# ЕДИНАЯ СИСТЕМА СБОРА, ОБРАБОТКИ, ХРАНЕНИЯ И ПРЕДСТАВЛЕНИЯ СТАТИСТИЧЕСКИХ ДАННЫХ

# ИНСТРУКЦИЯ ПО НАСТРОЙКЕ РАБОЧЕГО МЕСТА

2019 г.

# 1. Настройка браузеров для работы в онлайне

На клиентских станциях должна быть установлена одна из нижеперечисленных операционных систем:

- Microsoft Windows XP;
- Microsoft Windows Vista;
- Microsoft Windows 7;
- Microsoft Windows 8.1;
- Microsoft Windows 10

Для з**ап**олнения форм статистической отчетности через ON-line модуль подготовки отчетов требуется наличие на компьютере следующего программного обеспечения, в зависимости от версии используемой операционной системы:

Для операционной системы *Windows XP Service Pack 2* и выше должны быть установлены:

- любой из браузеров: Microsoft Internet Explorer 8.0 и выше, Google Chrome 10 и выше, Mozilla Firefox 10 и выше, Apple Safari 5 и выше, Opera 12 и выше;
- **Рекомендуем использовать браузер Mozilla или использовать ОС Windows 7 и выше, так как при заполнении отчета предыдущий период недоступен при работе в операционной системе Windows XP**.
- один из следующих криптопровайдеров: «КриптоПро CSP 3.6», VipNet CSP 3.2 и выше, Signal-COM CSP 2.2 и выше, ЛИССИ-CSP 1.17 и выше или другое СКЗИ, используемое в Росстате.

Для операционной системы *Microsoft Windows Vista Service Pack 1* должны быть установлены:

- любой из браузеров: Microsoft Internet Explorer 8.0 и выше, Google Chrome 10 и выше, Mozilla Firefox 10 и выше, Apple Safari 5 и выше, Opera 12 и выше;
- один из следующих криптопровайдеров: «КриптоПро CSP 3.6», VipNet CSP 3.2 и выше, Signal-COM CSP 2.2 и выше, ЛИССИ-CSP 1.17 и выше, или другое СКЗИ, используемое в Росстате.

Для операционной системы *Microsoft Windows 7* должны быть установлены:

- любой из браузеров: Microsoft Internet Explorer 9.0 и выше, Google Chrome 10 и выше, Mozilla Firefox 10 и выше, Apple Safari 5 и выше, Opera 12 и выше;
- один из следующих криптопровайдеров: «КриптоПро CSP 3.6», VipNet CSP 3.2 и выше, Signal-COM CSP 2.2 и выше, ЛИССИ-CSP 1.17 и выше, или другое СКЗИ, используемое в Росстате.

Для операционных систем *Microsoft Windows 8.1 и 10* должны быть установлены:

- любой из браузеров: Microsoft Internet Explorer 11.0 и выше, Google Chrome 50 и выше, Mozilla Firefox 50 и выше, Opera 40 и выше;
- один из следующих криптопровайдеров: «КриптоПро CSP 4.0», VipNet CSP 4.2 и выше, Signal-COM CSP 3.3 и выше, ЛИССИ-CSP 2.0 и выше, или другое СКЗИ, используемое в Росстате.

Для операционных систем *64 разрядных* необходимо запускать приложение ON-line модуля в 32 разрядном Internet Explorer.

Для работы онлайн модуль в Internet Explorer необходимо сделать настройки в браузере согласно подразделу 1.1.

Для работы в других браузерах не надо производить дополнительные настройки.

## 1.1. Настройки обозревателя Microsoft Internet Explorer

Установите следующие настройки обозревателя Microsoft Internet Explorer:

- добавить сайт on-line «**https://websbor.gks.ru/webstat»** в зону «Надежные узлы»
- установить для зоны «Надежные узлы» особый уровень безопасности, который позволяет использовать элементы ActiveX для подписания документов ЭП и всплывающие окна для просмотра шаблонов форм.

**Примечание**

Для браузера Internet Explorer версии 8-11, предусмотрены дополнительные настройки (п. 1.1.3 и 1.1.6).

### 1.1.1. Добавление сайта модуля on-line в зону «Надежные узлы»

#### 1.1.1.1 Автоматическая настройка параметров, при помощи утилиты

Утилита (файл SetTrusted.cmd) доступна для скачивания на сайте технической поддержки http://webstat.gmcrosstata.ru/ по ссылке http://webstat.gmcrosstata.ru/yaf_postst247_Utilita-konfighuratsii-rabochiegho-miesta.aspx.

Для работы с утилитой выполните следующие действия:

- скопируйте и распакуйте утилиту на рабочей станции;
- запустите файл SetTrusted.cmd;
- в строке для ввода укажите адрес **https://websbor.gks.ru/webstat**;
- проверьте, что сайт успешно добавлен в доверенные.

Для Windows 7 запуск утилиты необходимы выполнять используя права локального администратора «Run as..».

#### 1.1.1.2 Выполнение настроек браузера вручную

Для добавления сайта модуля on-line в зону «Надежные узлы» необходимо выполнить следующие действия:

1) В окне обозревателя выберите команду меню Сервис → Свойства обозревателя. Откроется окно «Свойства обозревателя». Перейдите на закладку «Безопасность».

2) Выберите зону Интернета «Надежные узлы» и нажмите кнопку «Узлы». Откроется дополнительное окно «Надежные узлы» («Trusted sites»).

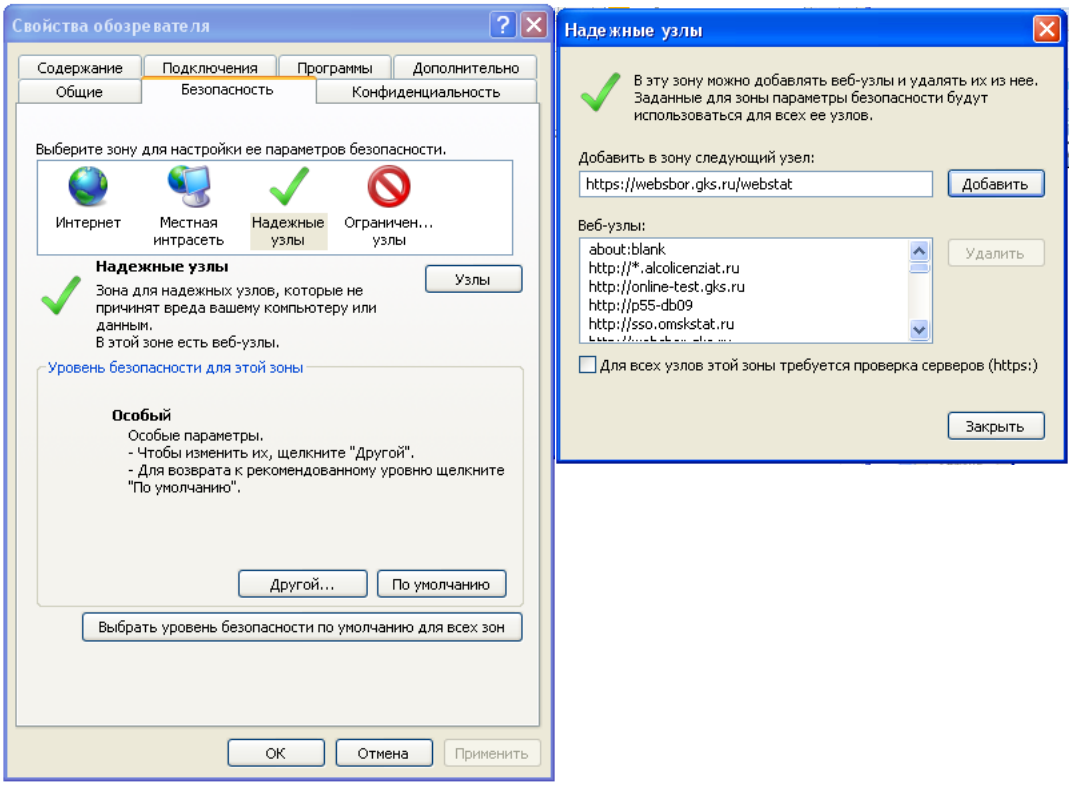


**Рисунок 1 - Добавление сайта модуля ON-line в зону «Надежные узлы»**

Добавьте сайт модуля ON-line в зону «Надежные узлы» («Trusted sites»). Для этого наберите адрес сайта (для сайта Омскстата: **«https://websbor.gks.ru/webstat»**) в поле «Добавить в зону следующий узел» и нажмите кнопку «Добавить». Закройте окно «Надежные узлы».

### 1.1.2. Выбор параметров безопасности, необходимых для использования ЭП

По умолчанию обозреватель Microsoft Internet Explorer использует уровень безопасности, который не позволяет загружать на компьютер пользователя компоненты ActiveX. Данная особенность не позволит Вам начать работу с ПО в полном объеме. Для корректной работы ЭП (которая использует ActiveX), необходимо после добавления сайта модуля On-line в зону «Надежные узлы» установить для этой зоны особый уровень безопасности. Для этого следует выполнить следующие действия:

1) В окне обозревателя выберите команду меню Сервис → Свойства обозревателя. Откроется окно «Свойства обозревателя». Перейдите на закладку «Безопасность».

2) Выберите зону Интернета «Надежные узлы» и нажмите кнопку «Другой» на панели «Уровень безопасности для этой зоны» Откроется окно «Параметры безопасности – зона надежных узлов» (рисунок 2).

