Лабораторная работа №19
Тема: «Защита от спама»

Теоретическая часть

Наиболее распространенной причиной получения спама являются сами пользователи. Они посылают электронные сообщения на веб-сайты или в компании, которые в ответ рассылают им свою рекламу или продают их адреса другим компаниям. Еще одна распространенная причина получения спама — **невнимательная подписка на различные новости и информационные рассылки**.

Поскольку программ для рассылки спама создано огромное количество, то непросто выбрать лучшую программу для борьбы с нежелательными рассылками. Не существует программы, которая фильтрует спам со 100%-ной гарантией. Если утилита будет отсекать около 90% нежелательной корреспонденции, это уже хороший результат. Одной из неплохих утилит является McAfee SpamKiller — программа для защиты от спама с ежедневным автообновлением базы по спамерам и легким созданием собственных фильтров. Работает SpamKiller в фоновом режиме, проверяет практически неограниченное число почтовых ящиков, выявляет полученный спам и удаляет его прямо на почтовом сервере — автоматически или в ручном режиме. В случае обнаружения новой почты возможна разнообразная сигнализация об этом, а также автоматический запуск почтовой программы.

Условно-бесплатный вариант программы имеется на множестве сайтов Интернета. Установщик находится в папке: «Установщики». После загрузки и запуска программы открывается окно для инсталляции утилиты (рис. 1). Нажимаем кнопку «Next».

