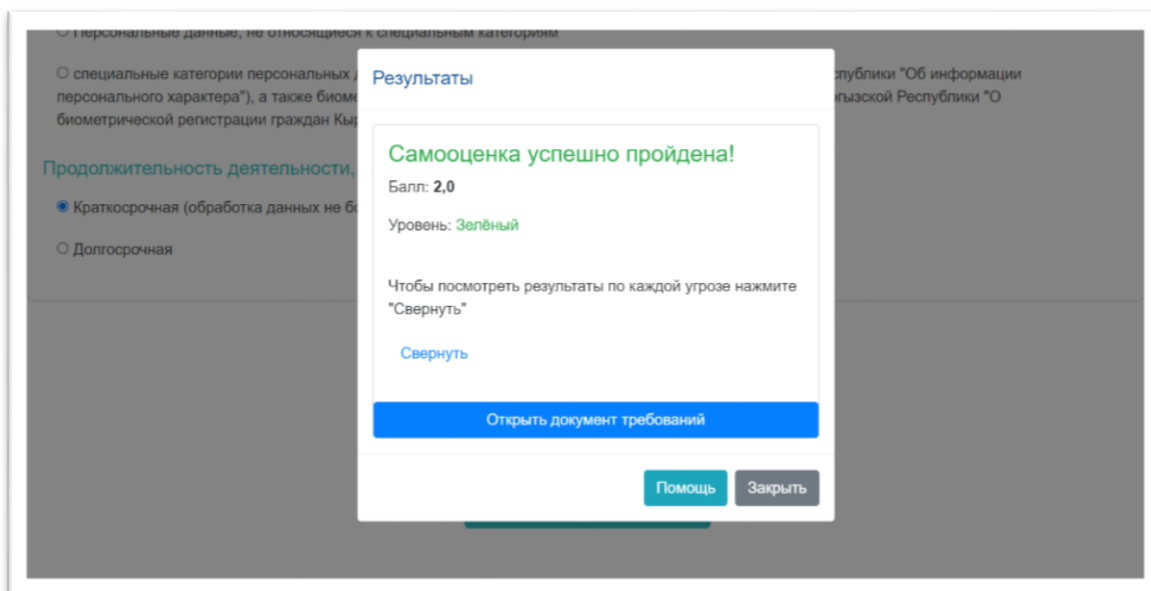


Рис.4. Окно результата.

5. Для более подробного просмотра результатов нажмите на кнопку “Свернуть”. См. Рис.5.

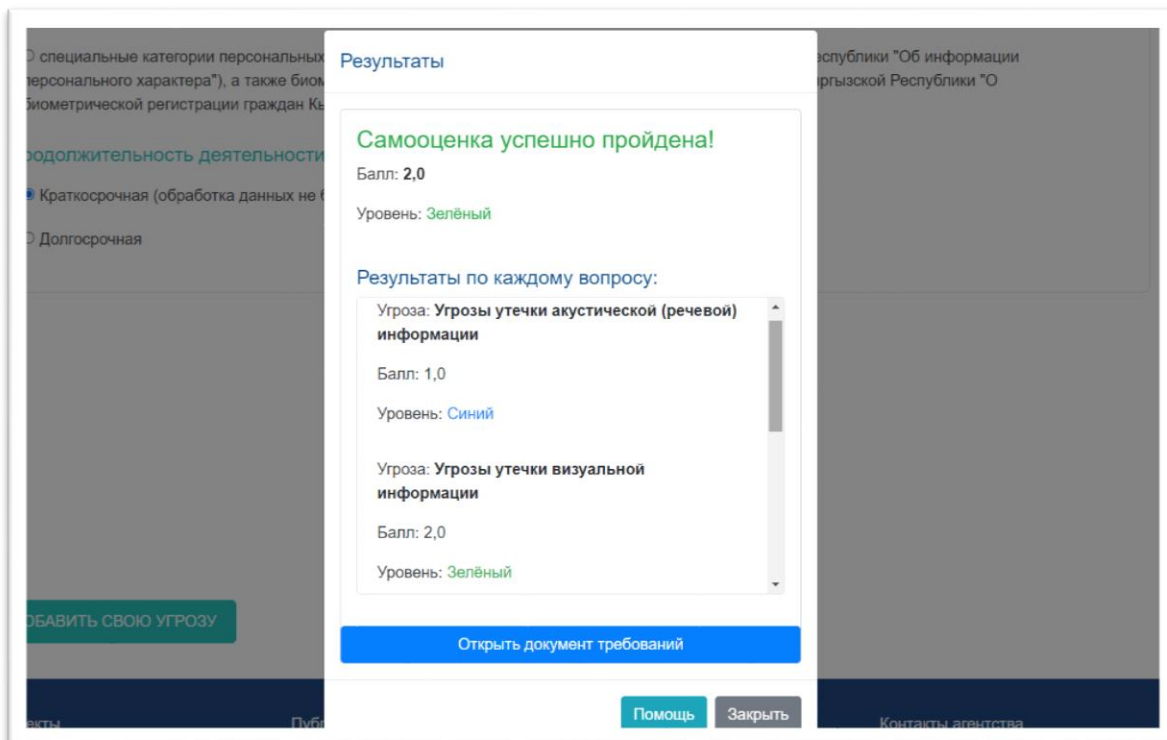


Рис.5. Свёрнутый результат для подробной информации.

6. При нажатии кнопки “Открыть документ требований” откроется документ требований соответствующий вашему уровню по результатам опроса (синий, зеленый, желтый и красный). См. Рис.6.

