ПАМЯТКА
пользователя по антивирусной защите

Антивирусное программное обеспечение Dr.Web устанавливается на автоматизированных рабочих местах (далее - АРМ) сотрудников в целях защиты от проникновения вредоносных программ.

Установка, конфигурирование и управление средствами антивирусной защиты осуществляется администратором сегмента системы АВЗ организации.

Пользователю запрещается самостоятельно вносить изменения в настройки антивирусного программного обеспечения, установленного на АРМ. Пользователю запрещается самостоятельно устанавливать программное обеспечение на АРМ.

Пользователю запрещается сохранять (скачивать) и открывать файлы на АРМ и переходить по гиперссылкам, полученным по электронной почте от неизвестных отправителей. Если отправитель известен, но есть сомнения в подлинности письма, необходимо уточнить у отправителя факт отправки письма лично, после чего сохранить вложение и перед открытием проверить антивирусным программным обеспечением. Действия пользователя описаны в приложении № 1

Пользователю АРМ запрещается использовать ресурсы сети Интернет в неслужебных целях.

Пользователь после включения АРМ, обязан контролировать запуск антивирусного программного обеспечения, которое запускается в автоматическом режиме, в области панели задач операционной системы должен отображаться значок  .

Пользователь АРМ перед открытием файлов, полученных из внешних источников (электронная почта, сеть Интернет и др.), обязан проверить их антивирусным программным обеспечением на наличие вредоносных программ. При подключении к АРМ съемных носителей информации (flash-накопители, оптические диски, жесткие диски USB и т.д.) пользователь обязан запустить проверку подключаемого носителя на наличие вредоносных программ. Действия пользователя описаны в приложении 1.

При возникновении подозрения на наличие вредоносных программ пользователь обязан запустить полное сканирование АРМ. Действия пользователя описаны в приложении 2.

При подозрении на заражение вирусом или его обнаружении, пользователь обязан приостановить эксплуатацию АРМ, отключить его от локальной вычислительной сети, и немедленно сообщить об этом администратору сегмента системы антивирусной защиты. Подключение АРМ к локальной вычислительной сети возможно только после удаления вредоносной программы и ее источника.

При появлении на экране АРМ предупреждающих сообщений (обнаружение вируса, истечения срока лицензии, неактуальность антивирусных баз) пользователь обязан сообщить о них в управление информационных технологий аппарата администрации Старооскольского городского округа по тел. **22-03-44** либо на адрес электронной почты **uit@so.belregion.ru**.

Пользователь АРМ несет персональную ответственность за нарушение требований по антивирусной защите.

Нарушение требований по антивирусной защите влечет за собой ответственность, предусмотренную действующим законодательством РФ.

Приложение № 1
к памятке пользователя
по антивирусной защите

Порядок контроля актуальности установленных антивирусных баз на АРМ пользователя

Для контроля актуальности установленных антивирусных баз на АРМ пользователю необходимо выполнить следующие действия:

1. В панели задач операционной системы нажать правой кнопкой мыши по значку (рисунок 1).