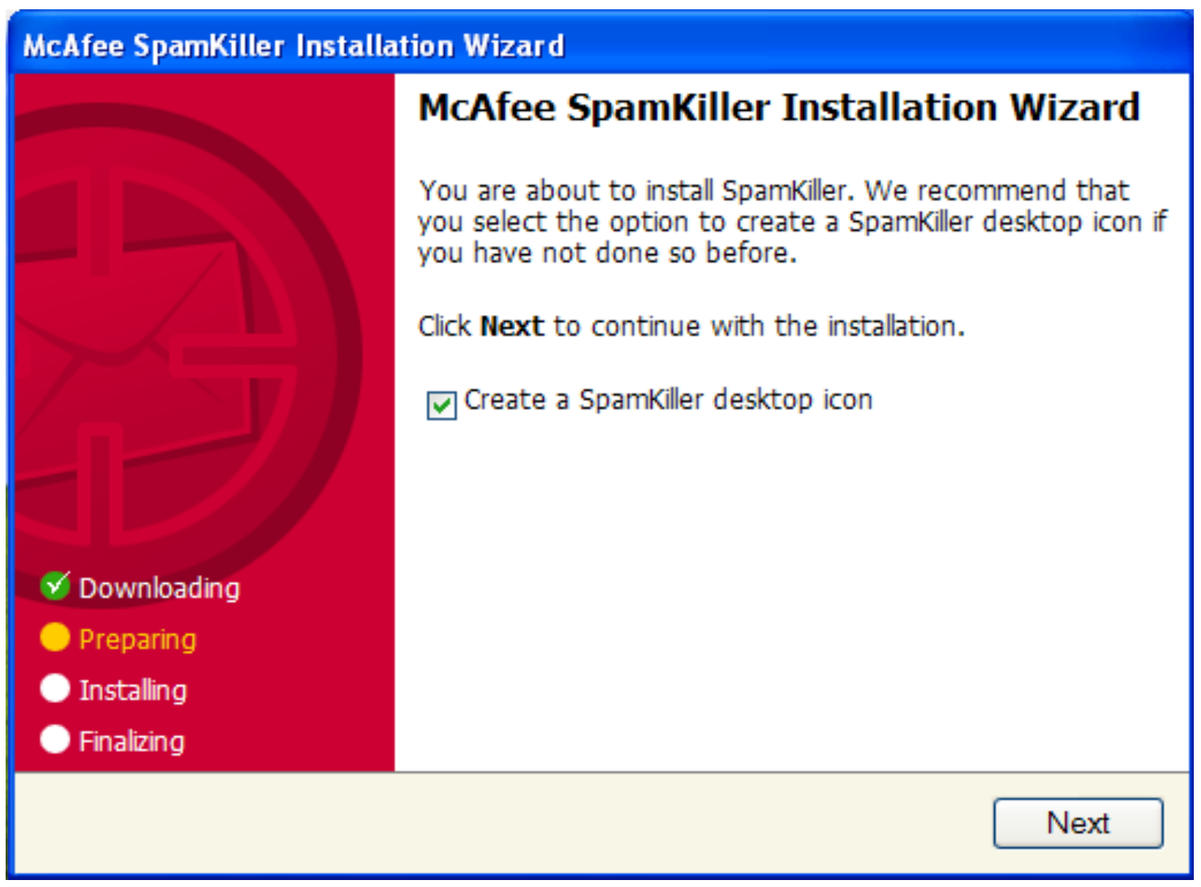

Рис. 1

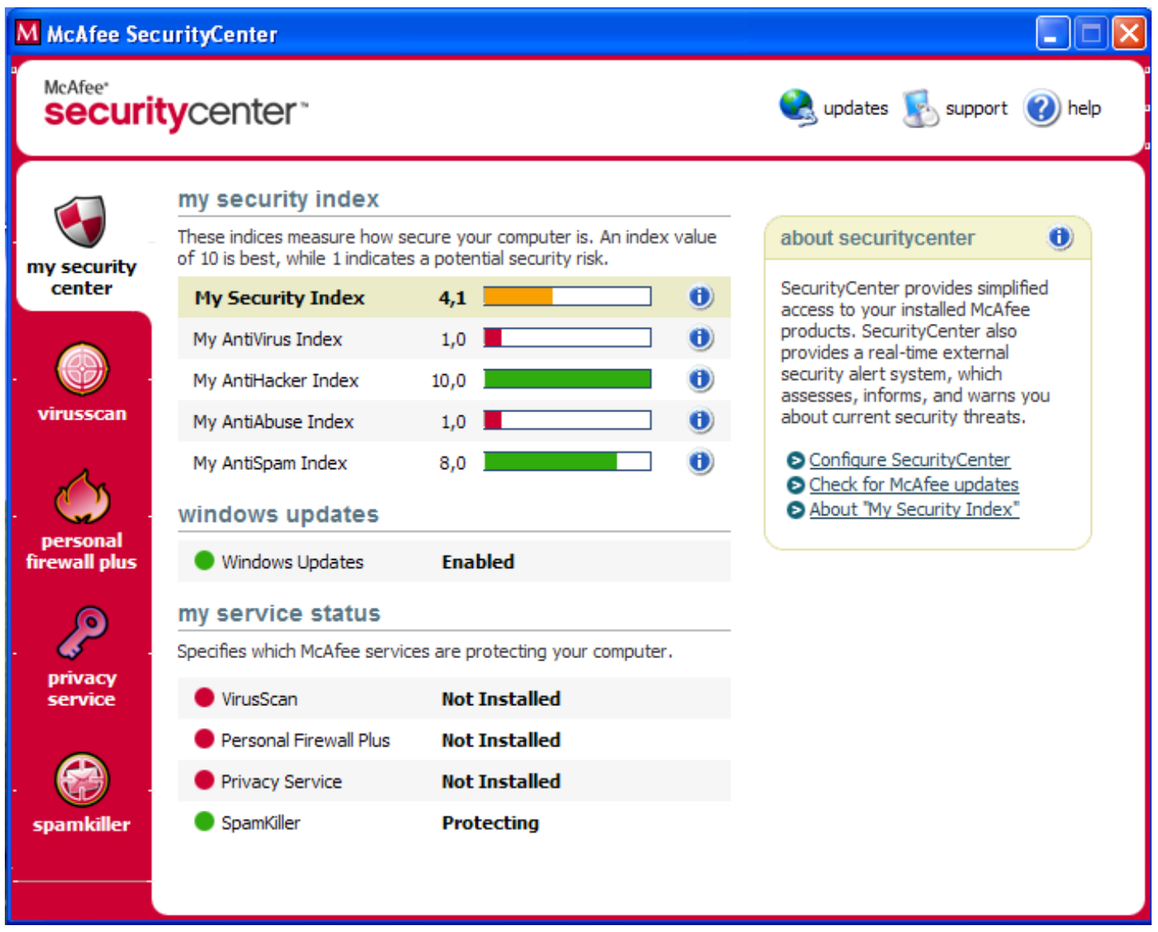

Рис. 2

Открыв окно McAfee SecurityCenter (рис. 2), сразу появиться меню (слева) и таблица показателей (оценки защиты). Таблица показывает, насколько защищен Ваш компьютер от тех или иных «угроз».

Меню слева предлагает установку «триальных» версий:

- Антивируса McAfee VirusScan;
- Брандмауэра McAfee Personal Firewall Plus;
- McAfee Privacy Service;
- McAfee SpamKiller (то, что было установлено ранее).

Выбираем «View E-mail Blocked by SpamKiller».

В представленном окне (рис. 3) слева есть меню:
«Summary» - отчет по успешным «блокировкам» спама, работающий в реальном времени;
«Messages» - здесь вводятся e-mail'ы пользователей, от которых, как вы считаете, «посылается» спам;
«Friends» - это, видимо, просто для добавления друзей (в виде e-mail адресов);
«Settings» - настройки SpamKiller'а.

Рис. 3

Если почтовый клиент пользователя поддерживает графические сообщения в формате HTML, то при каждом получении почты имеется вероятность того, что отправитель узнает, прочитал ли получатель его письмо. Это делается при помощи скрытых ссылок на изображения, обращающиеся к веб-серверу, на котором запущена специальная программа, отслеживающая подобные обращения. Когда пользователь открывает письмо со спамом, оно может послать сигнал на веб-сервер своего отправителя, сигнализируя ему, что электронный адрес получателя активен и что получатель читает приходящую почту. Если задержать сигналы, отправляемые на серверы распространителей спама, то возможно, что адрес получателя будет удален из баз данных серверов как неактивный.

Последние версии некоторых почтовых программ, например Outlook Express (после установки Windows XP Service Pack 2), автоматически блокируют все внешние ссылки в HTML-сообщениях. Режим блокировки внешних ссылок в Outlook Express можно включить во вкладке «Безопасность» в окне «Параметры», вызываемого из меню «Сервис». В Outlook Express также имеется список надежных отправителей, с помощью которого можно включать внешнее содержимое только для определенных отправителей. Чтобы разрешить использование рисунков и другого внешнего содержимого для определенного отправителя, нужно щелкнуть правой кнопкой мыши на сообщении от него и добавить отправителя в список надежных отправителей.

Практическая часть
Защита от вредоносных программ и вирусов

В настоящее время spyware-программы превратились в наиболее опасную угрозу для компьютеров. Скрываясь в свободно распространяемых приложениях, эти программы шпионят за пользователями компьютеров и затем отправляют собранную информацию злоумышленникам. Существует еще один вид вредоносных программ — adware-программы, тесно связанные со spyware-программами. Они также тайно устанавливаются на компьютеры пользователей и наблюдают за ними. Обычно подобные ситуации связаны с установкой программ, загружаемых с веб-сайтов. Пользователи часто перед установкой бесплатных программ не читают соответствующие соглашения о предоставлении услуг и пропускают сообщения, что данные программы будут отображать рекламу.