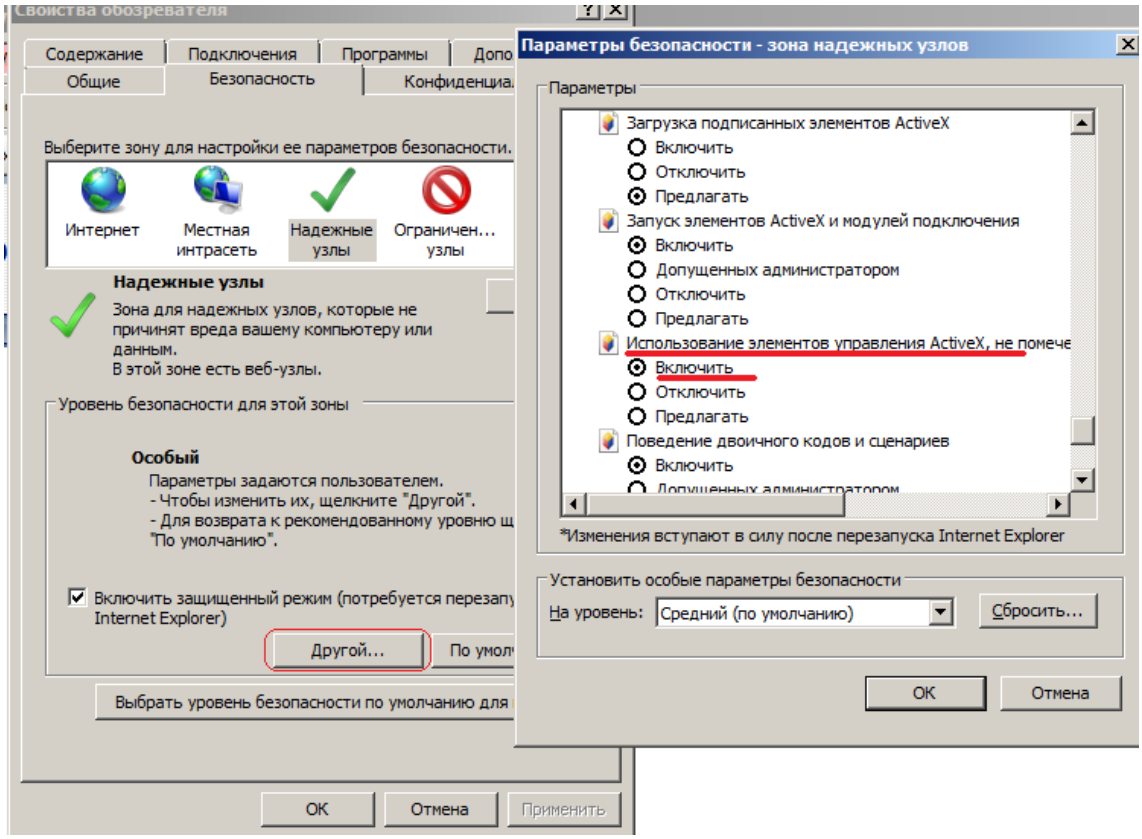


**Рисунок 2 - Включение использования элементов ActiveX**

3) Установите для зоны «Надежные узлы» опцию «Использование элементов ActiveX, не помеченных как безопасные для использования» = «Включить» («Initialize and script ActiveX not marked as safe» = «Enabled».

4) Установите для зоны «Надежные узлы» опцию «Загрузка неподписанных элементов ActiveX» = «Предлагать» («Download unsigned ActiveX controls» = «Prompt») (рисунок 3).

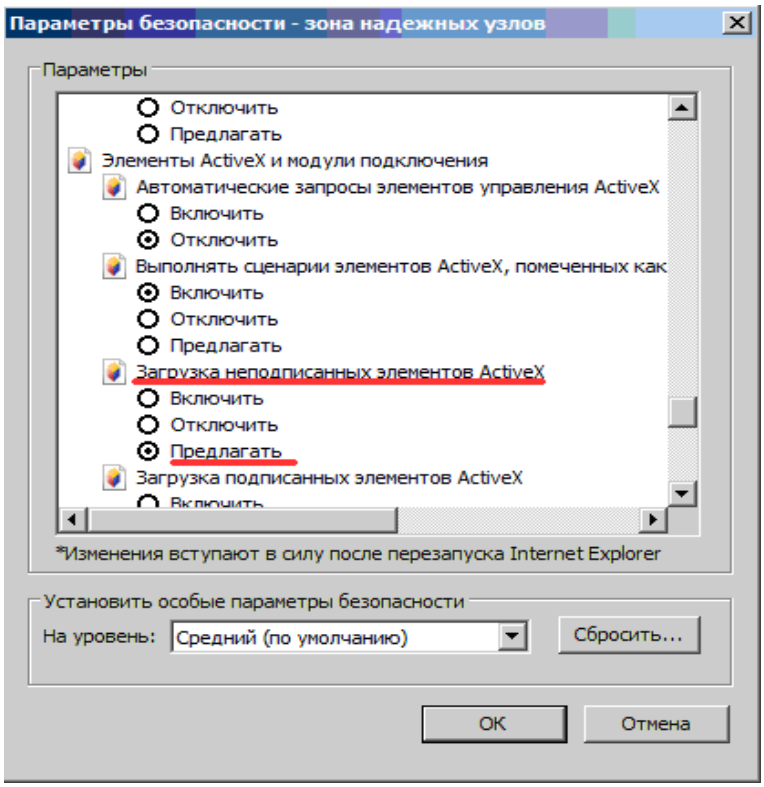


**Рисунок 3 - Установка уровня безопасности для параметра «Загрузка неподписанных элементов ActiveX»**

5) Нажать кнопку OK в окне «Параметры безопасности». В открывшемся диалоговом окне подтвердить изменения в настройках безопасности для зоны «Надежные узлы».

6) Нажать кнопку OK в окне «Свойства обозревателя».

Установленный для зоны «Надежные узлы» уровень безопасности будет действовать только для сайта On-line, и не будет уменьшать безопасность для любых других интернет-сайтов.

### 1.1.3. Особенность настроек обозревателя Internet Explorer 8

В случае если работа с системой будет производиться в IE8, необходимо выполнить дополнительные настройки. Изменить уровень безопасности надёжных узлов следует в соответствии со следующими рисунками (рисунки 4 - 6).