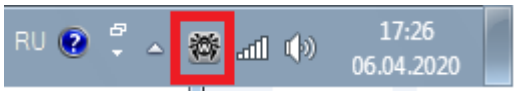
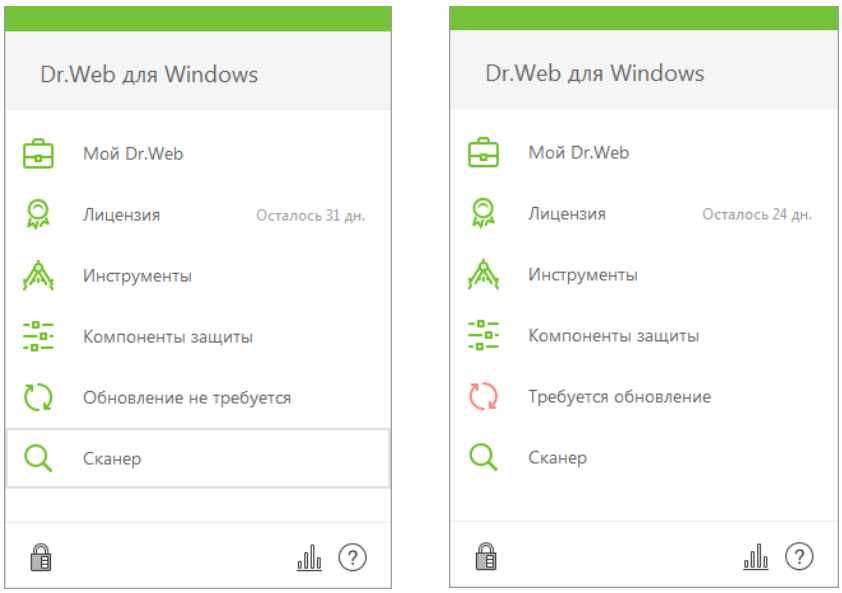


Рис. 1. Панель задач операционной системы

2. В раскрывшемся меню Dr.Web, представленном на рисунке 2 а), в случае актуальности обновлений появляется пункт «Обновление не требуется». Если обновления не актуальны, как на рисунке 2 б), то появится пункт «Требуется обновление».

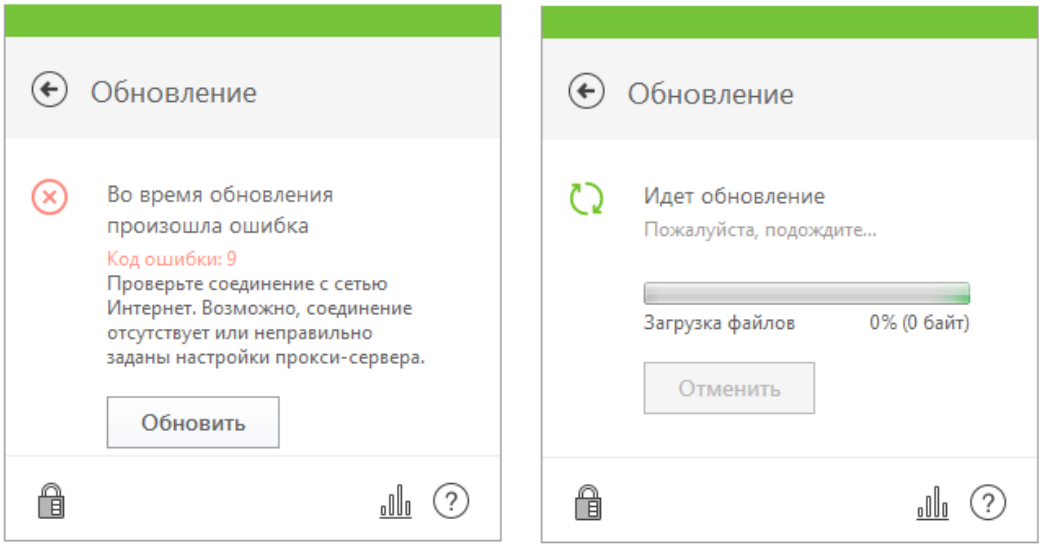


а) обновление не требуется б) требуется обновление

Рис. 2. Меню Dr.Web

3. При неактуальных антивирусных базах следует их обновить, нажав на кнопку «Требуется обновление». Откроется меню Dr.Web «Обновление».

4. В меню «Обновление», показанном на рисунке 3 а) нажать кнопку «Обновить». После этого начнется процесс загрузки и обновления антивирусных баз как на рисунке 3 б).