Шпионское программное обеспечение (Spyware) — относительно новый вид угрозы, который еще недостаточно широко обрабатывается стандартными антивирусами. Шпионское программное обеспечение, не проявляя себя, отслеживает поведение пользователя за компьютером, чтобы создать его «маркетинговый профиль», который также молча передается сборщикам информации, продающим данные пользователя рекламным организациям. Если в браузере появятся новые панели инструментов, которые явно не устанавливались, если браузер постоянно «падает» или стартовая страница неожиданно изменилась, вероятно, что в компьютере завелся «шпион». Но даже если не происходит ничего необычного, то «шпионы» все равно могут появляться, поскольку со временем все больше появляется программного обеспечения такого рода.

В Интернете имеется множество свободно распространяемых утилит, помогающих проверить

компьютер на наличие spyware- и adware-программ. Наибольшей популярностью пользуется программа Spybot Search & Destroy.

( )

Программа Spybot Search&Destroy («спайбот» — «найти и уничтожить») может обнаруживать и удалять с компьютера различного рода шпионское программное обеспечение.

После загрузки, инсталляции и запуска программы открывается ее окно с подменю Spybot Search & Destroy (рис. 4). При первом запуске нужно прочитать несколько соглашений об ответственности за использование программы.

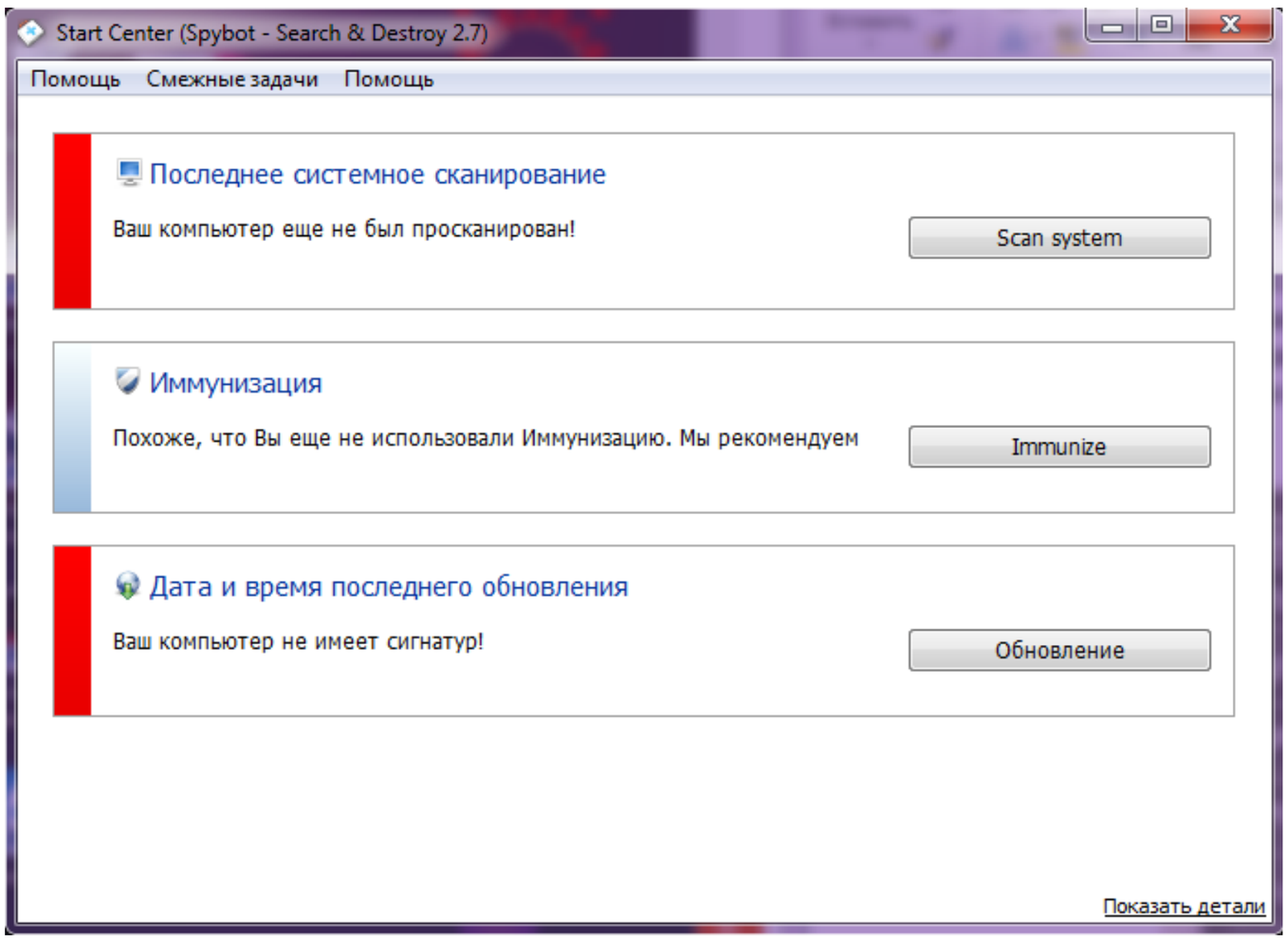

Рис. 4

Далее для работы с программой Spybot Search & Destroy нужно выполнить следующие действия:

1) Обновить файлы данных, для чего щелкнуть по кнопке «Последнее системное сканирование» - «Поиск сигнатур»;

2) Для их загрузки щелкнуть по кнопке «Обновление» (рис. 5);