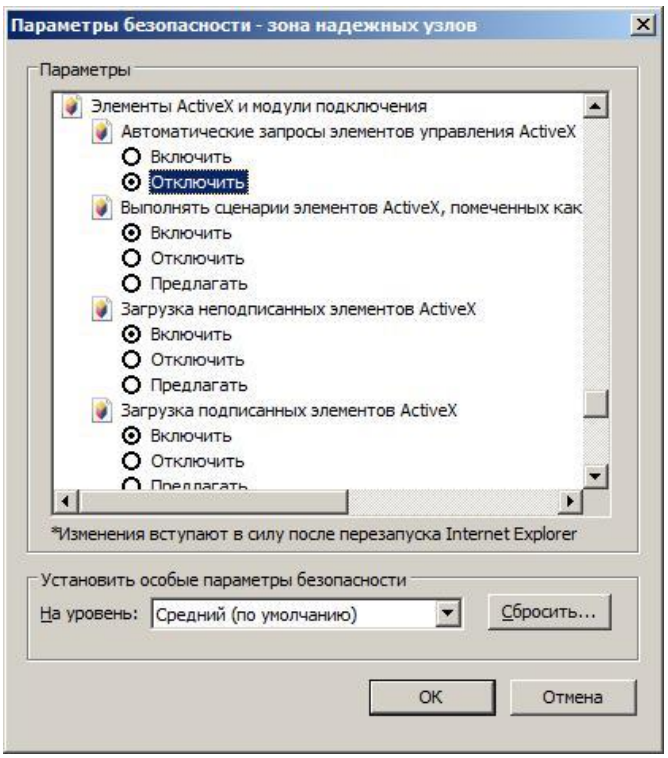


**Рисунок 4 - Установка параметров безопасности для IE8**

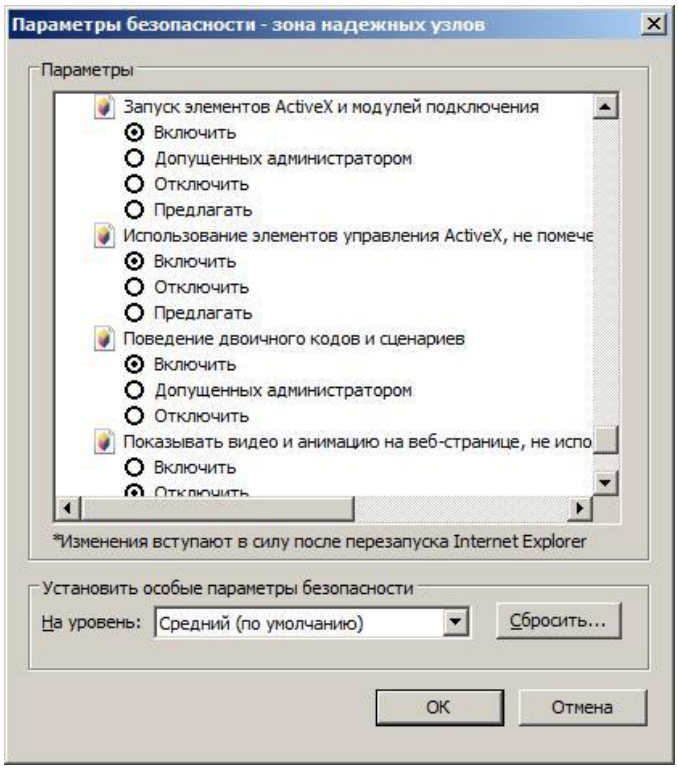


**Рисунок 5 - Установка параметров безопасности для IE8**

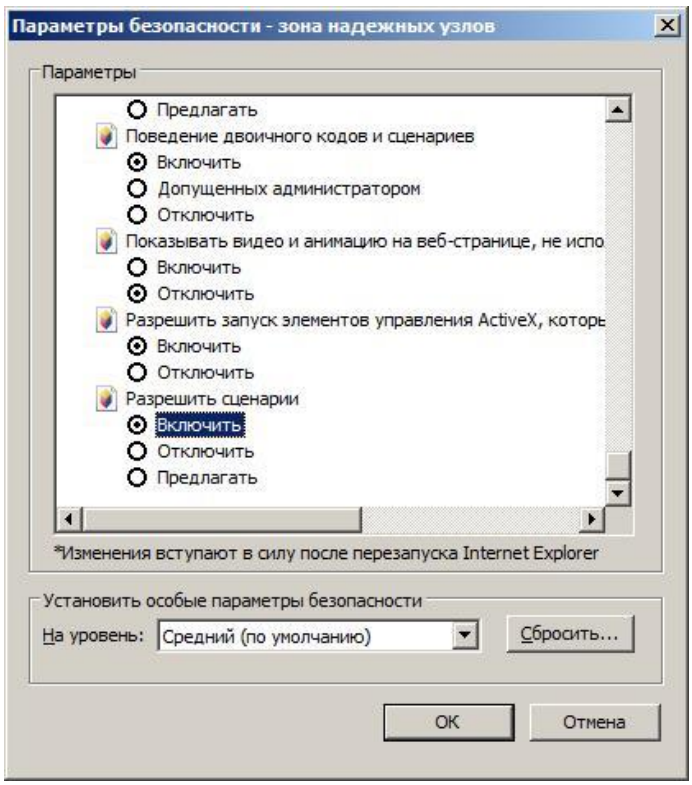


**Рисунок 6 - Установка параметров безопасности для IE8**

### 1.1.4. Особенность настроек обозревателя Internet Explorer 9

В случае если работа с системой будет производиться в IE9, необходимо выполнить дополнительные настройки. Изменить уровень безопасности надёжных узлов следует в соответствии со следующими рисунками (рисунки 25 - 27).

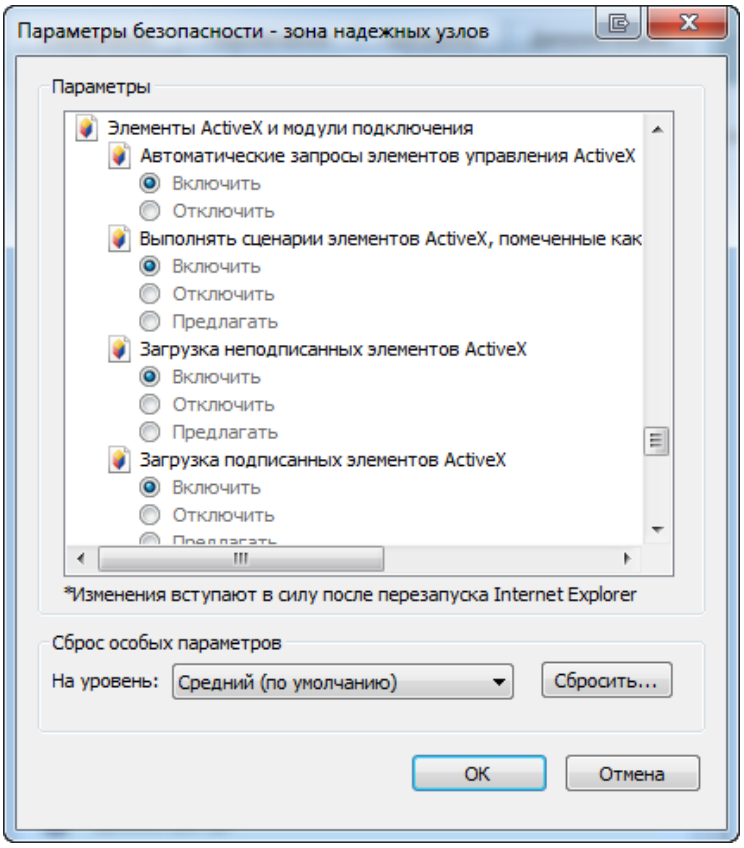


**Рисунок 7 - Установка параметров безопасности для IE9**

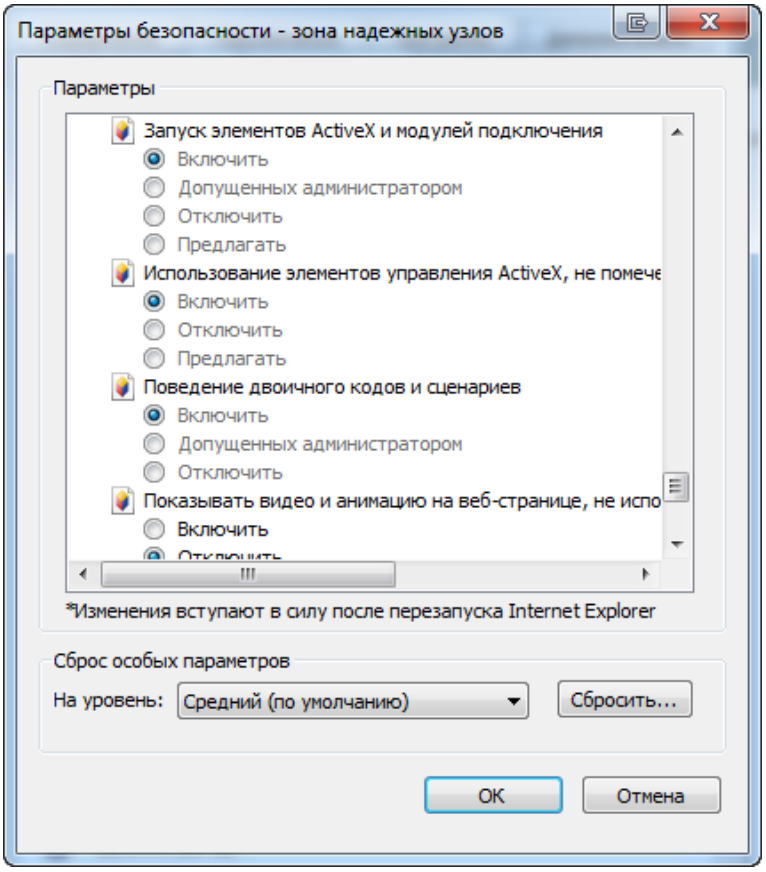


**Рисунок 8 - Установка параметров безопасности для IE9**

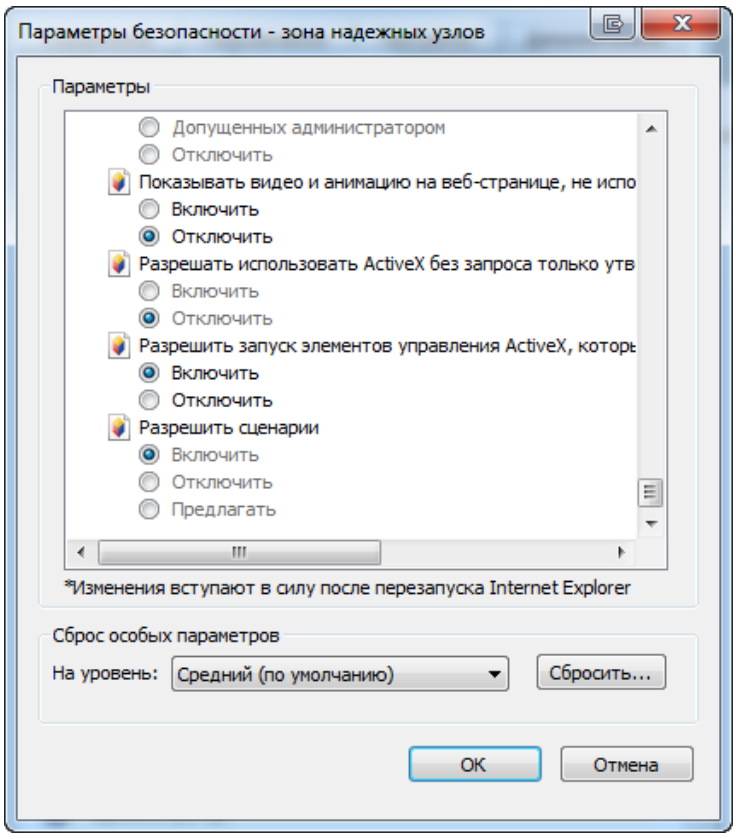


**Рисунок 9 - Установка параметров безопасности для IE9**

### 1.1.5. Особенность настроек обозревателя Internet Explorer 10

В случае если работа с системой будет производиться в IE10, необходимо выполнить дополнительные настройки. Изменить уровень безопасности надёжных узлов следует в соответствии со следующими рисунками (рисунки 28 -30).

**Внимание!** Настройка браузера и работа с приложением на Windows 8 должна проводиться только с рабочего стола. Режим Metro не поддерживается! Для корректной настройки браузер должен быть запущен от имени администратора.