а) меню «Обновление» б) загрузка антивирусных баз

Рис. 3. Обновление антивирусных баз

5. При возникновении ошибки обновления антивирусных баз пользователь обязан сообщить в управление информационных технологий аппарата администрации Старооскольского городского округа по тел. **22-03-44** либо на адрес электронной почты **uit@so.belregion.ru**.

Приложение № 2
к памятке пользователя
по антивирусной защите

Порядок выборочной проверки файлов, папок с файлами и съемных носителей информации

В антивирусной защите Dr.Web для организации выборочной проверки файла или папки с файлами необходимо выполнить следующие действия:

1. Зайти в папку, где расположен файл или папки с файлами.
2. Нажать правую кнопку мыши по имени проверяемого файла, или папки с файлами. После этого откроется меню, показанное на рисунке 1.

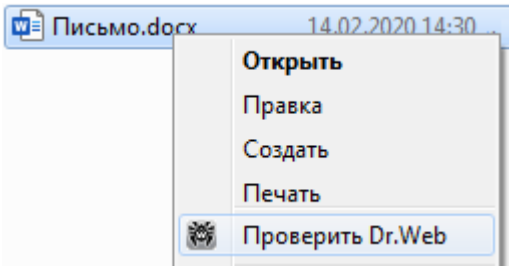


Рис. 1. Вызов контекстного меню на объекте проверки

3. В раскрывшемся меню выбрать пункт «Проверить Dr.Web». После этого запускается сканер антивирусной защиты и выполняется проверка на наличие угроз.
4. По окончании сканирования в окне отображается результат проверки с указанием обнаруженных объектов и угроз. Если угрозы отсутствуют, то как показано на рисунке 2 будет доступна кнопка закрыть.

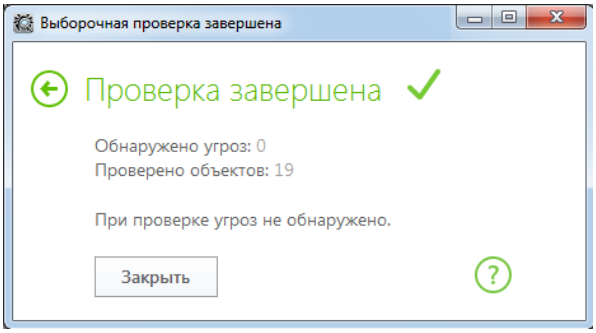


Рис. 2. Окно результатов сканирования

5. В случае обнаружении сканером угроз, он предложит их обезвредить, для этого, согласно рисунку 3 необходимо нажать кнопку «Обезвредить».

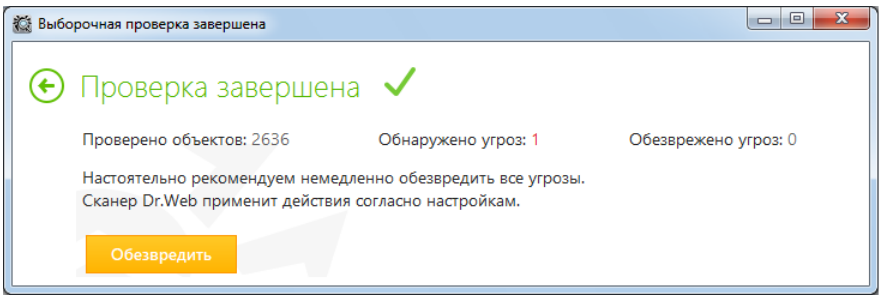


Рис. 3. Окно результатов сканирования

Для проведения проверки на наличие вредоносного программного обеспечения съемного носителя информации следует выполнить следующие действия:

1. Подключить к АРМ съемный носитель информации.

2. Открыть «Мой компьютер» и нажать правой кнопкой мыши по съемному носителю информации (рисунок 4).