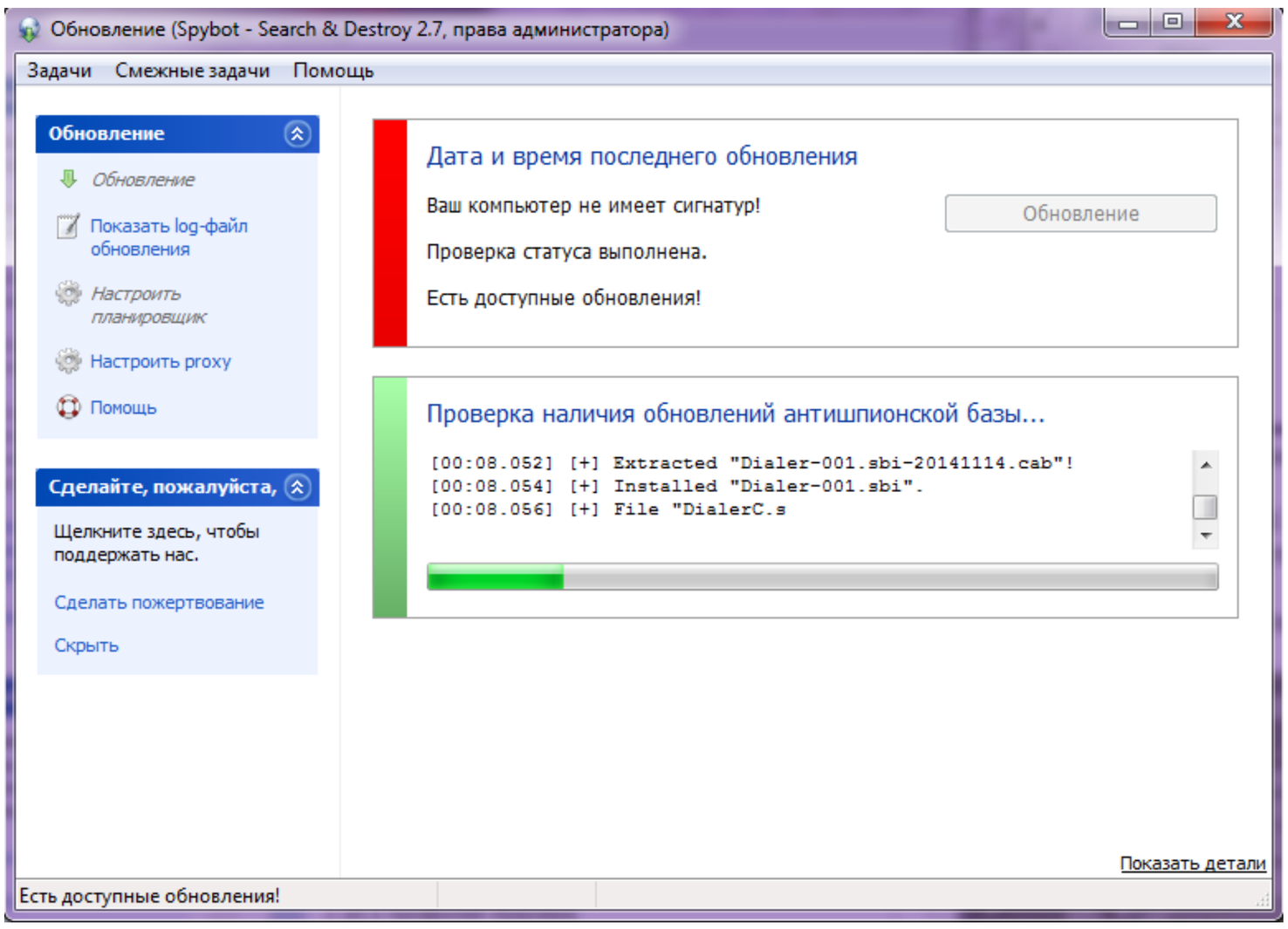

Рис. 5

3) Теперь необходимо щелкнуть по кнопку «Scan System». Начнется сканирование системы. Результаты сканирования через некоторое время будут выведены в окне результатов (рис. 6). Лучший результат показан на рис. 7.

4) Для устранения выявленных проблем нужно нажать клавишу «Исправить отмеченное». Устранению подлежат только файлы, помеченные флажками. Программа автоматически сохраняет резервные копии всех удаляемых объектов на случай возникновения проблем в ОС после удаления файлов и параметров реестра.

