# **Сценарий использования**

## **ПО «Программный модуль «\_\_\_»»**

1. **Целевой пользователь.**

- администратор информационной безопасности;

- юрист;

- пользователь ПК и сети Интернет.

1. **Проблема, которую хочет решить целевой пользователь.**

*Для администратора информационной безопасности*: выявить нарушения и уязвимости, связанных с формами для ввода персональных данных, чтобы предупредить кражу этих данных и исправить уязвимости.

*Для юристов*: выявить нарушения и уязвимости, связанных с формами для ввода персональных данных, чтобы включить эту информацию в судебный процесс в качестве обвинения или защиты.

*Для пользователя ПК и сети Интернет*: выявить нарушения и уязвимости, связанных с формами для ввода персональных данных, чтобы пользователь мог избежать ввода своих данных в уязвимые формы и предотвратить их кражу.

1. **Действия целевого пользователя.**

Чтобы решить проблему, пользователь должен выполнить следующие действия:

1) установить согласно инструкции ПО «Программный модуль «\_\_\_»», которое будет в качестве расширения для используемого браузера (браузеров);

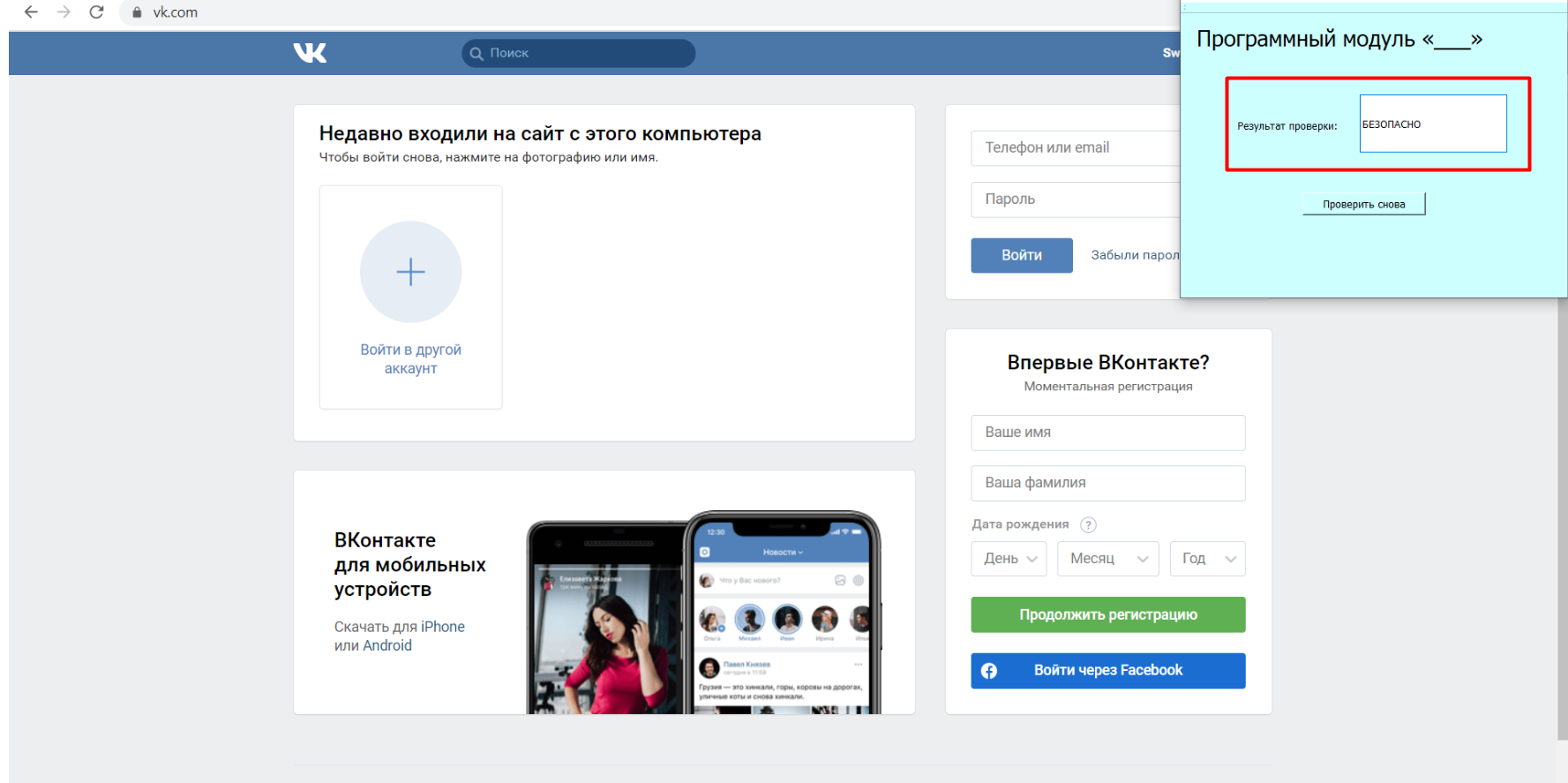
2) зайти на сайт, на котором пользователь хочет выявить нарушения;

3) открыть расширение ПО «Программный модуль «\_\_\_»» (рис. 1);