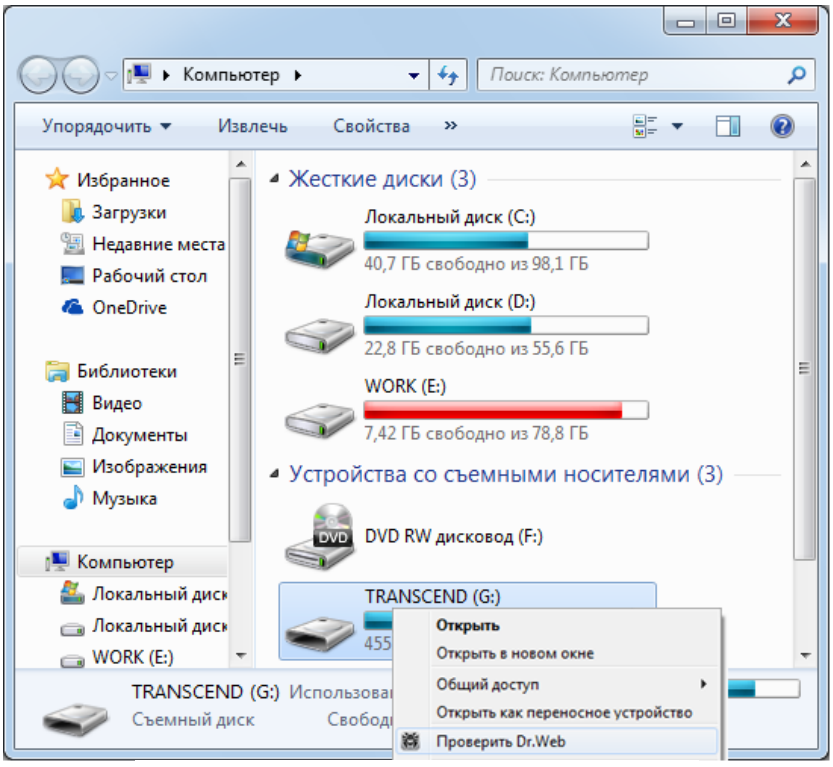


Рис. 4. Проверка съемного носителя информации

3. В раскрывшемся меню выбрать пункт «Проверить Dr.Web». После этого запускается сканер антивирусной защиты и выполняется проверка на наличие угроз.

4. По окончании сканирования в окне отображается результат проверки с указанием обнаруженных объектов и угроз. Если угрозы отсутствуют, то как показано на рисунке 2 будет доступна кнопка закрыть.

5. В случае обнаружении сканером угроз, он предложит их обезвредить, для этого, согласно рисунку 3 необходимо нажать кнопку «Обезвредить».

Приложение № 3
к памятке пользователя
по антивирусной защите

Порядок проведения полной проверки

Для проведения полной проверки АРМ на наличие вредоносного программного обеспечения следует выполнить следующие действия:

1. В панели задач операционной системы нажать, показанной на рисунке 1, правой кнопкой мыши по значку .

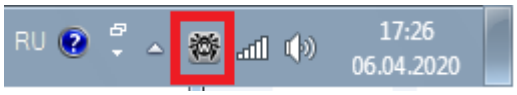
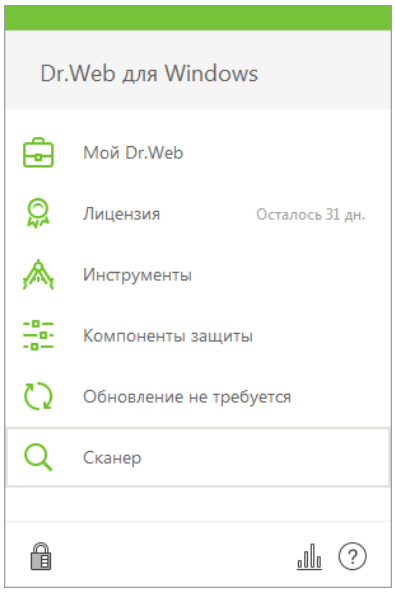
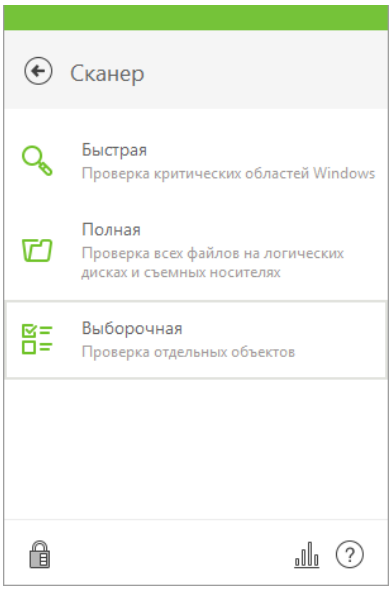