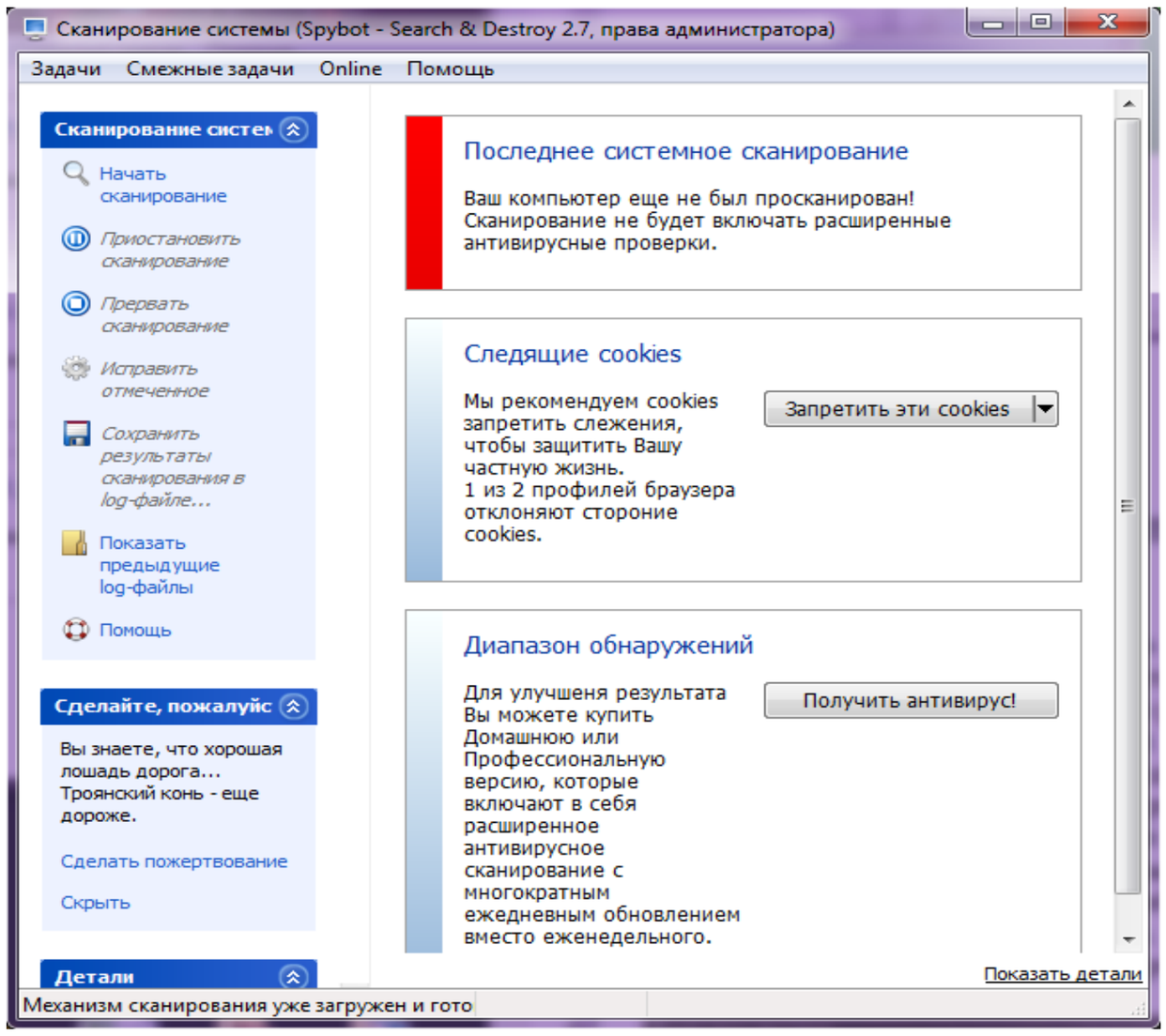

Рис. 6

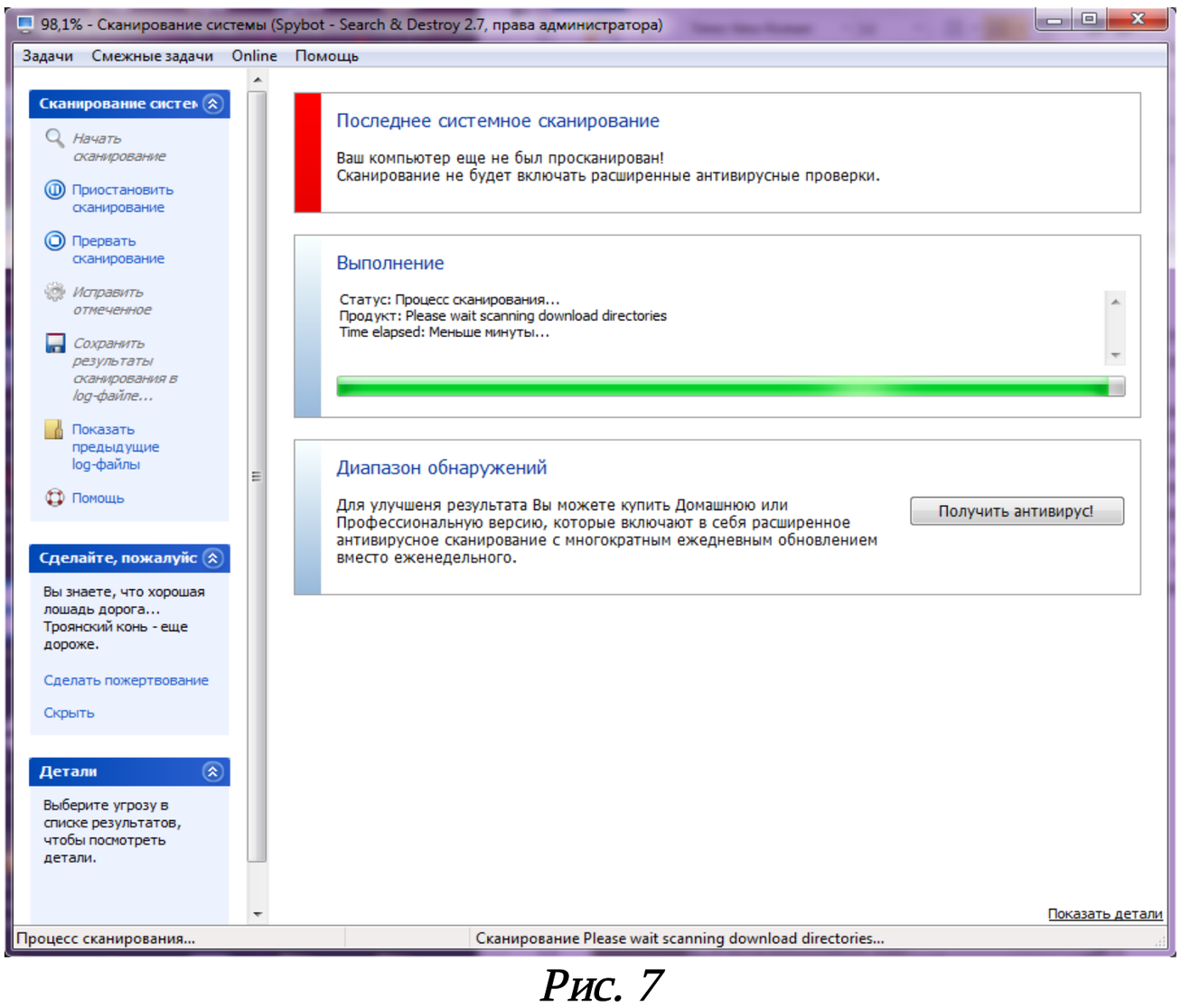

Рис. 7

Утилита Spybot Search&Destroy способна не только проверять компьютер и удалять spyware- и adware-программы. С ее помощью можно выполнять вакцинацию («Иммунизация»), защищающую компьютер от некоторых наиболее распространенных типов вредоносных программ, что значительно повышает защищенность компьютера в борьбе с spyware- программами. Для выполнения вакцинации следует запустить утилиту и щелкнуть по кнопке «Иммунизация» (рис. 8). После проверки, необходимо нажать кнопку «Применить иммунизацию» (рис. 9).

