Муниципальное бюджетное общеобразовательное учреждение
«Образовательный комплекс «Перспектива»
города Губкина Белгородской области

П Р И К А З

от «01» сентября 2022 г. № 62

О мерах по обеспечению
информационной безопасности
в МБОУ «Образовательный комплекс «Перспектива»

Во исполнения Федеральных законов от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», от 27.07.2006 № 149-ФЗ «Об информатизации, информационных технологиях и о защите информации», в целях реализации задачи исключения доступа обучающихся к ресурсам сети Интернет, содержащим информацию, причиняющую вред здоровью и развитию детей, не совместимую с задачами обучения и воспитания, а также информацию, распространение которой запрещено на территории Российской Федерации, и в целях предотвращения вирусных заражений персональных компьютеров и серверов и недопущения распространения вирусного программного обеспечения в локальных сетях организаций системы образования Губкинского городского округа

ПРИКАЗЫВАЮ:

1. Учителю информатики Горенко С.И. обеспечить установку средств антивирусной защиты на все персональные компьютеры и серверы организации до 01 сентября 2022 года;

1.1. Не допускать к эксплуатации персональные компьютеры и серверы организации без установленных и работающих должным образом средств антивирусной защиты;

2. Заместителю директора Васильевой В.Н. ознакомить всех членов коллектива, допускаемых к работе с персональными компьютерами, с памяткой по антивирусной защите (Приложение 1) под подпись, а также разместить текст памятки в непосредственной близости от персонального компьютера;

3. Учителю информатики Горенко С.И. обеспечить бесперебойную работу системы контентной фильтрации, установив настройки фильтра согласно законодательству Российской Федерации;

3.1. Взять под личный контроль вопросы защиты персональных данных, установки и использования системы контентной фильтрации и антивирусной защиты.

4. Назначить ответственным за размещение на официальном сайте МБОУ «Образовательный комплекс «Перспектива» Рагозина А.С. информации о контактных данных служб, оказывающих методическую и психологическую помощь в вопросах обеспечения информационной безопасности (ОГБУ «ЦБИ» (https:vk.com/tochka_podderzhki); Фонд Развития Интернет «Дети России онлайн (http:detionline.com/); контакты службы психологической помощи (https://psi.mchs.gov.ru/).

5. Назначить ответственной за размещение в соцсетях МБОУ «Образовательный комплекс «Перспектива» Кавтасьеву Л.Г. информации о

контактных данных служб, оказывающих методическую и психологическую помощь в вопросах обеспечения информационной безопасности (ОГБУ «ЦБИ» (https:vk.com/tochka_podderzhki); Фонд Развития Интернет «Дети России онлайн (http:detionline.com/); контакты службы психологической помощи (https://psi.mchs.gov.ru/).

6. Назначить ответственным за предупреждение публикации и распространения дезинформации на официальном сайте МБОУ «Образовательный комплекс «Перспектива» Рагозина А.С.

7. Назначить ответственной за предупреждение публикации и распространения дезинформации в социальных сетях МБОУ «Образовательный комплекс «Перспектива» Кавтасьеву Л.Г.

8. Контроль за исполнением данного приказа оставляю за собой.

Директор О.И. Павлова

С приказом ознакомлены:

Антипова М.А.
Алпеева Е.Н.
Белых И.С.
Беляева Е.Ф.
Богатырева Е.А.
Бакланова Т.В.
Белоглазова О.А.
Васильева В.Н.
Васильченко А.С.
Вигерина Н.С.
Васильева А.С.
Горенко С.И.
Домненко М.В.
Жданова Е.П.
Зайцева Н.В.
Кабанцова М.А.
Кавтасьева Л.Г.
Карташова С.И.
Котенева Е.И.
Кудинова Т.М.
Карабут О.Т.

Лаврухина М.И.
Лихачева М.И.
Овчинникова Т.А.
Палкина Т.П.
Петроченко В.М.
Рагозин А.С.
Светикова И.В.
Скобелкина Е.Н.
Труфанова Л.В.
Хворостянова Т.И.
Цыганкова С.В.
Чернолых Л.Ф.
Чернышова Т.В.
Шумская О.В.
Бессонова Т.И.
Болгова Н.П.
Борисенко В.Н.
Бородина И.Е.
Гапченко С.Н.
Жданова А.А.
Игнатенко Л.Н.

Изюмская Е.В.
Кирносова А.Н.
Кривчикова Н.Н.
Лопина С.А.
Лубышева Т.С.
Малахов Н.А.
Мишакина А.А.
Молодых Т.А.
Панкратова Н.И.
Рыбальченко Е.Н.
Ряховская Ю.Н.
Старосельцева Ю.А.
Ульянская А.Н.
Ускова Е.Н.
Филимонова Е.А.
Халеева С. Н.
Чернышова Л.Е.
Шестакова Л.А.
Яковлева А.С.

