МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНОБРНАУКИ РОССИИ)

Тверская ул., д. 11, стр. 1, 4, Москва, 125009, телефон: (495) 547-13-16,
e-mail: info@minobrnauki.gov.ru, http://www.minobrnauki.gov.ru

16.08.2022 № МН-19/868

На № _____ от _____

Генеральному директору
общества с ограниченной
ответственностью «Доктор Веб»

О направлении информации

Б.А. Шарову

125124, г. Москва,
ул. 3-я Ямского Поля, д. 2,
к. 12А

Уважаемый Борис Александрович!

Министерство науки и высшего образования Российской Федерации рассмотрело письмо общества с ограниченной ответственностью «Доктор Веб» от 27 июля 2022 г. № ГОС/822 и сообщает следующее.

В соответствии с Приказом Федеральной службой по техническому и экспортному контролю Российской Федерации от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (далее – Требования ФСТЭК России), Регламентом использования защищенной сети Минобрнауки России для предоставления внешним пользователям доступа к информационным системам и ресурсам ИТКИ Минобрнауки России от 19 ноября 2021 года, частным техническим заданием на развитие (модернизацию) подсистемы обеспечения информационной безопасности государственной информационной системы «Современная цифровая образовательная среда» (далее – ГИС СЦОС) от 17 декабря 2021 года на автоматизированных рабочих

местах (далее – АРМ) внешних пользователей должно функционировать средство антивирусной защиты, которое должно предусматривать:

– реализацию антивирусной защиты;

– установку, конфигурирование и управление средствами антивирусной защиты;

– проведение периодических проверок компонентов АРМ на наличие вредоносных компьютерных программ;

– проверку в масштабе времени, близком к реальному, объектов (файлов) из внешних источников (съемных машинных носителей информации, сетевых подключений, в том числе к сетям общего пользования, и других внешних источников) при загрузке, открытии и исполнении таких файлов;

– оповещение об обнаружении вредоносных компьютерных программ;

– определение и выполнение действий по реагированию на обнаружение объектов, подвергшихся заражению вредоносными компьютерными программами;

– автоматическое регулярное, не реже 1 раза в день, обновление антивирусных баз, согласно возможностям программного обеспечения. В случае сбоя автоматического обновление баз производится вручную с той же периодичностью;

– обновление версий программного обеспечения средств антивирусной защиты по мере их выпуска производителем;

– периодическую проверку работоспособности средств антивирусной защиты;

– сбор, запись и хранение информации о событиях безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти;

– мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них;

– защиту информации о событиях безопасности.

В государственных информационных системах 2 класса защищенности применяются средства защиты информации не ниже 5 класса, соответствующие 5 и более высокому уровню доверия, сертифицированные на соответствие обязательным требованиям по безопасности информации, установленным ФСТЭК России или на соответствие требованиям, указанным в технических условиях (заданиях по безопасности), при этом функции

безопасности таких средств должны обеспечивать выполнение Требований ФСТЭК России.

В связи с изложенным, применение сертифицированного ФСТЭК России средства антивирусной защиты «Dr.Web Enterprise Security Suite» допускается применять при подключении автоматизированных рабочих мест учебных заведений к ГИС СЦОС.

Заместитель директора
Департамента Цифрового развития В.В. Савченко

Варнавский Владимир Евгеньевич
(495) 547-12-60 (доб. 2572)