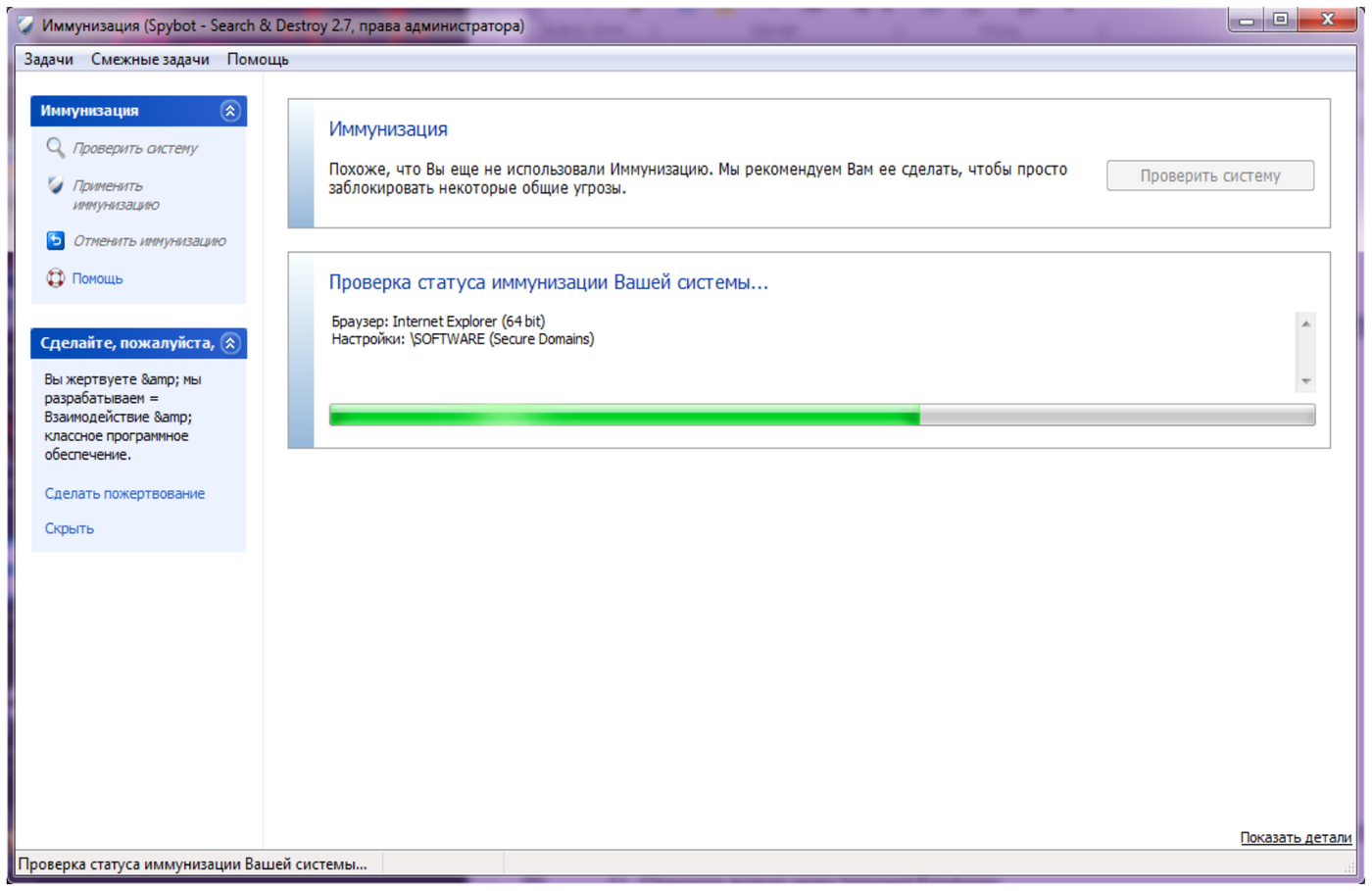

Рис. 8

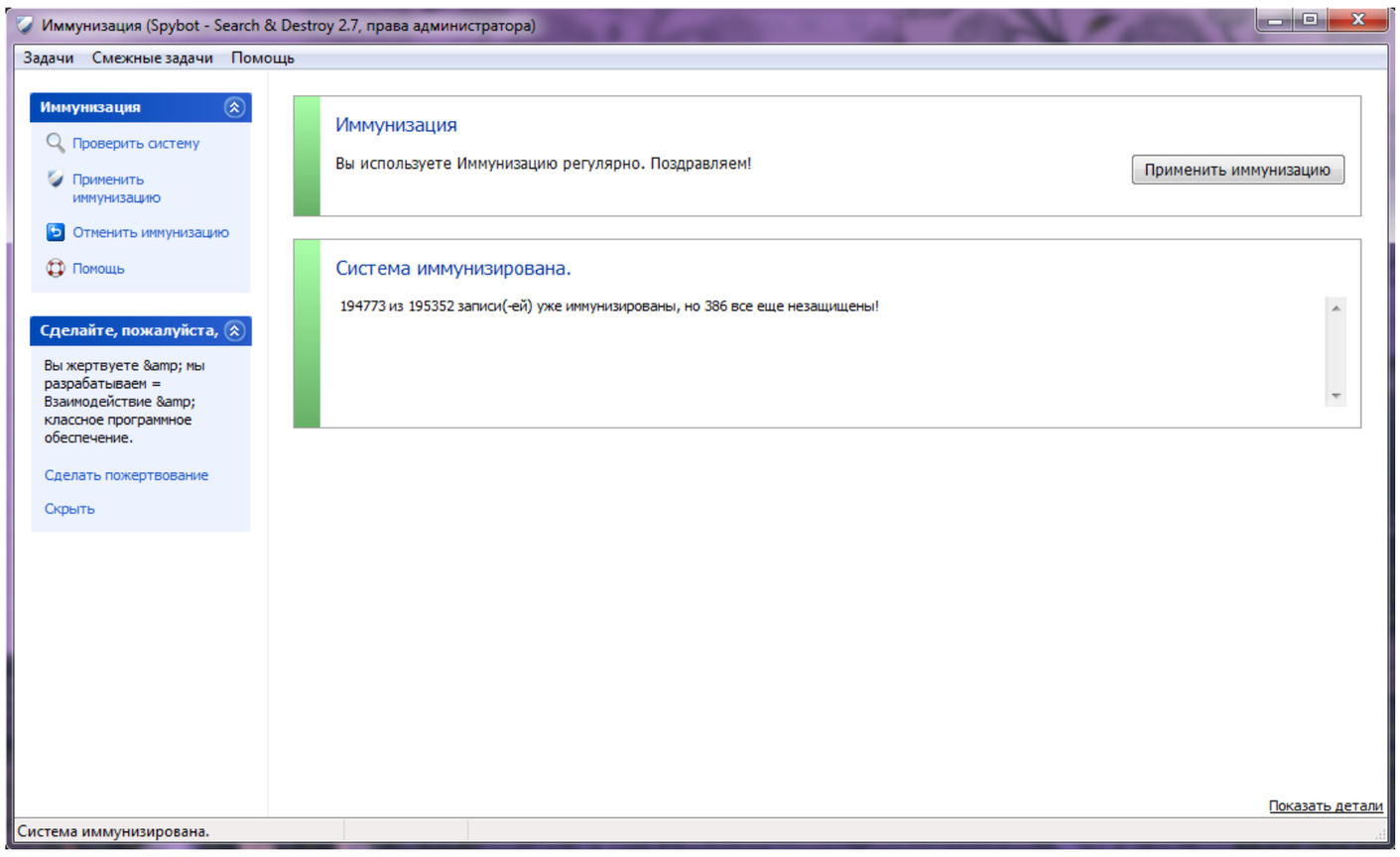

Рис. 9

Целесообразно изменить параметры установки элементов ActiveX (небольшие приложения, с помощью которых сайты предоставляют контент), запретив возможность их установки. Для этого необходимо выполнить следующие действия:

1) Открыть новое окно Internet Explorer;
2) Нажимаем CTRL один раз, сверху рядом с вкладками откроется меню;
3) Выбираем меню «Сервис» - «Свойства браузера» (рис. 9);

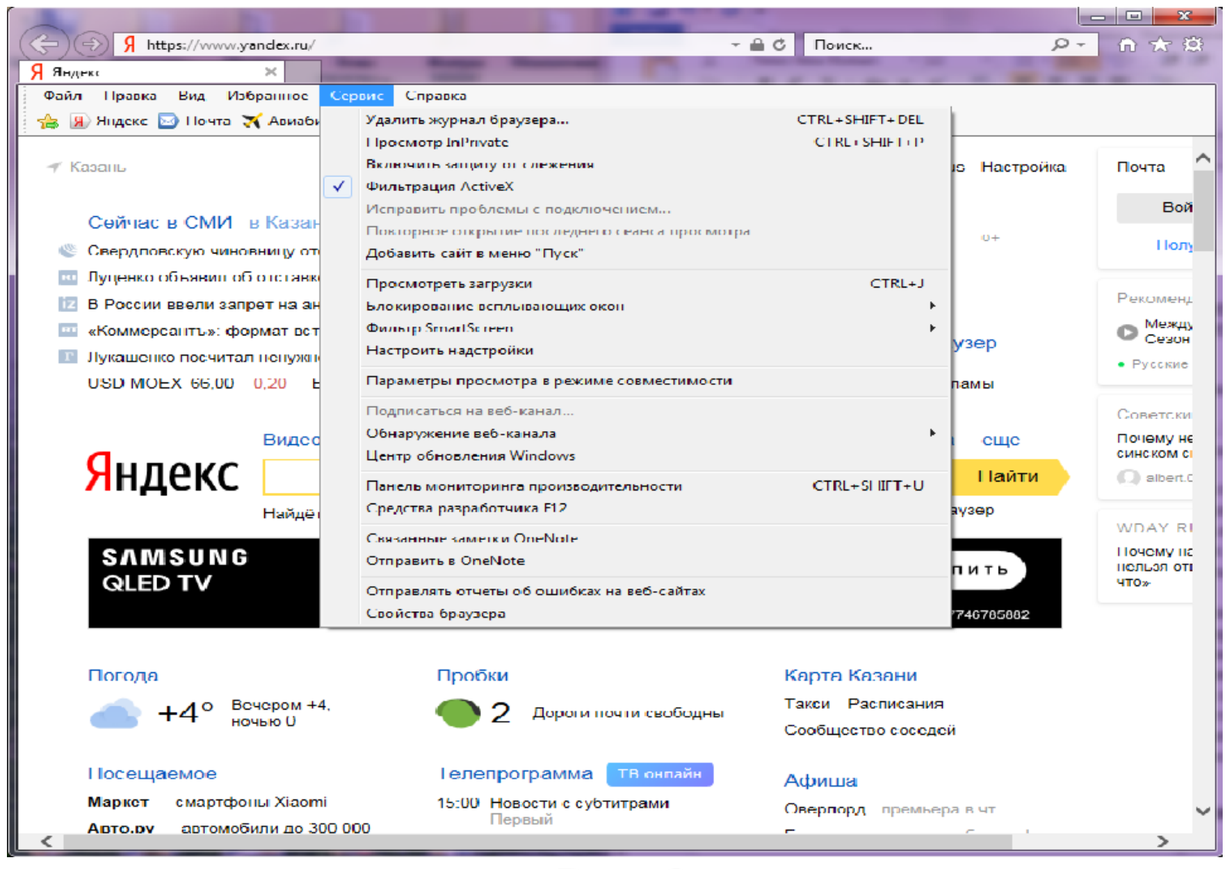

Рис. 9

4) Откроется окно «Свойства браузера»;
5) Необходимо перейти на вкладку «Безопасность» и щелкнуть по кнопке «Другой…» (рис. 10);