Приложение 1
от «01» сентября 2022 года № 52

ПАМЯТКА
пользователя по антивирусной защите

В целях защиты от проникновения вредоносных программ на автоматизированном рабочем месте (далее - АРМ) сотрудников органов власти устанавливается антивирусное программное обеспечение Dr.Web.

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

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 администратору сегмента системы антивирусной защиты муниципального образования.

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

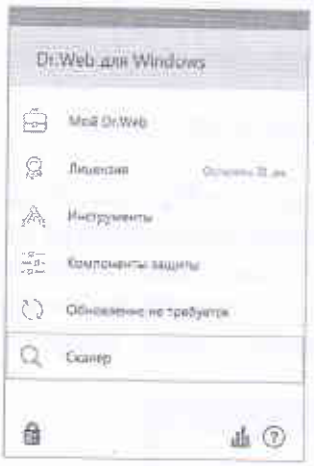
Порядок контроля актуальности установленных антивирусных баз на АРМ пользователя

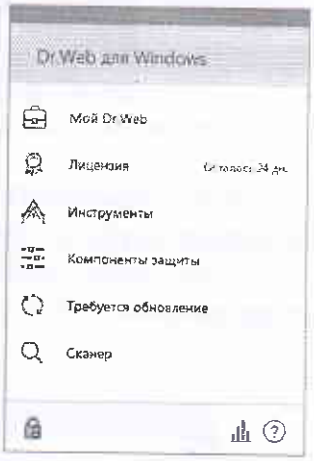
Для контроля актуальности установленных антивирусных баз на АРМ пользователю необходимо выполнить следующие действия:

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».



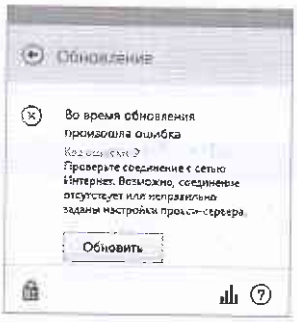


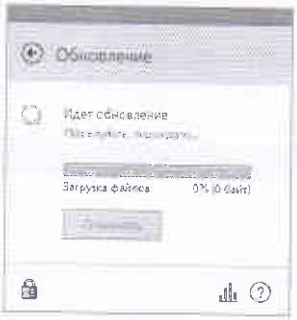
а) обновление не требуется б) требуется обновление

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 Сотрудникам ОГБУ «Белгородский информационный фонд» по телефону 32-55-32 или оформить заявку в системе HelpDesk (http://help.belregion.ru:8080/sd/).

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.

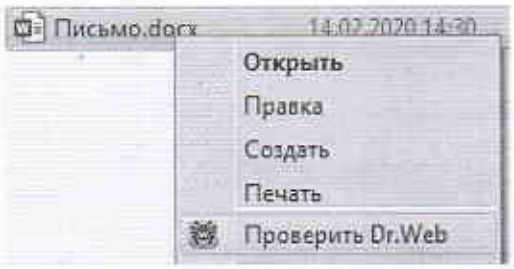


Рис. 1. Вызов контекстного меню на объекте проверки

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.

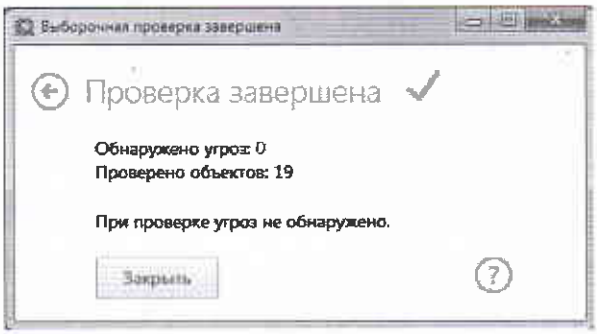


Рис. 2. Окно результатов сканирования

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

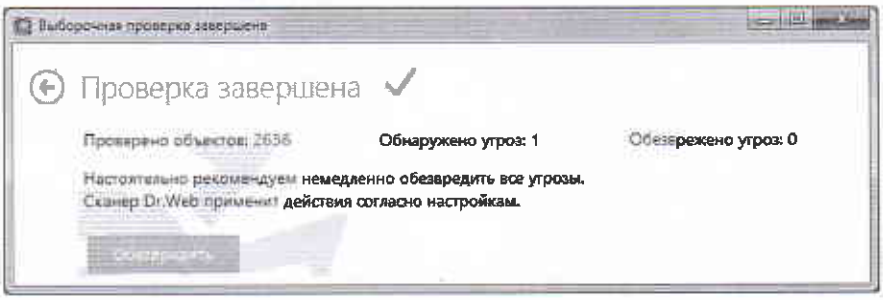


Рис. 3. Окно результатов сканирования

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 3).