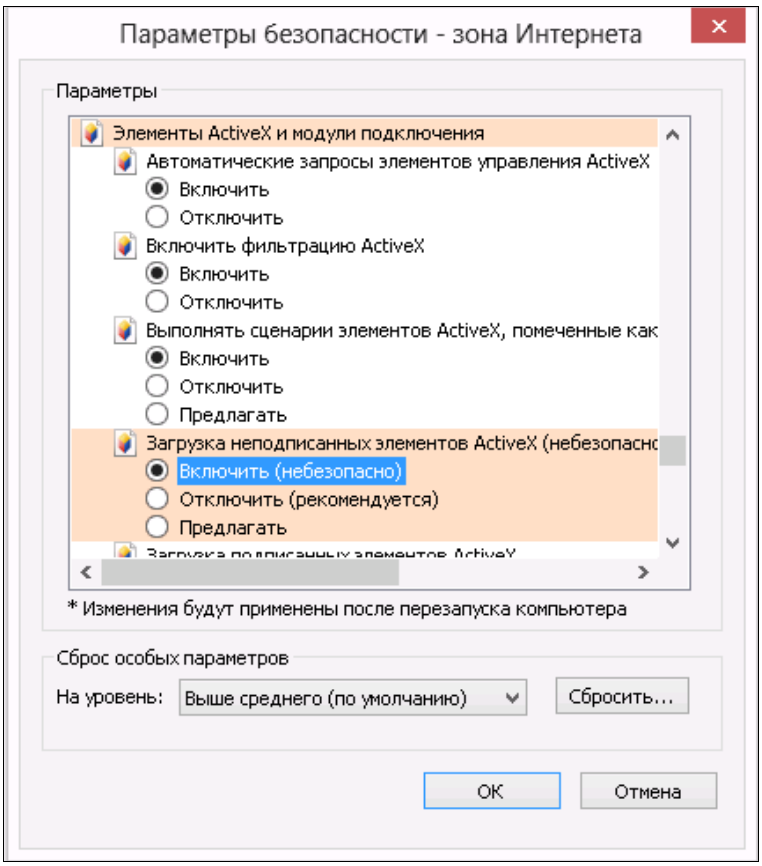


**Рисунок 10 - Установка параметров безопасности для IE10**

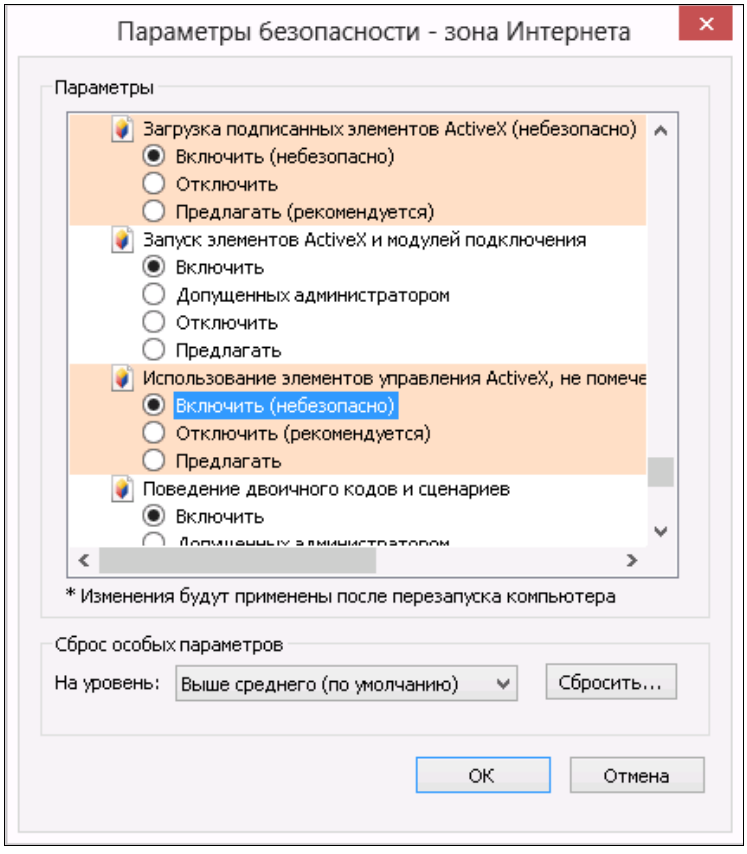


**Рисунок 11 - Установка параметров безопасности для IE10**

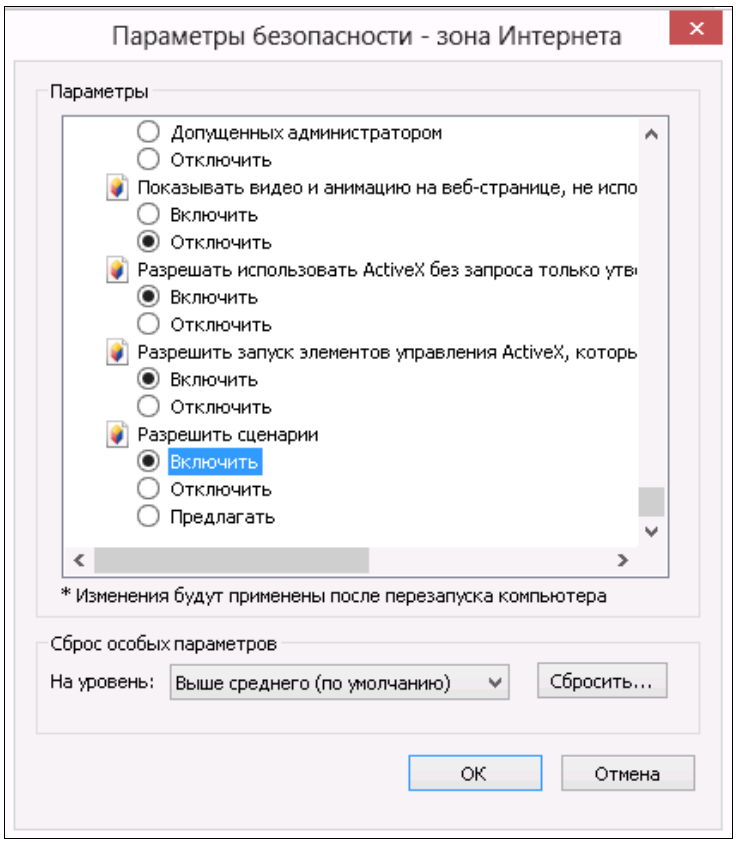


**Рисунок 12 - Установка параметров безопасности для IE10**

### 1.1.6. Особенность настроек обозревателя Internet Explorer 11

В случае если работа с системой будет производиться в IE11, необходимо выполнить дополнительные настройки. Изменить уровень безопасности надёжных узлов следует в соответствии со следующими рисунками (рисунки 31 -33).

**Внимание!** Настройка браузера и работа с приложением на Windows 8.1 должна проводиться только с рабочего стола. Режим Metro не поддерживается! Для корректной настройки браузер должен быть запущен от имени администратора.