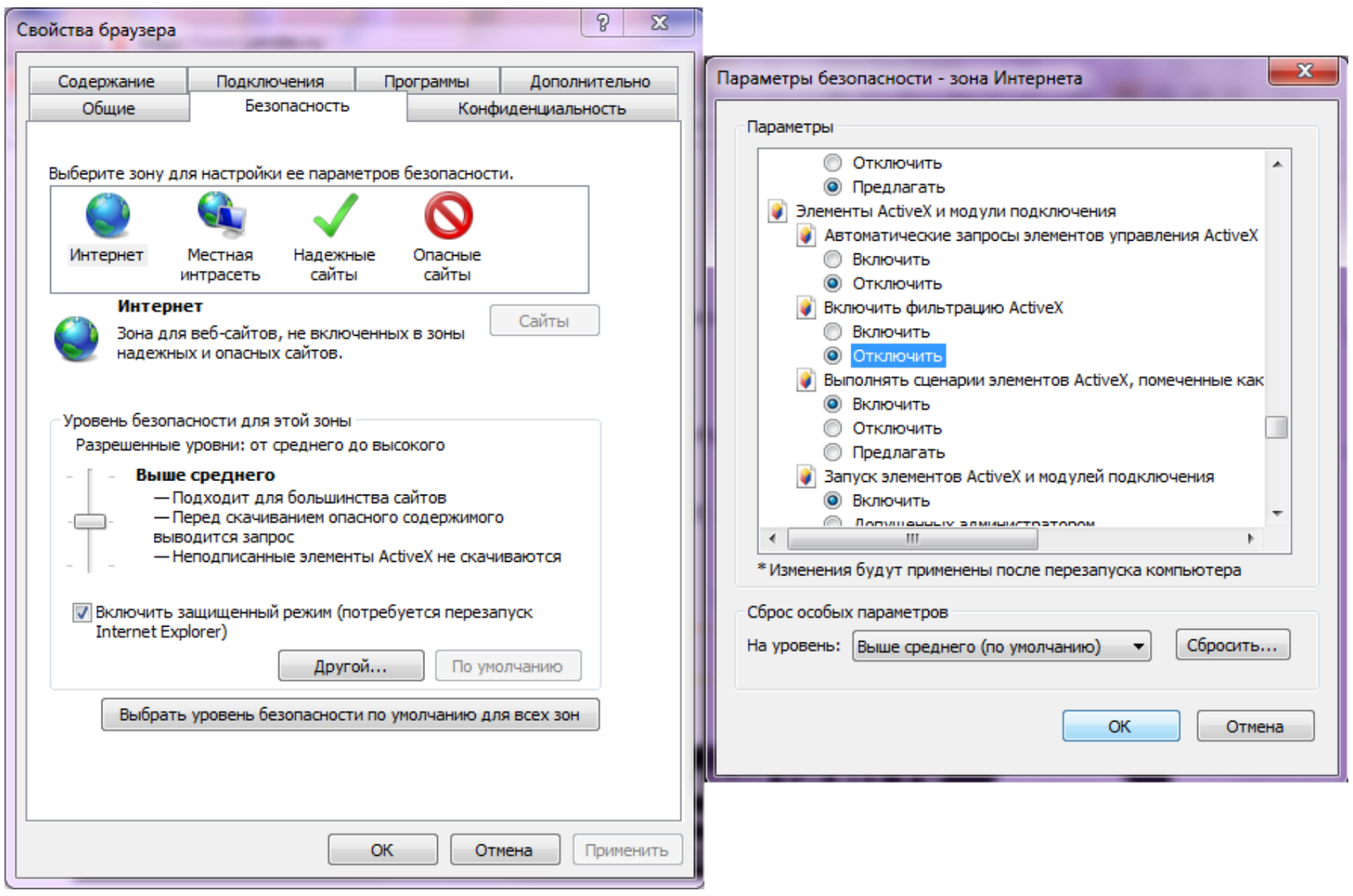

Рис. 10

6) Найти в списке группу переключателей «Загрузка подписанных элементов ActiveX» и установить переключатель в состояние «Отключить» (загрузка неподписанных элементов также должна быть отключена, рис. 10);
7) Щелкнуть по кнопке «OK», а затем — по кнопке «Да»;
8) Еще раз щелкнуть по кнопке «OK» для закрытия окна «Свойства обозревателя».

Выполненная процедура приведет к запрету установки элементов управления ActiveX с любых веб-сайтов (как хороших, так и плохих). Если при посещении какого-либо сайта возникнут проблемы с загрузкой его содержимого, то можно выполнить обратную процедуру, т.е. разрешить загрузку подписанных элементов ActiveX.

Контрольные вопросы

1. Что такое спам?
2. Назовите наиболее распространённую причину спама.
3. Что такое вирус?
4. Назовите основные методы защиты от вредоносных программ.
5. Чем отличается spyware-программы от adware-программы?
6. Есть ли уязвимости у утилит, «защищающих» от вредоносных программ, спама, spaware-, adware-программ?

Содержание отчета

В отчет о выполненной работе включить следующие материалы:
1. Тему и цель работы.
2. Результаты выполнения заданий: исследуемые схемы, полученные таблицы переходов.
3. Анализ полученных результатов.
4. Ответы на контрольные вопросы.
5. Выводы по работе.

20'