Рис. 1. Панель задач операционной системы

2. В раскрывшемся меню, представленном на рисунке 2, последовательно выбрать пункты «Сканер», затем «Полная». В результате выполненных действий запустится полная проверка АРМ.



а) выбор сканера защиты



б) запуск полной проверки

Рис. 2. Запуск полной проверки

3. По окончании сканирования в окне «Полная проверка завершена» отображается результат проверки с указанием обнаруженных объектов и угроз. Если угрозы отсутствуют, то как показано на рисунке 3 будет доступна кнопка закрыть.

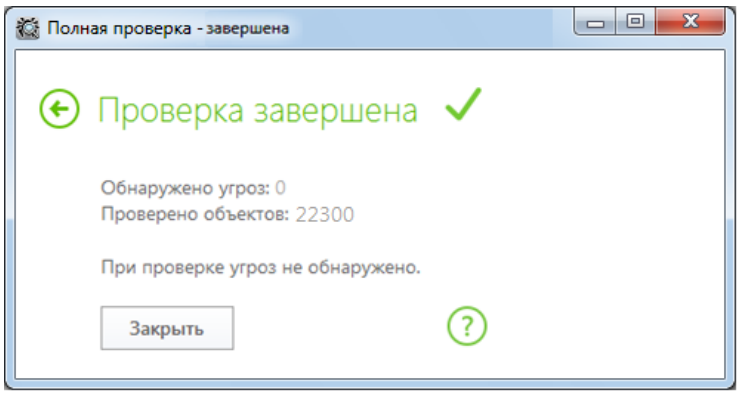


Рис. 3. Окно результатов сканирования

4. В случае обнаружении угроз, сканер предложит их обезвредить, для этого, согласно рисунку 4 необходимо нажать кнопку «Обезвредить».

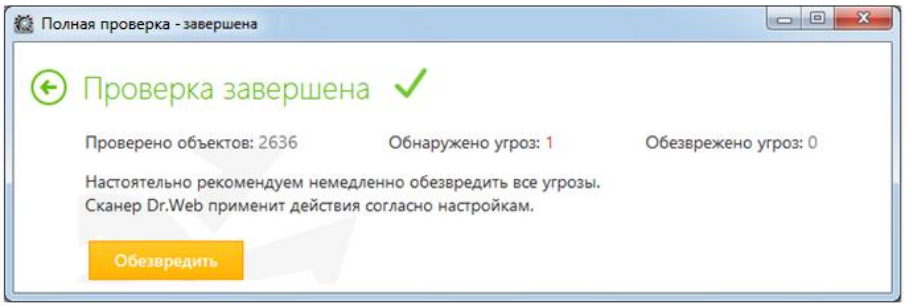


Рис. 4. Окно результатов сканирования при обнаружении угроз

Приложение № 4
к памятке пользователя
по антивирусной защите

ЛИСТ ОЗНАКОМЛЕНИЯ
С ПАМЯТКОЙ ПОЛЬЗОВАТЕЛЯ ПО АНТИВИРУСНОЙ ЗАЩИТЕ

____

наименование организации

____

подразделение

№ п/п	ФИО	Дата	Подпись