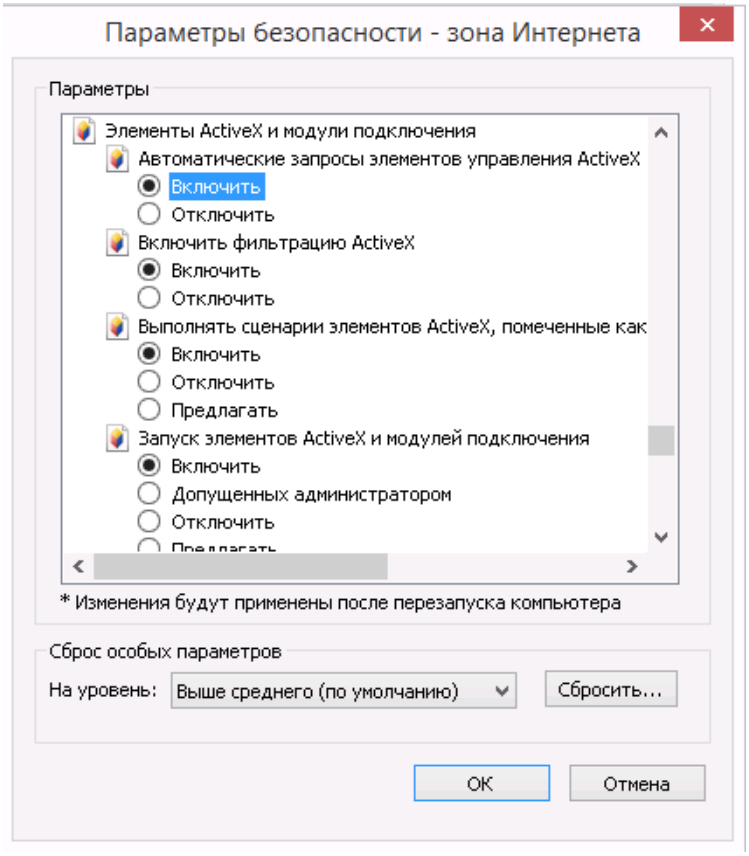


**Рисунок 13 - Установка параметров безопасности для IE11**

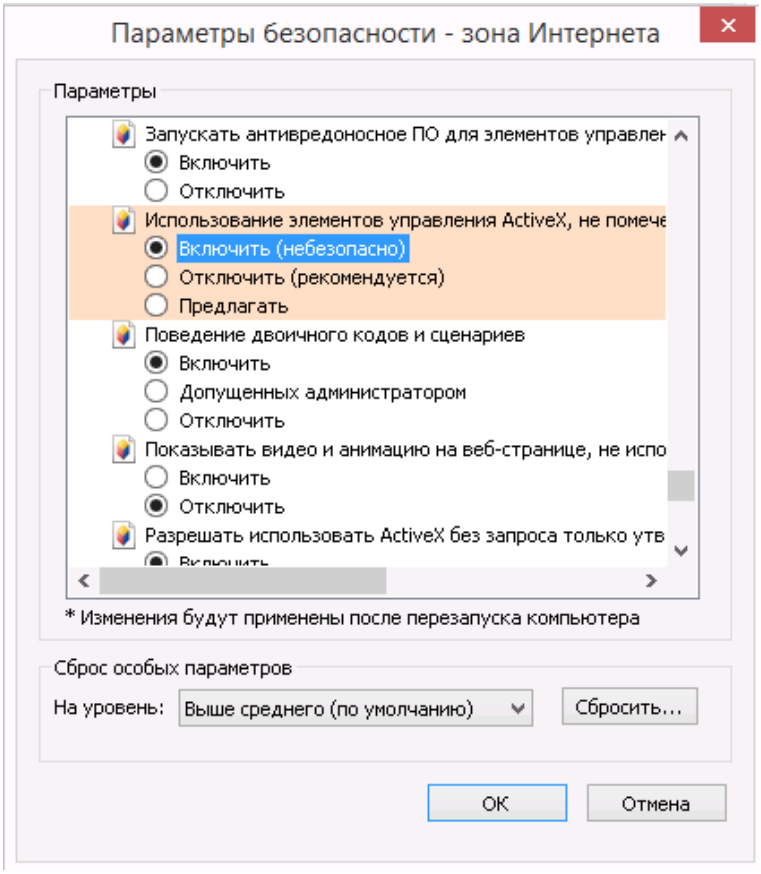


**Рисунок 14 - Установка параметров безопасности для IE11**

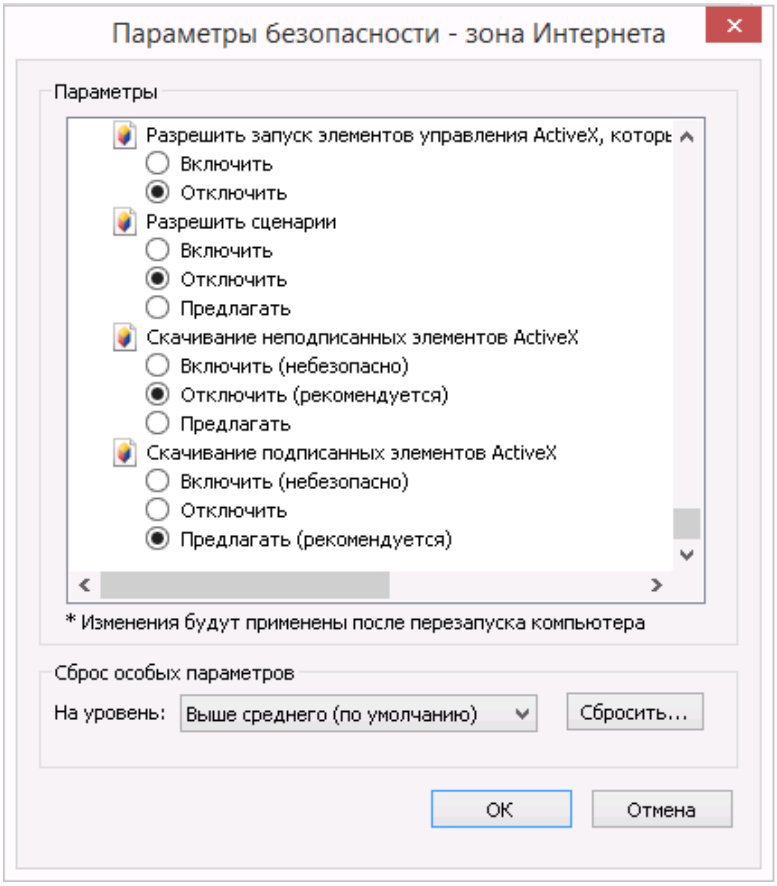


**Рисунок 15 - Установка параметров безопасности для IE11**

### 1.1.7. Установка параметров безопасности IE8-IE11. Выбор значений параметров безопасности, необходимых для просмотра шаблонов форм

Для того чтобы иметь возможность просматривать шаблоны форм на сайте модуля On-line, необходимо после добавления сайта модуля On-line в зону «Надежные узлы» установить для этой зоны особые значения для двух параметров безопасности.

**Примечание**

Установку параметров безопасности, необходимых для просмотра шаблонов форм, можно выполнять вместе с установкой параметров безопасности, необходимых для использования ЭП (подраздел 1.1).

Необходимо выполнить следующие действия:

1) В окне обозревателя выполните команду меню Сервис → Свойства обозревателя. Откроется окно «Свойства обозревателя». Перейдите на закладку «Безопасность».

2) Выберите зону Интернета «Надежные узлы» и нажмите кнопку «Другой» на панели «Уровень безопасности для этой зоны» Откроется окно «Параметры безопасности – зона надежных узлов» (рисунок 2).

3) В списке параметров безопасности найти параметр «Автоматические запросы на загрузку файлов» и установить для него значение «Разрешить» (рисунок 16).

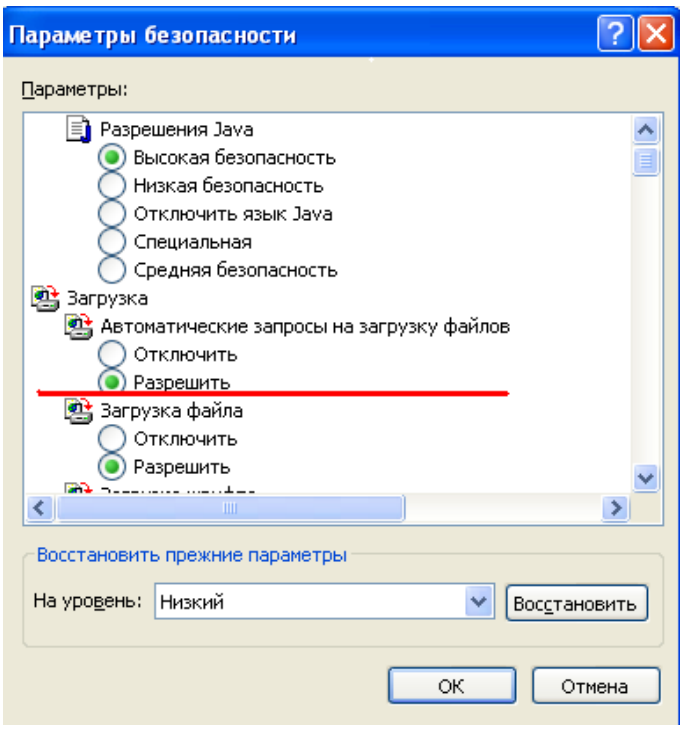


**Рисунок 16 - Выбор значения для параметра «Автоматические запросы на загрузку файлов»**

4) В списке параметров безопасности найти параметр «Блокировать всплывающие окна» и установить для него значение «Отключить» (рисунок 17).

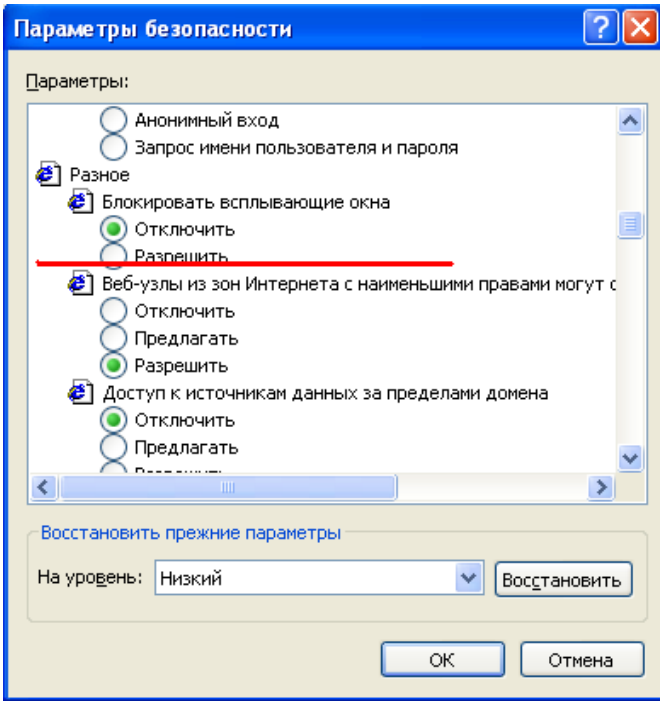


**Рисунок 17 - Выбор значения для параметра «Блокировать всплывающие окна»**

5) Нажать кнопку OK в окне «Параметры безопасности». В открывшемся диалоговом окне подтвердить изменения в настройках безопасности для зоны «Надежные узлы».

6) Нажать кнопку OK в окне «Свойства обозревателя».

При правильной настройке зоны «Надежные узлы» уровень безопасности будет действовать только для сайта On-line, и не должен изменять уровень безопасности для других интернет-сайтов.

Для предприятий с настроенной политикой безопасности рекомендуется первый запуск приложения и проверку работоспособности сайта выполнять под ролью локального администратора. Для этого необходимо нажать на ярлык IE8 правой клавишей мыши и в контекстном меню выбрать «Запуск от имени администратора».

Если при входе в онлайн модуль с помощью IE 8 на главной странице отображается сообщение (рисунок 18), необходимо в настройках браузера убрать совместимость с IE 7.