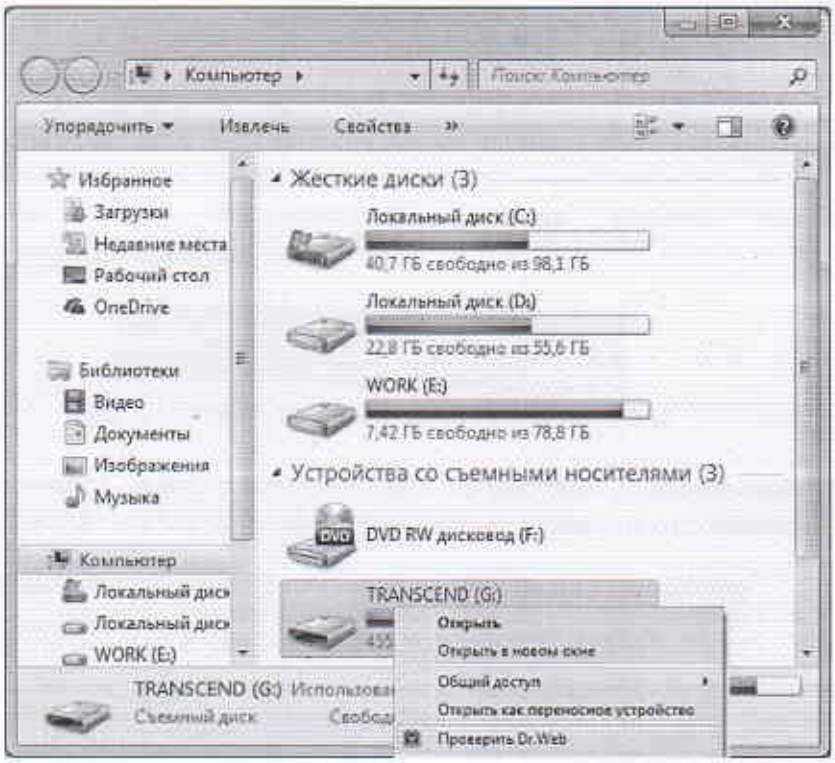


Рисунок 3. Проверка съемного носителя информации

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

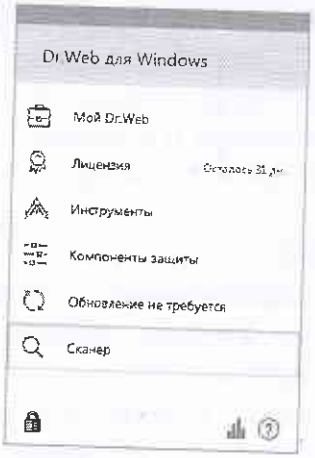
Порядок проведения полной проверки

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

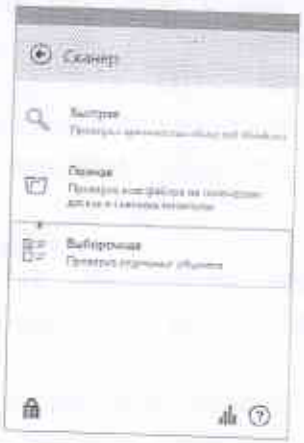
1. В панели задач операционной системы нажать, показанной на рисунке 1, правой кнопкой мыши по значку .

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.



б) выбор сканера защиты



в) 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.

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

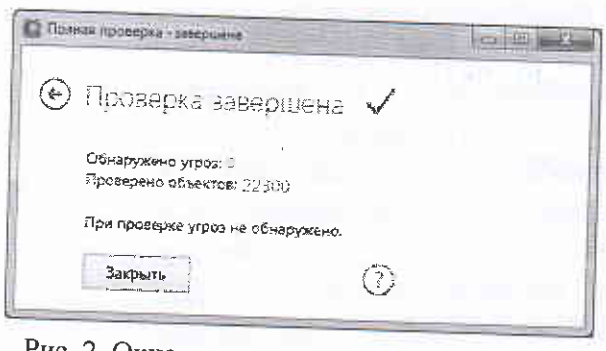


Рис. 2. Окно результатов сканирования

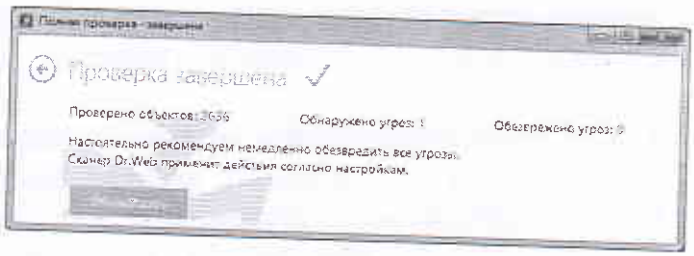


Рис. 3. Окно результатов сканирования при обнаружении угроз