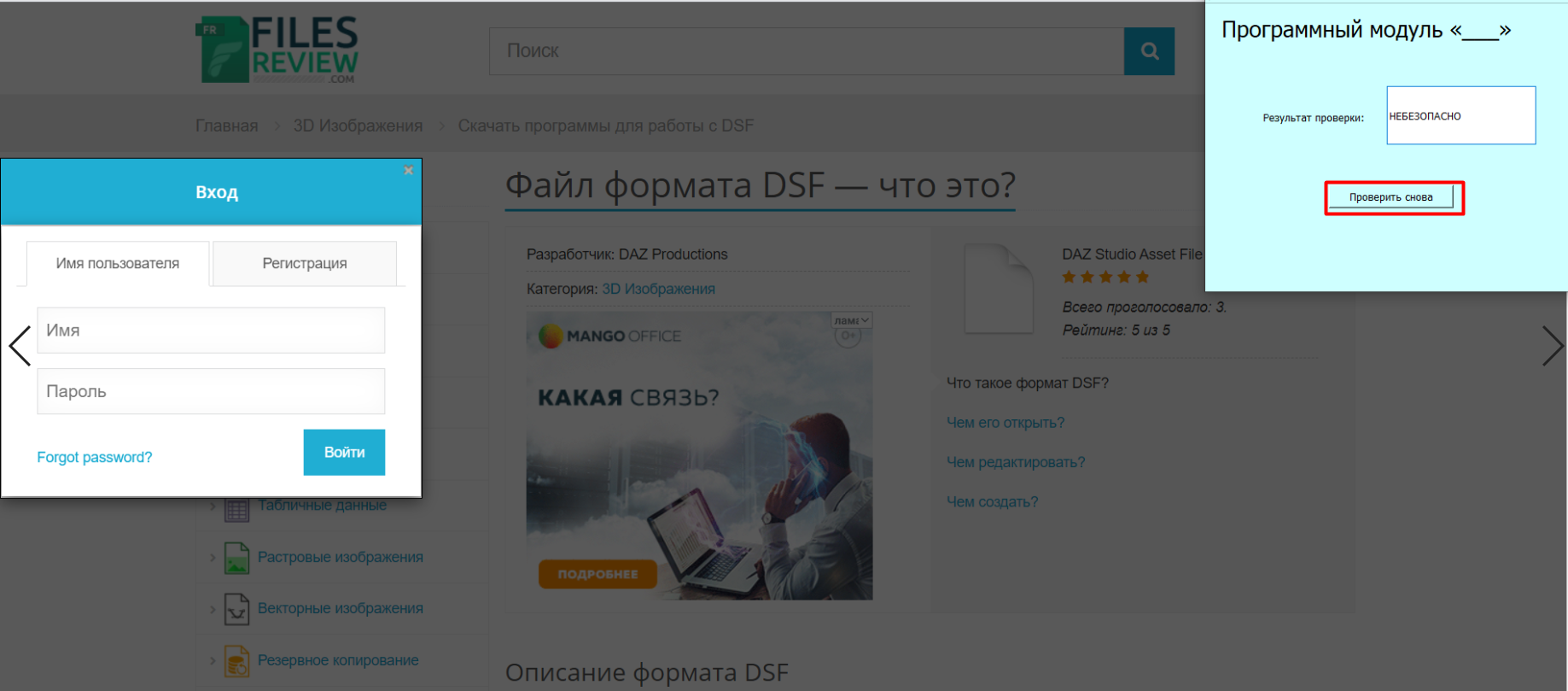
*Рис. 1 «Значок расширения в строке Google Chrome»*

1. посмотреть результаты автоматической проверки (рис. 2);



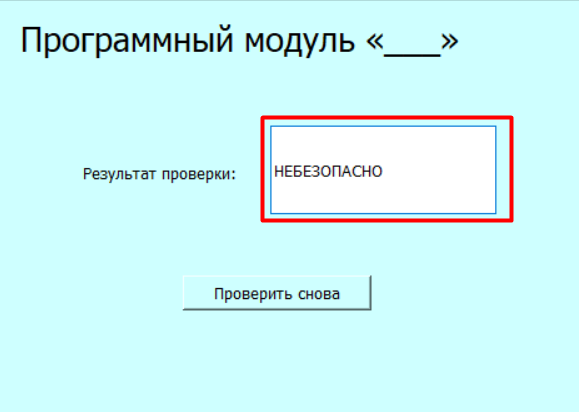
*Рис 2 «Результат проверки программного модуля на сайте vk.com»*

1. при желании пользователя он может нажать на кнопку «Проверить», чтобы провести повторную проверку сайта на наличие нарушений и уязвимостей (рис. 3);



*Рис. 3 «Кнопка повторной проверки безопасности форм»*

1. Ожидать результата проверки сайта на нарушения и уязвимости, связанных с формами для ввода персональных данных (рис. 4).



*Рис. 4 «Результат после нажатия кнопки»*

1. **Результат, полученный целевым пользователем.**

В окне расширения появится информация о том, являются ли формы ввода персональных данных на текущем сайте безопасными или имеются какие-либо уязвимости.

При наличии уязвимостей *администратору безопасности* будет сообщено, где именно, чтобы избежать кражи данных и исправить все нарушения.

При наличии уязвимостей *юристу* будет сообщено, где именно, чтобы включить эту информацию в судебный процесс.

При наличии уязвимостей *пользователю ПК и сети Интернет* будет сообщены возможные действия, чтобы избежать кражи данных из форм текущего сайта.