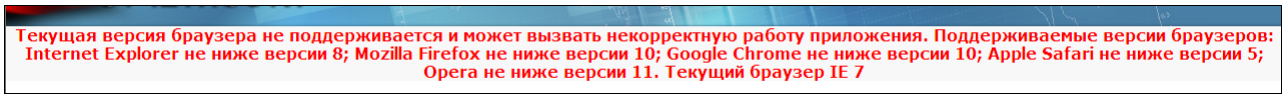


**Рисунок 18 - Сообщение в браузере**

Для того чтобы убрать совместимость с IE 7 необходимо выполнить следующие действия:

1) В окне обозревателя выполните команду меню Сервис → Параметры режима представления совместимости (Compatibility View Settings). Откроется окно «Параметры режима представления совместимости» (Compatibility View Settings) (рисунок 19).

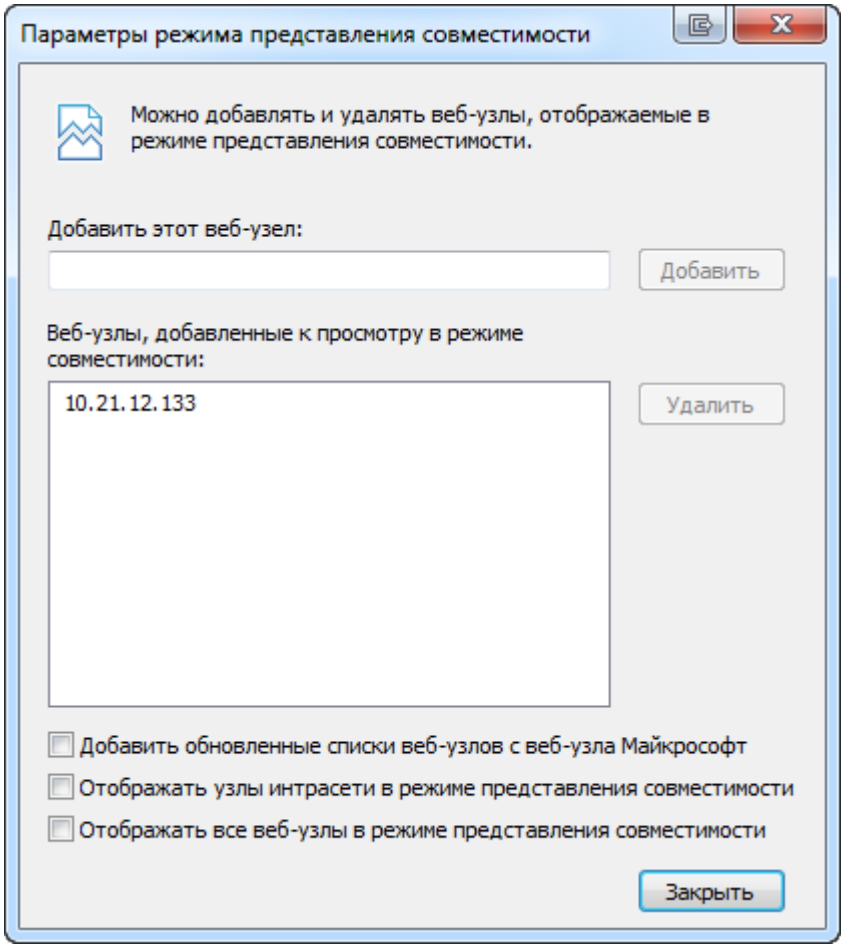


**Рисунок 19 - Окно «Параметры режима представления совместимости» (Compatibility View Settings)**

2) В поле «Веб-узлы, добавленные к просмотру в режиме совместимости» необходимо найти адрес онлайн модуля (рисунок 20).

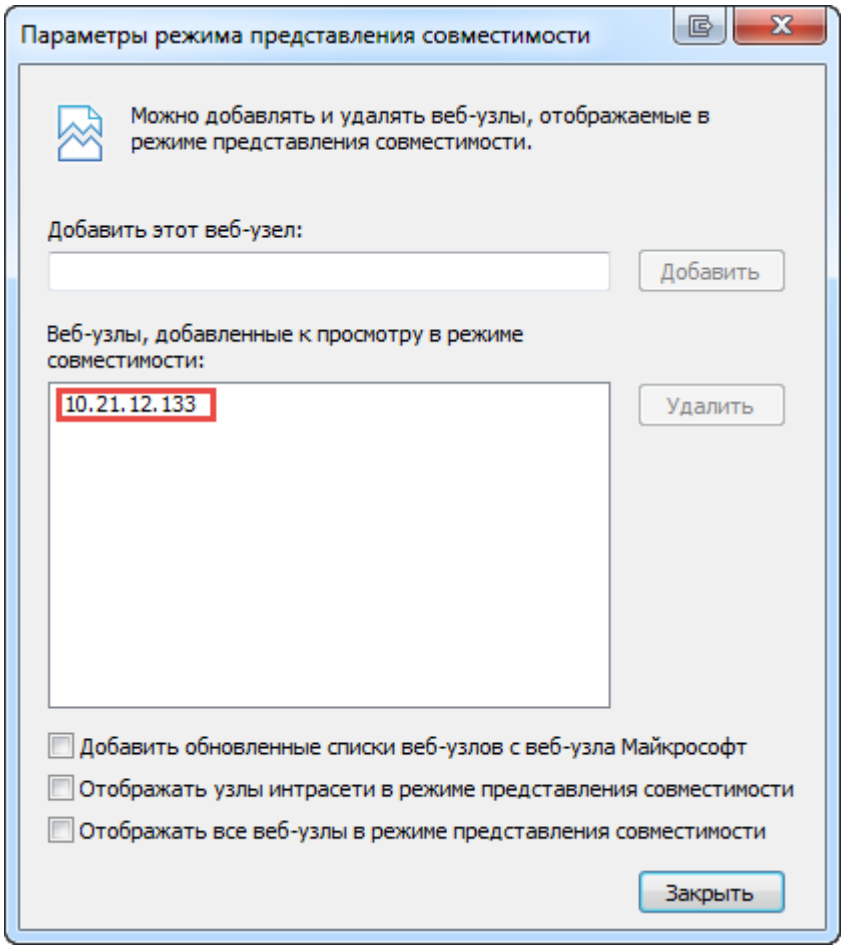


**Рисунок 20 - Адрес онлайн модуля (пример адреса)**

3) Для удаления адреса онлайн модуля необходимо в списке Веб-узлов выделить адрес и нажать на кнопку «Удалить» (Remove) (рисунок 21).

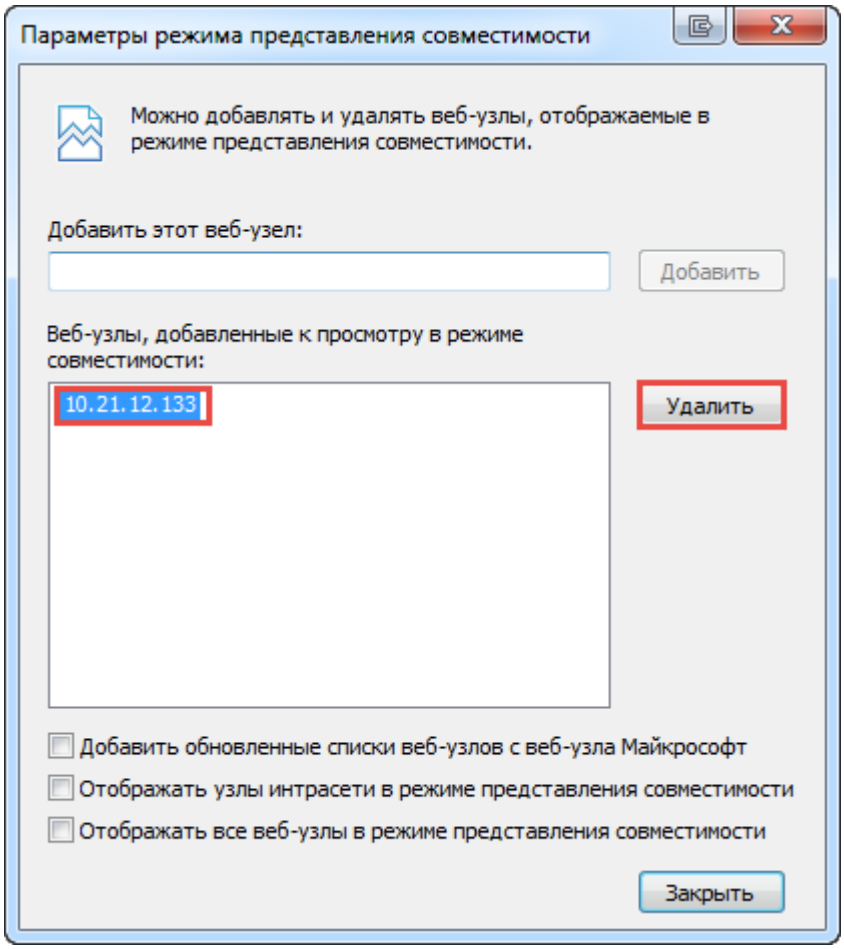


**Рисунок 21 - Выделенный адрес онлайн модуля**

4) После удаления адреса онлайн модуля в окне «Параметры режима представления совместимости» (Compatibility View Settings) необходимо нажать на кнопку «Закрыть». Обновить страницу.

После удаления адреса онлайн модуля из списка веб-узлов, которые доступны в режиме совместимости, с главной странице онлайн модуля уйдет сообщение о неправильно версии браузера.