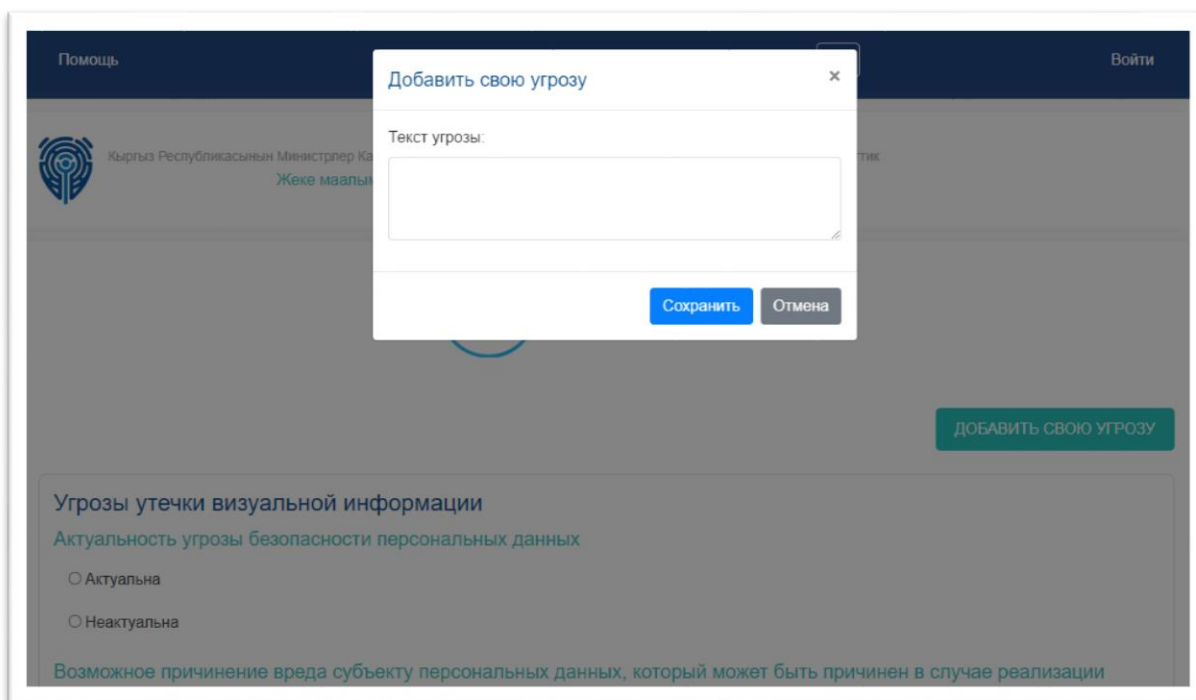
Требования для <b>зеленого</b> уровня	
-	принятием документа, определяющего политику держателя (обладателя) массива персональных данных в отношении обработки персональных данных, и доведением содержания данного документа до работников и контрагентов держателя (обладателя) массива персональных данных;
-	назначением лица (лиц), ответственных за обеспечение безопасности персональных данных при их обработке в информационных системах и проведением их инструктажа по требованиям Закона Кыргызской Республики "Об информации персонального характера" и настоящих Требований;
-	осуществлением внутреннего контроля соответствия обработки персональных данных требованиям Закона Кыргызской Республики "Об информации персонального характера", и настоящих Требований, иных документов, принятых по вопросам обработки персональных данных;
-	включением в трудовые договоры и должностные инструкции работников держателя (обладателя) массива персональных данных их обязанностей в отношении обработки персональных данных, положений о неукоснительном соблюдении требований Закона Кыргызской Республики "Об информации персонального характера", и настоящих Требований, иных документов, принятых по вопросам обработки персональных данных;
-	ведением (на бумажном носителе или в электронном виде) журнала учета машинных носителей персональных данных и списка лиц, в чьи должностные обязанности входит доступ к персональным данным;
-	при каждом вводе персональных данных в систему обработки данных, а также при изменении или уничтожении таких данных - указанием лица, осуществившего ввод (изменение, уничтожение) таких данных, даты и времени совершения операции;
-	созданием не реже одного раза в сутки резервной копии актуальных персональных

Рис.6. Документ требований.

**Уровни безопасности персональных данных в зависимости от угроз безопасности этих данных определяются для каждой информационной системы или группы информационных систем следующим образом:**

- 1) "синий" - наличие угроз с рейтингом не более 1 балла;
- 2) "зеленый" - наличие угроз с рейтингом 2 балла (но не более);
- 3) "желтый" - наличие угроз с рейтингом от 3 до 6 баллов включительно (но не более);
- 4) "красный" - наличие угроз с рейтингом более 6 баллов.

Для того чтобы добавить свою угрозу и пройти опрос в странице опроса на верхнем правом углу нажмите на кнопку “Добавить свою угрозу”. В открывшемся окне напишите свою угрозу и сохраните. См. Рис.7.



The image shows a web application interface with a modal window titled "Добавить свою угрозу". The modal contains a text input field labeled "Текст угрозы:" and two buttons: "Сохранить" (Save) and "Отмена" (Cancel). The background shows a sidebar with "Помощь" (Help) and "Войти" (Login) links, and a main content area with a "ДОБАВИТЬ СВОЮ УГРОЗУ" (ADD YOUR THREAT) button. Below the button, there is a section titled "Угрозы утечки визуальной информации" (Threats of visual information leakage) with a sub-section "Актуальность угрозы безопасности персональных данных" (Relevance of the threat to the security of personal data) and two radio buttons: "Актуальна" (Relevant) and "Неактуальна" (Not relevant). At the bottom, there is a text label: "Возможное причинение вреда субъекту персональных данных, который может быть причинен в случае реализации" (Possible harm to the subject of personal data, which may be caused in the event of realization).

Рис.7. Окно для добавления пользователем угрозы.