МИНИСТЕРСТВО ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖНОЙ ПОЛИТИКИ КРАСНОДАРСКОГО КРАЯ

Рашпилевская ул., д. 23, г. Краснодар, 350063
Тел. (861) 298-25-73, (861) 298-26-00
E-mail: minobrkuban@krasnodar.ru

20.01.2021 № 47-01-13-718/21

На № _____ от _____

Руководителям
муниципальных органов
управления образованием

Руководителям государственных
образовательных организаций

О направлении рекомендаций
по защите информационных ресурсов

Министерство образования, науки и молодежной политики направляет для использования в работе Рекомендации по защите информационных ресурсов и систем органов власти и управлений Краснодарского края, подведомственных им учреждений, разработанные департаментом информатизации и связи.

Приложение на 2 л. в 1 экз.

Начальник управления
общего образования Е.В. Мясищева

Дубинец Альбина Борисовна
+7 (861) 298-25-97

Рекомендации по защите информационных ресурсов и систем органов власти и управлений Краснодарского края, подведомственных им учреждений

В интересах недопущения реализации угроз безопасности РФ в информационной сфере необходимо:

обеспечить использование и регулярное обновление штатных средств антивирусной защиты;

обеспечить регулярное обновление используемого программного обеспечения;

для предотвращения возможных компьютерных атак, направленных на эксплуатацию уязвимостей, определить и заблокировать порты, протоколы и сервисы, не используемые для функционирования процессов;

использовать двухфакторную авторизацию при удаленном доступе в сеть;

запретить доступ с помощью сторонних сервисов, которые подключаются через промежуточные серверы и самостоятельно проводят авторизацию и аутентификацию;

включить политики безопасности, которые ограничивают доступ к ресурсам из черных списков;

заблокировать доступ на потенциально вредоносные домены, добавить возможность фильтрации веб-содержимого;

обеспечить ведение журналирования действий пользователей с максимально возможным периодом хранения журналов;

настроить период неактивных удаленных подключений пользователей с требованием повторной аутентификации;

удалить неиспользуемые учетные записи и группы пользователей на средствах вычислительной техники;

организовать и осуществить в постоянном режиме антивирусную проверку сообщений электронной почты;

ограничить или прекратить использование небезопасных протоколов "ftp", "telnet", и других, передающих авторизованные и аутентификационные данные пользователей в открытом виде;

организовать контроль за подключением внешних устройств, в том числе машинных носителей информации;

обновить пароли всех пользователей в соответствии с парольной политикой;

настроить и осуществить автоматическое резервное копирование информационных систем;

осуществить хранение входящего и исходящего сетевого трафика на всех сетевых сегментах с максимально возможным периодом хранения, но не менее, чем за последние 24 часа;

привести в актуальное состояние имеющиеся планы, инструкции и руководства по реагированию на компьютерные инциденты;

запретить использование платформы видеоконференции "Zoom" и её аналогов при осуществлении служебной деятельности.