2. **Установка расширений для других браузеров.**

Для браузера Google Chrome версии 42 и выше требуется установить расширение, размещенное по адресу: https://chrome.google.com/webstore/detail/croc-xml-signer/kiijhgpgjnhkhpagmcgihhigiolpogec;

Для браузера Opera версии 33 и выше необходимо:

- установить расширение «Download Chrome Extension», размещенное по адресу https://addons.opera.com/ru/extensions/details/download-chrome-extension-9/;
- установить плагин, доступный по ссылке: https://chrome.google.com/webstore/detail/croc-xml-signer/kiijhgpgjnhkhpagmcgihhigiolpogec.

Для браузеров Mozilla Firefox (и аналогов) требуется установить расширение, размещенное по адресу

https://online.gks.ru/webstat/Downloads/CrocXmlSigner/croc_xml_signer_fx.xpi.

# 3. Добавление сертификата для установления защищенного соединения

Для получения возможности обращаться к сайту On-line модуля подготовки отчетов, необходимо установить сертификат удостоверяющего центра (УЦ), который выдал сертификат для SSL-соединения.

Сертификат выложен для загрузки на сайте On-line. Его необходимо добавить в доверенные сертификаты. Скопируйте сертификат в папку на Вашем компьютере, если сертификат был заархивирован, извлеките файл из архива. В контекстном меню (правая кнопка мыши) выберите команду : « Установить сертификат» - Рис.40.

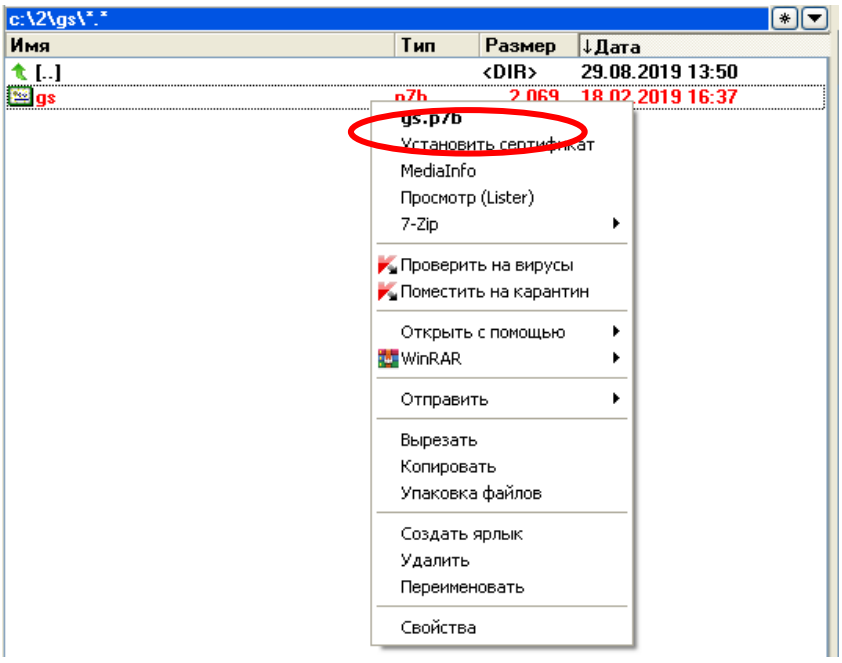


Рис.40

Осуществится запуск Мастера импорта сертификатов

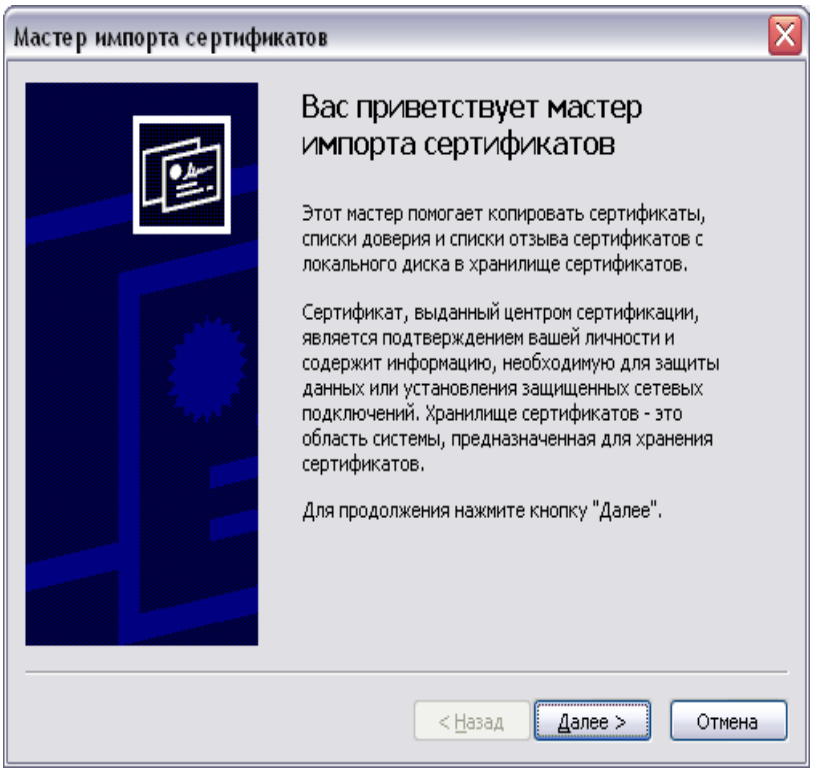


Рис.42

Нажмите кнопку Далее.
Система отобразит окно «Хранилище сертификатов», в котором необходимо указать, в какое хранилище требуется поместить сертификат.

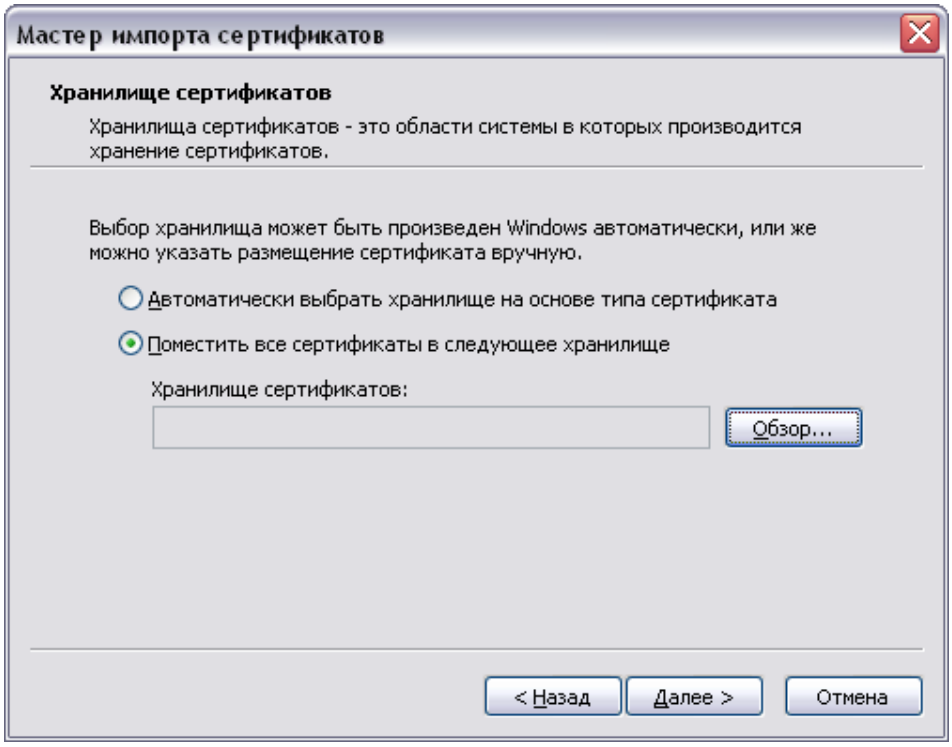


Рис.43

Нажмите на кнопку «обзор», в появившемся перечне хранилищ выберите «Доверенные корневые центры сертификации»

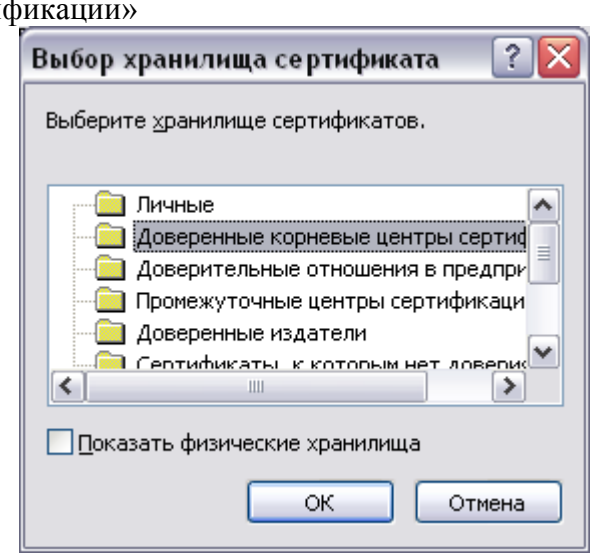


Рис.44

Нажмите кнопку Далее.
Система отобразит окно «Завершение работы мастера импорта сертификатов».

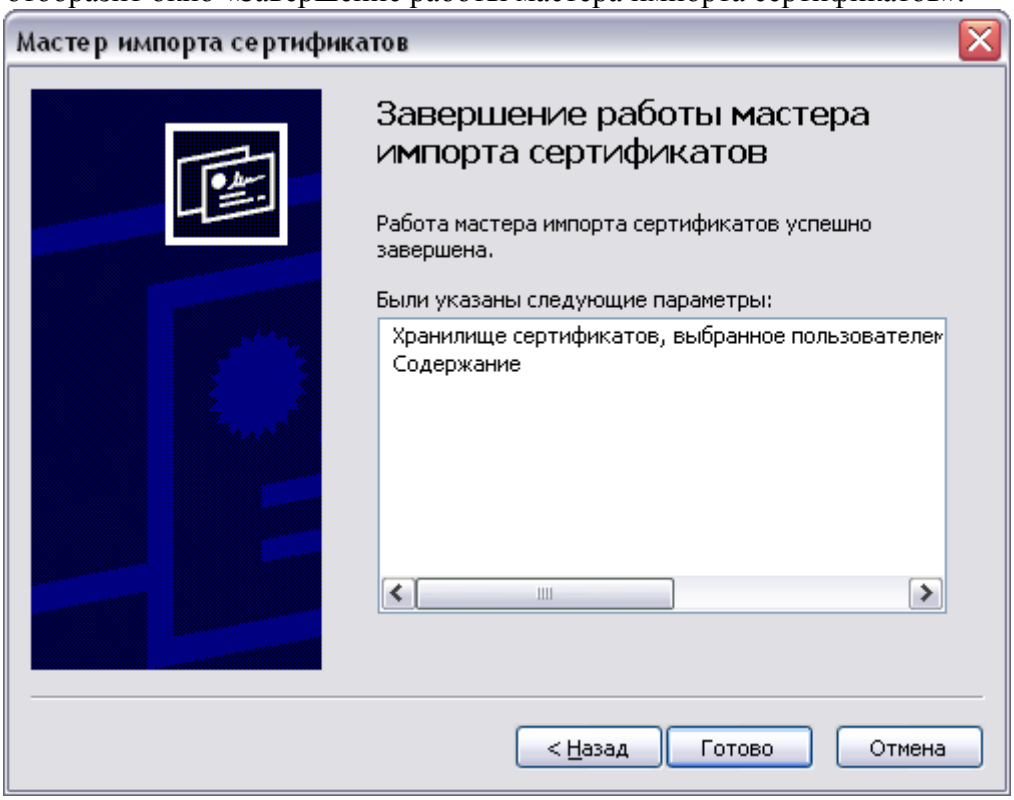


Рис.45

Нажмите кнопку Готово.
На запрос системы о необходимости установки данного сертификата

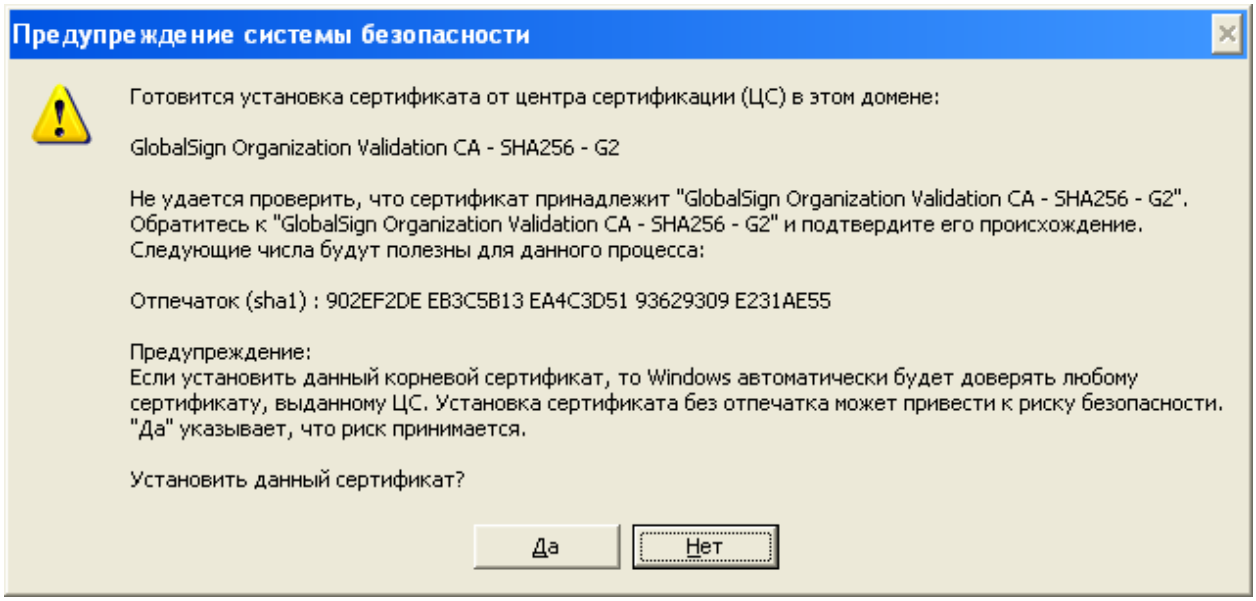


Рис.46

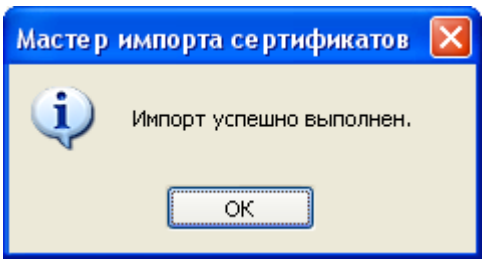


Рис.47

# 4. Установка плагина подписи для подписания отчетов.

Плагин доступен на главной странице ON-line модуля по ссылке: http://websbor.gks.ru/webstat/Downloads/CrocXmlSigner/CrocXmlSigner.rar

Разархивировать CrocXmlSinger.rar и запустить установщик CrocXmlSinger.msi.

Если на рабочей станции не был ранее установлен плагин подписи, то при попытке подписать отчёт на экране появится сообщение о необходимости установки плагина с активной ссылкой для скачивания «Скачать плагин» (Рис. 4848).

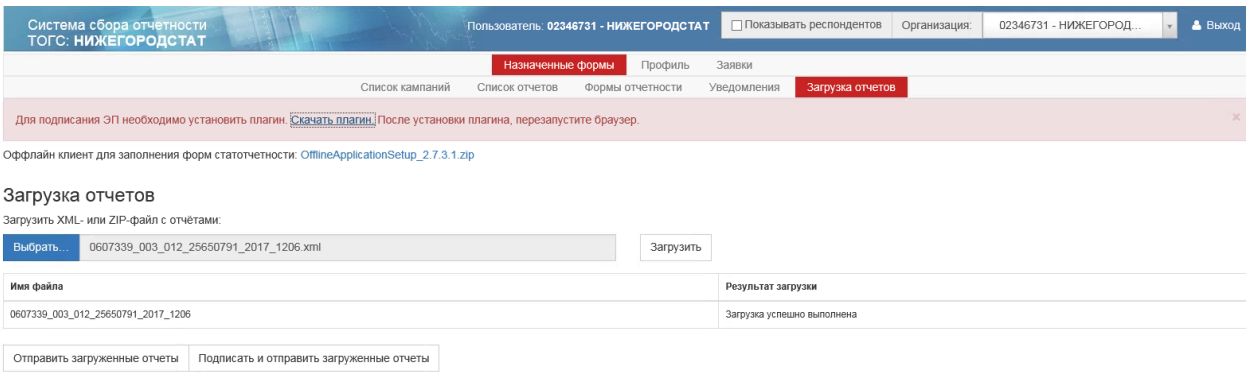


Рис. 48 – Сообщение о необходимости установки плагина подписи

При нажатии на ссылку «Скачать плагин», откроется окно «Загрузка файла».

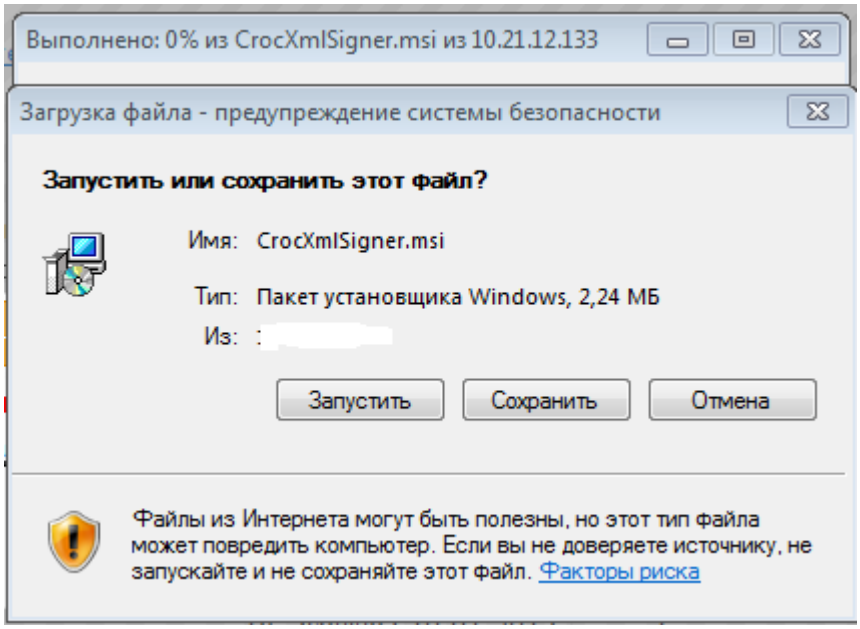


Рисунок 49 - Запрос на установку плагина

Для установки плагина, необходимо нажать кнопку «Запустить», после чего начнется процесс установки компоненты. После завершения установки, необходимо обновить окно браузера.

При последующем подписании отчета, запрос на установку компонента не будет происходить.

Если после установки плагин не работает, то необходимо установить вручную библиотеки Visual C++ Redistributable for Visual Studio 2015 x86 (https://www.microsoft.com/en-us/download/details.aspx?id=5638).